

CYBER SECURITY AWARENESS IN THE PROCESSING INDUSTRY

Keith Glynn

Stygian Vortex Security Consultants, USA

ABSTRACT

The focus of this paper is to integrate cyber security awareness into the operationalization of new products and processes in the cluster of ceramic companies of the Castellón, Spain region. This effort outlines the introduction of cyber security methods into the overall collaboration within this community to enhance inclusiveness, growth, and sustainability. The result is to modify the management systems to empower employees to be the key stakeholders of a quality and security focused work environment.

1. INTRODUCTION

Ignoti et Quasi Occulti – Unknown and Partially Hidden.

Fake delivery texts. Bank alerts that look real. AI-generated phishing emails. Account takeover scams. These cyber threats are becoming part of everyday digital life. According to the FBI Internet Crime Report 2025, Americans alone lost nearly \$21 billion to cyber-enabled crime in 2025. With a Mideast conflict that pushes energy costs up with heavy industry using roughly 30% of energy generated, it is clear the major industrial challenges of the Castellón region are energy, technology, geopolitical, and sustainability.

Much like safety in the processing industry, cyber security is a part of everything, every day. The task is to have all employees involved in cyber security awareness and active in the success of bringing together the operational components required to create a shift in focus for the future.

As process engineers, we are trained to view safety and consistency as primary attributes in industrial processing professions. Creating processing systems that conform to standards and produce product with lower risk and high efficiency is paramount. The Information Technology (IT) industry does not yet have the same roots. The process industry has decades of accidents with hard learned lessons that are now part of an operationalization and training effort. The advancement of Artificial Intelligence (AI) might be the engine that causes the IT industry to put safety first in the form of training and governance. This is an excellent way for the processing industry to see the current challenge and bring forth the two disciplines – overall product quality and cyber security – into one operating function.

Currently, the IT industry has created very robust information processing in the cloud, but it was not always that way. Twenty-five years ago, IT was just coming into its early stride. When a server needed to be moved or replaced, not all the users were defined in the system, or responsive to calls concerning the server shut down. An unwritten protocol was to let the helpdesk know that you would unplug the server so they could redirect the compliant calls directly to the IT engineering staff. Would a process engineer just shut down a heat exchanger?

Today, the demand of having process design and development sessions that include process, material, and data flow diagrams is at the front edge of operationalizing new products and processes. Risk governance that balances product profitability against incident costs is at the top of the management agenda.

Herein are a few points from history to bring forward a picture of our challenge today.

2. OVERVIEW OF CURRENT CYBERSECURITY CHALLENGES

There are two important security concepts to understand that will be used throughout this discussion. The two concepts are outlined below:

- The Principle of Least Privilege – “Least Privilege” is an information security concept that maintains that a user, process, or system should only have the minimum access rights or permissions necessary to perform its legitimate, authorized task, and no more.
- Opt In and Opt Out Data Governance – “Opt In” is the way data usage is generally governed in Europe. A user or entity must state that they will allow an organization to use their data from transactional business or querying by Opting In. The action is on the user or owner of the data to allow the other organization to use their data. “Opt Out” is

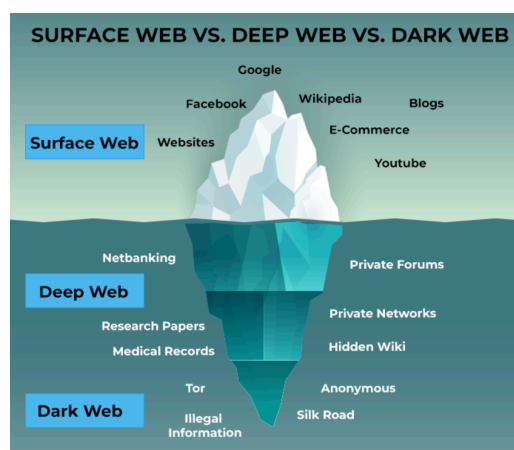
the opposite. This is where the user must tell the organization not to use their data. So, the "Opt Out" default is that an organization, let's say Google, can use your browsing data unless you tell it not to. This is the way is done in the United States today.

An interesting statistic from an IBM study is that 29% of people asked in a recent survey admitted to trying to disrupt or corrupt the company's AI tools. This supports the use of Least Privilege in that there is a tendency for users to "play" with data and applications to see what they could do to affect it. This is a good example of the difference that I found between the IT industry and the processing industry.

2.1. Brief Internet Overview

The World Wide Web (WWW) and the Internet. The difference between these two terms is that the WWW operates on top of the Internet. The Internet is the network – and the IT infrastructure – used to access contents on the WWW, while the WWW is the collection of information – webpages – accessed via the internet.

Below is a figure that explains the layers of the internet for purposes of understanding cyber security:



<https://www.spiceworks.com/security/dark-web-vs-deep-web/>

Understanding how to mine information from the deep and dark web becomes an essential skill for any cybersecurity professional working to protect IT systems in today's processing industry. A newly emerging field in cybersecurity is named "Cyber threat intelligence." Threat Intelligence collects and analyzes data from online public sources (the three web layers) to understand attacker's motivation and establish their future behavior. This gives cyber security decision-makers the insight to plan their future steps and to move from reactive to proactive defense.

2.2. Dark Web marketplace

Until recently, it was not widely known that there is a thriving commercial dark web marketplace where a variety of services are bought and sold. The growth of this marketplace over the last 20 years provides significant evidence of the sophisticated criminal and state sponsored cyber threat efforts.

In June 2025, Europol took down the Archetyp Market with an estimated 3200 registered vendors and 600,000 customers globally. The success of ransomware groups launching cyber-attacks from the dark web and injecting money into this marketplace have brought the level of cyber threats to a more complex level where AI is utilized to increase its effectiveness.

There are teams of hackers with very specialized skills that complete a small part of a hack into an organization and then sell that information in the dark web marketplace as a service. The processing industry is a high value target due to its proprietary information and, in some cases, because it is a part of critical infrastructure that our society is dependent on, such as transportation, fuel refineries, hospitals, etc.

This is the part of the reading where you might start feeling hopeless about defending against the onslaught of cybercrime. When I was studying for the Certified Ethical Hacker (CEH) cybersecurity certification, a mentor told me that I was going to feel this way. He told me it would pass as I learned ways to counter the threats and lower cyber risk. A way to process this feeling is – “There is no cause for panic. There is every cause for vigilance.”

2.3. Operational Technology (OT)

Operational technology (OT) refers to hardware and software that directly monitors, controls, and manages physical devices, processes, and infrastructure in industrial environments. Unlike IT, which focuses specifically on data, OT ensures physical systems—such as manufacturing robots, power grids, and valves—run safely and efficiently. The key to OT cybersecurity is to focus on data flows with equal intensity as we would material and energy flows.

OT dependency on connecting to the public cloud is a relatively new opportunity in business and technology that requires a cybersecurity perspective. Let's look at where the industry is coming from in terms of internet exposure.

The industrial processing and manufacturing history transpired over a few centuries starting back in the mid-1700's. The process industry began to scale up rapidly in the “second industrial revolution” after 1870 with growth springing from new innovations in steel-making processes, mass production, assembly lines, electrical grid systems, large-scale manufacture of machine tools, and use of advanced machinery in steam-powered factories. Manufacturing standards and techniques became streamlined and optimized over more than 100 years before information technology was even a term that was used to describe the IT industry.

When comparing the processing industry and the IT industry, a key metric is business development speed. The difference in IT business development speed happens at a much faster rate and is usually aligned with growth as described in Moore's Law. Moore's Law states that computer processor speed will double every 18 months.

Presently, IT and OT are merging with artificial intelligence (AI) playing a major role in emerging capabilities. This merger of technologies is creating a market disruption that will have both positive and negative consequences. Our effort is to minimize the negative and focus on the positive while empowering a community that is dependent on this industry for its livelihood.

2.4. Is your facility prepared to be digitally exposed?

All new OT is now digital. It is a cyber operation. Cyber systems have direct physical consequences in processing and manufacturing systems. This is no longer theoretical. Threat actors focus on abusing legitimate user access, not breaking it. Security must move at the same speed as operations. Resilience is measured in impact absorbed while continuing to operate.

The best defense can be viewed as having the best quality product. All employees must be involved and motivated to succeed. Castellón already has many ingredients necessary to continue, and expand, its global leadership in the ceramics industry. It has an educated and hardworking populace, an infrastructure, and leadership. The management tasks of security

and quality have several important aspects that can continue to differentiate this region from other global ceramics manufacturing competitors. Most importantly:

1. The meaning of quality, and now cyber security – Quality must be considered from the point of view of the user. One definition of quality is anything that enhances the product from the viewpoint of the customer. Some aspects of quality are easily identified, such as how well something works, its dependability, and the length of time before failure. Cyber security is the practice of protecting computer systems, networks, and data from digital attacks, and as applicable here, so that quality products be can manufactured sustainably.
2. Knowledge of variation in product and cyber security, and the need to put quality and cyber security first are fundamental axioms in this disruptive period of the processing industry.

An equally important axiom is the need for cooperation. Quality and cyber security cannot be obtained without cooperation. This includes cooperation among workers, among managers, between workers and managers, between the company and its suppliers, and even between the company and its competitors.

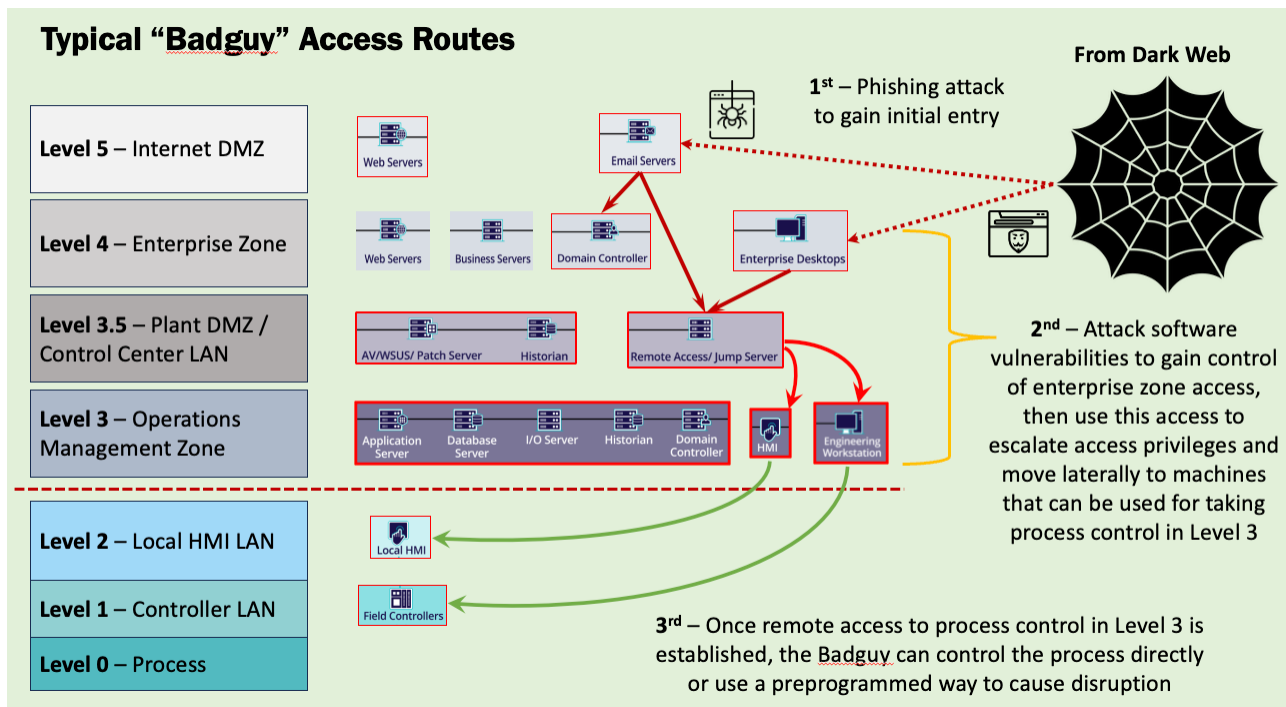
There are also major structural challenges in the marketplace geopolitically. There is a fair amount of cyber espionage of trade secrets that drive cyber criminals to collect corporate information for money, as in the dark web marketplace. Most industrial facilities that are separated from the internet, via an “air gap” for example, are still exposed digitally through maintenance vendors, shadow IT, or administrative access. These are significant challenges that require the attention of everyone involved to create secure processes.

2.5. Let's zoom into the industrial site as it is attached to the IT corporate network

A “Badguy” will use the detailed pattern shown in this framework, but for this conversation, a simplified pattern that is used in the Certified Ethical Hacker (CEH) training is:

- Reconnaissance – Risk reduction by using Opt In / Opt Out governance
- Scanning
- Gaining Access – Risk reduction by applying Least Privilege
- Maintaining Access
- Clearing Tracks

The illustration below is a simplified overview of how a hacker or Badguy would get access to the process control interface. Most OT networks are isolated both physically and digitally, and digital access mostly happens through the enterprise network. Physical access can happen also, however, let's focus on digital access for this example.



The Badguys would investigate what they could see about your fellow employees and network and evaluate the attack surface available with scans. Then, they will set up a way to deliver a mechanism to access your network. For example, they will launch a phishing attack to get a user to click on an email attachment that opens an application (malware) in the background, which will call back to the Badguys. Then, they assemble a package that is shaped to get access to the network. Larger groups of Badguys use specific tactics, techniques and procedures (TTPs) that can be used to identify them and where they are usually located on the dark web.

After their reconnaissance is completed, the Badguys will try to penetrate a desktop, laptop, or server on the target enterprise network through a phishing attack to gain a foothold on the network (1st Step). Once a phishing attack succeeds, remote access software is installed on the local machine, and it calls back to the Badguy on the dark web. Next the Badguy can use tools to “move laterally” by using the access privileges that the user and/or local machine has so the Badguy can gain access to machines on Level 3 – the operations management zone (2nd Step).

The Badguy can then change process controls when it has access and privileges on Level 3. This is why it is important to apply the Principle of Least Privilege. This will lower the risk by reducing the attack surface available to the Badguy (3rd Step).

2.6. Brief explanation of cybersecurity tools

2.6.1. Threat Intelligence

Also called cyberthreat intelligence (CTI) or threat intel—is detailed, actionable information about cybersecurity threats. Threat intelligence companies deploy people and sensors into the dark web to collect information that will be assembled in a database. Years of data collated on numerous attacks creates contextual data that can be correlated to form actionable intelligence.

Threat intelligence helps security teams take a more proactive approach to detecting, mitigating, and preventing cyberattacks, which is far more effective than a reactive approach. It is more than just raw threat information. It is threat information that has been correlated and analyzed to give cyber security

professionals an in-depth understanding of the potential threats their organizations face – including how to stop them.

Threat intelligence has three key characteristics that distinguish it from raw threat information:

- **Organization-specific:** Threat intelligence goes beyond general information about hypothetical threats and attacks. Instead, it focuses on the organization's unique situation: specific vulnerabilities in the organization's attack surface, the attacks these vulnerabilities enable, and the assets they expose.
- **Detailed and contextual:** Threat intelligence covers more than just the potential threats to an organization. It also covers the threat actors behind the attacks, the tactics, techniques, and procedures (TTPs) they use, and the indicators of compromise (IoCs) that might signal a successful cyberattack.
- **Actionable:** Threat intelligence gives cyber security teams insights that they can use to address vulnerabilities, prioritize threats, remediate risks, and improve overall security posture.

According to IBM's Cost of a Data Breach Report, the average data breach costs the victim organization USD 4.44 million. Detection and escalation costs account for the most significant portion of that price tag at USD 1.47 million.

Threat intelligence programs give security professionals information that can help detect attacks sooner and **completely** stop some attacks from happening. These faster, more effective responses can reduce detection costs and significantly limit the impact of successful breaches.

2.6.2. Network Security

- a. Next Generation Firewalls (NGFW) – Use a combination of Least Privilege and Threat Intelligence to control access to the organization's network.
- b. Virtual Private Networks (VPN) – Use encryption to protect data traffic so attackers cannot gain access to the data.

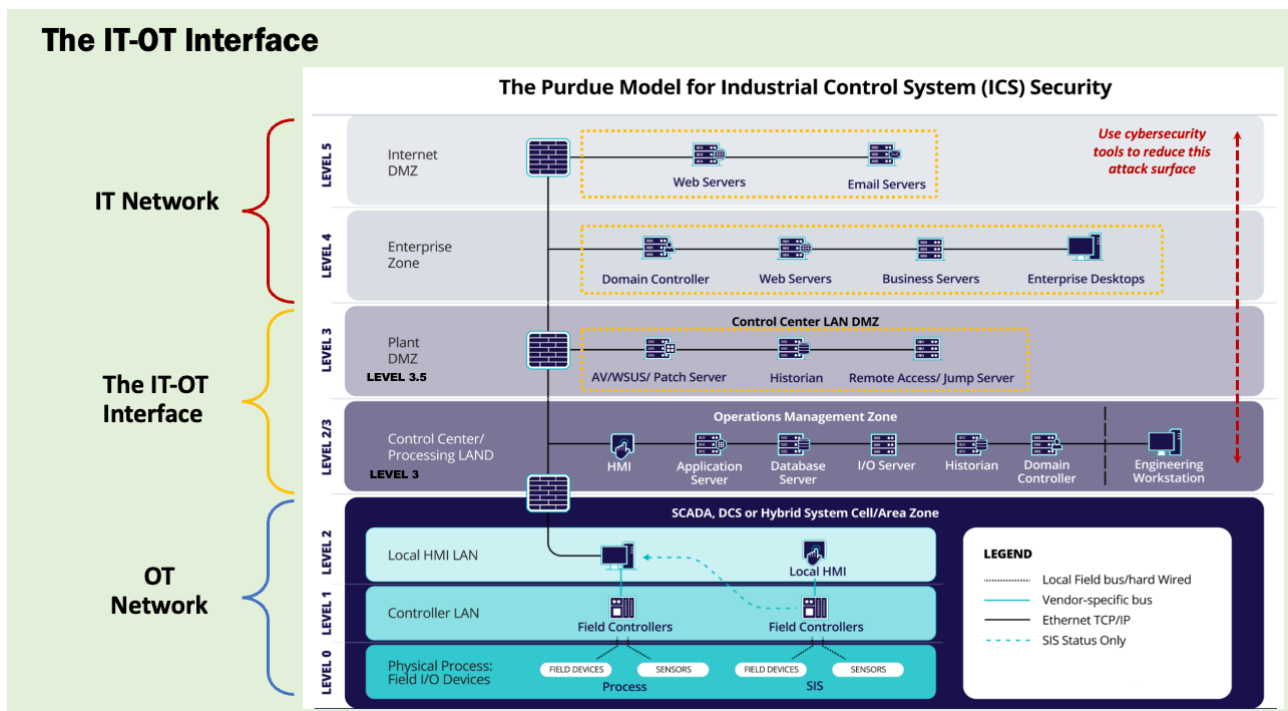
2.6.3. Endpoint Security

- a. Endpoint Detection and Response (EDR) – Uses an agent on the server, desktop, or laptop to protect it from being accessed and controlled by an attacker.
- b. Anti Data Exfiltration (ADX) – Uses Threat Intelligence to see where the data from the endpoint is going to determine whether it should be allowed.
- c. Endpoint Level Segmentation – Uses endpoint and user level permissions to control what that endpoint can access.
- d. AI Governance at the user level – Uses an agent to apply Least Privilege to Large Language Model (LLM) access.

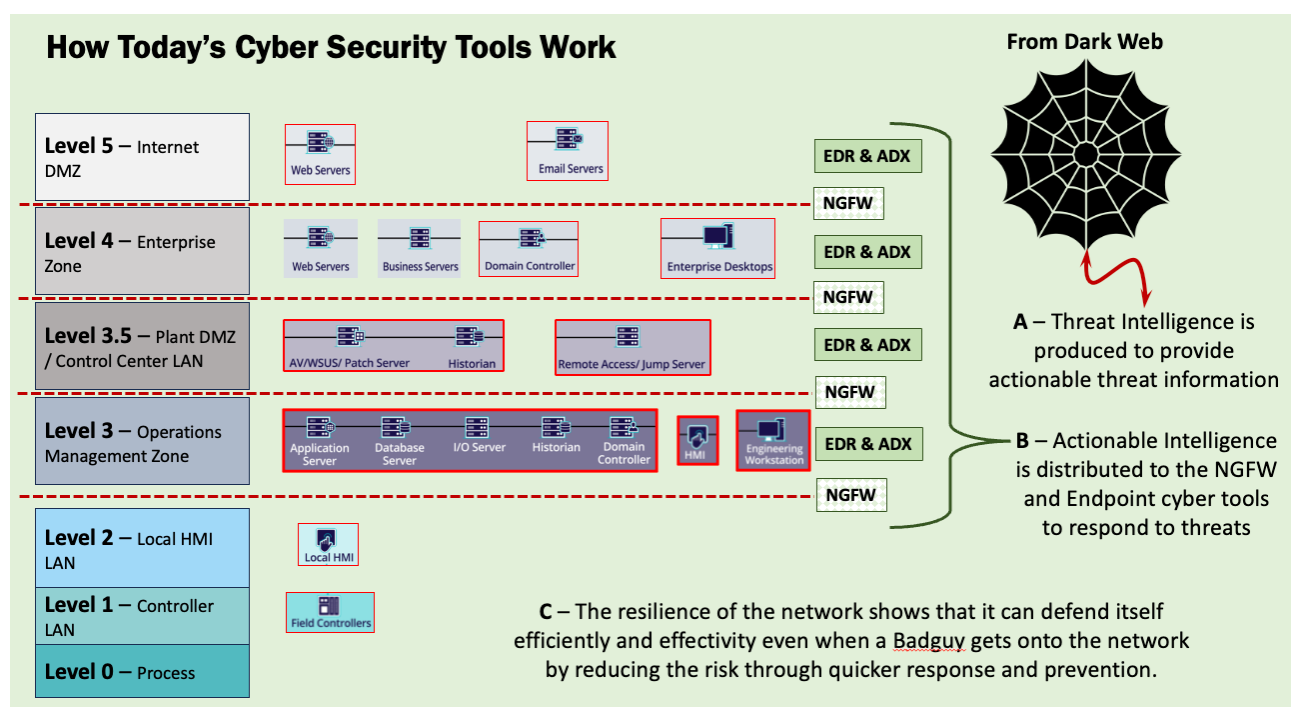
2.7. How do these specific security tools work on an OT network?

We will reduce the cyber risk to an organization by using cyber security tools in a layered approach to prevent attacks and reduce the damage they can cause when inside the network.

Cyber security tools are used to reduce the attack surface from Level 3 through Level 5 in the illustration below:



Below is a graphical overview of how cyber security tools are advanced enough to restrict attacks at the endpoint:



2.8.Integration of Digital Technologies

The triple point of our challenge today is the union between cybersecurity, artificial intelligence (AI), and the process industry in the Castellón region. Efficient and cutting-edge manufacturing

balanced with cybersecurity are at the heart of this challenge. Risk management is used to measure this task, but more importantly, how do we use our inherent assets to create safe and sustainable growth.

Cyber security needs to be part of every step along the way and not just a consideration after the digital process is completed. Cyber security is more effective as everyone begins to live it as we move along in the process of creating and operationalizing production. Operationalizing cyber security with existing and future process engineering requirements requires a structured approach for increased effectiveness. Holistically, the digitalization discussion is one of process design & development, operational optimization, and cybersecurity.

Below is an outline of tasks from a cybersecurity viewpoint:

- Use cases of data and data processing – Risk assessment for each use case to periodically review existing and new use cases with controls and/or acceptance of risk and insurance.
- Review of Least Privilege – Risk reduction through data governance – who can see data and where it can be sent or exposed.
- Training and User Governance – Activating the employee to be involved.
- How to consistently think of AI in automation and the use of AI agents

A few examples of industrial digital process tools and methods that are being utilized today include:

- RMIS Architecture – <https://rmis.jrc.ec.europa.eu/>
- eMation – <https://emation.de/>
- Data Fabric – <https://appian.com/>

These tools represent the standard interface in an industry database, and specific digital applications that would be used in a manufacturing environment. Questions that need to be asked about the data flows:

- Where is the data coming from and where is it going?
- Who has access to the data?
- How is the data secured as it moves across the network? Or internet?
- How is the data protected at rest?

We can review data process flow diagrams just like we can review a material flow or energy flow diagram of the process. There needs to be a cyber security person who views these data flows with the company's interest in mind. Using and storing data and parsing it out to vendors as required rather than giving vendors access to your network device directly would be the best place to start reducing the attack surface of your data and your network.

An excellent illustration of where we should use Least Privilege is the example of Lenovo being allowed to connect to the Lenovo servers so they can monitor the server performance. Lenovo is a Chinese company that works for a government that has been making a concerted effort to collect information about industries in all forms. Some of the uses that the data Lenovo collects may not be in the best interest of a company in Spain.

One suggestion, from an astute observer, is to use a data lake to store the data. A data lake is a centralized, highly scalable repository that stores vast amounts of structured, semi-structured, and unstructured data in its native "raw" format. It allows organizations to ingest data as-is without needing to define a structure first, storing information economically until it is needed for analysis. There can be a conversation with the vendor regarding what data they require and when it can be sent to them rather than opening a direct communication to the vendor.

2.9.A Brief Artificial Intelligence (AI) Overview

We must put AI in the proper context so we can operate with it as we inject more of it into our work and personal lives. This is especially true for the processing industry. The main idea with AI usage in the processing industry is to consider it a separate entity. As we go into some of the Key Points and Overview below, you will see that we are dealing with an actual entity where Least Privilege and Opt In / Opt Out are very important items to apply to it.

There are new cyber security tools that can see what AI an endpoint is using and block the ones that are not allowed in company use policy. As AI begins to push towards profitability, the low-cost AI era is now ending and usage along with cost require monitoring.

Key points about AI that are impacting the processing industry:

- Different types of AI solve different problems: generative AI creates, predictive AI forecasts, assistive AI supports work, and agentic AI performs tasks autonomously.
- Large language models (LLMs) and multimodal systems now dominate the modern workplace, particularly in knowledge work.
- Agentic AI and multimodal AI are accelerating rapidly, reshaping how organizations evaluate AI capabilities.
- Choosing the right type of AI starts with identifying a business need, mapping it to the correct AI category, selecting appropriate model technology, scaling responsibly, and applying Least Privilege.

AI Status as it is in May 2026

AI capabilities have been evolving steadily since the breakthrough development of artificial neural networks in 2012. Unlike basic machine learning models, these deep learning models allow AI applications to learn how to perform new tasks that need human intelligence, engage in new behaviors, and make decisions without human intervention. As a result, deep learning has enabled task automation, content generation, predictive maintenance, and other capabilities that can positively impact process design, development, and operations.

Due to deep learning and other advancements, the field of AI remains in a constant and fast-paced state of flux. Our collective understanding of realized AI and theoretical AI continues to shift, meaning AI categories and AI terminology may differ from one source to the next.

The general kinds of AI based on capabilities are as follows:

1. **Artificial Narrow AI** – Also known as Weak AI, is the only type of AI that exists today. Any other form of AI is theoretical. It can be trained to perform a single or narrow task, often far faster and better than a human mind can. It cannot perform outside of its defined task. Instead, it targets a single subset of cognitive abilities and advances in that

spectrum. Siri, Amazon's Alexa, and IBM Watson® are examples of Narrow AI. Even OpenAI's ChatGPT is considered a form of Narrow AI because it's limited to the single task of text-based chat.

2. Strong AI – Also known as Artificial General Intelligence (AGI), is today nothing more than a theoretical concept. AGI can use previous learnings and skills to accomplish new tasks in a different context without the need for human beings to train the underlying models. This ability allows AGI to learn and perform any intellectual task that a human being can.
3. Super AI – Commonly referred to as artificial superintelligence and, like AGI, is strictly theoretical. If ever realized, Super AI would think, reason, learn, make judgements, and possess cognitive abilities that surpass those of human beings.

2.10. Communication Enabling Future Growth within Collaborative Channels

The Castellón cluster of ceramic businesses provides the community with an opportunity to be more in control of the success of the industry in the region and with the local livelihood. This is a huge opportunity that can be recognized by envisioning it and following up on it in the disciplined way of building relationships with trusted colleagues.

We first should look at what we have in the local industry and business community:

- A global cluster of similar businesses that are in fact unique in a local way. The businesses are big enough to have a significant global market share, and the personnel are mostly local to the Castellón area.
- There are also unique skills that exist due to the age and size of the business. The methods of mentoring engineers into the business through learning what is currently operational to retrofitting operations with upgrades and new product production. These methods are a large part of what "technology" is, and this transferable knowledge is valuable and unique.
- We have an example of how collaboration can work in the Castellón area by looking at what Japanese manufacturers, most notably Toyota, did with the Deming Quality Management effort. This was taught to the Japanese by Dr. W. Edward Deming, who was the world's foremost statistician and quality control expert in the 1940s and 1950s.

The result of properly incentivized collaboration between current manufacturing operations management, design and process development, and cybersecurity will ensure future growth and stability.

Someone might ask – "How is that going to happen?"

Let's look at Toyota. The marketplace views Toyota's products as the global gold standard for reliability, durability, and high resale value. Consumers see the brand as a sensible, risk-free investment that balances affordability with trusted engineering, making it the most valuable automaker globally, (until just recently). That sounds to me like it says – the gold standard for quality.

How can the companies in Castellón achieve this standard? Currently, the key points of this challenge are focused on:

- Geopolitical competition
- Proper AI use and governance

- Streamlining current manufacturing techniques to use less energy
- Develop new products that push into new markets. For example, technical ceramics
- Provide market leadership and employee mentorship for company growth and stability

The answer to managing this growth program is that it is a constant balance. View the system of working together as the challenge and not point at the employee as the problem. Employees want to feel an integral part of a system that works.