International Journal of Safety and Security Engineering
Vol. 13, No. 2, April, 2023, pp. 195-204
Journal homepage: http://iieta.org/journals/ijsse

Cybersecurity Index to Evaluate the Implementation of the Bi-Level Architecture for Efficient Manufacturing (BLAEM)

Abdelkarim Remli*, Amal Khtira, Bouchra El Asri

IMS Team, ADMIR Laboratory, Rabat IT Center, ENSIAS, Mohammed V University, Rabat 10112, Morocco

Corresponding Author Email: abdelkarim_remli@um5.ac.ma

https://doi.org/10.18280/ijsse.130202

Received: 12 October 2022
Accepted: 15 April 2023

Keywords:
manufacturing systems, cybersecurity, industrial security, computer integrated manufacturing, systems architecture

ABSTRACT

Manufacturing companies aim for the optimization of their processes by means of Computer Integrated Manufacturing (CIM), in order to keep-up with the competition and the evolution of clients' needs. This transformation is based on connecting the shop floor systems to the high business layer ones. Based on the limitations of the existing architectures in the literature, we proposed the BLAEM architecture (Bi-Level Architecture for Efficient Manufacturing), an ISA95- based architecture that relies on six major aspects, among which we can cite Cybersecurity. In this paper, we focus on this specific aspect, and we try to elaborate a security index to evaluate the implementation of our architecture.

1. INTRODUCTION

Industrial companies have had to adapt to changing situations due to fierce competition driven by increasing customer demands. To efficiently control the development of products, processes, and production systems, companies have had to integrate technologies and data from other areas with the process of manufacturing [1]. This change is known by various names, including Smart Manufacturing [2] and Computer-Integrated Manufacturing [3, 4].

The key drivers of this trend are the automation of industrial processes and the facilitation of data exchange, which can be achieved by integrating every system within the manufacturing process into the same architecture. The aim is to create a fully connected plant where all the retrieved information is reusable to optimize the various business processes and thereby create a smart factory.

To attain this, the connection between different levels of the factory must be ensured, ranging from the shop floor where production machines are located to the most advanced level of the plant where the company's strategies are defined. However, the aggregation and contextualization of data from heterogeneous systems throughout the production life cycle pose a significant challenge. This affiliation is challenged by the normal trouble of agglomerating and contextualizing data from heterogeneous frameworks over the generation life cycle [5].

In this way, we came up with a reference design competent of interfacing the generation and data frameworks of the company. This architecture is based on six major aspects: Data integration, Systems integration, Security, Monitoring & Data analysis, Mobility and finally Cloud computing.

In this paper, we will handle the security aspect for its major role of ensuring a stable and successful implementation of BLAEM. To help companies evaluate their implementation using quantitative indicator, we will elaborate a security index based on cybersecurity directives collected from some of the relevant standards.

2. BACKGROUND

This digitization of processes for the industrial companied is fulfilled through interfacing the genuine world to the virtual one, utilizing cyber physical frameworks, sensors and IT Frameworks. Be that because it may, the utilization of a few frameworks and advances inside the same environment is especially challenging, ordinarily due to the dissimilarities between them and particularities of each one of them. Consequently, analysts have been able to propose structures able of enveloping each framework within the CIM setting.

2.1 CIM architectures

A systematic literature review (SLR) has been conducted on this subject. Its fundamental destinations were to examine the diverse approaches proposed to handle computer integrated manufacturing architectures, in order to identify the nature of contributions in this area and to determine the diverse aspects addressed by them [6].

Twelve papers examined as part of our research have put forth various architectures. One such example is the architecture proposed by Sprock and McGinnis [7], aimed at bridging the gap between system data and analysis models for smart manufacturing. Similarly, Tang et al. [8] proposed the Cloud-Assisted Self-Organized Architecture (CASOA), which creates a vertically enabled system for data consolidation, another architecture, the Cloud Based Framework developed by Caggiano et al. [9], offers real-time diagnosis for smart monitoring of machining. Tao et al. [10] also presented their Data-Driven Smart manufacturing Framework, which utilizes data collected during the manufacturing process to enhance its efficiency.

2.2 CIM-related aspects

After the analysis of the chosen papers, we identified six

aspects that we considered basic to handle in a contribution:

•**Systems Integration:** The ability of a solution to facilitate the integration and cooperation between multiple IT systems within a single architecture [10].

•**Data Integration:** It consists of contextualizing data from diverse systems throughout the production life cycle [11].

•**Security**: The solution's capacity to establish secure connections for system integration and safeguard the access to production data from external sources [12].

•**Monitoring & Data Analysis:** This aspect involves leveraging gathered manufacturing data to enhance productivity, which can be categorized into two types of data. The first type is Real-time Data that is typically utilized for monitoring, while the second type is Historic Data employed for data analysis [13].

•**Mobility:** Consists of using mobile oriented applications and terminals for data monitoring [14].

•**Cloud Computing:** This aspect pertains to the solution's ability to utilize cloud computing for some or all of its functionalities [15].

2.3 Bi-level architecture for efficient manufacturing (BLAEM)

To address the shortcomings of the approaches analyzed in the SLR, we suggest implementing the Bi-Level Architecture for efficient Manufacturing (BLEAM), which is based on the hierarchical structure of the ANSI/ISA-95 standard. The proposed system prioritizes the arrangement of systems, with the ERP positioned at the top of the pyramid and the machines situated at the bottom. Additionally, the architecture is designed based on the concept that the Manufacturing Execution System (MES) is the central component of the Computer Integrated Manufacturing (CIM) and links the entire production system to enterprise resources [16].

Our proposal advocates for the division of the company's production system into two distinct levels. as appeared in Figure 1:

- **Plant level:** In this level, we can find company's local production system nearby portion. This one is specific to each factory. It moreover obliges all the physical generation frameworks and the shopfloor components. To quote but a number of illustrations; there are the fabricating machines and their controllers, the printers, the workstations and at final but not slightest, the MES.
- **Corporate level:** It is the pivotal segment of the production systems destined to be shared amongst the firm's plants. It exclusively contains the ERP system.

In order for us to establish evidence of the architecture's consistency, we will be projecting it upon the six aspects we recovered from the literature.

2.3.1 Systems integration

BLAEM enables the company's systems to communicate by means of common communication protocols:

•**OPC Server / PLCs- Measuring Apparatuses**: An OPC Server can communicate using various protocols, depending on the specific machine it is connected to. It can leverage the OPC UA protocol if the machine is already utilizing it, or alternatively, it can utilize the specific PLC Driver of the machine.

•**MES / OPC Server:** The MES system is treated as an OPC Client, and communication is established using the OPC UA protocol or, in some cases, HTTPS. To meet these requirements, software editors are integrating OPC-UA interpreters into their systems.

•**Workstations / MES:** The data generated by the MES can be approached using HTTP by means of workstations or any other sort of Graphical User Interface.

•**Print Server / MES:** The printing server and the MES are linked through the TCP/IP protocol, and with the Printers through The IPP protocol.

•**ERP / MES:** This connection is generally accomplished through HTTPS. However, for certain solutions, Request for Comments (RFC) protocol or even some niche canals of communication are mandatory.

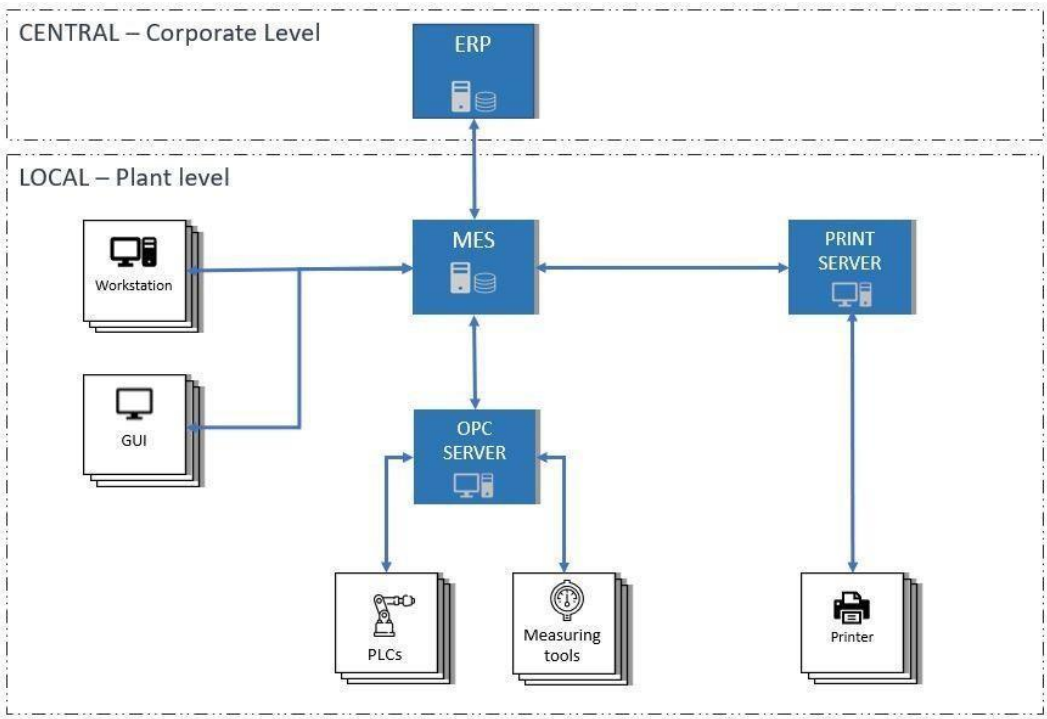

Figure 1. BLAEM architecture

2.3.2 Data integration

This aspect can be reduced to 2 main points:

- The Shopfloor data is formatted and normalized in the OPC Server, in order for it to be integrated within the MES.
- The communication between MES and ERP establishes data transfer between the two systems.

2.3.3 Monitoring & data analysis / mobility

The MES applications invest us the capacity to uncover generation information in arrange to expend it by Client- sort applications by implies of web-services and Web- attachments. Besides, modern MES Arrangements give modules of advancement which empowers the client to create cross-platform Web Applications. Not as they are these applications for Generation observing, they moreover play out in traceability and Dashboarding applications like ANDONS and Cockpits. These applications are able of devouring the distributed information. This permits for real-time palpability on the production's life-cycle, gives decision-makers direction, and speaks to Mobile-Friendly applications for a straightforward get to data.

2.3.4 Cloud computing

As previously mentioned, BLAEM consists of two levels: the corporate level that encompasses the ERP shared among all the company's plants and deployed on a Cloud server, and the Plant level that includes the remaining systems, which are deployed on-premise.

3. SECURITY ASPECT FOR CIM

The digital transformation has made a real impact on the industrial companies, by improving their efficiency by 15 to 20 percent [17], not to mention the benefits that result from analyzing all the collected data from the CIM context. This transformation can never be successful without relying on stable environments and secured systems, which makes the Security aspect one of the most relevant challenges to be dealt with.

The Cisco 2018 Annual Cybersecurity Reports [18] showed that 31% of organizations have experienced cyber-attacks on Operational Technology (OT). A survey conducted by the Small Business Administration (SBA) showed that 88% of small business owners felt their business was vulnerable to a cyber-attack. while 64% of leaders of organizations declared that cybersecurity and technology related risks are currently managed in an "inadequate" or "to be improved" way.

Despite these statistics, only 16% of organizations are ready to face cybersecurity challenges, as per other surveys. This is due to the lack of accurate reference standards and the lack of managerial and technical skills to understand and implement them [19].

In this section we demonstrate the importance of the Security aspect, and why it has to be taken seriously. For that, we will go over the most important vulnerabilities that can be related to our architecture assets, the common threats in the industrial domain, and the business impacts they can leave on the company. And to countermeasure that, we will present some security standards that can provide us with the best guidelines to be applied for maximum security.

3.1 Vulnerabilities

Vulnerabilities are defined as weaknesses within the IT system that might be exploited by intruders to compromise the cyber-physical system [20]. In a more common point of view, NIST glossary of key information security terms [21] allude to vulnerability as weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. According to the Kaspersky report in 2015, the number of vulnerabilities rose from 2 to 189 between the years 1997 and 2015. [22] Based on 4 reports established by the Kaspersky Lab [23], the U.S Department of Homeland security [24], Norton LifeLock formerlyknown as Symantec [25, 26], and Positive technologies [27], we came up with a list of the most common vulnerabilities in the industrial environment:

- **Misconfigurations:** These vulnerabilities occurs when devices and systems that will be used in the company are configured inappropriately, by preserving default settings for example or not controlling what to be installed on the devices.
- **Flaws in network:** It can be caused by physical- Based assets such as Hardware Issues and physical security or Software-Based assets such as Outdated or Unmanaged Software.
- **Buffer overflow:** It is a programming error, where software overwrites adjacent memory locations while writing data to a buffer. Writing outside the bounds of a block of allocated memory can corrupt data, crash the program, or cause the execution of malicious code.
- **Hardcoded or weak credentials:** Such as passwords typically create a significant hole that allows hackers to easily bypass the authentication that has been configured by the administrator.
- **Cross-Site Scripting (XSS):** Enables attackers to inject client-side scripts into web pages, which can be used to steal user authentication data or spread malware through the systems.
- **The Cross-Site Request Forgery (CSRF):** Occurs when a server is designed to receive a request from a client without any mechanism for verifying that it was sent intentionally.
- **Cleartext transmission and storage of data:** These vulnerabilities allow an unauthorized actor to get sensitive data in a communication channel or from a storage point in Plain-Text format, this data can include even passwords stored in a Recoverable Format.
- **Zero-day:** One of the most common vulnerabilities in cybersecurity (also known as 0- day) which is technically a hole in a software that is unknown to the vendor or that is known but there is still no patch to correct it. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it.

We will utilize the Common Vulnerability Scoring System (CVSS) as a standardized method to assess the severity of the vulnerabilities mentioned earlier. This system provides a quantitative indicator to allocate severity scores for cybersecurity threats, enabling users to prioritize responses and allocate resources accordingly. The latest version, CVSS v3.1, which was released in 2019 [28], will be used. The scoring is based on a formula that considers various metrics to estimate the ease and impact of an exploit. The scores range from 0 to 10, with 10 being the most severe. Those are the metrics that are used:

- **Attack Vector (AV):** This metric measures the possible context for exploiting a vulnerability. If the attacker can exploit the vulnerability from a remote location, then the

metric value will be higher. The values that are provided by the calculator are ranked as follows: Network, Adjacent Network, Local, and Physical.

- **Attack Complexity (AC):** This metric evaluates the conditions that an attacker must meet beyond their control to exploit the vulnerability. In other words, it estimates the difficulty of carrying out an attack on the vulnerability. A high value of this metric indicates that it is difficult for an attacker to exploit the vulnerability, while a low value means that it is easy to exploit.
- **Privileges Required (PR):** This metric evaluates the level of authorization that an attacker must have to exploit the vulnerability. The higher the privileges required, the more difficult it is for an attacker to exploit the vulnerability. Conversely, a low value of this metric indicates that an attacker can exploit the vulnerability with minimal privileges or without any privileges at all.
- **User Interaction (UI):** This metric evaluates the level of user interaction needed for the vulnerability to be exploited.
- **Scope (S):** This metric evaluates the ability of a vulnerability to spread from one component to affect other components within the system.
- **Confidentiality Impact (C):** This metric assesses the impact of a vulnerability exploitation on the confidentiality of the system's information.
- **Integrity Impact (I):** This metric measures the impact of a successfully exploited vulnerability on the integrity of the system.
- **Availability Impact (A):** This metric measures the impact of a successfully exploited vulnerability on the availability of the affected component.

We applied the scoring system for the already listed vulnerabilities, and we recorded the results in Table 1.

3.2 Cyber-security threats

The NIST glossary characterizes threat as "any circumstance or occasion with the potential to antagonistically affect organizational operations (counting mission, capacities, picture, or notoriety), organizational resources, people, other organizations, or the Country through a data framework by means of unauthorized get to, annihilation, divulgence, adjustment of data, and/or dissent of service".

A systematic literature review that has been conducted on this topic by Lezzi et al. [20]. This research analyzed 40 scientific papers in order to identify the major security threats that has been treated in the literature. The top 8 threats can be listed as follows:

- **Denial of Service (DoS) attack:** A DOS attack is an attempt by an attacker to prevent users from accessing the information system resources, it can be done through flooding the network in order to reduce the user's bandwidth and prevent access to a service [29].
- **Phishing attack:** It is a method of tricking users into unknowingly providing personal and financial information or sending funds to attackers [30].
- **Malware and worms' infections:** Malware is brief for Malicious software. It could be a program code that's threatening and regularly utilized to degenerate or abuse a framework. Presenting malware into a computer arrange environment has distinctive impacts depending on the plan aim of the malware and the arrange format [31]. Worms are self-replicating computer Malwares, their ability to rapidly spread across the network makes them a real threat, since before the user knows what has happened, much damage is already done [32].
- **Virus infection:** Stands for "Vital Information Resource under Siege". A computer virus is a computer program/software that is loaded into the system without your authorization and run-in opposite to your permissions [33].
- **Escalation of privilege:** It can be defined as an attack that incorporates picking up illegal get to of hoisted rights, or benefits, past what is anticipated or entitled for a client. This assault can incorporate a performing artist or an insider. Benefit heightening customarily incorporates the misuse of a benefit heightening defenselessness, such as a framework bug, misconfiguration, or insufficient get to control [34].

Table 1. Vulnerabilities with their associated CVSS score

Vulnerabilities	AV	AC	PR	UI	S	C	I	A	Score
Misconfigurations	Adjacent Network	Low	Low	None	Changed	High	High	High	**8.4**
Flaws in network	Network	High	High	None	Changed	High	High	High	**8**
Buffer overflow	Local	low	Low	None	Unchanged	None	Low	High	**7.8**
Hardcoded or weak Credentials	Adjacent Network	Low	Low	None	Unchanged	High	Low	Low	**6.8**
Cross-Site Scripting	Network	Low	Low	Required	Changed	High	High	High	**9**
The Cross-Site Request Forgery	Network	Low	None	Required	Unchanged	High	High	High	**8.8**
Cleartext Transmission	Adjacent Network	Low	High	None	Unchanged	High	High	None	**6.5**
Zero Day	Adjacent Network	High	Low	None	Unchanged	High	High	High	**8.1**

Table 2. Threats with their associated CVSS score

Threats	A V	A C	P R	U I	S	C	I	A	score
Denial of Service (DoS) attack	Network	High	None	None	Changed	Low	High	High	**8.9**
Phishing attack	Adjacent Network	High	Low	Required	Changed	High	High	Low	**8.3**
Malware and worms' infections	Local	Low	None	Required	Changed	High	High	None	**8.2**
Virus Infection	Adjacent Network	Low	None	Required	Changed	High	High	None	**8.5**
Escalation of privilege	Adjacent Network	High	Low	None	Changed	High	High	High	**8**
Eavesdropping	Network	High	High	Required	Unchanged	High	High	Low	**7.9**
Advanced Persistent Threat (APT)	Network	High	Low	None	Changed	High	High	High	**8.5**
Data tampering or Spoofing	Adjacent Network	High	High	Required	Unchanged	High	High	Low	**7.5**

- **Eavesdropping:** It is when a hacker intercepts, deletes, or modifies data that is transmitted between two devices. Eavesdropping, also known as sniffing or snooping, relies on network in which traffic is not secured or encrypted.
- **Advanced Persistent Threat (APT):** It comprises of a complex sort of assaults that takes information by remaining within the contaminated framework for a long time. When Able assaults take place in a complex foundation such as the cloud, their discovery is truly troublesome [35].
- **Data tampering or Spoofing:** Which means technically electronic identity theft, where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Indenting to evaluate the threats above, we will be using the CVSS calculator to assign severity scores to the threats, we used the same metrics as in section 3.1, and we recorded the results in Table 2.

3.3 Business impacts

In cybersecurity, Impact refers to the potential for loss, harm or pulverization of resources or information in a company. It can be caused by a vulnerability being exploited or an attack that occurs. There are many types of impacts, such as:

- Disrupt to the complete basic framework or focused on components: For example, misfortune of discernibleness, controllability or eventually the misfortune of control within the physical framework. Theft of industrial trade secrets and intellectual property.
- Denial of service of networks and computers.
- Life-threatening situations for the workers.

Those impacts are related directly to one of those three aspects: Confidentiality, Integrity, and Availability. These are the three center components of the CIA set of three, a data security demonstrate implied to direct an organization's security methods and arrangements.

3.4 Security standards

Cyber security standards are methods laid out in published documents that endeavor to ensure the cyber environment of a client or an organization. This environment includes users, systems, networks, tools, applications, and data that can be connected directly or indirectly to networks [36]. The main purpose is to diminish the risks that can be endured from cyberattacks. These documents comprise of tools, policies, concepts, guidelines, training, best practices and technologies.

Some of the most relevant standards are described below. These are security standards that can be adopted in the industrial context and can be applicable to various assets:

- **ISA/IEC 62443:** The International Society of Automation (ISA) developed a series of standards in 2007, which were approved by the International Electrotechnical Commission (IEC) in 2021 [37]. This series, known as ISA/IEC 62443, aims to address cybersecurity concerns for operational technology in automation and control systems. The primary goal of this standard is to enhance the safety, availability, and confidentiality of Industrial Automation and Control Systems (IACS) components and provide criteria for the procurement and implementation of secure IACS [38]. ISA/IEC 62443 is divided into various sections and covers technical as well as process-related aspects of cybersecurity for automation and control systems.
- **API 1164:** It is a standard proposed by the American Petroleum institute (API) in 2007 and revised in 2021. It offers guidelines and best practices to operators from Oil and Gas industries to improve the cybersecurity of the Supervisory Control and Data Acquisition (SCADA) systems. It also offers a detailed analysis of vulnerabilities for a SCADA system, that can be exploited by external users and cause threats to the whole company.
- **NIST 800-82:** The National Institute of Standards and Technology (NIST) developed a set of documents in 2015 known as the NIST Special Publication 800-82. These documents describe the computer security policies, procedures, and guidelines for the United States federal government [39]. One of the documents provides guidance on how to secure Industrial Control Systems (ICS), which includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control systems such as Programmable Logic Controllers (PLC).
- **UL 2900:** It is a series of standards published by Underwriters Laboratories (UL) in 2016, a safety consulting and certification company and also one of several companies approved to perform safety testing by the U.S. federal agency, Occupational Safety and Health Administration (OSHA). UL 2900 presents foundational security requirements software cyber- security requirements for network-connectable products and industrial control systems [40].
- **ISO/IEC 27000-series:** Also known as the ISO27K. It is a series of cybersecurity standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This series gives best practices suggestions on information security management and the administration of data risks within the context of an overall Information security management system (ISMS). The ISO/IEC 27000- Series is purposely wide in scope, covering more than privacy, confidentiality and IT technical cybersecurity issues. It is pertinent to organizations of all shapes and sizes [41].

4. SECURITY ASPECT FOR BLAEM

After listing the most common vulnerabilities and the potential threats in a CIM Context, we will elaborate a list of directives that could help counter them or minimize their risks. In this section we will project the five security Standards on BLAEM, so that we can come up with the technical best practices that can be applied to our architecture when being implemented. To do so, we will start by listing all the possible assets we will be dealing with in our architecture Guidelines:

- **Physical Server:** It is a computer device that provides resources, data, services, or programs to other computers. Servers are major assets in our architecture, it is where we deploy most of our systems such as the MES or the OPC server.
- **Cloud Server:** It is a type of virtual server that operates within a cloud computing infrastructure. It is created, hosted, and delivered via a cloud computing platform and can be accessed remotely over the internet. In our case, the Cloud Server will serve as the hosting platform for our

ERP system, as part of our Bi-level approach to improve cybersecurity measures.

- **Systems:** They are a set of integrated software that read, write, process, and store data for a predefined purpose, such as the Manufacturing execution system (MES) and Enterprise Resource Planning (ERP).
- **Network:** Or computer network. It alludes to interconnected computing devices that can exchange information and share assets with each other. These networked devices use a system of rules, called communication protocols, to transmit data over physical or wireless technologies.
- **Workstations:** They include all the computer and mobile devices used to provide the operators with Human Machine Interfaces (HMI) that enable them to interact with the systems.
- **Industrial controllers:** They include all industrial computers dedicated to control and supervise shop-floor components such as assembly lines, machines and robotic devices. We can distinguish two types of controllers in our architecture, the Programmable logic controller (PLC) and the Supervisory Control and Data Acquisition (SCADA) [42].
- **Data:** It is the information processed and stored by a workstation or transported through the network.

4.1 Cyber security guidelines for BLAEM

After analyzing the standards listed above, those are the guidelines that we assume could help protect our architecture

1. **Control access points:** The access to servers, devices such as Workstations and controllers, should be subject to protected o protected access using identity management and access control methods such us user authentication and multiple-terminal authorization. This can help prevent flaws in network and can protect from DOS and phishing attacks.
2. **Network segregation:** The networks should be separated with VLANS and the communication through it should be secured using Virtual Private Network (VPN), Secure Sockets Layer and IP Security. For workstations, a separated network has to be created for each plant section with a specific address to each workstation, in order to minimize misconfigurations vulnerabilities and Network flaws that can lead to potential infection threats.
3. **Account management:** A strong account management policy should be defined by the company, and this should be applied to Workstations, servers and controllers. Hence, no default or hardcoded credentials should be tolerated besides the usage of strong passwords that have to be changed regularly. This guideline can help companies prevent spoofing and APT attacks.
4. **Configuration solidifying:** The installations and configurations for all the hardware assets such as workstations, controllers and servers should be done by experts. This helps avoid flaws in network, misconfigurations issues and Zero-day vulnerabilities, that can potentially lead to DOS, APT and Phishing threats besides the escalation of privileges. Some of the best practices are:
   - Installing only necessary software.
   - Avoiding default configuration.
   - Installing Antivirus and anti- Malware.
   - Closing ports that are unnecessary for the functioning of the asset.
   - Implementing an ACL (Access- Control List) to control authorizations and roles.
5. **Warnings monitoring:** This includes the configuration of alerts for relevant events related to all the assets and the activation of traceability functions such as system logs and windows events. This guideline can help avoid Phishing attacks and system infections.
6. **Backup and restoration:** A backup policy should be established for physical assets such as servers, and also for digital ones such as data. This can be achieved by putting in place a backup server for each physical one, and by defining which data should be backed-up and storing it in a safe store point in a secure way. By achieving this directive, the company can reduce the risks coming from malware and viruses and can quickly recover in case of a DOS attack
7. **Up-to-date management:** A strong patch and updates policy should be applied to all the physical assets in order to fix software-based vulnerabilities such as Zero-days, Cross-Site Scripting and Cross- Site Request Forgery. This shall be applied to Operating systems (OS) as well. By applying this guideline, the company can help prevent DOS and APT threats and all types of infections.
8. **Controllers' safety:** The controllers are to be secured and configured properly for their major role in the manufacturing process. The digital access to the PLC and SCADA should be protected by passwords and two-factor authentication. Physical access should be restricted as well, and the links ought to be protected through shielded wires.
9. **Encryption:** This technique is based on converting the original representation of data, known as plain text, into an alternative form known as cipher text, which can be decoded only by authorized parties who have a key. Encryption has to be used to secure the data flow between the hardware assets and systems and has to be implemented for stored data as well.
10. **Technical audit:** A wide-range audit has to be conducted regularly every six months by security experts. All the assets are to be included. This audit should involve:
    - Vulnerability scan and assessment on both physical and digital assets.
    - Fuzzing to detect software errors and bugs.
    - Static source code analysis to look for software weaknesses.
    - Penetration testing to exploit the vulnerabilities.

    A Regular and well conducted audit can help detect configuration, data issues, and also common vulnerabilities such as Zero-days, Cross- Site Scripting and Cross-Site Request Forgery. Moreover, it gives the company the upper hand against critical threats such as Denial of Service attacks, infections, Advanced Persistent threats, Data tampering and Eavesdropping.
11. **Isolation and zoning:** This concern the physical and cloud servers that should be protected from external threats such as Denial of Service attacks and viruses. This practice can be done through the usage of firewalls and demilitarized zones (DMZ) and can also be applied to systems by installing Web Proxy Servers to secure them.
12. **Separation of environments:** The environments should be isolated depending on their main purpose. Hence, development and sandbox environments should not be connected to quality and production systems by any

means, in order to prevent misconfiguration vulnerabilities to spread from testing environments to crucial ones. This practice concerns the systems and the servers as well, and it helps prevent Malware, Worms and Viruses infection, Escalation of privileges and Phishing attacks.

13. **Data decentralization:** The data should be kept distributed on many storage points instead of being centralized into one vulnerable central storage point. By applying this guideline, companies can minimize the impacts caused by data tampering and Eavesdropping threats.
14. **Traffic control and analysis:** An Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) have to be in place in order to monitor and control the network and the systems for malicious activities such as Advanced Persistent Threat and infections that can be caused by Misconfigurations and Network Flaws.

In Table 3 we listed all the guidelines, and we specified for each guideline the list of threats it can cover and the vulnerabilities it can fix, this specification has been done based on the cyber-security standards and technical experimentations [43].

Based on the scores associated to each threat from Table 2, we calculated a threat Score (St) for each guideline (The sum of the scores for all the threats covered by the guideline). For example, the guidelines Encryption helps to avoid Data tampering, Eavesdropping, Advanced Persistent Threat and Phishing attacks. And from Table 2, we have a score associated to each of those threats which is:

- Data tampering: 7.5
- Eavesdropping: 7.9
- Advanced Persistent threat:8.5
- Phishing attacks: 8.3

$$St = 7.5 + 7.9 + 8.5 + 8.3 = 32.2$$

The same logic goes for vulnerabilities to calculates the Sv.

5. CYBER SECURITY INDEX FOR BLAEM

5.1 Elaborating the index

To appraise the safety of BLAEM, we emphasized on the security aspect. Thus, based on a list of standards, we shaped up a set of guidelines that we will follow in our design and implementation.

To evaluate the implementation of BLAEM from a safety point of view, we propose an index that will enable the company to assess its implementation using a quantitative indicator. The index will allow us to evaluates the implementation of BLAEM using quantitative indicator, it will be calculated based on the implemented directives listed above, the more the guidelines are being respected and applied, the more the index will be high which means that the implementation is well secured. This index will be based on the 14 directives listed above and will be defined in three steps.

1) A score will be associated to each guideline, based on the threats it can protect from and the vulnerabilities it helps fix and it shall be calculated using the following formula:

$$Sg = 0.1 * \sum_{i=1}^{n} St_i + 0.1 * \sum_{j=1}^{m} Sv_j$$

$$\{ 1 \leq i \leq n \; and \; 1 \leq j \leq m \; and \; i, j \epsilon \aleph \}$$

where,

- Sg: The score associated to the specific guideline.
- St: The score associated to the threats.
- Sv: The score associated to the vulnerabilities.
- n: The number of threats covered by the guideline.
- m: The number of vulnerabilities that can be fixed by the guideline.

2) The calculation is done using data from Table 1 for the vulnerabilities scores and Table 2 for the threats scores. The result can be found in table.

The architecture security index is calculated based on the scores associated to the guidelines that has been applied.

$$I_S = \sum_{i=0}^{P} Sg_i$$

$$\{1 \leq i \leq p \leq 14 \; and \; i \epsilon \aleph \}$$

where, p is the number of applied guidelines. Its value is 0 if no security guidelines are applied in the architecture and 14 if all the guidelines are applied.

The index value range is 0 to 60, with 60 being the sum of the scores for all the 14 guidelines.

3) A gauge shall be defined with a scale from 0 to 60. To evaluate the security index, we will define 3zones in the gauge based on 2 thresholds:
   - From 0 to 36: We can evaluate the implementation as inadequate and unsecured.
   - From 36 to 51: The implementation has been done properly and the security Index is acceptable.
   - From 51 to 60: The implementation has been done as recommended and the security level is high.

As shown in Figure 2, we dedicated 60% of the gauge to unsecured Zone, in order to push companies to apply the maximum number of guidelines all scores combined. This choice is also motivated by the fact that reaching an acceptable level of security is not a light task.

The same thing goes for the second zone that covers 25% of the gauge, which would push companies into implementing more guidelines in order to achieve a high security level.

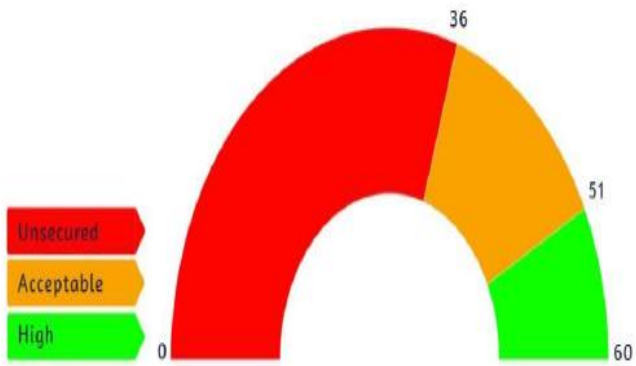

Figure 2. Security index gauge

5.2 Case study

To give a concrete example of the usage of the Index, we are going to simulate a case study from the automotive

industry. This one consists of a firm that possesses two factories, the first one located in Nantes, and the second one in Houara.

For the first factory, we can count four production work centers, with a PLC for each, three printers and five workstations. For the second factory, we define five work centers, besides the PLC that all the machines got, the work centers are equipped with sensors for efficient data collect, those machines are controlled by an MES installed on ten work station in the local level is insured by using separated systems and networks for the two plants, besides controlling the traffic in the network. The Servers and the work centers are highly secured using identity management, a strong account management policy and an up-to-date policy. A technical audit is planned regularly to ensure that everything is in order.

The data is Secured using encryption algorithms, and a decentralization policy, Backup servers are in place to ensure the availability of the data in the assets.

In this implementation, we applied the following security guidelines: Control access points, Network segregation, Account management, Backup and restoration, Up-to-date management, Encryption, Technical Audit, Data decentralization, Traffic control and analysis,

From Table 3, we can retrieve the Guideline Score (Sg) associated to each guideline.

- Control access points: 2.5
- Network segregation: 3.3
- Account management: 2.9
- Backup and restoration: 3.2
- Up-to-date management: 6.8
- Encryption: 3.9
- Technical Audit: 9.7
- Data decentralization: 3.1
- Traffic control and analysis: 4.2

The security index for this implementation shall be counted as follow: Is = 2.5 + 3.3 + 2.9 + 3.2 + 6.8 + 3.9 + 9.7 + 3.1 + 4.2 = 39.6, the index is located in the range between 36 to 51. Se we can conclude that the implementation has been done properly and the security Index is acceptable.

Table 3. Guidelines score calculation

Guideline	Threats	St	Vulnerabilities	Sv	Sg
Technical Audit	· Denial of Service · Malware and worms · Advanced Persistent Threat · Viruses infection · Data tampering · Eavesdropping	49	· Misconfigurations · Weak Credentials · Cross-Site Scripting · The Cross-Site Request Forgery · Cleartext Transmission of data · Zero-day	47,6	9,7
Up-to-date management	· Malware and Worms · Viruses infection · Denial of Service · Advanced Persistent Threat	34,1	· Flaws in network · Zero-day · Cross-Site Scripting · The Cross-Site Request Forgery	33,9	6,8
Configuration solidifying	· Denial of Service · Advanced Persistent Threat · Escalation of privilege · Phishing	24,8	· Zero-day · Misconfigurations · Flaws in network · Buffer overflow	32,3	5,7
Traffic control and analysis	Advanced Persistent Threat · Malware and Worms · Viruses infection	25,2	· Misconfigurations · Flaws in network	16,4	4,2
Warnings Monitoring	· Phishing Malware and Worms · Viruses infection	25	· Buffer overflow · Flaws in network	15,6	4,1
Encryption	· Data tampering · Eavesdropping · Advanced Persistent Threat · Phishing attacks	32,2	· Cleartext Transmission of data	6,5	3,9
Isolation and zoning	· Denial of Service · Viruses infection	17,4	· Misconfigurations · Flaws in network	16,4	3,4
Separation of environments	· Malware and Worms · Viruses infection · Escalation of privilege · Phishing attacks	24,8	· Misconfigurations	8,4	3,3
Network segregation	· Malware and worms · Viruses infection	16,7	· Misconfigurations · Flaws in network	16,4	3,3
Controllers safety	· Data tampering · Denial of Service	16,4	· Flaws in network · Buffer overflow	15,8	3,2
Backup and restoration	· Malware and Worms · Viruses infection · Denial of Service	25,6	· Cleartext Transmission of data	6,5	3,2
Data decentralization	· Data tampering · Eavesdropping	15,4	· Misconfigurations · Harcoded or weak Credentials	15,2	3,1
Accounts managements	· Data tampering · Advanced Persistent Threat	16	· Weak Credentials · Cleartext Transmission of data	13,3	2,9
Control access points	· Denial of Service · Phishing	17,2	· Flaws in network	8	2,5

6. CONCLUSION AND FUTURE WORK

Today, many industrial companies tend to digitize their processes in order to satisfy the customers' needs and to keep up with the competition. However, the utilization of different systems and technologies within the same environment is a challenging task.

In a previous work, we have proposed a reference architecture for computer integrated manufacturing entitled The Bi-Level Architecture for Efficient Manufacturing (BLAEM), which is able to encompass every system in the CIM context. This architecture is based on the ANSI/ISA-95 standard and takes into account six major perspectives: Data integration, Systems integration, Security, Monitoring & Data analysis, Mobility and finally Cloud computing.

In this paper we focused on the security aspect by presenting the most important vulnerabilities and threats related to our architecture assets and their business impacts on the company. Then, we proposed a set of security guidelines based on the best standards used in industry. Finally, to evaluate the implementation of BLEAM, we proposed a quantitative index calculated based on different security guidelines. We tried to gather many commonly known security standards such as ISA/IEC 62443 and NIST 800-82, etc. and apply their guidelines to our architecture. These guidelines will enable us to appraise the safety of the architecture once implemented. We provided 14 security directives to be applied by the company, and associated a weight to each of them based on the vulnerabilities that can be fixed by the guideline and threats covered by the guideline. The security index is calculated based on the scores of the guidelines put in place. And the security evaluation is done through predefined thresholds.

This index will help companies to assess quantitatively the security level in their architecture, and can be extended in future works, if we take into consideration more security standards, which will result in enlarging the list of guidelines.

In a future work, we will apply our architecture on a real case study, and we will provide quantitative results by calculating the architecture index.

REFERENCES

[1] Meziane, F., Vadera, S., Kobbacy, K., Proudlove, N. (2000). Intelligent systems in manufacturing: Current developments and future prospects. Integrated Manufacturing Systems, 11(4): 218-238. https://doi.org/10.1108/09576060010326221

[2] Li, Q., Pu, Y., Xu, Z., Wei, H., Tang, Q., Chan, I., Jiang, H., Li, J., Zhou, J. (2019). Architecture of integration of industrialization and informatization. In: Debruyne, C., Panetto, H., Guédria, W., Bollen, P., Ciuciu, I., Meersman, R. (eds) On the Move to Meaningful Internet Systems: OTM 2018 Workshops. OTM 2018. Lecture Notes in Computer Science (), vol 11231. Springer, Cham. https://doi.org/10.1007/978-3-030-11683-5_1

[3] Hedberg Jr, T., Feeney, A.B., Helu, M., Camelio, J.A. (2017). Toward a lifecycle information framework and technology in manufacturing. Journal of Computing and Information Science in Engineering, 17(2): 021010. https://doi.org/10.1115/1.4034132

[4] Li, Q., Jiang, H., Tang, Q., Chen, Y., Li, J., Zhou, J. (2017). Smart manufacturing standardization: Reference model and standards framework. Springer, Cham. https://doi.org/10.1007/978-3-319-55961-2_2

[5] Tolio, T., Sacco, M., Terkaj, W., Urgo, M. (2013). Virtual factory: An integrated framework for manufacturing systems design and analysis. Procedia CIRP, 7: 25-30. https://doi.org/10.1016/j.procir.2013.05.005

[6] Remli, A., Khtira, A., El Asri, B. (2020). Computer integrated manufacturing architecture: A literature review. KMIS, 249-256. https://doi.org/10.5220/0010148002490256.

[7] Sprock, T., McGinnis, L.F. (2015). A conceptual model for operational control in smart manufacturing systems. IFAC-PapersOnLine, 48(3): 1865-1869. https://doi.org/10.1016/j.ifacol.2015.06.358

[8] Tang, H., Li, D., Wang, S., Dong, Z. (2017). CASOA: An architecture for agent-based manufacturing system in the context of industry 4.0. IEEE Access, 6: 12746-12754. ttps://doi.org/10.1109/ACCESS.2017.2758160

[9] Caggiano, A., Segreto, T., Teti, R. (2016). Cloud manufacturing framework for smart monitoring of machining. Procedia CIRP, 55: 248-253. https://doi.org/10.1016/j.procir.2016.08.049

[10] Tao, F., Qi, Q., Liu, A., Kusiak, A. (2018). Data-driven smart manufacturing. Journal of Manufacturing Systems, 48: 157-169. https://doi.org/10.1016/j.jmsy.2018.01.006

[11] Thames, L., Schaefer, D. (2016). Software-defined cloud manufacturing for industry 4.0. Procedia CIRP, 52: 12-17. https://doi.org/10.1016/j.procir.2016.07.041

[12] Leitão, P., Barbosa, J., Foehr, M., Calà, A., Perlo, P., Iuzzolino, G., Petrali, P., J.Vallhagen, Colombo, A.W. (2017). Instantiating the PERFoRM system architecture for industrial case studies. In: Borangiu, T., Trentesaux, D., Thomas, A., Leitão, P., Oliveira, J. (eds) Service Orientation in Holonic and Multi-Agent Manufacturing. SOHOMA 2016. Studies in Computational Intelligence, vol 694. Springer, Cham. https://doi.org/10.1007/978-3-319-51100-9_32

[13] Lia, Q., Tanga, Q., Chana, I., Weia, H., Pua, Y., Jiangb, H., Lib, J., Zhou, J. (2018). Smart manufacturing standardization: Architectures, reference models and standards framework. Computers in Industry, 101: 91-106. https://doi.org/10.1016/j.compind.2018.06.005

[14] Bousdekis, A., Papageorgiou, N., Magoutas, B., Apostolou, D., Mentzas, G. (2015). A real-time architecture for proactive decision making in manufacturing enterprises. Springer, Cham. https://doi.org/10.1007/978-3-319-26138-6_17

[15] Menezes, S., Creado, S., Zhong, R.Y. (2018). Smart manufacturing execution systems for small and medium-sized enterprises. Procedia CIRP, 72: 1009-1014. https://doi.org/10.1016/j.procir.2018.03.272

[16] Weihrauch, D., Schindler, P.A., Sihn, W. (2018). A conceptual model for developing a smart process control system. Procedia CIRP, 67: 386-391. https://doi.org/10.1016/j.procir.2017.12.230

[17] Remli, A., Khtira, A., El Asri, B. (2021). Reference architecture for efficient computer integrated manufacturing. In ICEIS, pp. 328-334. https://doi.org/10.5220/0010497903280334

[18] Bauer, H., Scherf, G., von der Tann, V. (2017). Six ways CEOs can promote cybersecurity in the IoT age. https://www.mckinsey.com/featured-insights/internet-of-things/our- the-iot-age, accessed on 2022-01-15.

[19] Cisco. (2016). Cisco 2018 Annual Cybersecurity Report. Retrieved May 22, 2023, from https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.

[20] Lezzi, M., Lazoi, M., Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry, 103: 97-110. https://doi.org/10.1016/j.compind.2018.09.004

[21] Jansen, C., Jeschke, S. (2018). Mitigating risks of digitalization through managed industrial security services. Ai & Society, 33: 163-173. https://doi.org/10.1007/s00146-018-0812-1

[22] Paulsen, C., Byers, R.D. (2019). Glossary of key information security terms. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology. https://www.nist.gov/publications/glossary-key-information-security-terms-2.

[23] Asghar, M.R., Hu, Q., Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. Computer Networks, 165: 106946. https://doi.org/10.1016/j.comnet.2019.106946

[24] Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S.I., Timorin, A.A. (2016). Industrial control systems vulnerabilities statistics. Kaspersky Lab, Report.

[25] Common cybersecurity vulnerabilities in industrial control systems. (2011). Cisa.gov. https://www.cisa.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf.

[26] Smarter security for manufacturing in the industry 4.0 era industry 4.0 cyber resilience for the manufacturing of the future. (n.d.). https://docs.broadcom.com/doc/industry-4.0-en.

[27] Positive technologies. (2021). Information security risks at industrial companies. Retrieved on May 22, 2023 https://www.ptsecurity.com/ww-en/analytics/ics-risks-2021/.

[28] Scarfone, K., Romanosky, S., Mell, P. (2006). Common vulnerability scoring system. IEEE Security and Privacy Magazine, 4(6): 85-89.

[29] Lau, F., Rubin, S.H., Smith, M.H., Trajkovic, L. (2000). Distributed denial of service attacks. In SMC 2000 conference proceedings. In 2000 IEEE International Conference on Systems, Man and Cybernetics.'Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions'(cat. no. 0, Nashville, TN, USA, 2275-2280. https://doi.org/10.1109/ICSMC.2000.886455

[30] Chaudhry, J.A., Chaudhry, S.A., Rittenhouse, R.G. (2016). Phishing attacks and defenses. International Journal of Security and Its Applications, 10(1): 247-256. http://dx.doi.org/10.14257/ijsia.2016.10.1.23

[31] Shah, D., Vaibhav Shah, H.S.P.P.K. (2017). Survey on computer worms. https://doi.org/10.17762/ijritcc.v5i8.1190

[32] Namanya, A.P., Cullen, A., Awan, I.U., Disso, J.P. (2018). The world of malware: An overview. 2018 In IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), Barcelona, Spain, 2018, pp. 420-427, https://doi.org/10.1109/FiCloud.2018.00067

[33] Maity, S., Dey, D. (2021). Computer virus attacks. In La Pens´ee, 51: 585-59. https://doi.org/10.6084/m9.figshare.19258763.v1

[34] Haber, M.J. (2022). Privilege escalation attack and defense. - https://www.beyondtrust.com/blog/entry/privilegeescalation-attack-defense-explained, accessed on 2022-01-10.

[35] Chen, P., Desmet, L., Huygens, C. (2014). A study on advanced persistent threats. In: De Decker, B., Zúquete, A. (eds) Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science, vol 8735. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-44885-4_5

[36] May, W. (2014). Guidelines for Smart Grid Cybersecurity. NIST Interagency Internal Report (NISTIR) 7628 Revision 1, National Institute of Standards and Technology.

[37] ISA/IEC 62443 series of standards. (n.d.). Isa.org. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

[38] Corallo, A., Lazoi, M., Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114: 103165. https://doi.org/10.1016/j.compind.2019.103165

[39] Stouffer, K., Falco, J., Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST Special Publication, 800(82): 16-16.

[40] UL (2020). (ANSI/CAN/UL Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, Standard 2900-1, Edition 1 2020. Retrieved on May 22, 2023, from https://www.ul.com/services/healthcare-cybersecurity-solutions.

[41] Schweizerische, S.N.V. (2013). Information technology-Security Techniques-Information Security Management Systems-Requirements. ISO/IEC International Standards Organization.

[42] Tubbs, S. (2018). Programmable logic controller (plc) tutorial. In Siemens Simatic S7-1200. Publicis MCD Werbeagentur GmbH; 3rded.

[43] Remli, A., Khtira, A., El Asri, B. (2022). Reference architecture for CIM the Bi-level architecture for efficient manufacturing BLAEM. Journal Europeen des Systemes Automatises, 55(5): 665-670. https://doi.org/10.18280/jesa.550512