FEFCO CYBERSECURITY HANDBOOK

IN CORRUGATED SECTOR

FEFCO
Corrugated Packaging

TABLE OF CONTENT

“

The corrugated industry cannot ignore the increased risk of cyberattack on our manufacturing assets.

As an industry, we increasingly use connected machines, both internal and external facing. This is essential to remain competitive on the market, respond to traceability requirements from our customers and to embrace new opportunities, such as IE4.0 and artificial intelligence.

Furthermore, the industry has to deal with structural complexity, as we have a high level of dependency on our supply chain partners, the machine suppliers. We are often unable to directly patch or control our PLC/SCADA systems that sit inside our manufacturing lines. And upgrading control systems in isolation on a production line is often prohibitively costly.

For this reason we have forged a strong collaboration between corrugated producers and their partners in the supply chain, to re-define their cooperation. The goal is to make clear agreements on what to expect from both parties in order to reduce risk.

This handbook offers practical suggestions to begin the journey that brings our cyber protection to an appropriate level.

Thanks to everyone who contributed in this collaborative process. This handbook is the result of your open, deep and insightful discussions!

Hans Christian Hansen
FEFCO Cybersecurity Committee Chairman

EXECUTIVE SUMMARY

Cyber security is a strategic priority for senior management, crucial for maintaining reputation, financial stability and operational continuity. As cyber threats become more sophisticated, they pose risks not only to internal operations but also to the entire ecosystem of suppliers, partners and customers. In the corrugated packaging industry, a cyber incident can disrupt supply chains, forcing customers to seek alternative suppliers and potentially damaging long-term relationships. Regulatory frameworks like the NIS2 Directive and the Cyber Resilience Act (CRA) provide best-practice guidelines for creating cyber resilience. Investing in cyber security reduces risks and strengthens the organisation’s position in a vulnerable market. The EY 2024 Global Cyber security Leadership Insights Study highlights trends such as AI integration, which helps detect and respond to incidents faster but also introduces new vulnerabilities.

Operational Technology (OT) is vital for the corrugated board production sector, controlling machinery and ensuring product quality. Cyber threats targeting OT systems can halt production and cause significant financial loss. Disruptions can affect the entire supply chain, emphasising the need for robust cyber security. Protecting OT involves unique challenges: legacy systems not designed for modern cyber security, increased attack vectors due to IT-OT convergence, security measures that must not interrupt production, limited visibility of OT networks and continuous adaptation to sophisticated attacks. Manufacturers must incorporate cyber security in new equipment to reduce vulnerabilities.

This handbook, based on the NIST 2.0 framework, provides strategies to strengthen security protocols, improve incident response and advance threat intelligence. It aims to improve sector-wide resilience against cyber threats. A workshop with experts prioritised best practices to address common challenges and improve cyber security maturity. The corrugated packaging industry must prioritise cyber security by adopting frameworks like NIST 2.0, ISO 27001 and ISA/IEC 62443. FEFCO’s guidance helps address sector-specific challenges. By following best practices, companies can strengthen cyber security, improve recovery strategies and ensure OT security, creating a secure and resilient supply chain.

FOREWORD

SECTOR PERSPECTIVE AND KEY CYBER RISKS

The corrugated board industry relies heavily on interconnected systems, making cyber security essential. OT manages key production processes like cutting and printing, ensuring efficiency and quality. However, its growing connectivity introduces risks of cyberattacks that could disrupt operations and compromise sensitive data. Robust OT security is critical for business continuity.

Equipment manufacturers support cyber security by designing machines with built-in protection, such as encryption and secure firmware. Similarly, IT vendors play a vital role by ensuring software and cloud solutions meet strict security standards.

Auxiliary systems and converting machinery, integral to production, also require safeguards such as firewalls, network segmentation and regular updates to prevent disruptions. Securing these components through collaboration across the supply chain is vital for resilience and operational integrity.

SECURING THE ECOSYSTEM AND SUPPLY CHAIN

The digital supply chain in the corrugated board production industry is increasingly interconnected, with automation linking machinery, software and data systems. This integration improves efficiency and real-time monitoring but also introduces new cyber security risks. As systems like ERP manage data across production, logistics and scheduling, vulnerabilities can expose the entire supply chain to cyber threats. Any disruption from cyber incidents can impact not only manufacturers but also suppliers and customers, making robust cyber security essential for safeguarding operations and ensuring continuity.

Role of OT

OT is essential in corrugated board production, managing the automated processes that turn raw materials into precise, high-quality packaging. As a form of Cyber-Physical Systems (CPS), OT systems seamlessly integrate physical operations, such as cutting, gluing and printing, with digital controls, ensuring consistency and efficiency. Real-time monitoring within these systems upholds product quality and minimises waste. A breach could disrupt production, compromise quality and expose sensitive information. It could even have health and safety implications.

OT also enables predictive maintenance by analysing machine data, reducing unexpected downtimes and extending equipment life. Additionally, it supports safety protocols, helping meet regulatory requirements and protect workers.

As OT systems and CPS become more connected, securing them against cyber threats is crucial. A breach could disrupt production, compromise quality and expose sensitive information. In today's industry, robust OT security safeguards both production integrity and business continuity.

Role of equipment manufacturers

Machinery and equipment manufacturers are crucial to the cybersecurity landscape of corrugated production.

'Manufacturer' means any natural or legal person who:

- manufactures products within the scope of the Regulation[1] on machinery or who has those products designed or manufactured and markets those products under their name or trademark; or
- manufactures products within the scope of the Regulation on machinery and puts those products into service for their own use.

They are responsible for designing equipment that integrates seamlessly with digital control systems and automation technologies while maintaining robust security features. These manufacturers must adopt secure development practices, ensuring that their machines are resilient against known vulnerabilities and have built-in protections such as network security, access controls and secure firmware updates. Partnering with machinery manufacturers who prioritise cybersecurity can help corrugated producers safeguard their operations.

In the corrugated industry, the role of integrators and manufacturers is often the same.

Role of OT business partners

IT/OT Vendors and technologies

IT/OT vendors who supply software solutions, data management systems and cloud-based services to corrugated manufacturers must adhere to stringent cybersecurity standards. These technologies, which manage sensitive operational data and enable remote access to critical systems, must be protected against data breaches, ransomware and other cyber threats. Vendors must ensure that their software complies with security best practices, including sophisticated means of authentication, encryption and regular security audits. For corrugated manufacturers, working with vendors who follow industry security frameworks, such as ISO/IEC 27001, ensures that all digital tools and software applications are secured against potential attacks.

Corrugator manufacturers
The deep data integration between MES (Manufacturing Execution System), Production Schedulers, Internal Logistics software and Corrugator Machines can expose all the departments that work on the transformation of paper reels into corrugated boards to a high cyber risk, leading to potential downtime with a huge impact on plant OEE (Overall Equipment Effectiveness).

Auxiliary systems manufacturers
This covers various support processes, including ink and starch preparation, energy monitoring, steam, OCC management and dust removal. They are increasingly integrated with digital control systems and cyber compromises in these areas can lead to security risks and potential downtime, affecting production schedules and output quality.

Effective cybersecurity measures in these areas include monitoring network activity, controlling access to these critical systems, network segmentation and deploying physical security measures to protect sensitive infrastructure.[2 3]

Converting machinery manufacturers
The process of converting corrugated board into packaging products (such as boxes) relies on an array of specialised machinery, all of which are increasingly connected to digital control systems. These machines, including flexo printers, digital printers, flatbed or rotary die-cutters, folder gluers and casemakers are integral to efficient production. However, their digital integration makes them susceptible to cyber threats. Machines often communicate with automation systems like pre-feeders, bundle breakers, stackers and palletisers, forming an intricate network that, if compromised, can disrupt production.

Internal logistic manufacturers (transfer, warehouse, LGV etc.)
The internal process of moving and storing production materials (principally corrugated boards and finished packaging) is becoming increasingly automated and software driven. The deep data integration between internal logistic software/system with MES, Production Planning software and finally ERP (material inventories) could increase cyber threats, posing new challenges for cyber security.

Final packaging/palletising line manufacturers
This is the final production station before warehouses, with strapping, palletising and filming machines, all of them software driven, normally with specific recipes sent by MES or other production/product configuration software.

The data integration or request for remote support services in our sector is huge. Securing IT/OT software and machinery requires implementing cybersecurity measures such as firewalls, secure communication protocols and role-based access control to limit who can access specific systems. Additionally, regular security updates and patch management are critical to keeping these systems resilient against emerging threats.

LEGAL CONTEXT

As the corrugated packaging and machinery sectors increasingly adopt digital technologies, the associated cyber security risks grow alongside operational efficiencies. While EU regulations, such as those governing connected devices and critical infrastructure (like NIS2), do not directly apply to corrugated board production, they are relevant to machinery manufacturers supporting the production process and supply chain. These regulations offer best practices that companies can voluntarily adopt, improving their cyber security posture. By implementing these guidelines, organisations can strengthen their risk management strategies, secure interconnected systems and safeguard both production operations and the broader supply chain's resilience. This section is detailed in Chapter 3.3.

CYBER RESILIENCE, A STRATEGIC PRIORITY FOR OUR INDUSTRY

With evolving cyber threats and the industry becoming a larger target for hacking and cyber-attacks, the corrugated packaging sector needs to prioritise cyber resilience to ensure operational continuity, long-term security and downstream value chains. The increasing reliance on digital technologies makes the sector susceptible to disruptions that could affect production, supply chains and sensitive data. Additionally, the growing importance of remote support for operational technology systems underscores the need for robust cyber security measures.

To address these challenges, the sector requires clear, actionable guidance across all areas of cyber risk management. This includes identifying vulnerabilities, implementing protective measures, monitoring for threats and establishing response and recovery protocols. FEFCO plays a pivotal role in providing sector-specific guidance, enabling companies to improve their cyber security posture by adopting best practices tailored to their needs.

By focusing on a comprehensive approach to cyber security, FEFCO empowers the industry to build resilience not only through effective recovery plans but also by strengthening preventive measures, threat detection capabilities and incident response strategies. This holistic approach ensures companies can adapt to emerging risks, maintain operational integrity and uphold client and stakeholder trust.

NIST 2.0 provides a systematic approach to implementing cyber security controls across IT and OT environments. It organises the cyber security activities into six functions: Govern, Identify, Protect, Detect, Respond, Recover.

HANDBOOK OVERVIEW

HANDBOOK PURPOSE

The primary goal of this handbook is to support the corrugated packaging production industry in strengthening its cybersecurity posture, fostering a transition towards more resilient and secure production processes and supply chains.

It provides practical guidance and actionable recommendations to help organisations achieve cyber maturity or make significant cybersecurity improvements within a relatively short timeframe.

- One of the biggest challenges is balancing business continuity with necessary security measures. IT systems require critical business continuity, while OT systems, essential for industrial operations, often prioritise continuous availability at the expense of security.
- OT hardware is expensive and difficult to update regularly. Unlike IT systems, which benefit from frequent software and hardware updates, OT systems are often used for decades, leaving security issues unaddressed.
- Vulnerability management is a major challenge. IT systems follow established patch and update protocols, while OT systems often rely on outdated software, making timely fixes difficult.
- Interoperability and compatibility complicate the landscape. IT systems are designed for integration and interoperability, while OT systems often depend on proprietary technologies or sector-specific protocols.
- IT and OT environments have different security emphases. IT systems focus on logical security, such as firewalls and data encryption, while OT systems emphasise physical security measures.
- The priorities of IT and OT teams are often not aligned. IT teams focus on confidentiality, integrity and data availability, while OT teams concentrate on safety and operational continuity.
- Incident management differs between IT and OT. IT incidents are quickly detected and addressed with advanced monitoring tools, while OT incidents, which can affect physical safety and production, often lack rapid detection and response mechanisms.
- There are gaps in training and awareness. IT professionals are generally well-versed in cybersecurity best practices, but OT operators often lack equivalent knowledge, increasing the likelihood of human error and vulnerabilities.

These challenges underscore the need for a more integrated and collaborative approach between IT and OT teams to establish strong cybersecurity measures while maintaining uninterrupted operations.

METHODOLOGY

This framework will provide a comprehensive evaluation of the companies' cybersecurity strengths and weaknesses, identifying current gaps. It serves as a reference point, documenting the company's starting position, status and future objectives. This section is detailed in chapter 5.

EVALUATING LANDSCAPE READINESS

This handbook is designed to improve the cybersecurity resilience of corrugated packaging production and its supply chain by leveraging the practical tools and templates provided in the annexes.

- **Annex I**: A checklist based on the NIST 2.0 framework enables organisations to assess their cybersecurity maturity. The checklist serves as a structured tool to evaluate current capabilities and identify areas for improvement. Detailed instructions on how to use the checklist are provided later in the handbook.
- **Annex II**: A Supplier Declaration of Conformity ensures that suppliers align with the organisation's cybersecurity requirements and adhere to best practices. This declaration form aims to extend robust cybersecurity measures across the entire supply chain, fostering a unified approach to risk mitigation.
- **Annex III**: Guidelines for developing templates for Mutual Information Security Agreements (ISA) are included to help organisations formalise security commitments with their customers. These templates facilitate clear, structured agreements that promote trust and accountability in safeguarding shared data and systems.

REGULATION AND STANDARDS

LEGAL AND REGULATORY FRAMEWORK

The following chapter will dig into the developed regulatory frameworks, outlining specific requirements for cyber security. By combining security and compliance, these standards help organisations strengthen their resilience against cyber risks while ensuring full adherence to applicable laws.

NIS2 Directive (EU 2022/2555)

The NIS2 (Network and Information Systems) Directive is a European law designed to strengthen cyber security within the European Union. It obliges organisations to follow stricter security standards to improve the level of cyber security.

By 17 October 2024, Member States had to adopt and publish the transposition measures necessary to comply with the NIS2 Directive, which applied from 18 October 2024 onwards.

NIS2 law applies to public or private entities which are, in principle, established in Europe and that provide a service listed in Annexes I or II of the law within the European Union.

The NIS2 Directive builds upon the original NIS Directive, expanding its scope to cover more sectors, including manufacturing and industrial production. NIS2 emphasises risk management, incident reporting and collaboration between companies and national cybersecurity authorities.

The NIS2 Directive is aimed at organisations of a certain size that provide services in critical sectors listed in Annexes I and II of the Directive. The size ("size cap") and the service provided are the two main criteria for determining whether the NIS2 Directive applies to an organisation.

Among the "other critical sectors" (Annex II) in scope of the NIS2 Directive, reference is made to undertakings carrying out any of the economic activities referred to as NACE Rev. 2 [4] (NACE C 26-30). For example, 28.95 Manufacturer of machinery for paper and paperboard production.

It is essential for each company to determine whether they are subject to the NIS2 law, either at the directive level or the country-specific level. As previously mentioned, manufacturers of machinery for paper and paperboard production are already within the scope of NIS2. The actual manufacturers of paper and paperboard are not included in the directive's scope, but they may become subject to it if specific countries decide to include them.

If a company undertakes activities beyond producing paper and paperboard, such as generating and selling energy (or other services listed in the table above), it must adhere to the NIS2 directive. This adherence may classify the company as either an essential entity or an important entity, based on the specific sub-activity performed.

SECTORS OF HIGH CRITICALITY (ANNEX I)	OTHER CRITICAL SECTORS (ANNEX II)
Energy (electricity, district heating and cooling, petroleum, natural gas, hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Manufacturing, production and distribution of chemicals
Financial market infrastructure	Production, processing and distribution of food
Health	Manufacturing of medical devices and in vitro diagnostic medical devices; computer electronic and optical products; electrical equipment; machinery and equipment N.E.C., motor vehicles, trailers and semi-trailers; other transport equipment
Drinking water	Digital providers
Waste water	Research
Digital infrastructure	
ICT service management	
Public administration	
Space	

Cyber Resilience Act (CRA, EU 2024/2847)

The Cyber Resilience Act (CRA)[5] is an EU Regulation aimed at improving the cyber security of all connected products. Effective from 11 December 2024, it will significantly impact Europe's cyber security landscape, benefiting society and the economy.

National cybersecurity authorities are preparing to help economic operators comply with the new rules. The CRA introduces EU-wide cybersecurity requirements for the design, development, production and market availability of hardware and software products, preventing overlapping regulations across EU member states. Products will bear the CE marking to indicate compliance with these requirements, ensuring high safety, health and environmental standards in the European Economic Area (EEA).

The regulation applies to all products with digital elements, including software, hardware and their remote data processing solutions, with some exceptions like medical devices, aeronautical products and cars. The CRA also empowers consumers to consider cyber security when choosing products with digital elements. Additionally, it ensures that machines and digital systems in the corrugated packaging industry meet strict cyber security standards, safeguarding production continuity, protecting sensitive data and reducing vulnerabilities, thereby improving the industry's overall resilience.

Machinery Regulation

The Machinery Regulation (EU) 2023/1230[6] replaces the Machinery Directive 2006/42/EC, modernising the legal framework to ensure the safety and compliance of machinery within the European Union. Adopted on 14 June 2023, the regulation introduces updated safety requirements that align with technological advancements, including artificial intelligence, autonomous systems and cyber security. The regulation will apply directly in all EU Member States starting 20 January 2027.

The regulation impacts industries relying on machinery, including the corrugated packaging industry, by enforcing stricter safety and performance standards for machines used in production. For this industry, the updated requirements for cyber security, risk assessment and digital documentation are particularly relevant.

The Machinery Regulation ensures that machines involved in corrugated packaging production meet high safety and reliability standards, mitigating risks associated with software failures, unauthorised access, or unsafe operational processes. By requiring compliance with state-of-the-art safety measures, the regulation promotes innovation and the adoption of more efficient and secure machinery in the corrugated packaging sector, ultimately improving operational resilience and production quality.

General Product Safety Regulation (GPSR, EU 2023/988)

The General Product Safety Regulation (EU) 2023/988[7] (GPSR) replaces Directive 2001/95/EC and modernises the framework for product safety across the European Union. Adopted on 23 May 2023, the regulation takes effect from 13 December 2024. It ensures that products offered to consumers meet stringent safety requirements, addressing the challenges of emerging technologies such as connected devices and software updates.

Contractual obligations

Cybersecurity clauses in contracts with customers and suppliers (machines, tools, equipment manufacturers, business partners, equipment vendors etc.) are increasingly crucial in the corrugated packaging industry. These clauses outline required cybersecurity measures, incident reporting protocols and liability in case of a breach, ensuring that all parties protect their systems and data.

Customers

Customers rely on manufacturers to safeguard sensitive data and maintain secure operations. Contracts typically include clauses that require encryption, secure networks and adherence to recognised cybersecurity standards. Breaching these terms can lead to reputational and financial damage.

Partners

Mid- to long-term partnerships often involve interconnected digital systems for data exchange and remote services. Contracts between different suppliers regarding machines, tools and equipment, raw materials, production materials, business partners etc. set expectations for secure data sharing, incident response and access controls. Non-compliance can disrupt the supply chain, highlighting the need for strong cyber security in these agreements. Since breaches or downtime can disrupt production, these clauses are critical to ensuring equipment security and minimising risk across operations.

Non-compliance with these contractual obligations can lead to legal consequences and financial penalties, making adherence to cyber security standards essential for all parties involved.

RELEVANT CYBERSECURITY STANDARDS

In cyber security, adhering to standards is essential for maintaining top-level security for operations and information. These standards provide the foundation for building robust cyber security frameworks, helping companies secure their systems and data. For the corrugated packaging and machinery production sectors, these standards are vital protocols against cyber threats and serve as a basis for regulatory compliance. This section lists and explains the standards used in this handbook, highlighting their role in meeting regulatory requirements and improving overall security posture.

NIST Cybersecurity Framework

Developed by the National Institute of Standards and Technology (NIST) in the United States, this framework offers a voluntary but widely adopted approach to managing cybersecurity risks. It is particularly relevant for manufacturers in critical infrastructure sectors, including those involved in packaging and machinery production.

NIST 2.0

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies and other organisations to manage cyber security risks. It offers a taxonomy of high-level cyber security outcomes that can be used by any organisation - regardless of size, sector or maturity - to better understand, assess, prioritise and communicate its cyber security efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes.[8]

ISO/IEC 27001 (Information Security Management)

This standard outlines requirements for establishing, implementing, maintaining and continuously improving an information security management system (ISMS). Corrugated and machinery producers can adopt ISO 27001 to systematically manage sensitive information, ensuring that cybersecurity risks are effectively mitigated. Compliance with this standard is often required for companies operating internationally or dealing with global supply chains.

ISA/IEC 62443 (Industrial Control Systems Security)

IEC 62443 is a critical standard for machinery producers, offering comprehensive guidance on securing industrial automation and control systems (IACS). It addresses both technical and organisational aspects of cybersecurity, ensuring that IACS are protected from cyber threats throughout every stage of the production lifecycle.

For corrugated manufacturers and their equipment suppliers, compliance with IEC 62443 is key to mitigate system vulnerabilities. System integrators may orient their practices towards IEC 62443-3-3, which focuses on system security requirements and security levels. Meanwhile, component suppliers should align with IEC 62443-4-2, which specifies requirements for secure product development.

VDMA guidance

Another piece of material that can be seen as highly relevant is the supply chain security specification of the German VDMA. It is characterised by pragmatic simplicity and clarity. Also, it puts a focus on the entire supply chain and why it is applicable in many kinds of manufacturing industries. Elaborated together with German BSI, it is also backed by big expertise on the crucial elements.

However, the purpose of the document is to ease purchasing processes while unnecessarily reducing cyber security requirements. Therefore, it appears as a checklist of acceptance criteria for machine procurement which is not the objective of this document.

Furthermore, the document is of course primarily, although not exclusively, aimed at members of the association and so is specific for the German market.

NETWORK REFERENCE ARCHITECTURE

PRACTICAL EXAMPLE: THE INTEGRATED PLANT

We have developed a simple reference architecture for the secure integration of IT and OT with two approaches. In the first approach, the local network is provided by the manufacturer and used within the OT environment. In the second approach, the network is managed by the producer. The focus of these plans is on zone segmentation, network separation through a local firewall and securing mutual access. This separation also applies in the case of remote access for maintenance purposes by the manufacturer. The appliances should ultimately be installed in a separate network behind the local firewall. The local firewalls used for separation should always remain under the control of the producer. Please note that all network schematics are simplified.

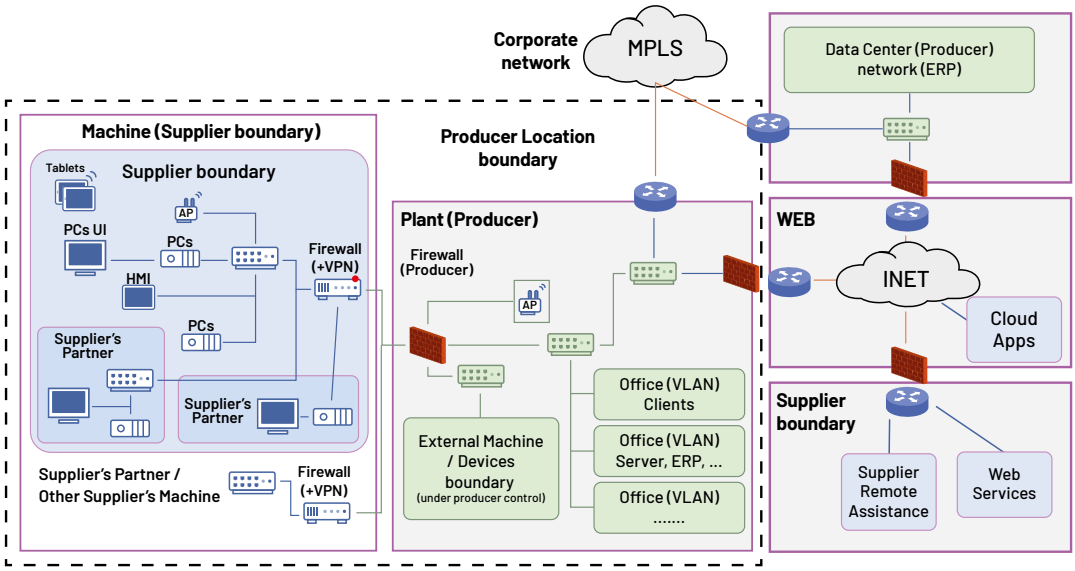
TECHNOLOGY LANDSCAPE IN INTEGRATED PLANTS

The corrugated packaging industry's shift to advanced technologies such as automation, Industrial Internet of Things (IIoT) and interconnected supply chains brings significant benefits but also cybersecurity challenges. Automated processes and IIoT devices improve efficiency and enable real-time monitoring, yet they introduce vulnerabilities that can disrupt production or compromise data.

With interconnected systems, supply chain security becomes even more critical, as cyber incidents can cascade across partners. Protecting these integrated technologies is essential to maintain operational continuity, safeguarding data and ensuring a resilient production environment.

Integrated Plant - Reference Architecture

Supplier privided Network Equipment



SYMBOL	DESCRIPTION	SYMBOL	DESCRIPTION
	Switch / L2 / L3 network device		Plant-managed device/service
	Router L3 device (producer)		Supplier-managed device/service
	Firewall (producer)		Plant-managed connection
	Router / VPN / Firewall network device (supplier)		Supplier-managed connection
	PC / PLC User Interface		Supplier-managed data flow
	Mobile devices (Tablet, smartphone)		
	Wifi Access Point		

CYBERSECURITY FRAMEWORK

CYBERSECURITY STANDARDS ADOPTED

The checklist is built around the NIST 2.0 framework, with ISO 27001 integrated to highlight areas of alignment and clarify where compliance is achieved. ISA/IEC 62443 is incorporated to address OT security aspects, providing guidance on aligning with this framework to secure operational technology.

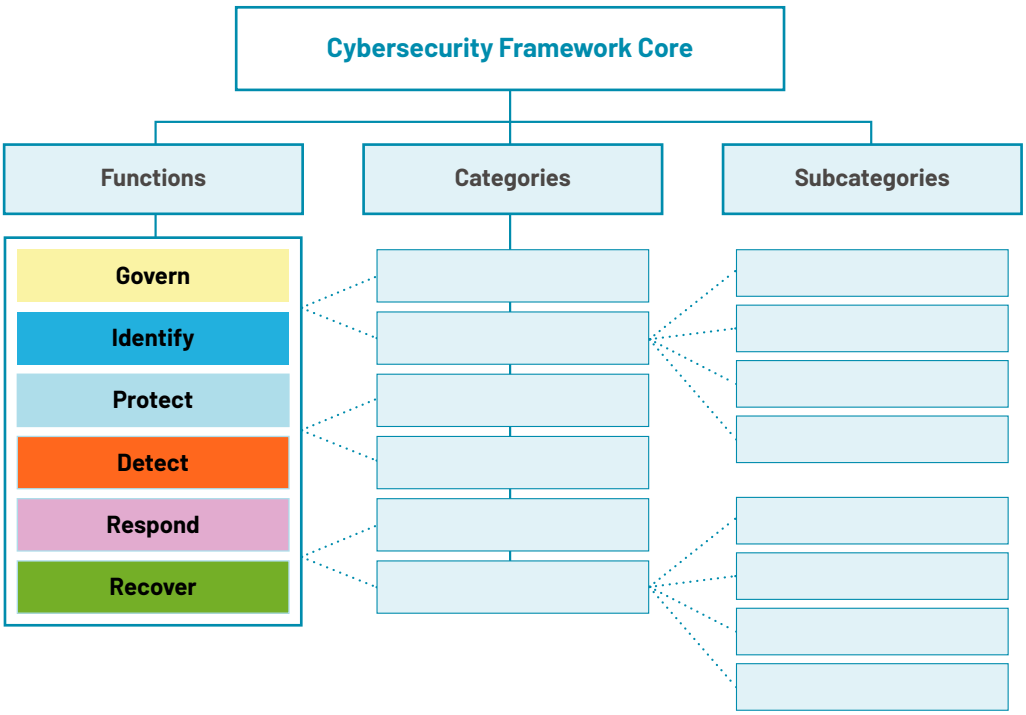
These standards serve as enablers to meet the requirements of emerging regulations. As cyber threats multiply and industries such as corrugated packaging and machinery production increasingly rely on digital technologies and interconnected systems, regulatory compliance has become a critical priority.

NIST 2.0

The CSF Core is a set of cyber security outcomes arranged by function, category and subcategory. These outcomes are not a checklist of actions to perform; specific actions taken to achieve an outcome will vary by organisation and use case, as will the individual responsible for those actions. Additionally, the order and size of functions, categories and subcategories in the Core does not imply the sequence or importance of achieving them. The structure of the Core is intended to resonate most with those charged with operationalising risk management within an organisation.

- Govern: Implement the organisation's cybersecurity risk management strategy and processes.
- Identify: Establish an understanding of IT/OT assets, systems and vulnerabilities, including risk assessments specific to the sector.
- Protect: Implement safeguards to defend IT/OT systems from unauthorised access, ensuring the integrity and security of operations and data.
- Detect: Enable continuous monitoring and real-time detection of potential cybersecurity threats or anomalies within IT/OT environments.
- Respond: Predefine and execute actions to mitigate the impact of cybersecurity incidents, minimising downtime and operational disruptions.
- Recover: Ensure the rapid restoration of IT/OT systems and continuity of operations after an incident, minimising the impact on production and supply chains.

CSF's use will vary based on an organisation's unique mission and risks. With an understanding of stakeholder expectations and risk appetite and tolerance (as outlined in GOVERN), an organisation can prioritise cyber security activities to make informed decisions about cyber security expenditures and actions. An organisation may choose to handle risk in one or more ways - including mitigating, transferring, avoiding, or accepting negative risks and realising, sharing, improving or accepting positive risks - depending on the potential impacts



and likelihoods. Importantly, an organisation can use the CSF both internally to manage its cyber security capabilities and externally to oversee or communicate with third parties. Regardless of the CSF's utilisation, an organisation may benefit from using the CSF as guidance to help it understand, assess, prioritise and communicate cyber security risks and the actions that will manage those risks. The selected outcomes can be used to focus on and implement strategic decisions to improve cyber security postures and maintain business continuity of essential functions while taking priorities and available resources into account.

The CSF provides a basis for improved communication regarding cyber security expectations, planning and resources. CSF fosters a bidirectional information flow between executives who focus on the organisation's priorities and strategic direction and managers who manage specific cyber security risks that could affect the achievement of those priorities. The CSF also supports a similar flow between managers and the practitioners who implement and operate the technologies.

INTEGRATION WITH OTHER RISK MANAGEMENT PROGRAMS

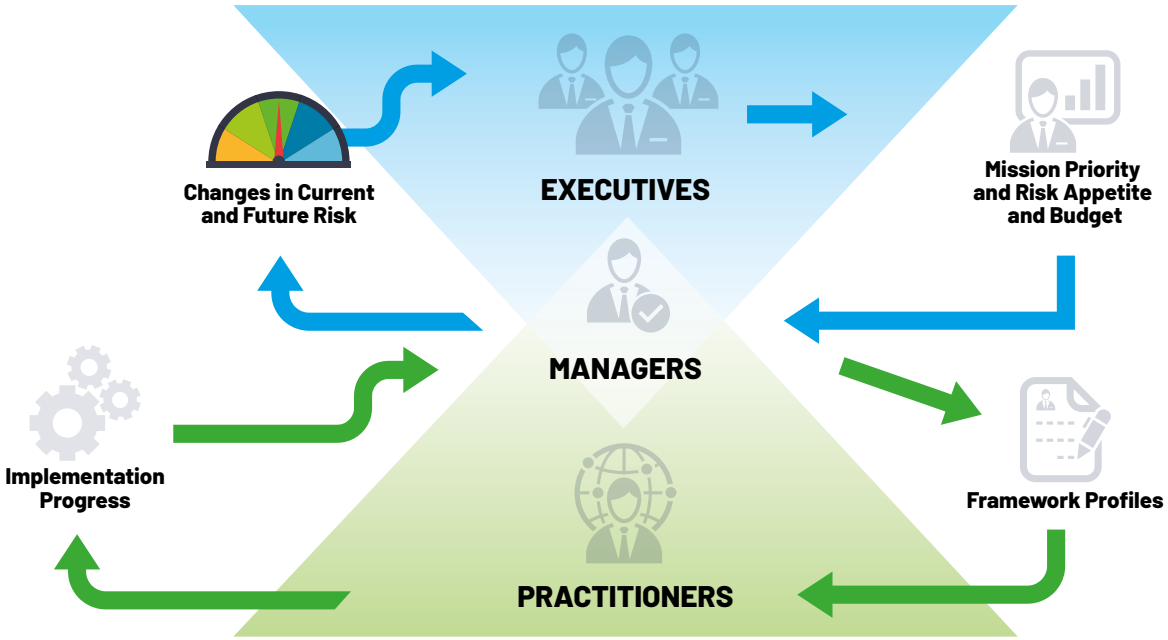
Every organisation faces numerous types of ICT risk (e.g., privacy, supply chain, artificial intelligence) and may use frameworks and management tools that are specific to each risk. Some organisations integrate ICT and all other risk management efforts at a high level by using ERM, while others keep the efforts separately to ensure adequate attention on each. Small organisations by their nature may monitor risk at the enterprise level, while larger companies may maintain separate risk management efforts integrated into the ERM. Organisations can employ an ERM approach to balance a portfolio of risk considerations, including cybersecurity, to make informed decisions.

The framework helps organisations to translate their terminology for cybersecurity and cybersecurity risk management into general risk management language that executives will understand.[9 10]

FRAMEWORK MAPPING

NIST 2.0 forms the foundation of the cybersecurity checklist, with its categories and subcategories mapped to other key legislations and standards such as NIS2, CRA, ISO 27001 and ISA/IEC 62443. This mapping ensures that companies can assess their compliance not only with NIST 2.0 but also with other important frameworks relevant to their operations.

By aligning the checklist with these standards, companies gain a comprehensive view of their cybersecurity posture, helping them identify gaps or overlaps across different regulations. This approach simplifies compliance management and allows companies of all sizes to assess and improve their cybersecurity practices in a unified manner. The mapping ensures the checklist and handbook are adaptable and provide a practical, robust resource for improving cybersecurity in line with industry's best practices and legal requirements.



MATURITY PRINCIPLES

For this handbook, we have created a 4-level scale to assess the maturity of each criterion, detailed below. The evaluation of maturity is conducted across four categories: Policy, Process/implementation, Communication & awareness and Measuring & monitoring. Each category has four descriptions corresponding to the four different levels, which can essentially be interpreted as follows:

- Level 1 = no actions in place
- Level 2 = partially implemented
- Level 3 = actions in place but governance/process to be performed
- Level 4 = actions in place and governance/process well managed and monitored

All this can be seen in the table below.

TARGET MATURITY LEVEL

It is important to clarify that the maturity scale outlined in this handbook is different from the **ISA/IEC 62443 Maturity Level/Scale**. While ISA/IEC 62443 maturity levels/scale focus on assessing an organisation's cybersecurity practices and compliance in industrial control systems, the FEFCO handbook's 4-level scale has been specifically designed to provide a practical framework for evaluating the readiness and robustness of internal processes across broader organisational criteria.

We have chosen this approach to better align with our industry's priorities and to provide a straightforward, actionable framework tailored to the unique needs of our specific industry. This 4-level maturity scale emphasises continuous improvement across areas critical to operation, offering clarity and flexibility without being constrained by external standards, thus giving us a good foundation to establish a starting point to measure our maturity and also a way to plan and continue to improve our cyber "level".

The contextualisation done by the FEFCO working group has established a baseline level of the framework, which serves as a recommended minimum starting point for every FEFCO

MATURITY NUMBER	POLICY	PROCESS/ IMPLEMENTATION	COMMUNICATION & AWARENESS	MEASURING & MONITORING
1	Is not documented	None of the key requirements have been implemented	Little to no formal communication regarding cybersecurity. Employees are unaware of cybersecurity risks or policies. There is no structured awareness program in place	There is no formal process for measuring or monitoring cybersecurity performance. Responses to incidents are purely reactive
2	It is fully documented/defined, but partially implemented	Some of the key requirements have been implemented	Basic communication exists, often reactive. Some initiatives to raise cybersecurity awareness, like occasional training or emails, but it is not structured	Some basic measurements exist, such as reactive logging and monitoring of incidents, but there is no structured measurement and monitoring process
3	It is fully documented/defined, performed by all stakeholders. Necessary governance in place	Most of the key requirements have been implemented	Regular communication about cybersecurity, including formal awareness programs and training. Employees understand their role in maintaining cybersecurity and are aware of current threats	Regular monitoring of systems and processes is established. Methods are in place to evaluate the effectiveness of cybersecurity measures, with periodic reports generated for review
4	It is fully documented / defined, performed by all stakeholders. Necessary governance in place and performs regular monitoring and reporting on the implementation.	All key requirements have been implemented	Cybersecurity is fully embedded in the organisation's culture. There is a continuous, comprehensive communication program focusing on proactive awareness, with frequent updates and exercises for employees at all levels	There is a comprehensive measuring and monitoring process providing real-time insight into cybersecurity status. Performance indicators are continuously evaluated and improved to optimise the security posture

member. This baseline is defined by all the MANDATORY controls, with a minimum total evaluation for the maturity level equal to two. This should be the minimum evaluation level and the starting point.

Organisations are advised to use the handbook and implement the framework step by step. Start by implementing the Mandatory subcategories, followed by the Recommended subcategories and finally the Points of improvement subcategories, always aiming for at least a maturity level of 2 for each criterion.

If the company's evaluation is below this baseline, the goal should be to analyse the gaps, allocate a budget for the necessary remediations and implement a plan to achieve the baseline as soon as possible. Conversely, if the initial evaluation is above the baseline, the first framework evaluation can be used as a starting point for further improvement, initiating a process of continuous improvement of the company's cyber security posture.

Investigate the challenges, receive indications or inputs from the Board/Executive or stakeholders and analyse the risks to help the company identify its future cyber security target posture. These inputs should be translated into impacts on the respective framework controls list, enabling each FEFCO member to create its own future target.

From this new future scenario as a target, it is possible to analyse the gaps, allocate a budget and implement a plan to achieve the new targets in a continuous and virtuous loop of improvement: a typical 360-degree process of continuous improvement.

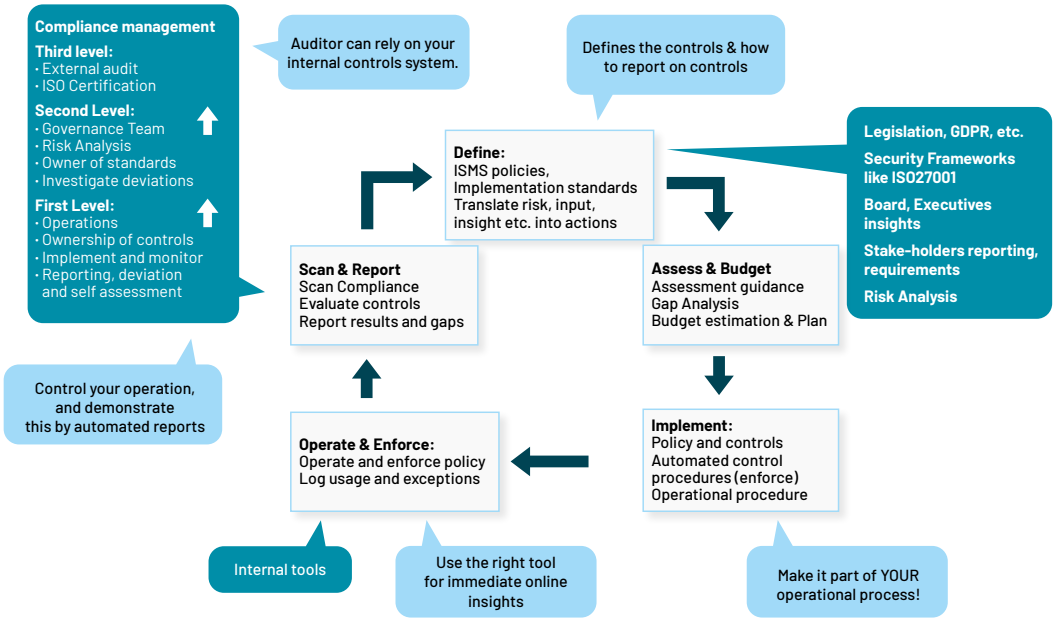
HOW TO USE THE FRAMEWORK AND ANNEXES

Preparing to create and use Organisational Profiles involves gathering information about organisational priorities, resources and risk direction from executives. Managers then collaborate with practitioners to communicate business needs and create risk-informed Organisational Profiles. Actions to close any gaps identified between the Current and Target Profiles will be implemented by managers and practitioners and will provide key inputs into system-level plans. As the target state is achieved throughout the organisation - including through controls and monitoring applied at the system level - the updated results can be shared through risk registers and progress reports.

As part of ongoing assessment, managers gain insights to make adjustments that further reduce potential harm and increase potential benefits. The GOVERN function supports organisational risk communication with executives. Executives' discussions involve strategy, particularly how cybersecurity-related uncertainties might affect the achievement of organisational objectives. These governance discussions support dialogue and agreement about risk management strategies (including cybersecurity supply chain risk); roles, responsibilities and authorities; policies and oversight. As executives establish cybersecurity priorities and objectives based on those needs, they communicate expectations about risk appetite, accountability and resources.

The overall cyber security objectives set by executives are transferred top-down to managers. When implementing the framework, managers will focus on how to achieve risk targets through common services, controls and collaboration, as expressed in the Target Profile and improved through the actions being tracked in the action plan.

A possible model of Governance



Practitioners focus on implementing the target state and measuring changes in operational risk to help plan, carry out and monitor specific cyber security activities. As controls are implemented to manage risk at an acceptable level, practitioners provide managers and executives with the information (e.g., key performance indicators, key risk indicators) they need to understand the organisation's cyber security posture, make informed decisions and maintain or adjust the risk strategy accordingly. Executives can also combine this cyber security risk data with information about other types of risk across the organisation. Updates to expectations and priorities are included in updated Organisational Profiles as the cycle repeats.

The idea behind the Cyber Security Handbook is to give a practical "ready-to-use" tool to assess the information and communication technology (ICT) infrastructure to understand the current cyber security posture of the company.

This process involves reviewing the list of controls and evaluating them using numerical ratings across four distinct levels as defined above.

The focal point is obviously not the tool itself, but the process behind it, where the company is pushed by a continuous process of analysing risk and defining targets, assessing the current state, identifying gaps, defining a plan to close the gaps, implementing them and starting again.

Here is a practical example of a possible scenario of governance of the process just explained.

Breakdown of the framework components

NIST 2.0 checklist

This section introduces the NIST 2.0 framework, covering functions, categories and subcategories, with implementation examples.

Following the implementation examples, the Guidance column offers additional details on complying with the category, providing in-depth information beyond the implementation examples.

Guidance

The organisation covered by NIS legislation has a responsibility to know the other organisations in the same sector in order to work with them to achieve the objectives set by NIS for that particular sector.

Information protection needs should be determined and the related processes revised as necessary.

This assessment should identify and prioritise potential negative impacts to the organisation from the risks associated with the distributed and interconnected nature of ICT/OT product and service supply chains. This list should include suppliers, vendors and partners contact information and the services they provide, so they can be contacted for assistance in the event of an outage or service degradation.

After this, you will see the class of relevance value: 'Mandatory', 'Recommended' and 'Point of improvement'. 'Mandatory' indicates a mandatory subcategory recommended for every FEFCO company. 'Recommended' means it is beneficial to have, while 'Point of improvement' indicates voluntary adoption. These values have been predefined by the expert group.

The subsequent sections will include four columns, to evaluate both IT and OT aspects. This means the maturity assessment is only applied at category level and not subcategories. Subcategory maturity may be assessed if it supports determining the category's maturity level, but these evaluations will not appear in the results.

- Policy
- Process/implementation
- Communication & awareness
- Measuring & monitoring

Where IT and OT environments are not adequately segregated, it is recommended that the OT site should default to IT security controls and maturity assessments until proper segmentation can be implemented.

Annex I: Checklist of control points to ensure sufficient cyber security

The Checklist				IT vs OT areas		To be compiled			
Function	Category	Subcategory	Implementation Examples	CLASS FOR IT	CLASS FOR OT	Policy	Process/ Implementation	Communication and awareness	Measuring & monitoring
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.		Chart Area			(3) It is fully documented/defined, performed by all stakeholder. Necessary governance in place	(1) Non of the key rquirements have been implemented	(3) Regular communication about cybersecurity, including formal awareness programs and training. Employees understand their role in maintaining cybersecurity and are aware of current threats	(2) Some basic measurements exist, such as reactive logging and monitoring of incidents, but there is no structured measurement and monitoring process
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	Ext: Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	Mandatory	Mandatory	(2) It is fully documented/defined, but partially implemented	(3) Most of the key requirements have been implemented	(2) Basic communication exists, often reactive. Some initiatives to raise cybersecurity awareness, like occasional training or emails, but it is not structured	(4) There is a comprehensive measuring and monitoring process providing real-time insight into cybersecurity status. Performance indicators are continuously evaluated and improved to optimize the security posture

Maturity for IT and OT is assessed together based on four criteria: Policy, Process/implementation, Communication & awareness and Measuring & monitoring. These levels and criteria are all explained in depth in the section above. Not all the categories are relevant for OT, hence there is a separate column where it is indicated which categories are relevant for OT.

It is crucial that both IT and OT personnel evaluate and rank each maturity category accurately, following the NIST 2.0 framework.

In cases where IT and OT are integrated without a clear distinction within the company, it is advisable to follow the IT standards outlined in the checklist and complete the first four columns accordingly.

Notes for specific subcategories can be found in the last column if needed.

Evaluation methodology

This section explains:

- Every function of NIST 2.0.

FUNCTION	GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and
	IDENTIFY (ID): The organization's current cybersecurity risk is understood
	PROTECT (PR): Safeguards to manage the organization's cybersecurity risk are used
	DETECT (DE): Possible cybersecurity attacks and compromises are found and analyzed
	RESPOND (RS): Actions regarding a detected cybersecurity incident are taken
	RECOVER (RC): Assets and operations affected by a cybersecurity incident are restored

- Details each class of relevance value.

CLASS OF RELEVANCE	MANDATORY = mandatory to have, we strongly raccomend it to every FEFCO company
	RECO = good to have
	POINT OF IMPROVEMENT = vouluntary adoption

- And defines the maturity levels for each category (see the table in the "Maturity Principles section)

The tables below (in the checklist) show the maturity levels of each NIST 2.0 category for each function from the checklist sheet, used for the graphs in the "Results Graphs" sheet. These calculations are only for the graphs and do not contain essential information for the checklist user, so no deep dive is necessary.

There is no necessity to make modifications to this Excel sheet.

Results

This section provides summary graphs of the maturity findings for each function. These will help you identify areas where your company can improve and find growth opportunities.

NIST 2.0 vs other frameworks

This part lists the NIS2, CRA, ISO 27001 & 27002 and ISA/IEC 62443 requirements for each NIST 2.0 subcategory. There are sometimes gaps between NIST 2.0 and the other frameworks because not every subcategory has a corresponding requirement in the other frameworks or laws.

Understanding the alignment between the NIST 2.0 framework and specific laws (such as NIS2, CRA) or frameworks (like ISO 27001, ISA/IEC 62443) is important for an organisation. This knowledge allows a company to identify areas where it is already compliant with certain regulations or standards, as well as areas where it requires improvement to be compliant with specific laws or to achieve certification for frameworks.

NIS2 transposition status

This sheet includes a table that shows in which member states the directive has been transposed and whether NACE 17.21 is included. If NACE 17.21 is included, it indicates that corrugated packaging manufacturers will be subject to the NIS2 law in that member state.

Step by step guidance for implementation

Step 1: Identify the classes of relevance for the different subcategories

The initial step is to identify the Mandatory subcategories and assess their implementation within the organisation. It is recommended to document this in the 4 maturity columns next to the class of relevance, as it will facilitate the determination of the overall maturity level of a category.

After identifying the Mandatory subcategories, ensure the company complies with it before evaluating the Recommended and Point of Improvement subcategories.

NIST 2.0 vs other frameworks

Function	Category	Subcategory	Implementation Examples	NIS2 -Directive (EU) 2022/2555	ISO 27001:2022	ISO 27002:2022	ISA 62443

Function	Category	Subcategory	Implementation Examples	CLASS FOR IT	CLASS FOR OT	Policy	Process/ Implementation	Communication and awareness	Measuring & monitoring
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	**Organizational Context (GV.OC):** The circumstances – mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements – surrounding the organization's cybersecurity risk management decisions are understood.					**(3) It is fully documented/defined, performed by all stakeholder. Necessary governance in place**	**(1) Non of the key requirements have been implemented**	**(3) Regular communication about cybersecurity, including formal awareness programs and training. Employees understand their role in maintaining cybersecurity and are aware of current threats**	**(2) Some basic measurements exist, such as reactive logging and monitoring of incidents, but there is no structured measurement and monitoring process**
		GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission	**Mandatory**	**Mandatory**	**(2) It is fully documented/defined, but partially implemented**	**(3) Most of the key requirements have been implemented**	**(2) Basic communication exists, often reactive. Some initiatives to raise cybersecurity awareness, like occasional training or emails, but it is not structured**	**(4) There is a comprehensive measuring and monitoring process providing real-time insight into cybersecurity status. Performance indicators are continuously evaluated and improved to optimize the security posture**
		GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related	**Mandatory**	**Mandatory**				

CLASS FOR IT	CLASS FOR OT	Policy	Process/Implementation	Communication and awareness	Measuring & monitoring
		(3) It is fully documented/defined, performed by all stakeholder. Necessary governance in place	(1) Non of the key rquirements have been implemented	(3) Regular communication about cybersecurity, including formal awareness programs and training. Employees understand their role in maintaining cybersecurity and are aware of current threats	(2) Some basic measurements exist, such as reactive logging and monitoring of incidents, but there is no structured measurement and monitoring process
Mandatory	Mandatory	(2) It is fully documentend/defined, but partially implemented	(3) Most of the key requirements have been implemented	(2) Basic communication exists, often reactive. Some initiatives to raise cybersecurity awareness, like occasional training or emails, but it is not structured	(4) There is a comprehensive measuring and monitoring process providing real-time insight into cybersecurity status. Performance indicators are continuously evaluated and improved to optimize the security posture

Step 2: Determine the maturity of the categories

After identifying the classes of relevance, determine the maturity of each function category using four pillars: Policy, Process/implementation, Communication and awareness and Measuring & monitoring. While subcategories can be assessed to support the overall evaluation, the focus should remain on the maturity of each function category.

When calculating the overall score, prioritise the Mandatory subcategories, as these are critical for FEFCO's objectives. This structured approach provides a clear understanding of both IT and OT maturity, enabling targeted improvements where needed. Only when a subcategory has a class of relevance, then this subcategory is relevant for OT.

Step 3: Analyse the results

When the maturity for each category has been assessed, it is important to analyse the result graphs in the results sheet. This allows the person responsible for IT or management to easily identify where the organisation is lacking in a specific category of a particular function.

Upon identifying a deficiency in a specific function, you can dive into the relevant category and examine the subcategories to pinpoint the exact area of weakness. This process requires manual effort, as it is not reflected in the overall result graphs.

Step 4: Improving

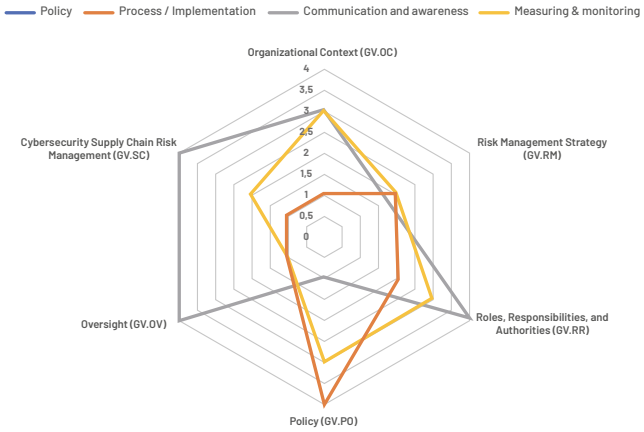
Upon identifying gaps, it is crucial to take definitive actions to address these deficiencies. The designated individuals should prioritise which gaps to address first, with the goal of achieving the target maturity profile: level 2.

Step 5: Reassess

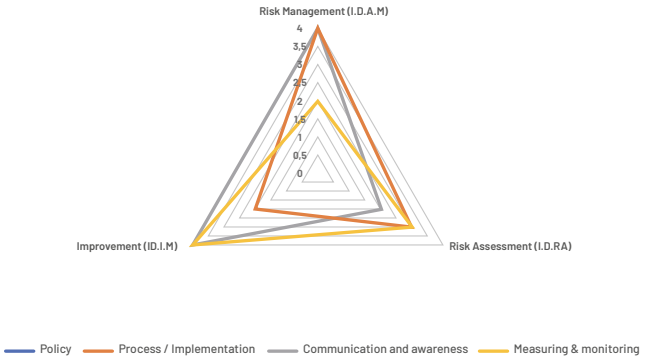
It is essential to emphasise that this checklist and its application, constitutes an ongoing process. The exercise should be repeated annually to clearly identify areas of improvement and those where the company has regressed in maturity.

Compliance with all the Mandatory subcategories is essential. Once this is achieved, the organisation can then consider improvements in the Recommended and Point of Improvement subcategories.

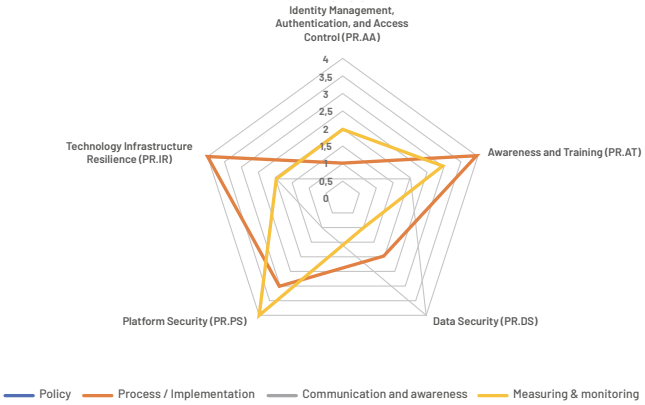
Govern



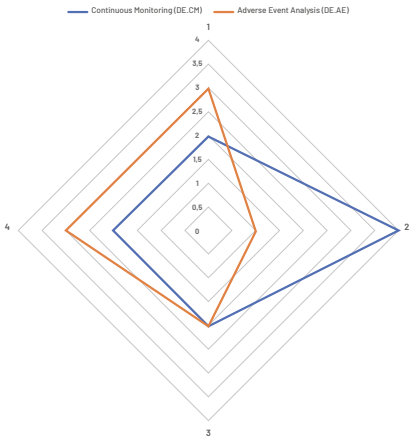
Identify



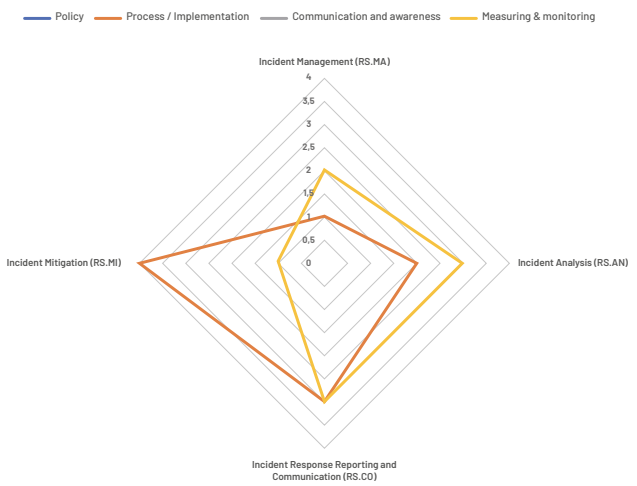
Protect



Title ?



Respond



Recover

LEGACY SYSTEMS

In today's rapidly evolving technological landscape, many factories and organisations still rely on legacy systems, particularly in the realm of OT. These systems, often critical to operations, present unique challenges when it comes to maintaining and improving security, especially when they cannot be patched or modified. This section provides a comprehensive guide on how to improve the security of legacy systems without direct modifications. The legacy system and all the control points that will be enumerated subsequently are the result and objective of using the handbook, aimed at reducing risk in this context for FEFCO members.

While it may not always be possible to implement all recommended measures, it is crucial to document and be aware of the risks. Reporting these risks to leadership ensures that they are informed and can make strategic decisions to mitigate potential threats. You may be able to do one or more of the following measures.

Risk assessments: Regular risk assessments should be conducted to identify vulnerabilities and threats in the OT environment. These assessments should evaluate the potential impact of identified risks on operations and determine the likelihood of their occurrence. Involving key stakeholders in the risk assessment process ensures a comprehensive understanding of the OT environment and its specific challenges.

Network segmentation: One of the most effective strategies for securing legacy systems is network segmentation. By isolating OT and IT networks, you can limit the spread of threats between these environments. Implementing security zones and conduits within the OT network helps to segment different levels of criticality, ensuring that a breach in one area does not compromise the entire system.

Access control: Strict access control is essential for protecting legacy systems. Implement robust access management protocols, including strong authentication methods, to ensure that only authorised personnel can access OT systems. For remote access, use secure solutions such as Virtual Private Networks (VPNs) with multi-factor authentication (MFA) to add an extra layer of security.

System hardening: Hardening legacy OT systems involves applying security measures to minimise vulnerabilities and improve the security of the systems. This process includes deploying firewalls, intrusion detection and prevention systems, access controls and other security mechanisms to mitigate the risk of cyberattacks.

Furthermore, organisations should deactivate or eliminate any superfluous or unused services, protocols and applications that could be vulnerable to exploitation by attackers. This includes disabling non-essential ports, removing default accounts and passwords and restricting access to critical systems and components.

Monitoring and detection: Continuous monitoring and detection are crucial for identifying and responding to potential security threats. Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network activities for suspicious behaviour. Enable logging and auditing of all activities to detect and analyse any abnormal behaviours, allowing for timely intervention.

Device management: Effective device management is another key aspect of securing legacy systems. Use device control solutions to manage and monitor all devices connected to the OT network. Maintain an up-to-date inventory of all OT assets to better understand and manage the risks associated with each device.

Training and awareness: Human error is often a significant factor in security breaches. Therefore, it is vital to train employees on best security practices and raise awareness about the specific risks related to OT systems. Conduct regular simulation exercises and drills to prepare staff to respond effectively in case of a security incident.

Patch and update management: While patching legacy systems may not always be possible, having a patch management plan is still essential. Establish a plan to manage security updates as soon as they become available. In cases where patching is not feasible, look for workarounds or compensating controls to mitigate the vulnerabilities.

Incident response planning: Create an incident response plan that outlines procedures for OT environments, considering the possible physical impacts of cyber incidents. Additionally, develop disaster recovery plans to restore operations with minimal downtime in case of a cybersecurity incident.

Physical security: Physical security measures are just as important as digital ones. Ensure that areas housing OT systems are secure and that physical access is strictly controlled. Protect critical equipment from unauthorised access and physical tampering to prevent potential security breaches.

Collaboration with vendors: Working closely with vendors can provide valuable insights into vulnerabilities and potential solutions. Maintain open communication with your vendors to understand the risks associated with your legacy systems and explore possible mitigation strategies. Ensure that contracts and service level agreements (SLAs) include security clauses to hold vendors accountable for their role in maintaining system security.

ANNEX II:
SUPPLIER DECLARATION OF CONFORMITY CHECKLIST

DEFINITION

The Supplier Declaration of Conformity is the official declaration of "compliance" done by suppliers in relation to the product sold and current cyber security legislations, guidelines or standards.

INTRODUCTION

In an interconnected world, the European corrugated board industry has increasing demands for robust cyber security measures from its suppliers. This chapter outlines the essential security expectations that suppliers must meet to ensure the availability and integrity of their products and services.

While the VDMA Supply Chain Security Specification is comprehensive it is often considered too specific for machine builders. The IEC 62443 standard, although widely recognized, is not mandatory for providing equipment to the corrugated Packaging industry. Therefore, this declaration of conformity presents a carefully curated selection of controls from various sources, highlighting the minimum requirements, attributes and practices necessary for machine builders and IIOT/Cloud service providers. These controls are designed to address four of the most critical and commonly utilized use cases in the industry.

It is essential to consider the implications for existing applications. Applying this declaration of conformity to retrofit scenarios could significantly increase the complexity and cost of upgrading existing products. This raises a crucial question: Is this added complexity something that producers are willing to accept?

Ultimately, this declaration should not be viewed as a mere checkbox exercise. Instead, it aims to foster greater transparency among producers, particularly OT- and IT security engineers. By providing clear and detailed information, it enables more informed decision-making and comprehensive risk assessments, thereby enhancing the overall security posture of the industry.

TEMPLATE

ID	**NIST control**
Category	
Description	Normative/Informative
Comments	Reserved
IEC 62443-3-3 mapping	Derived from explanation // for use cases 1-3
IEC 62443-4-2 mapping	Derived from explanation // for use cases 1-3
VDMA mapping	Derived from explanation // for use cases 1-3
NIST 2.0 framework mapping	Derived from explanation // for use case 4

USE CASES

Use case 1 – Remote Access

This use case describes the remote connectivity from a supplier's personnel and associates into the plant and to the machinery and subsystems of the supplier, for troubleshooting, maintenance and other means of remote servicing.

General constraints

Supplier shall implement and maintain appropriate technical and organisational measures to prevent and minimize the impact of cybersecurity incidents, including but not limited to unauthorized access, disruptions, or damage to network and information systems.

Supplier shall notify to customer without undue delay and promptly of any cybersecurity incidents affecting the availability, integrity, or confidentiality of the goods or services provided. The Supplier agrees to cooperate in good faith and relevant authorities in the investigation, mitigation and resolution of cybersecurity incidents.

Supplier shall be enabled to provide his own remote access solution to deliver the best possible level of remote services.

If the supplier does not meet (all) the requirement we suggest that the producer only establish the connection (connect the cable, turn on router) when intervention from the supplier is needed (and unplug the cable, disconnect the router after the needed remote support).

RA – 001	**PROTECT**
Remote Architecture	
The remote party can connect to the site via a secure, encrypted, state-of-the-art remote access solution. Devices must be CE certified.	Normative
–	Reserved
62443-3-3 SR 4.1 RE 2	The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.
62443-4-2 CR 4.1	Components shall • provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and • support the protection of the confidentiality of information in transit as defined in IEC 6244333 SR 4.1.
CSRS-SI-NRA-1	The existing remote maintenance solution must be used. (See documentation xyz. doc) Remote access is required for this machine / system. The connection must be established from the production facility. Only an encrypted connection to a rendezvous server is permitted. Control element for users in the production facility to establish the connection and signal that a connection has been established.

RA – 002	PROTECT
Remote Architecture	
Unauthorized access to data in use, data in transit, data at rest and interception of data is prevented.	Normative
–	Reserved

62443-3-3 SR 4.1 RE 2	The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.
62443-4-3 CR 4.1	Components shall • provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and • support the protection of the confidentiality of information in transit as defined in IEC 6244333 SR 4.1.
CSRS-SI-NRA-1	The existing remote maintenance solution must be used. (See documentation xyz. doc) Remote access is required for this machine / system. The connection must be established from the production facility. Only an encrypted connection to a rendezvous server is permitted. Control element for users in the production facility to establish the connection and signal that a connection has been established.

RA – 003	PROTECT
Remote Architecture	
Secure, encrypted, state-of-the-art communication protocol is being used.	Normative
State-of-the-Art: The most advanced and recognized security technologies and practices in the industry.	Reserved

62443-3-3 SR 4.3	If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.
62443-4-2 CR 4.3	The component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.
CSRS-SI-NRA-1	The existing remote maintenance solution must be used. (See documentation xyz. doc) Remote access is required for this machine / system. The connection must be established from the production facility. Only an encrypted connection to a rendezvous server is permitted. Control element for users in the production facility to establish the connection and signal that a connection has been established.

RA – 004	GOVERN
User accounts	
Only personalized accounts are used.	Normative
–	Reserved

62443-3-3 SR 1.1 RE 1	The control system shall provide the capability to uniquely identify and authenticate all human users.
62443-4-2 CR 1.1	Components shall provide the capability to identify and authenticate all human users according to IEC 6244333 SR 1.1
CSRS-SI-UAC-1	The integrator undertakes to define suitable roles and user groups and to implement them in a technically mandatory manner, which are dependent on the environmental risks (e.g. special authentication and authorization for configuration changes, software changes, etc.).

RA – 005	GOVERN
User accounts	
A strong authentication method is applied.	Normative
–	Reserved
62443-3-3 SR 1.1 RE 2	The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).
62443-4-2 CR 1.1	Components shall provide the capability to identify and authenticate all human users according to IEC 6244333 SR 1.1
CSRS-SI-UAC-2	The integrator undertakes to use individual passwords in accordance with the role and rights concept during commissioning. All temporary and unnecessary user accounts must be deleted during commissioning.

RA – 006	GOVERN
User accounts	
Accounts are centrally managed.	Normative
–	Reserved
62443-3-3 SR 1.3 RE 1	The control system shall provide the capability to support unified account management.
62443-4-2 CR 1.3	Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to IEC 6244333 SR 1.3.
CSRS-SI-UAC-3	The integrator undertakes to operate the machines only via the user or group accounts and not to use the administrator account during normal operation.

RA - 007	GOVERN
Site access	
Access to individual machines/endpoints follows concept of least privilege.	Normative
Least privilege concept also applies to 3rd party connection (services providers, 3rd party machinery, etc.).	Reserved
–	–
–	–
CSRS-SI-NRA-2	Remote access may only be made to IT/OT components of the machine/system that are necessary or intended for the remote connection. A risk analysis must be used to demonstrate which systems or components may be accessed without remote access posing a risk to employees at the machine.

RA - 008	GOVERN
Site access	
Access requests from supplier need to be authorized by producer.	Normative
–	Reserved
62443-3-3 SR 1.13 RE 1	The control system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role.
–	–
CSRS-SI-NRA-3	Remote access is explicitly approved by the operator for technical and/or organisational reasons.

RA – 009	GOVERN
Logging & Monitoring	
Remote connections from supplier are monitored and logged by supplier.	Normative
–	Reserved
62443-3-3 SR 6.1/SR 6.2	The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis. / The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.
–	–
CSRS-SI-NRA-4	Remote access to the selected system must be logged. This describes the user, date, duration, IT/OT component that was accessed, the activity of the remote accesser and the client.

RA – 010	GOVERN
Logging & Monitoring	
Remote activities from supplier are monitored and logged by supplier.	Normative
Please also refer to informative section for implementation details.	Reserved
62443-3-3 SR 6.1 / SR 6.2	The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis. / The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.
–	–
CSRS-SI-NRA-4	Remote access to the selected system must be logged. This describes the user, date, duration, IT/OT component that was accessed, the activity of the remote accesser and the client.

RA – 011	RC
Backup & Recovery	
For recovery software backups of site component exist.	Normative
–	Reserved
62443-3-3 SR 7.3	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.
–	–
CSRS-SI-AVA-1/ CSRS-SI-AVA-2	The integrator undertakes to document the necessary steps for carrying out backups and, if necessary, to train the staff and, in addition, to create a backup after final acceptance. The integrator undertakes to document and test the possibility of restoring the factory settings.

RA – 012	RC
Backup & Recovery	
The location of the backup is documented and accessible to the producer.	Normative
–	Reserved
–	–
–	–
CSRS-SI-SCS-6	The integrator will hand over the current configuration of the machine and systems to the operator and to document the setup, in such a way, that the operator will be able to restore the configuration after an incident.

INFORMATIVE SECTION

RA-I – 001	PROTECT
Remote Architecture	
Direction of connection initialization	Informative

◯ Outbound from site component
◯ Outbound from supplier component
◯ Both

RA-I – 002	GOVERN
Server Type	
Remote access server location.	Informative

◯ Supplier
◯ Producer
◯ Cloud
◯ Else:

RA-I – 003	GOVERN
Site Component	
Site Component Owner.	Informative

◯ Supplier
◯ Producer
◯ Else:

RA-I – 004	GOVERN
Server Type	
Responsible for maintenance.	Informative

◯ Supplier
◯ Producer
◯ Else:

RA-I – 006	GOVERN
User Accounts	
Responsible managing remote users.	Informative
◯ Supplier ◯ Producer ◯ Else:	

RA-I – 007	PROTECT
Site Component Authentication and Authorization.	
Type	Informative
◯ Credentials ◯ Client certificates ◯ Keycards ◯ Else:	

RA-I – 008	PROTECT
Site Component Authentication and Authorization.	
Credentials or certificate validity.	Informative
days months years	

RA-I – 009	PROTECT
Site Component Authentication and Authorization.	
Credentials or certificate revocation possible.	Informative
◯ Yes ◯ No	

RA-I – 010	PROTECT
Supplier personnel and 3rd party Authentication and Authorization.	
Typec	Informative
◯ Credentials ◯ Client certificates ◯ Keycards ◯ Else:	

RA-I – 011	PROTECT
Supplier personnel and 3rd party Authentication and Authorization.	
Credentials or certificate validity	Informative
days months years	

RA-I – 012	PROTECT
Supplier personnel and 3rd party Authentication and Authorization.	
Credentials or certificate revocation possible	Informative
◯ Yes ◯ No	

RA-I – 013	PROTECT
Configuration of site component.	
Administrative tasks protected by secure protocols (https, etc.)	Informative
◯ Yes ◯ No	

RA-I – 014	PROTECT
Configuration of site component.	
Access to configuration interface protected	Informative
◯ Credentials ◯ Client certificates ◯ Keycards ◯ Else:	

RA-I – 015	PROTECT
Security patches for site component.	
Provided by supplier	Informative
◯ Yes ◯ No	

RA-I – 016	PROTECT
Security patches for site component.	
Installed by supplier	Informative
◯ Yes ◯ No	

RA-I – 017	GOVERN
Awareness	
Security awareness training	Informative
◯ Supplier services engineers ◯ Producer side users	

RA-I – 018	GOVERN
Logging & Monitoring	
Remote connections from supplier are monitored and logged by supplier.	Informative
◯ Yes ◯ No	

RA-I – 019	GOVERN
Logging & Monitoring	
Remote activities from supplier are monitored and logged by producer.	Informative
◯ Yes ◯ No	

RA-I – 020	GOVERN
Logging & Monitoring	
Connection log is provided by the supplier on demand.	Informative
◯ Yes ◯ No	

RA-I – 021	GOVERN
Backup & Restore	
For recovery redundant site components exist.	Informative
◯ Hot-Standby ◯ Cold-Standby ◯ Spare parts service available ◯ No	

RA-I – 022	GOVERN
Backup & Restore	
For recovery software backups of remote component exist.	Informative
◯ Yes ◯ No	

RA-I – 023	DETECT
Compromising of remote access	
Are there any means to detect unauthorized remote access provided by the supplier?	Informative
◯ Yes ◯ No	

RA-I – 024	DETECT
Compromising of remote access	
Which means are provided to detect unauthorized remote access by the producer / by the supplier?	Informative
◯ Yes ◯ No	

RA-I – 025	RESPOND
Compromising of remote access	
In the event of suspicious activity, access is tracked.	Informative
◯ Yes ◯ No	

RA-I – 026	RESPOND
Compromising of remote access	
In the event of suspicious activity, connection can be cut by the producer.	Informative
◯ Yes ◯ No	

RA-I – 027	RECOVERY
Compromising of remote access	
Recovery services offered by supplier?	Informative
◯ Yes, which? ◯ No	

RA-I – 028	RECOVERY
Compromising of remote access	
Time and effort to redeploy remote connection, paid service or free?	Informative
◯ Yes ◯ No	

USE CASE 2 – INTERCONNECTIVITY

This use case describes the interconnectivity between the supplier's network and the producer's enterprise network, between the supplier's network and other supplier's machine or subsystem networks and between the supplier's network and the internet.

Suggestions for Firewall models

This section outlines the basic requirements for firewalls to ensure they are up-to-date, modern, and future proof. These requirements serve as suggestions and guidelines for providers to ensure the devices sold meet the most recent necessary standards as from publication date.

Core Security Requirements:

- Layer 7 Inspection: Application-aware traffic analysis for deep visibility and security control.
- Encrypted & Private Traffic Protection:
  - Support for SSL VPN, IPSec, and WireGuard for secure tunneling.
  - Secure handling of TLS 1.3 and future cryptographic standards.
- Identity & Access Management (IAM):
  - Enforced Multi-Factor Authentication (MFA) with modern methods like FIDO2/WebAuthn.
  - Integration with centralized identity providers (e.g., Active Directory, SAML, OAuth).
  - Role-Based Access Control (RBAC) for fine-grained permissions.
- Network Security Controls:
  - Geo-IP Filtering to restrict access based on geographic location.
  - IP-Based Access Control for enhanced threat mitigation.
  - Zero Trust Network Access (ZTNA) principles for securing remote connections.
- Network Segmentation:
  - Support for VLANs, microsegmentation, and software-defined networking (SDN).
- SIEM Integration:
  - Compatibility with Security Information and Event Management (SIEM) solutions.
  - Ability to export logs via Syslog and support for common security event formats (e.g., CEF, JSON, LEEF).
- Industry-Recognized Configuration Standards: Compliance with best practices such as the CIS (Center for Internet Security) Benchmarks and NIST 800-41.

- Advanced Threat Protection:
  - Deep Packet Inspection (DPI) for detecting and blocking malicious content.
  - Automated Threat Intelligence & Response with real-time signature updates.
  - Behavior-based anomaly detection using AI/ML.
  - Sandboxing and file analysis for unknown threats.

Recommended Features:

- SSL/TLS Inspection:
  - Ability to decrypt and analyze encrypted traffic while ensuring compliance with privacy laws.
  - Support for TLS 1.3 and integration with Certificate Transparency logs.

Intrusion Detection & Prevention (IDP/IPS):

- AI-driven threat correlation across multiple attack vectors.
- Signature-based and heuristic detection mechanisms.
- Prevention of zero-day exploits through machine learning analysis.

Cloud & Hybrid Environment Support:

- Secure connectivity for multi-cloud and hybrid cloud architectures.
- Integration with cloud-native security services like AWS Shield, Azure Sentinel, or Google Chronicle.
- SASE (Secure Access Service Edge) capabilities for securing remote workforces.

Automated Configuration & Compliance Auditing:

- Built-in policy validation and automatic misconfiguration detection.
- Continuous compliance monitoring for frameworks like ISO 27001, NIS2, and GDPR.

IC – 001A	**GOVERN**
Network segregation	
Supplier must be allowed to provide firewall functionality to segregate his machine network.	Normative
—	Reserved
62443-3-3 SR 5.4	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.
CSRS-SI-INF-3	The integrator undertakes to separate the machine/system network from the operator's network and to only allow necessary access.

IC – 001B	**GOVERN**
Network segregation	
Producers provide needed network equipment (switchports, network cable etc.).	Normative
—	Reserved
62443-3-3 SR 5.4	The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.
CSRS-SI-INF-3	The integrator undertakes to separate the machine/system network from the operator's network and to only allow necessary access.

IC – 002A	PROTECT
Network segregation	
Firewall functionality is used to segregate producer IT network from supplier OT and enterprise network, Firewall must be unique connection point to supplier network.	Normative
–	Reserved
62443-3-3 SR 5.1 RE 3	The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.
62443-4-2 NDR 5.2	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.
CSRS-SI-NCC-2	The integrator undertakes not to directly connect the real-time network („field level") and the production networks. The real-time network and the production networks must be separated by a physical interface.

IC – 002B	PROTECT
Network segregation	
Firewall functionality is provided and used to segregate producer IT network from supplier OT and enterprise network, Firewall must be unique connection point to supplier network.	Normative
–	Reserved
62443-3-3 SR 5.1 RE 3	The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.
62443-4-2 NDR 5.2	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the riskbased zones and conduits model.
CSRS-SI-NCC-2	The integrator undertakes not to directly connect the real-time network („field level") and the production networks. The real-time network and the production networks must be separated by a physical interface.

IC – 003A	GOVERN
Network segregation	
Firewall rules are implemented and reviewed.	
–	Reserved
62443-3-3 SR 7.6	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.
62443-4-2 CR 7.6	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.
–	–

IC – 003B	GOVERN
Network segregation	
Firewall rules are provided and reviewed by supplier	
–	Reserved
62443-3-3 SR 7.6	The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.
62443-4-2 CR 7.6	Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.
–	–

IC – 004A	DT
Network segregation	
Firewall rules are monitored and logged.	
–	Reserved
62443-3-3 SR 5.2	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.
62443-4-2 NDR 5.2	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the riskbased
–	–

IC – 004B	DT
Network segregation	
Firewall rules are provided by the supplier.	
–	Reserved
62443-3-3 SR 5.2	The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.
62443-4-2 NDR 5.2	A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the riskbased zones and conduits model.
–	–

IC – 005A	RC
Network segregation	
In the recovery area, we have firewall backups.	
–	Reserved

62443-3-3 SR 7.3	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.
–	–

INFORMATIVE SECTION

IC-I – 001	PROTECT
Security patches for Firewall	
Provided by supplier.	Informative
◯ Yes ◯ No	

IC-I – 002	PROTECT
Security patches for Firewall	
Installed by supplier.	Informative
◯ Yes ◯ No	

IC-I – 003	PROTECT
Data encryption	
Connections between supplier networks and other networks are encrypted.	Informative
◯ Yes ◯ No	

IC-I – 004	PROTECT
Data encryption	
Administrative tasks are protected by secure protocols.	Informative
◯ Yes ◯ No	

IC-I – 005	PROTECT
Availability	
Which means are taken to make interconnectivity sufficiently robust?	Informative
◯ Yes ◯ No	

IC-I – 006	PROTECT
Miscellaneous	
Machine-to-machine communication is protected against data loss, tampering and loss of availability.	Informative
◯ Yes ◯ No	

IC-I – 007	PROTECT
Miscellaneous	
External connections are logged.	Informative
◯ Yes ◯ No	

IC-I – 008	PROTECT
Miscellaneous	
All data communication is done over secure and defined interfaces.	Informative
◯ Yes ◯ No	

IC-I – 009	PROTECT
Miscellaneous	
Data must be encrypted to ensure security and confidentiality.	Informative
◯ Yes ◯ No	

IC-I – 010	PROTECT
Authentication	
Communication partners must accept each other before exchanging data (Zero Trust aspect).	Informative
◯ Technical ◯ Contractual ◯ Else:	

IC-I – 011	GOVERN
Conceptional	
Supplier will provide to producer concept and architecture before implementation or changes.	Informative
◯ Yes ◯ No	

IC-I – 012	GOVERN
Conceptional	
Necessary information e.g., firewall rules will be provided to producer before implementation of supplier equipment.	Informative
◯ Yes ◯ No	

USE CASE 3 – PHYSICAL ACCESS

This use case describes the direct on-site access to digital assets of a supplier.

PA – 001	PROTECT
Wireless networks	
There is a partial segregation of the internet: The PC, PLCs/HMIs of the machines are on the corrugator net, the internal machine mesh is segregated from the corrugator mesh.	Normative
–	Reserved
62443-3-3 SR 1.6	The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.
–	–

PA – 002	PROTECT
Wireless networks	
Wi-Fi is protected by state-of-the-art authentication mechanisms.	
–	Reserved
62443-3-3 SR 1.6	The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.
–	–

PA – 003	PROTECT
Wireless networks	
Secure, state-of-the-art Wi-Fi encryption is being used.	
–	Reserved
62443-3-3 SR 2.2 / SR 2.3	The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices. / The control system shall provide the capability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices.
–	–

PA – 004	PROTECT
HMIs / PC systems	
PCs run kiosk applications (graphical interfaces limit the access to the operating system)	
–	Reserved
62443-3-3 SR 7.7	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.
CSRS-SI-CHA-2	The integrator undertakes to carry out basic system hardening and measures recommended by component manufacturers: such as deactivating unused USB ports and deactivating unnecessary services.

PA – 005	PROTECT
HMIs / PC systems	
USB ports are enabled but not directly/uncoveredly (physically) accessible.	
–	Reserved
62443-3-3 SR 7.7	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.
CSRS-SI-CHA-2	The integrator undertakes to carry out basic system hardening and measures recommended by component manufacturers: such as deactivating unused USB ports and deactivating unnecessary services.

PA – 006	PROTECT
HMIs / PC systems	
USB ports are disabled.	
–	Reserved

62443-3-3 SR 7.7	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.
CSRS-SI-CHA-2	The integrator undertakes to carry out basic system hardening and measures recommended by component manufacturers: such as deactivating unused USB ports and deactivating unnecessary services.

PA – 007	PROTECT
HMIs / PC systems	
We are reducing all possible physical ethernet accesses on machines (eth plug).	
–	Reserved

62443-3-3 SR 7.7	The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.
CSRS-SI-CHA-2	The integrator undertakes to carry out basic system hardening and measures recommended by component manufacturers: such as deactivating unused USB ports and deactivating unnecessary services.

PA – 008	PROTECT
HMIs / PC systems	
Access to HMIs needs to be authenticated and authorized.	
–	Reserved

62443-3-3 SR 1.7 / SR 2.1	For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. / On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.
CSRS-SI-UAC-1	The integrator undertakes to define suitable roles and user groups and to implement them in a technically mandatory manner, which are dependent on the environmental risks (e.g. special authentication and authorization for configuration changes, software changes, etc.).

PA – 009	GOVERN
HMIs / PC systems	
Default administrative accounts are renamed where possible.	
–	Reserved

–	–
CSRS-SI-UAC-2	The integrator undertakes to use individual passwords in accordance with the role and rights concept during commissioning. All temporary and unnecessary user accounts must be deleted during commissioning.

PA – 010	ID
HMIs / PC systems	
Security awareness training has been done.	
–	Reserved
–	–
CSRS-SI-TRA-2	As part of the commissioning, the integrator instructs the operator's employees in dealing with all necessary security issues relating to the system or machine.

PA – 011	ID
HMIs / PC systems	
User training includes safe storage of devices when they are not in use.	
–	Reserved
–	–
CSRS-SI-TRA-3	The operator instructs the integrator's employees in relation to the security requirements that apply to them. The integrator undertakes to instruct them again if employees change.

PA – 012	GOVERN
Physical access control	
Physical access control of people around the site needs to be provided by producer.	
–	Reserved
–	–
CSRS-SI-INF-1	The integrator undertakes to instruct its employees to only stay in the assigned areas on the operator's premises.

INFORMATIVE SECTION

PA-I – 001	GOVERN
Mobile devices	
Central device management (MDM) is used.	Informative
◯ Yes ◯ No	

PA-I – 002	GOVERN
Network devices	
Management ports of devices are protected.	Informative
◯ Yes ◯ No	

PA-I – 003	GOVERN
Network devices	
Physical access to sensitive equipment is being protected by producer.	Informative
◯ Yes ◯ No	

PA-I – 004	GOVERN
Network devices	
Network components correctly mounted in lockable and purpose-oriented spaces.	Informative
◯ Yes ◯ No	

PA-I – 005	GOVERN
Network devices	
Network devices will be regularly patched.	Informative
◯ Yes, by supplier ◯ Yes, by producer ◯ No	

PA-I – 006	RECOVER
Wireless networks	
Wireless security configuration is managed centrally and standardized.	Informative
◯ Yes ◯ No	

PA-I – 007	GOVERN
HMI/PC Systems	
There are standardized and documented security configurations for client devices and access points.	Informative
◯ Yes ◯ No	

PA-I – 008	RECOVER
HMI/PC Systems	
Programs, data and configurations are constantly backed up in a workmanlike manner.	Informative
◯ Yes ◯ No	

PA-I – 009	RECOVER
HMI/PC Systems	
There is a recovery for PC programs and it is automatic, while for PLCs it is manual.	Informative
◯ Yes ◯ No	

PA-I – 010	PROTECT
Endpoint protection and hardening	
Endpoint protection is on the computers with OS installed.	Informative
◯ Yes ◯ No	

PA-I – 011	PROTECT
Endpoint protection and hardening	
Services on the PCs are running with service users and without admin rights on OS.	Informative
◯ Yes ◯ No	

PA-I – 012	PROTECT
Endpoint protection and hardening	
PCs and PLCs are kept inside the electrical panels under lock and key.	Informative
◯ Yes ◯ No	

USE CASE 4 - SAAS

This use case covers the relevant topics related to Software as a Service (SaaS) solutions. The topics have been aligned with NIST2.0 and provide guidance for the mandatory controls included in the NIS 2 directive.

SaaS-001	**GOVERN**
—	
Organisational Context: The circumstances — mission, stakeholder expectations, dependencies and legal, regulatory and contractual requirements — surrounding the organisation's cybersecurity risk management decisions are understood	Normative
Business impact analysis, continuity plans and contingency plans are regularly verified, updated and tested (at least annually and after major changes). These tests involve customers and relevant third parties, are documented and results are utilized to enhance future safeguards. When outsourcing cloud services, security measures are mandatory. Contracts with external providers must include the following: Secure software development requirements (design, development, testing), evidence of adequate testing conducted by the provider and acceptance tests for service quality based on agreed requirements.	Reserved

GV.OC-03	Legal, regulatory and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.
GV.OC-04	Critical objectives, capabilities and services that stakeholders depend on or expect from the organisation are understood and communicated.

SaaS-002	**GOVERN**
—	
The organisation's cybersecurity risk management strategy, expectations and policy are established, communicated and monitored	Normative
During the annual combined risk assessment with producers and suppliers, the organisation(s) address how to accept, avoid, reduce or share risks in accordance with to the risk management process. Business impact analysis, continuity plans and contingency plans are regularly verified, updated and tested at least annually and after major changes. Thes tests involve customers and relevant third parties, are documented and the results are utilized to enhance future safeguards. During the annual combined risk assessment with producers and suppliers, the organisation(s) address how to accept, avoid, reduce, or share risks in accordance with the risk management process. Business impact analyses, continuity plans and contingency plans are regularly verified, updated and tested at least annually and after major changes. These tests involve customers and relevant third parties, are thoroughly documented and the results are utilized to enhance future safeguard.	Reserved

GV.RM-01	Risk management objectives are established and agreed to by organisational stakeholders.
GV.RM-03	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.

SaaS-003		IDENTIFY
–		
Risk Assessment: The cybersecurity risk to the organisation, assets and individuals is understood by the organisation.		Normative
Policies and safeguards are documented and communicated to facilitate the quick identification and resolution of vulnerabilities in the cloud service. This includes the regular identification and analysis of vulnerabilities, as well as the consistent implementation of safeguards, such as installing security updates.		Reserved
ID.RA-01	Vulnerabilities in assets are identified, validated and recorded.	
ID.RA-08	Processes for receiving, analysing and responding to vulnerability disclosures are established.	

SaaS-004		PROTECT
–		
Identity Management, Authentication and Access Control: Access to physical and logical assets is limited to authorized users, services and hardware and managed commensurate with the assessed risk of unauthorized access		Normative
A documented policy ensures proper management of system and data access based on business and security needs. It includes: Granting and changing access based on the 'least-privilege' and 'need-to-know' principles. • Regularly reviewing access permissions. • Approving and documenting access management. • Withdrawing access when employment changes. • Separating operational and control functions. • Separating roles in administration, approval and granting of access. • The confidentiality of user login information is protected by: • Identity checks using trusted methods. • Industry-standard authentication and authorization (e.g., multi-factor authentication, no shared login info, automatic expiry). • Mandatory multi-factor authentication for administrators (e.g., smart card or biometrics). Procedures and technical safeguards for secure key management include at least the following aspects: • Generation of keys for different cryptographic systems and applications, • Issuing and obtaining public-key certificates, • Provisioning and activation of the keys for customers and third parties involved, • Secure storage of provider's own keys, • Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised, • Handling of compromised keys, • Withdrawal and deletion of keys, for example in the case of compromising or staff changes.		Reserved
PR.AA-01	Identities and credentials for authorized users, services and hardware are managed by the organisation.	
PR.AA-02	Identities are proofed and bound to credentials based on the context of interactions.	

PR.AA-03	Users, services and hardware are authenticated, including multi-factor authentication.
PR.AA-05	Access permissions, entitlements and authorizations are defined in a policy, managed, enforced and reviewed and incorporate the principles of least privilege and separation of duties.

SaaS-005	**PROTECT**
–	
Awareness and Training: The organisation's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks	Normative
Cyber security training	Reserved
PR.AT-01	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind

SaaS-006	**PROTECT**
–	
Data Security: Data are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity and availability of information	Normative
Sensitive customer data is encrypted for storage with exceptions made only for data that can't be encrypted for functional reasons. Private keys are known only to the customer unless a controlled procedure is established in agreement with the cloud provider. Strong encryption and authentication procedures are implemented for transmitting cloud customer data over public networks. Policies and safeguards ensure regular data backup and restoration. Documented procedures are communicated and made available. Data retention practices align with agreements made with cloud customers and the provider's business needs. Access to backed-up data is restricted to authorized personnel only. Restoration processes are controlled and approved by authorized individuals in accordance with agreements or internal policies.	Reserved
PR.DS-01	The confidentiality, integrity and availability of data-at-rest are protected.
PR.DS-02	The confidentiality, integrity and availability of data-in-transit are protected.
PR.DS-11	Backups of data are created, protected, maintained and tested.

SaaS-007	**PROTECT**
–	
Platform Security: The hardware, software (e.g., firmware, operating systems, applications) and services of physical and virtual platforms are managed consistent with the organisation's risk strategy to protect their confidentiality, integrity and availability	Normative
Logs are stored on secure central servers and are deleted when no longer needed. Authentication and encryption ensure the integrity and authenticity of the logs during transmission. Access to the source code and related development information is restricted and monitored to prevent unauthorized changes.	Reserved
PR.PS-04	Log records are generated and made available for continuous monitoring.
PR.PS-06	Secure software development practices are integrated and their performance is monitored throughout the software development life cycle.

ANNEX III:
CONTENTS OF AN INTERCONNECTION SECURITY AGREEMENT (ISA)

Reference: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-47.pdf

DEFINITION

ISA is a document that defines the security-related aspects of an intended connection between two parties' information system. The ISA is the agreement signed between a FEFCO member and a customer or supplier in case there is an interconnection with their information systems.

An Interconnection Security Agreement (ISA) should contain a cover sheet followed by a document of four numbered sections. The information presented within those four sections should address the need for the interconnection and the security controls required and be implemented to protect the confidentiality, integrity and availability of the systems and data.

The four sections are as follows:

- Section 1: Interconnection Statement of Requirements
- Section 2: Systems Security Considerations
- Section 3: Topological Drawing
- Section 4: Signatory Authority

Defining the required security considerations that need to be documented can be challenging without detailed knowledge of each system being interconnected. Each specific interconnection must be contextualized and analyzed before providing precise guidance on the contents of the four sections.

SECTION 1: INTERCONNECTION STATEMENT OF REQUIREMENTS

Use this section to document the formal requirement for connecting the two systems. Explain the rationale for the interconnection justifying the activity. The information presented should include:

- The requirement for the interconnection, including the benefits derived
- The names of the systems being interconnected
- The names or organisations that are part of the interconnection
- The specific roles and duties assigned to each party within the interconnection.
- The obligations of each party to protect sensitive information shared within the interconnection.
- Sanctions in case of non-compliance with the interconnection agreement.

SECTION 2: SYSTEM SECURITY CONSIDERATIONS

Use this section to document the security features that are in place to protect the confidentiality, integrity and availability of the data and the systems being interconnected. The following points should generally be addressed (all the listed points or part of it):

- General Information/Data Description: Describe the information and data that will be made available, exchanged, or passed one-way only by the interconnection of the two systems
- Services Offered: Describe the nature of the information services (e.g., e-mail, file transfer protocol [FTP], database query, file query, general computational services) offered over the interconnection by each organisation
- Data Sensitivity: Enter the sensitivity level of the information that will be handled through the interconnection, including the highest level of sensitivity involved (e.g., Privacy Act, Trade Secret Act, Law Enforcement Sensitive, Sensitive-But-Unclassified, GDPR) and the most restrictive protection measures required
- User Community: Describe the "user community" that will be served by the interconnection, including their approved access levels and the lowest approval level of any individual who will have access to the interconnection. Also, discuss requirements for background investigations and security clearances, if appropriate
- Information Exchange Security: Describe all system security technical services pertinent to the secure exchange of data between the connected systems
- Rules of Behavior: Summarize the aspects of behavior expected from users who will have access to the interconnection. Each system is expected to protect information belonging to the other through the implementation of security controls that protect against intrusion, tampering and viruses, among others
- Formal Security Policy: Enter the titles of the formal

security policy(ies) that govern each system (e.g., "Information Systems Policy and Procedures, Number xxxx" for "Organisation A"). +

- Audit Trail Responsibilities: Describe how the audit trail responsibility will be shared by the organisations and what events each organisation will log. Specify the length of time that audit logs will be retained. If no audit trail is performed, so state.
- Security Parameters: Specify the security parameters exchanged between systems to authenticate that the requesting system is the legitimate system and that the class(es) of service requested is approved by the ISA
- Training and Awareness: Enter the details of any new or additional security training and awareness requirements and the assignment of responsibility for conducting training and awareness throughout the life cycle of the interconnection
- Specific Equipment Restrictions. Describe any revised or new restriction(s) to be placed on terminals, including their usage, location and physical accessibility
- Connectivity: Describe any special considerations for broadband connections to any system in the proposed interconnection, including security risks and safeguards used to mitigate those risks.
- Third parties: Describe security measures for third-party engagements, including vetting, contractual obligations and compliance with security controls to prevent unauthorized access or data compromise.
- Back-ups: Summarize backup procedures, including frequency, retention and protection measures to ensure data integrity and confidentiality.
- Data destruction: Describe agreed methods for secure data disposal, such as wiping or physical destruction, ensuring compliance with policies and regulations.
- Notification procedure: Summarize incident notification processes, including contacts, escalation and reporting timelines. Each party follows its own response policies unless otherwise specified.
- Compliance with laws and regulations: Describe how the interconnection ensures adherence to applicable laws, regulations and industry standards. Each party is responsible for maintaining compliance and addressing any regulatory requirements.
- Incident Reporting. Describe the agreements made regarding the reporting of and response to information security incidents for both organisations. For example, "Each organisation will report incidents in accordance with its own (procedure name) procedures." If no incident reporting is performed, state.

SECTION 3: TOPOLOGICAL DRAWING

The ISA should include a topological drawing illustrating the interconnectivity from one system to the other system (endpoint to endpoint). The drawing should include the following:

The title "SECTION 3: TOPOLOGICAL DRAWING."

All communications paths, circuits and other components used for the interconnection, from "Organisation A's" system to "Organisation B's" system

The drawing should depict the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices and computer workstations)

SECTION 4: SIGNATORY AUTHORITY

The ISA should include a signature line. This section should include the following:

- The expiration date of the agreement
- Periodic review requirements, such as the date of the next review
- Plan for reversibility: Describe the agreed procedures to ensure a secure and orderly termination of the interconnection, including data retrieval, transfer and deletion to prevent unauthorized access.
- Other statements as required by the Parties, if any
- The signatures of the Managers from each organisation and the date of the signatures.

LIST OF ABBREVIATIONS

ABBREVIATION	EXPLANATION
BSI	British Standards Institution
CA	Cyber Attack
CD	Cyber Defence
CEO	Chief Executive Officer
CI	Critical Infrastructure
CPS	Cyber-Physical System
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CS	Cyber Security
CSF	Cybersecurity Framework
CyCLONe	Cyber Crisis Liaison Organisation Network
DRC	Disaster Recovery Plan
DT	Detect
ERP	Enterprise Resource Planning
FEFCO	European Federation of Corrugated Board Manufacturers
GV	Govern
HMI	Human-Machine Interface
IACS	Industrial Automation and Control System
IAM	Identity and Access Management
ICS	Industrial Control System
ICT	Information and Communication Technology
ID	Identify
IE	Industrial Engineering
IEC	International Electrotechnical Commission
INET	Industrial Network
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISA	Information Security Agreement
IT	Information Technology
LGV	Laser-Guided Vehicle
MES	Manufacturing Execution System

MFA	Multi-Factor Authentication
MPLS	Multiprotocol Label Switching
NACE	Nomenclature of Economic Activities
NIS	Network and Information System
NIST	National Institute of Standards and Technology
OCC	Old Corrugated Container
OT	Operational Technology - in this document we often use OT as a generic term, meaning it also covers a full machine (line) such as a corrugator, converting machine or work in progress (WIP) delivery
PR	Protect
RC	Recover
RS	Respond
SaaS	Software as a Service
SME	Small and Medium Enterprise
VDMA	Verband Deutscher Maschinen- und Anlagenbau (German Mechanical Engineering Industry Association)
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

ACKNOWLEDGEMENTS

This handbook is the result of a collaborative effort between FEFCO corrugated packaging producers and their suppliers, with the support of EY consultants and the FEFCO team. We extend our sincere gratitude to the individuals and organisations whose contributions made this resource possible.

Hans Christian Hansen
Cyber Security workgroup Chairman
DS Smith Packaging

Marc Van Damme
Operations and Innovation Committee Chairman
VPK Group

Eleni Despotou
Director General
FEFCO

Daniele Plazzi
FEPA

Armin Kaltenbacher
BHS Corrugated

Schremser Gerald
Prinzhorn Holding

Talha Minty
Smurfit Westrock

Thomas Albers
Minda

Gianluca Berrettini
Fosber

Laurent Bonherbe
Dunapack Packaging

Greg Carter
eProductivity Software

Huib de Beijer
OMP

Francisco Gonzalez
BOBST

Florian Göpfert
Göpfert

Erik Govers
VPK Group

Antoine Harb
Unipakhellas Group

Alexander Hopp
Klingele Paper & Packaging

Houriet Lefebvre
FEFCO

Mazzei Laura
FEFCO

Peerts Hans-Frederik
VPK Group

Dan Roth
Göpfert

Hubert Strauss
BHS Corrugated

Phil Thürmer
Minda

Giacomo Vitolo
Fosber

Steve Whillis
eProductivity Software

Viktor Van Puyvelde
EY

Xavier Vecchiato
EY

REFERENCES

1 Regulation - 2023/1230 - EN - EUR-Lex

2 Cascading effects of cyber-attacks on interconnected critical infrastructure | Cybersecurity | Full Text (springeropen.com)

3 Impact, Vulnerabilities and Mitigation Strategies for Cyber-Secure Critical Infrastructure (mdpi.com)

4 Commission Delegated Regulation (EU) 2023/137 of 10 October 2022 establishing the statistical classification of economic activities NACE Revision 2 (Text with EEA relevance) ELI: http://data.europa.eu/eli/reg_del/2023/137/oj

5 Regulation - 2024/2847 - EN - EUR-Lex

6 Regulation - 2023/1230 - EN - EUR-Lex

7 Regulation - 2023/988 - EN - EUR-Lex

8 CSWP 29, The NIST Cybersecurity Framework (CSF) 2.0 | CSRC

9 NIST CSF 2.0: https://www.nist.gov/cyberframework/nists-journey-csf-20

10 A National cyber security framework: https://www.cybersecurityframework.it/en

The Federation of Corrugated Board Manufacturers
Avenue Louise 250
B – 1050 Brussels
Tel + 32 2 646 40 70
www.fefco.org
X (formerly Twitter): @FEFCO

General information and requests for publications:
info@fefco.org