Journal of Software Engineering and Applications, 2023, 16, 714-743
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

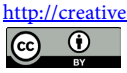
Enhancing Security for Legacy Factory Machines: A Continuous Key Renewal Algorithm for Securing Group of Machines

Nicolas Ferry[1], Paul-Eric Dossou[2,3], Gabriel Ihowa[2], Gaspard Laouenan[2]

[1]Icam Nantes, Carquefou, France
[2]Icam Grand Paris Sud, Carré Sénart, Lieusaint, France
[3]IFSTTAR/AME/SPLOTT, Université Gustave Eiffel, Marne-la-Vallée, France
Email: nicolas.ferry@icam.fr, paul-eric.dossou@icam.fr, gabriel.ihowa@2023.icam.fr, gaspard.louenan@icam.fr

How to cite this paper: Ferry, N., Dossou, P.-E., Ihowa, G. and Laouenan, G. (2023) Enhancing Security for Legacy Factory Machines: A Continuous Key Renewal Algorithm for Securing Group of Machines. *Journal of Software Engineering and Applications*, **16**, 714-743.
https://doi.org/10.4236/jsea.2023.1612037

Received: November 20, 2023
Accepted: December 26, 2023
Published: December 29, 2023



Abstract

Companies are generally focused on how to improve their global performance. Concepts, methods and tools are regularly used to transform them. Key performance indicators are used to measure how performance is increased. Industry 4.0 concepts and sustainability expectations actually contribute to this performance improvement. Indeed, cybersecurity as one of these concepts is required to increase the company performance. Even if it is well-known and applied in companies through the protection of their information systems, progress is expected in research on how to ensure the security of data and factory processes in the manufacturing, as the number of cyberattacks towards industries is growing these last few years. This paper aims to increase the company performance and sustainability to enforce factory machines protection by creating private security network groups. But currently, most of the Programmable Logic Controller PLC protocols have not been securely designed. Thus, the creation of secure groups of machines by combining strong authentication, strong or lightweight ciphering, and data stream integrity is proposed. The security is enforced by a continuous key's renewal algorithm. An experiment on an industry's architecture has been led to validate the concepts of the proposition. The study is compared to existing OPC-UA and MACsec standards in terms of drawbacks and advantages. This work could be implemented in hardware for further performance improvement.

Keywords

Sustainable Industries, Cybersecurity, Networks, Protocols,

Side-Channel Analysis

1. Introduction

With the global supply chain digitalization, cybersecurity has become a key point for global industries to maintain production and preserve their competitive edge. Indeed, adopting new technologies for remote machine access has therefore been one of the most effective ways to build resilience into industrial operations. But this remote access has also opened a door to sensitive assets and created an OT cybersecurity problem. This problem is significant; in fact, according to IDC Worldwide IT/OT Convergence 2022 forecasts [1], by 2025, 30% of G2000 manufacturers will integrate connected technologies into their products to increase reliability.

Since Stuxnet [2], it has been demonstrated that industries are potentially vulnerable. The number of cyberattacks targeting industries has been in constant growth in recent years [3]. Thus, cybersecurity in the factory process has become a major concern for many companies' priority [4]. Nevertheless, securing a production system can represent a considerable and costly upgrade. Indeed, the machines have long life cycles, and replacement is not always feasible. However, one major weakness remains: many PLC protocols are not secure at all. Since, PLCs are the key components bridging the gap between digital control systems and physical processes. Unauthorized access can have a major impact on organizations whose turnover depends on the availability of physical processes. The foremost challenge for industry is to maintain the continuous services availability.

Furthermore, as explained by the European Commission with the industry 5.0 paradigm [5], maintaining companies' production systems must be done in a sustainable manner. In particular, the choices that companies can make to secure cyber physical systems will have an impact on various sustainability issues. Thus, this paper therefore aims to provide a sustainable framework enabling companies to address cybersecurity issues and bypass the implementation disruptions associated with older equipment and assets. The challenge is to ensure continuous, sustainable availability of services with minimum of changes to the infrastructure. When it comes to sustainability, a key performance indicator of the environmental impact is energy consumption.

Nowadays, IT confidentiality heavily relies on the AES cipher suite [6], since their approbation as a standard by the NIST [7]. And this holds particularly true for numerous secure communications systems that all have chosen to use it: SSH, TLS, OpenVPN, IPSec, MACsec and all web-based HTTPS. The solutions discussed in this article highlight the new opportunities offered by the new Authenticated Encryption with Associated Data (AEAD) algorithms. They combine confidentiality, and integrity signing all-in-one. Some new lightweight encryption candidates appeared as Chacha [8], ACORN, Ascon [9] and others [10], because compromises often have to be made between robustness, performance

and energy consumption.

To test the framework and take advantage of those opportunities, the use case presented in this paper explores a way to establish a factory machine group at the network level to cover old factory machines avoiding the need to software upgrade them (as with layer 4 - 7 or TLS protocols needs), or to change hardware switches for MACsec (layer 2). In this article, a protocol enabling authentication, confidentiality and integrity for messages exchange to guarantee machines' autonomy and availability is proposed in addition to standard network segregation, isolation and a comprehensive security management policy.

The paper is organized as follows: Section 2 will present literature search and existing state of the art for aspects related to industrial sustainability and cybersecurity. Section 3 will describe the concepts and methodology applied. Section 4 will detail the global proposition and the experiments conducted. Section 5 will present a study along three axes: security/robustness, performance and energy consumption. The last sections of the paper are focused on the analysis of various solutions and a synthesis on the results.

2. Literature Review

2.1. Industry 4.0 for the Company Performance Improvement

During the past decade, industries went through the 4th revolution supported by the development of new information and communication technologies (ICT). The use of these technologies in industries comes in response to the urgent need of production flexibilization due to a shift towards a mass customization paradigm [11]. At least 9 pillars of these new technologies are considered, including Industrial Internet of Things (IIoT), cybersecurity, artificial intelligence, big data or system integration.

Methodologies have been developed to support industry 4.0 implementation in companies [12]. For instance, in [13] a framework including horizontal and vertical integrations, and the end-to-end optimization with the value chain improvement has been presented. These methodologies are used with success in large companies but need to be adapted to SMEs.

Brakes need to be lifted within the company in order to implement a successful digital transformation. Resistance to change and inertia [14] come with several challenges while trying to transform a company. This way, implementing new technologies needs to be methodologically structured. Organizational methodologies such as lean manufacturing [15], DMAIC (Define, Measure, Analyze, Innovate, Control) method, [16], DOE (Design Of Experiments) method [17] or GRAI (Graphe de Réseaux d'Activités Interreliées) method [18] help lifting brakes in the digital transformation process. Designing and choosing the right key performance indicators (KPIs) are important in the success of the transformation. For cybersecurity issues, several KPIs can be derived from the data collected by monitoring industrial equipment, for example in process control applications [19].

Digital transformation is a radical process to improve competitiveness of companies through the use of new technologies. It allows to enhance both operation-

al excellences, with increased efficiency and effectiveness in production processes, and value creation, especially through customer experience [20]. Manufacturing processes optimization involves the use of the triptych quality, cost and lead time (QCD) to increase the company performance. Indeed, reducing machine tool downtime corresponds as presented in [21] to an objective to reach through predictive maintenance by exploiting artificial intelligence techniques such as machine learning and deep learning. The minimization of the machine downtime increases the company performance efficiency in part production processes [22]. Predictive maintenance workflow [23] includes processes such as sensor embedded physical systems, data collection and processes, feature extraction, model development, Remaining Useful Life (RUL) prediction, and decision making that have to be optimized. Artificial intelligence tools are used to interpret the data collected and assist manufacturers in determining the optimal time to schedule downtime [21]. Methodologies and tools using industry 4.0 concepts on manufacturing processes and mainly maintenance are numerous as presented in [24], but there is a lack of them on manufacturing processes and machines' cybersecurity. The company's digital transformation also needs to exploit adapted information systems and to manage the high volume of data that will contribute to the company's performance improvement. For instance, this information system optimization can be done through deep learning techniques in a cloud manufacturing environment [25]. This manufacturing processes optimization through the use of predictive maintenance with the exploitation of industry 4.0 concepts such as artificial intelligence or internet of things, can be extrapolated to cybersecurity to increase manufacturing performance. As presented in [26], IoTs and connected objects are used in manufacturing processes to increase their performance with deep learning algorithms exploitation. Cyber-physical systems allow the integration of computational and physical processes, in which digital twins are used as a copy of the physical system to perform real-time optimization [27] [28]. IoTs and Cyber-physical systems are used to connect the physical layer to the virtual layer by linking the physical system to the informational tools [29]. But their utilization introduces an opportunity of hacking in the manufacturing system.

In the literature, Industry 4.0 evaluation methods have been developed such as presented in [30]. Indeed, the evaluation of new technologies is suggested. The methodology integrates measures on IoTs, cyber-physical systems and digital twins, advanced 3D simulation, additive manufacturing, autonomous and collaborative robots, vertical and horizontal integration, big data and analytics, cloud computing, and cybersecurity implementations in the manufacturing systems. But the description of the cybersecurity measure is focused on information systems such as ERP, or MES protection. It appears that developing methods and tools to protect machines and manufacturing processes will be innovative.

2.2. Sustainability as an Industrial Performance Improvement Criterion

As defined by the Brundtland report published by the United Nations in 1987

[31], sustainable development is "the development that meets the needs of the present without compromising the ability of the future generations to meet their own needs". Considering factors of production, sustainability is evaluated through the combination of various social, economic and environmental criteria. With the 4th industrial revolution, digital transformation offers solutions to address sustainability issues related to those criteria, such as flexibility of production and resilience to external threats: for example, the COVID-19 pandemic with the digitization of customer experience.

According to the European Commission, the changes introduced by Industry 4.0 concepts are deemed inadequate in addressing social and environmental concerns, such as dependence on fossil fuels, climate change (see IPCC), pollution, and more. Consequently, the European Commission defines the shift towards Industry 5.0 [32] as the sustainable transformation of industries which effectively address those issues with a human-centered approach. While the strategic view towards Industry 5.0 is essential, it is imperative that companies have more than just a high-level perspective. They require a robust operational framework and incentives, which should be underpinned by a solid legal structure and relevant KPIs. Industry 5.0 is defined as "a vision on industry that aims beyond efficiency and productivity towards respect to human value and contributing to vital society needs" [33]. This comprehensive approach is vital to guarantee a sustainable digital transformation. Corporate environmental sustainability contributes to link organizational performance to social, economic, technological and organization factors [34].

As presented in [35], the SMEs require a high level of agility and flexibility to meet the performance that they expect and for their digital transformation, sustainable aspects as social, environmental, economic and resource-related issues are concerned [36]. For a company digital transformation, the industry 4.0 technologies are able to be combined with industry 4.0 design principles such as agility, flexibility, modularity, virtualization, autonomy but also corporate social responsibility to increase the quality of bottleneck analysis based on detection, diagnosis, prediction, and prescription [37]. Indeed, the success of the new technologies integration in the company transformation requires a methodology including sustainable aspects with the possibility to be adapted to each company context and expectations. For instance, in [38], a direct relation between circular economy principles [39] and industry 4.0 disruptive technologies in the company supply chain digital transformation. As explained in [40] the company degree of maturity can be measured and be considered for defining the adapted tools for an efficient transformation. This paper will present a sustainable digital methodology that will be able to ensure this company's manufacturing continuous transformation. This manufacturing transformation involves the exploitation of the new technology tools such as cybersecurity of machines or people in the manufacturing processes to increase the company performance.

Indeed, cybersecurity and management of the information system impact the

production performance. On operational, technological and organizational levels, failures may cause wastes; implementing the wrong technology can impact energy consumption or leave breaches for external threats or internal failures [41]. Choosing the right technology to address cybersecurity issues is a part of a multiple-criteria decision-making (MCDM) problem. Furthermore, choosing the right framework for continuous improvement of cybersecurity in companies is also a parameter to consider [42] [43].

Attempts to retrospectively quantify impacts of "green" cybersecurity [44] on Triple Bottom Line (TBL) sustainability have shown limited correlation between addressing cybersecurity issues and environmental impact [45] in some cases. Although other studies also highlight opportunities to address a larger scope of sustainability issues [46] [47], the global impact of cybersecurity initiatives is very dependent on the economic strategies of organizations anyway, which is why the European Commission highlights the need to implement a sustainable framework that considers all decisional levels in companies' management.

The development of a sustainable digital methodology based on industry 5.0 concepts and focusing on manufacturing processes is required. The next section makes a focus on the cybersecurity in companies as a criterion to consider in the company transformation.

2.3. Industrial Cybersecurity in Industry

The main protection objective of any industrial manufacture is to guarantee availability as the top priority for plant security. Nowadays, attacks seem to be increasingly sophisticated and organized, such as in industry domain or in the hospital in Corbeil-Essonne, France. Most of the time the hacker's motivations are linked to money: the threat of ransomware, or commercial competition: as malware injecting with complete supply chain shutdown. An abbreviated list of common attacks on PLCs is presented in **Table 1**. They could be considerably mitigated by enforcing communication confidentiality, integrity and strong authentication. It is important to be aware that protecting a system has a cost. The level of security deployed on a system is proportional to the level of threat encountered. The constant increase in the attack surface remains a major challenge.

There are numerous specialized protocols used for industrial automation and monitoring. Most of them are designed for reliability, efficiency, real-time operation to help monitoring and control data. Fieldbus protocols are highly heterogeneous, outdated, vulnerable. They lack in security because they have not been designed to bear state-of-the-art encryption algorithms or authentication mechanisms. This is still a nascent topic when it comes to reducing the power consumption [49].

The ubiquitous presence of the Ethernet and IP protocol down to the field level didn't make it better, as many protocols have been modified to run on it. This has led numerous protocols to be potentially vulnerable even at level 2.

Table 1. Common type of attacks on PLCs [48].

Devices	Possible Attack Vectors	Possible Attack Methods	Possible Consequences
Controller (PLC)	Engineering Workstation	Engineer/technician misuse	Manipulation of controlled processes
	Operator HMI	Network exploitation of industrial protocol	Controller fault condition
	Standalone Engineering tools	Know vulnerability	Manipulation inputs/outputs data to/from controller
	Rogue device in control zone	Network replay attack	Plant upset/ shutdown
	USB/Removable media	Network DoS via communication buffer overflow	Command and control
	Controller network	Direct code/malware injection via USB	
	Controller (device) network	Direct access to device via rogue network/remote control	

Further industrial protocols information can be found in this survey [50] which provides a review and discussion of the IoT paradigm, focusing on protocols, their associated vulnerabilities, attacks, and possible security issues.

The need of security has never been as important as today, more than a technological issue, it now has a social, economic, and even political dimension. Common attacks include man-in-the-middle attacks, denial-of-service attacks, replay attacks, side-channel analysis attacks and more… Several ways exist for protecting assets in the automation industry pyramid such as network segmentation and segregation, IPS, IDS, firewalls etc. [48].

Another way to secure networks is authentication. But designing an appropriate and efficient authentication key exchange protocol between devices is not trivial. Possible solutions include Public Key Infrastructure (PKI), protocols based on symmetrical cryptography, certificateless protocols and Physical Unbreakable Functions (PUF), that are the four most common cryptographic approaches for IIoT key management [51].

There are several things to manage such as storage, updating, revocation of long-term keys and so on. In the PKI architecture "each device has a public and a private key, and a trusted certificate authority (CA) issues certificates which guarantee that a given public key belongs to a certain device on the network." The PKI nevertheless has some drawbacks essentially because of lack of trust on

the issued certificate and the fact that operations are computationally expensive due to the RSA method.

A case study within a smart Lab industry 4.0 setup shows that certificateless protocols can possibly stand as an alternative to the PKI [52]. It is not sure as "the need to distribute public keys reintroduces some of the overhead of PKI-based protocols that identity-based cryptography avoids, and the problem of key revocation needs to be addressed as well. But it is not clear that this approach is currently preferable to PKI in practice".

Another approach to device authentication and key exchange for low power devices, with the physical unclonable function (PUF). PUF is a hardware circuit, given input, which produces an output that is deterministically dependent on the input, but otherwise unpredictable.

The main benefit of these protocols is that they can function in an environment with extremely limited computing power, strength and memory. As a drawback, these protocols either require the active participation of a trusted central server during key exchange or require a separate setup phase for each IIoT device and each server it needs to communicate with.

Then, the decision is to keep on the well accepted local-PKI server for maintaining certificate validity and exchange. On the cryptographic side, the Advanced Encryption Standard (AES) is particularly well-designed to ensure data high confidentiality. As it is by far the most used and studied symmetric cipher. The Rijndael cipher was built by Joan Daemen and Vincent Rijmen [6]. It has three key variants 128, 192 or 256-bits size and seems to have resisted cryptanalytic attack until nowadays. AES in Galois Counter Mode (AES-GCM) is a so-called authenticated encryption with associated data (AEAD) algorithm, which means that it encrypts and authenticates data in the same flow. It also takes advantage of modern general-purpose CPUs instructions or ASIC hardware acceleration.

New Lightweight Cryptography (LWC) challengers [8] [9] [10] emerged and refers to the set of cryptosystems that can be integrated into resource-constrained platforms in time, space, or energy. In March 2021, NIST announced ten finalists of its lightweight competition: ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, Sparkle, TinyJambu, and Xoodyak. Finally, the competition winner was Ascon [9]. However, at the beginning of the project presented in this paper, the NIST competition was still ongoing. Therefore, it was decided to base the research work on the TLS v1.3 specifications, then to select Chacha20-Poly1305 [8] and AES-GCM [6] as serious candidates for implementing the group key renewal proposal.

The literature has revealed that the ChaCha20-Poly1305 are pretty-well suited to optimize the performance of the MACsec protocol for Industrial networks [53] [54].

Finally, the objective of this paper is to develop a global cybersecurity supervision that can monitor and guarantee the means of communication. The

small-scale deployment of a network infrastructure for an industrial process is proposed. The continuous renewal of security keys for an industrial IoT group of machines has been studied. The next section presents the methodology and concepts that have been developed in this paper.

3. Concept and Methodology

3.1. Sustainable Digital Methodology for Manufacturing Processes Security

As presented in the literature review, many frameworks allow to implement industry 4.0 concepts in companies for their digital transformation. For instance, [13] presents the digital transformation through a framework with horizontal and vertical integration exploiting clearly the new technology tools. These frameworks meet success in large companies but not in SMEs, because of brakes related to economic, environmental, social or societal aspects. The solution has been presented by the European commission as Industry 5.0, introducing sustainability as the kernel of the digital transformation. The framework presented in [13], integrates these aspects in the company's sustainable digital transformation. The following framework in **Figure 1** focuses on how to integrate security aspects in the company manufacturing processes sustainable digital transformation. For the secure sustainable digital transformation of the company manufacturing, mainly the security of machines is treated in addition to classical information systems security. The framework is composed of three axes:

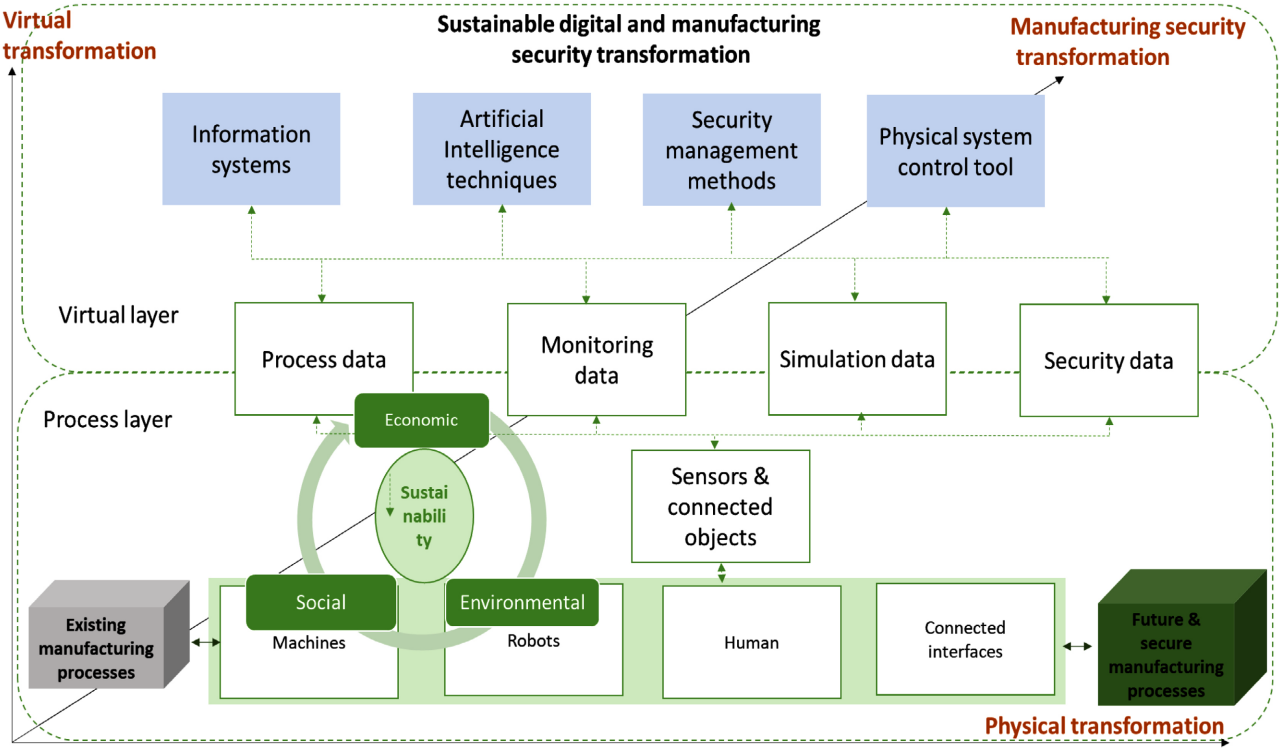


Figure 1. Manufacturing security in a global factory transformation.

- The physical transformation axis focusing on the physical transformation that will facilitate the machines transformation according to the security tools and techniques.
- The virtual transformation axis to integrate digital techniques and software tools essential to protect the manufacturing processes.
- And the manufacturing security transformation axis to include all algorithms that will secure the manufacturing processes against hacking and viruses.

The secure manufacturing sustainable digital transformation involves the exploitation of the sustainability (economic, environmental, social criteria) at each step of the transformation. Two layers compose the framework: The process layer and the virtual layer. In the process layer, the company's existing situation is measured, and the continuous sustainable transformation allows to improve the company performance by ensuring the security of machines, robots, human and connected interfaces. The result is the company secure sustainable digital transformation. Sensors and connected objects are used to collect data for the virtual system. Process, monitoring simulation and security data are collected. The virtual layer contains classical manufacturing virtual tools such as information systems, and physical system control tools but also artificial intelligence techniques and the security management methods that will be used for ensuring the security of each machine.

This paper focuses on the security management methods to use on machines in the manufacturing system. It aims to elaborate at the process layer level the adapted system to be used for the machine's security, and at the virtual layer level, models, methods, architecture and tools that would be exploited to ensure the security of the manufacturing system.

3.2. Security Deployment Methodology

For any organization, the lack of defense in depth with the equipment connected to their network opens a door for a potential hacker. Thus, deploying an industrial 4.0 factory starts by defining all the physical assets linked to the networks. Set up logical & physical separation into groups as security zones are paramount for the first step of security measure within an architecture. The idea of group segregation is to assign specific and different functionalities to each one. This practice is called network segregation. It helps to greatly minimize the attack surface. For instance, a logical separation could have been made with the IT and OT by a firewall. It reduces the possibility for a hacker to access the IT while infecting an OT device. This concept is defined in the Purdue Reference Model for CIM and standardized by the IEC in the IEC-62443 reference. Then, establishing gateways within each group can be required when, for example, a maintenance supervisor desires to obtain distant access within the processes.

3.3. Process Supervision

Industry involves multiple agents, and physical processes. It is necessary to de-

velop a global security strategy for the company. A 3-level layered security model has been implemented for this experience, in Figure 2. The supervision part is provided here by tools supplied by a partner specialized in deploying MES solutions for businesses. They notify us that most of their clients are either unaware, totally unprepared in terms of security or the necessity of a MES (or a SIEM) to monitor their systems. To date, the group doesn't integrate any specific cybersecurity solution. They were willing to collaborate to prepare their possible future investment in the security department & solution.

The supervision enables production management, process flow synoptic, but also security aspects. A global view of the supervision is presented in Figure 3. The security aspect is included on the bottom right screen, where "checkMK" software has been deployed for monitoring installed equipment. A process flow synoptic in the bottom middle displays the OT-Conveyor process in real-time. Globally speaking the scenario is to collect OT data from machines with an OPC-UA historian approach, and to send them into a cloud server for dashboarding purposes.

3.4. Network Global Architecture

Information Technology has evolved massively through Internet communication and will tend to merge with the IoT network. As a result, IT security will influence many aspects of plants at physical layer level. Firewalls need to isolate domains such as IT and technical domains. Finer network segregation with VLAN is recommended to isolate processes and applications. Next, communications between sub-domains should be scheduled using a flow matrix with ACL permissions on switches and firewalls.

Network Access Control (NAC) is also recommended to authenticate machines and assets for network access. This is mainly done with the 802.1X standard using a RADIUS or TACACS+ server, which grants access to network resources. Better than passwords, strong authentication is recommended using

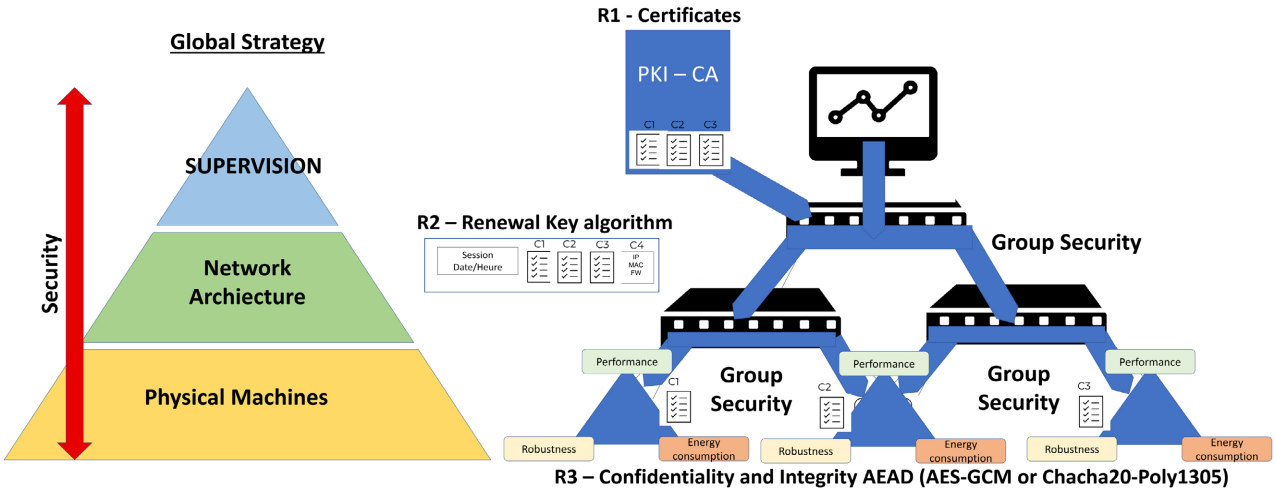


Figure 2. Global Strategy applying groups security reinforcement.

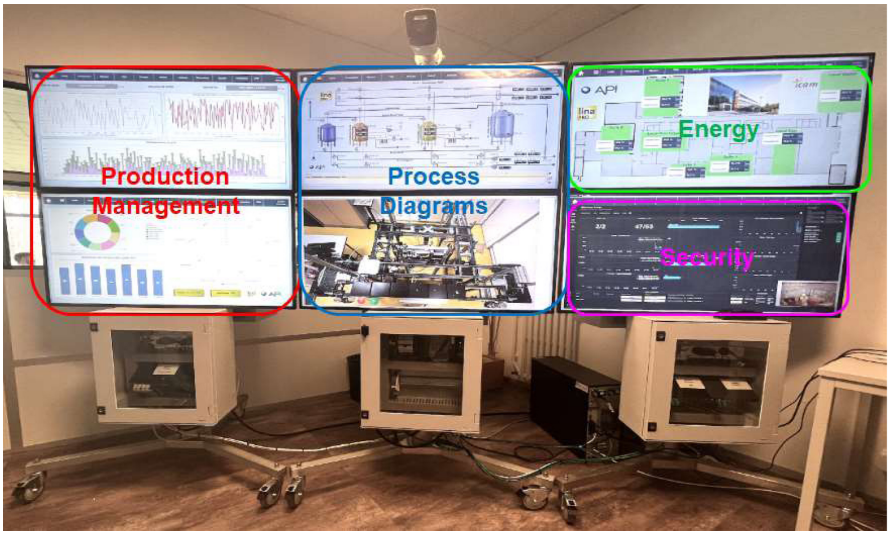


Figure 3. Modular process SKID-MES Lina of API group with process and security screens.

X.509 certificates with a local public key infrastructure (PKI) [5]. However, this deployment comes at the cost of certificate management and revocation (CRL), which have a substantial impact on overall management.

Figure 4 shows an overview of the architecture and a table of all the equipment deployed in the architecture.

Global virtualization and establishing zones seem to be the way of dealing with this complexity [48]. Looking at machinery legacy facing this transformation, a classification has been drawn up to categorize the measures to be taken according to the equipment's state of life. For the older ones, it is proposed to attach a complementary Front-End Module Device (FEMD) to the system.

3.5. Methods of Comparison

OPC-UA is mandatory for the communication and information layers of Industry 4.0, as defined by RAMI4.0, and defines a basis for interoperability between different suppliers, each with their own protocols. But many PLCs have been designed at time where security and IT/OT merging were not in the scope. These legacy protocols are not secure, as they do not fully guarantee completely the confidentiality, integrity and authenticity.

OPC-UA is a unified model standardized as IEC 62541. It supersedes the previous OPC (DCOM) standards and evolves to be open, sustainable, multiplatform, scalable, and designed with security in mind. Including several security features such as authentication, encryption, integrity, to secure the communication and the data that is transmitted over the network. In particular, the OPC-UA protocol relies on basic128/256 cipher and AES-128/256 cipher, SHA256 for integrity check, and RSA signing for authentication. The security of OPCUA is multilayers.

The native binary data mode (port 4840) has his own UA Secure conversion

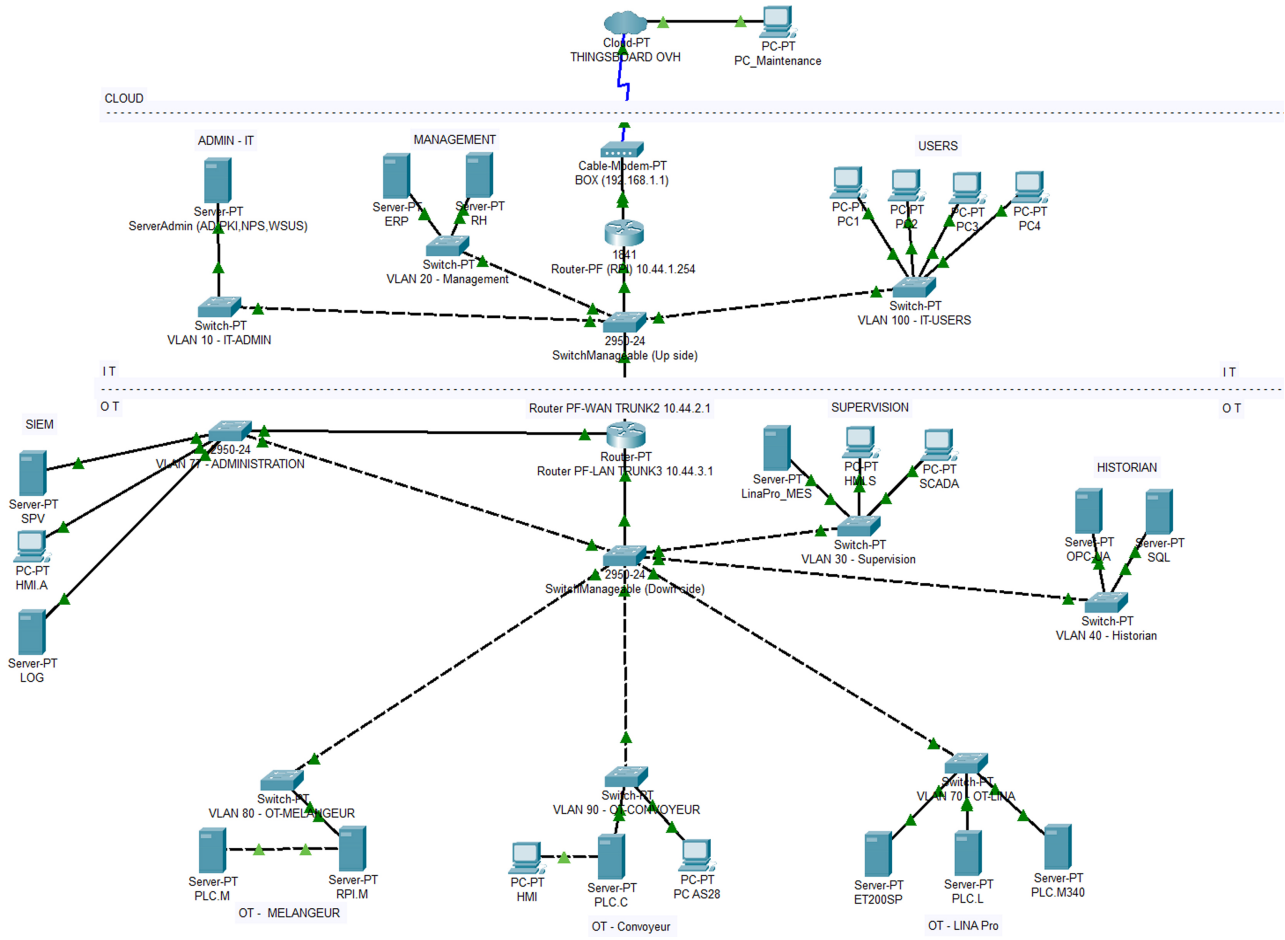


Figure 4. The global experimental architecture separating IT and OT domains, based on multiple VLANs areas.

module (using the mentioned ciphers). And for HTTP/HTTPS mode (port 80, port 443) relies on the Transport layer (OSI Layer 5) using a security channel over a TLS channel (v1.0 deprecated, v1.1 standard and old devices, v1.2 for perfect forward secrecy). Introducing TLS v1.3 which includes AES-GCM and Chacha20-Poly1305 will be probably the next step.

Additionally, a session identification is provided to authenticate the user/device. This enables user's-based rights to grant access to specific data objects or control/commands actions. The different modes are none for no identification, login/password identification, and certificate exchange. The last approach is the most secure even in machine-to-machine applications.

In the other side, MACsec is a security protocol that emerged in 2010 within a Linux kernel option and now has been standardized to provide encryption on OSI layer 2. It has been standardized as IEEE 801.1AE. The purpose is different from TLS secure channel because MACsec is more low level it can protect various low-level Ethernet protocols (*i.e.* ARP, DNS, DHCP…) and so secure old related PLCs unsecured protocol (Modbus, S7, HTTP web server…). Limitations are that some spanning tree protocols cannot be protected.

MACsec is most a switch secure channels protocol, that could be used in con-

junction of 801.1X for Network Access Control to authenticate and authorize to join a secure network.

Authentication is done with PSK (a Pre-Shared Key) or by EAP (and all their possible variant, EAP-TTLS, PEAP, EAP-TLS…) to a Radius (or TACACS+) server which send an EAP-Success (or reject) to grant for physical switch port access.

The PSK or the Master Key exchanges with EAP protocol provide the CAK, the Channel Association Key. There is a secure channel from one device to the other containing at least two Secure Associations in Rx (one active, one waiting for the key workaround) and two in Tx direction, each has its own SAK secret-key.

Periodically the EAP-MKA protocol exchange MKPDU packets that carrying the new keys for the secure channels, to reenable the SAKs secret-keys. The MKPDU protect the SAK key by using a KEK encryption key wrap (a manner to protect the key using AES again), and an Integrity Check Value which used the ICK key. Both KEK (confidentiality) and ICK (integrity) keys are deduced from the CAK key.

Note that each frame is decrypted on reception, to be in clear in the switch, then retransmitted on another port where it is encrypted again on the new secure association. AES is used on almost all stages to optimize the global performance, but with the problem of the multiplication of keys shared at all levels, which add lot of complexity.

MACSec has an interest in Cloud server architecture to provide protection within a Cloud data center avoiding spying of communications shared with other clients, but also, into a car ECUs for secure bus transactions, and in this document, for factories where it could be used as low-level protection for machines.

The strategy is to compare the challengers: OPC-UA which is a high layer security, MACsec which is most a low layer level security, with the proposal renewal key algorithm which could be seen as a compromise and a lighter's competitor. The comparison will be studied based on *confidentiality* criterion. More precisely on the robustness, the power consumption and the performance will be evaluated. The *integrity* references the hash function involved and if frame counter is used to prevent replays attacks. The *keys* criterion lists the different keys generated/needed by the algorithm. *Authentication* checks the constraint to support certificates to resist to man-in-the-middle attack for example. *Key derivation* exposes the key derivation technique employed. *Performance* means the minimal setup time to initialize a new device-to-device communication. *Cost* is an estimated criterion which estimates the cost to deploy the solution. The more + signify more expansive cost, and the values between parenthesis the cost if hardware materials like PLCs, switches need to be completely changed. *Security* describes the supported ciphers classification, light weighted or strong cipher. Finally, *Certified* mentions if the solution is an international certified standard.

4. Proposition

Global industries are recognizing the importance of prioritizing security. Since the continued disruption to the global supply chain, industrial organizations have put in place strategies to maintain production to preserve their competitive edge. Adopting new technologies for remote machine access has therefore been one of the most effective ways to build resilience into industrial operations. But this remote access has also opened a door to sensitive assets and created an OT cybersecurity problem. This problem is significant, and it is crucial to provide security of a group of machines. As many new technologies need to change material and/or reprogram software/PLC, once can imagine creating a security network group that encapsulates traffic into a secure channel.

In our approach the channel is shared for each group member, as opposed to MACsec [54] which creates for each Rx and Tx bidirectional channels and for all member's combinations, involving a lot of SAKs secret-keys generations and renewals. In the system, the add or the suppression of a member must be avoided as much as possible since it requires a complete authentication and keys' regeneration which is costly. In practice, a new machine is not added so often, it is even a way to detect a malicious group connection. Suppression or failure could be used as a warning of the group's state of health.

The security group algorithm is described in **Table 2** and is working as follows. Each machine must authenticate on the network, but every PLCs does not support 802.1X EAP Authentication, which could be an issue. The security feature could be provided by a Front-End Module Device (FEMD) which encapsulates security and certificates transparently. The proposition is that FEMD embedded and exchanged the machine's certificate to authenticate them. This could be after the 802.1X EAP challenge/response first phase for compatibility reasons. The certificates could embed optional fields including specific MAC address, static IP address, the firmware version, the program version, and ideally a small hash of the binary program uploaded. The local certificate authority checks every certificate for each member of the group and rejects the invalid ones by sending a response message and closing corresponding 802.1X ports.

After authentication, the server calculates a master key by performing a SHA256 hash on a session number id, a timestamp (date an hour), the certificates of each group member based on the port number port binding in the architectural network tree (*i.e.* 1.2.4 for the domain 1 - subdomain 2 - switch port 4), and any useful additional information. Then a random numbers generator is used to produce a Salt (S) and a Nonce (number only used once). The master key hash and the salt produces the final secret key used for confidentiality exchanges in **Figure 5**.

Nonce and the Secret-Key are together sent to each participant by using double RSA ciphering, the first to encrypt and sign with the CA private key and the second one with the public key of the participant (provided by its valid certificate). Only the FEMD concerned can decrypt its content and validate the proof

Table 2. Key renewal algorithm—derivate secret-key from the network global architecture.

Proposition for a group - Key Renewal Algorithm

#--- Establish network group connection
Affect each port binding a machine
Request Authentication 802.1X + Ask machine's Certificate
  Check their validity with the help of the Private Certificate Authority (CA)
  [optional] Check Certificate content for MAC, IP Address, correct binding
  [optional] Check Certificate program release and signing for malware detection
  Authentication - Valid or Reject on 802.1X Port based response (NAC)
 	
#--- PKI-CA or group Master - master key renewal algorithm (precompute for next renewal)
Initiate the group SHA256-Hash with a random number.
Hash a Session number and a Timestamp (date/hour), others parameters if needed…
On all valid/activated port:
  Calculate a SHA256-Hash of All Certificates signature - port ordered
Hash the total machines involved in the group, the result produces the master key
Store the Master-key secret in a private protected area

#--- Method1 - Chacha20-Poly1305 cipher is used
Create a Salt as a random number of 32 Bytes
Create a Nonce as a random number of 12 Bytes # Nonce 12 Bytes is TLS Version
Generate the secret-key SK with scrypt (Master_key, Salt, key_len = 32, N = 2**17, r = 8, p = 1)
 	
# Create a cipher object to encrypt data 	
Create a new cipher ChaCha20_Poly1305 object using the SK and Nonce
# ChaCha20-Counter is incremented according to packed number (init from Nonce) 	
For each packet:
  Encrypt and digest plaintext data with the cipher object
  Send Packet and increment packet Number
  if packet Number overlap: use new (SK, Nonce)
 	
#--- Method2 - AES-128-GCM cipher used
Create a Salt as a random number of 32 Bytes
Create a Nonce as a random number of 16 Bytes for GCM # IV_Nonce
Generate the secret-key SK with scrypt (Master_key, Salt, key_len = 16, N = 2**17, r = 8, p = 1)
 	
# Create a cipher object to encrypt data 	
Create a new AES cipher in MODE_GCM and the Nonce
# AES-GCM increment packed number from the starting IV Nonce 	
For each packet:
  Encrypt the plaintext data with the cipher object (GCM mode)
  Send Packet and increment packet Number
  if packet Number overlap: use new (SK, Nonce)

of the sender with the certificate authority's public key.

Last part concerns the communications into the group. The secret key and the nonce are directly reused into the targeting ciphers, in this case, AES-128-GCM, AES-256-GCM, or Chacha20-Poly1305. Because of their internal state structure each cipher will integrate secret key, Nonce number, and the packet number into

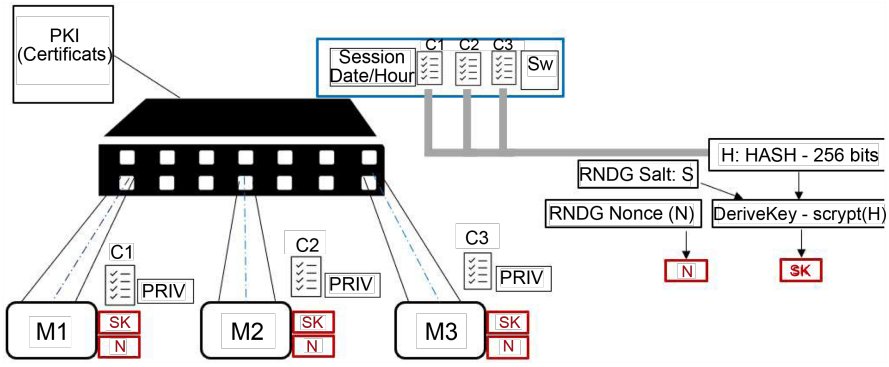


Figure 5. Global exchanges for group keys initialization producing le master key from session and signature certificate hashing to produce the Secret-Key and the Nonce.

the Chacha20's cipher Counter field and the IV (Initialization Vector) field for the GCM counter.

Only one Nonce is regenerated to cover the key renewal during packet number wraparound, this could be less than 2 seconds on a fast 10 GB/s network. Thus, an update packet must be sent to every group member to provide the next Nonce number, and this must be done before the effective wraparound of the packet number. MACsec uses a similar approach to double-buffer the keys wraparound on with at least two SAK keys. The new Nonce can be sent to the group using the complete double RSA exchange (secure but time costly) or for simplicity and speed by using the actual secret key as a traditional ciphered packet (potential security hole not investigated). Or better, by using a Key Wrap Algorithm like RFC3394 to send the protected new secret (MACsec approach).

Global SK and Nonce are finally renewed for handling long periods. A complete renewal based on the day could easily be imagined for plants where schedules are planned on one-day time slots.

The next section studies the behaviors and compares the final ciphers Cha-Cha20-Poly1305 and AES-128-GCM in terms of robustness, performance and power consumption.

5. Experimentation Strategy

For implementing our strategy, several assumptions have been made about what requirements would guide us to converge through our solution to the issue.

- R1 – X.509 Certificate exchange to provide authentication.
- R2 – Derivation of a confidential secret key (and an integrity/nonce) on the group.
- R3 – Confidentiality and integrity ensured by AEAD algorithms.

Some constraints are subsequently imposed:

- C1 – Must be able to interface with older machines, without changing the existing.
- C2 – Must simplify key management as much as possible.
- C3 – Must offer strong authentication.

- C4 – Must guarantee high performance (no slowdown if real-time flows).
- C5 – Must offer a reduced installation cost.

5.1. Performance Experiment

For the performance experiment in **Figure 6**, the goal is to measure the speed performance difference between the lightweight and the strong cipher. Both are software written in Python running on a Raspberry. Thus, the prerequisites are a 5 V power supply, the Raspberry Pi 3B+ (Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC@ 1.4 GHz). A set of classic HCI equipment where the ciphers algorithms can be controlled/analyzed.

Performance results - DeltaT method:

- Implementation Software AES/ChaCha20 (lib python CryptoDome)
- Nb iterations 10 K

The software was implemented using the CryptoDome library in Python. In this test, a 16-byte message of 1 block is encrypted for AES and Chacha to measure the differential performance. The algorithm executes the cipher 10k times, then takes the average speed (for one block) to obtain better measurement accuracy.

- AES Performance: 1.5967662 ms (1 run/10k of 1 plaintext bloc)
- Chacha Performance: 1.1700523 ms (1 run/10k of 1 plaintext bloc)

Our results showed that Chacha is slightly more efficient than AES, because of the simplest XLR instructions of Chacha and globally have less cipher complexity despite its internal state size that is greater. In practice, hardware ASIC or dedicated ICs are used to achieve better performance to handle fast networks without performance drawbacks.

5.2. Robustness Experiment

The robustness experiment goal is to verify the ciphers robustness against attacks that could break the whole group's security. In this experiment in **Figure 7**, a Differential Fault Analysis type of attack which is derived from Side-Channel Analysis is conducted by [55] [56]. This attack has been led by a Chipwhisperer card also used to break the post-quantic NIST winner algorithm (CRYSTALS-Kyber) [57].

Chipwhisperer is a complete open-source toolchain that offers learning about

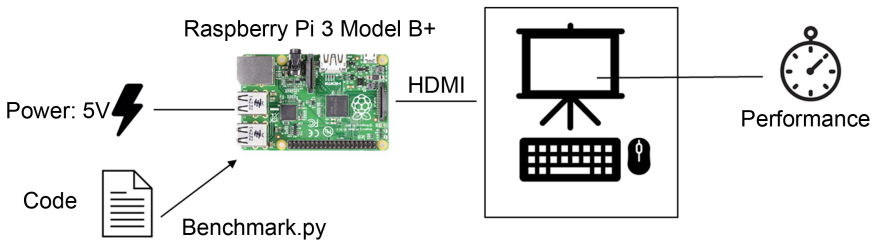


Figure 6. Performance experience on raspberry Pi 3B+ (Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC@1.4 GHz applying groups security reinforcement.

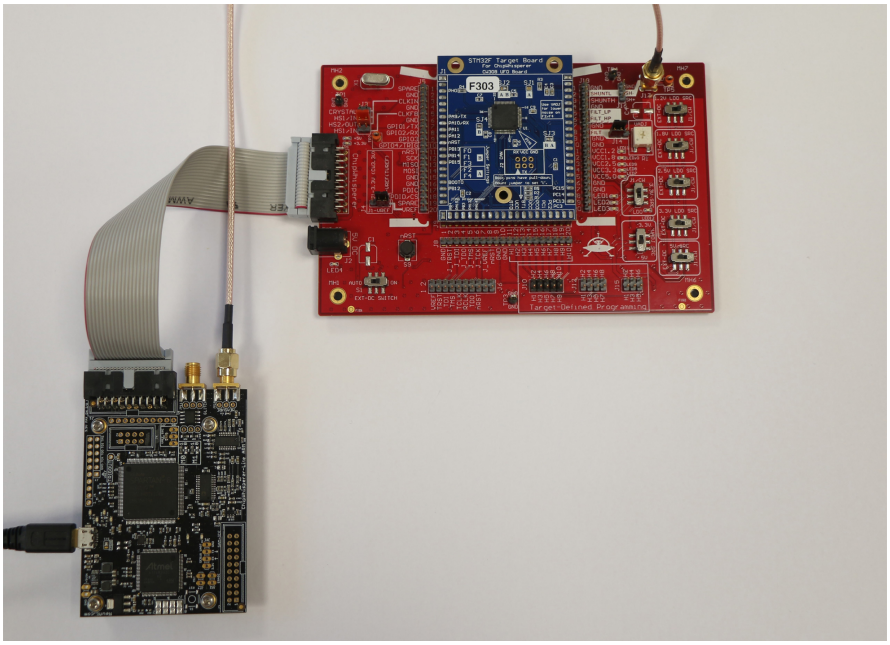


Figure 7. Cryptanalysis – NAE-SCAPACK-L1 – An embedded security analysis.

side channel attacks on embedded devices and explores the faults injection resistance of these devices. Particularly, it focuses on power analysis, which uses information leaked by a device's power consumption to mount an attack, as well as voltage and clock glitching attacks, which briefly disrupt a device's power or clock to cause unintended behavior. The idea of this attack is to inject, during encryption or decryption, successive faults to the hardware. This disturbance causes bit changes on the result of the cipher text. Recovery of the secret key is then possible by analyzing the different outputs.

This toolchain helped us to lead an attack on the AES 128-bit cipher which is composed of 10 rounds. An AES key has been successfully recovered on all complete rounds. Note that, there is no actually known way to break AES in reasonable time on all rounds [55] [56]. This attack focuses on a dedicated hardware which reveals the key by successive fault injections. This requires that an attacker have access to the physical hardware and could connect the probe to perform an analysis. Physical security drastically mitigates these possibilities for a real factory scenario.

For the Chacha cipher, the attack has not been directly reproduced, but literature shows that similar attacks have been successfully done [58] [59]. In these papers, the side-channel analysis completely reveals the secret key. The authors proposed to add mitigations to hardness the Chacha cipher at the price of performance cost.

5.3. Power Experiment

The power consumption experiment in **Figure 8** aims at instantaneously measuring voltage, intensity and power behaviors between the lightweight and the

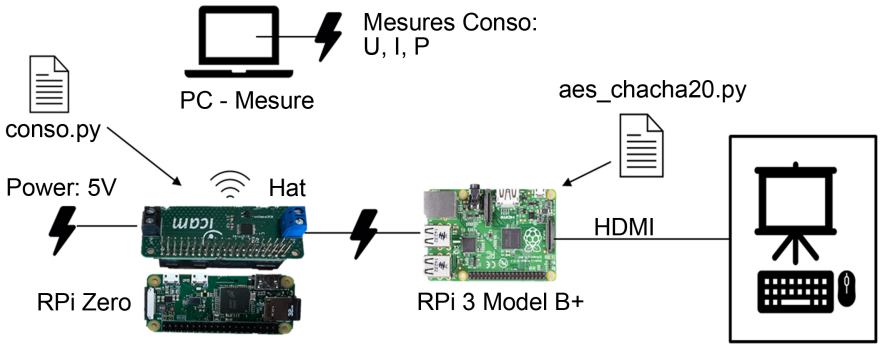


Figure 8. Power measurement of AES and Chacha using Raspberry boards.

strong cipher suite. This is done by using a power supply dedicated board developed internally (based on INA260) as a RPI Hat. One Raspberry Pi 3B+ (Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC@ 1.4 GHz) and one Raspberry Pi Zero W: 1 GHz, single-core CPU + Hat Measurement are used. A PC where the algorithm to collect the data is running.

6. Analysis

The methodology consists of taking a collection of the voltage (V), current (I) and power (P) d51ata versus time in milliseconds, because there is a 10-millisecond delay between each measurement by the raspberry.

These values are collected from 12 variant pairs and thanks to the embedded card developed by ICAM laboratory.

- data analysis by displaying different plots crossing V, I, P.
- Application of the integral of power versus time to obtain a characteristic equation (energy versus time in Watt Hours $E = F(T)$.

Data collect Procedure:

$$P = [16, 32, 64, 128] \times [100; 1000; 10000] \quad (1)$$

Here are the selected couple parameters obtained for (NbSize; NbBench):

$$\forall (\text{NbSize}, \text{NbBench}) : p1(100;16), p2(1000;16), p3, \cdots, p12(10000;128) \quad (2)$$

NbSize stands as the length of the message that is encrypted during the algorithm. NbBench stands as the iteration choice of encryption (number of rounds). Increasing these parameters allows us to know the evolution of the power of the different ciphers. But to obtain an average of the results which we believe to be more precise, the more data there is in input the more precise an average is.

A set of samples have been measured for the couple of parameters defined in Equation (2). Results in **Figure 9** show the functions $P(t)$ integrated over time to observe the variation of the energy in Watt per hour (Wh) for the gray-curve, in mA for the intensity orange-curve and in blue for the voltage curve. As the task occupied near 100% of the cpu activity, the task power consumption saturates at a constant value of 200 mA for the software cipher implementations. The Raspberry Pi is near 1 W of total power consumption. Thus, the main criteria to

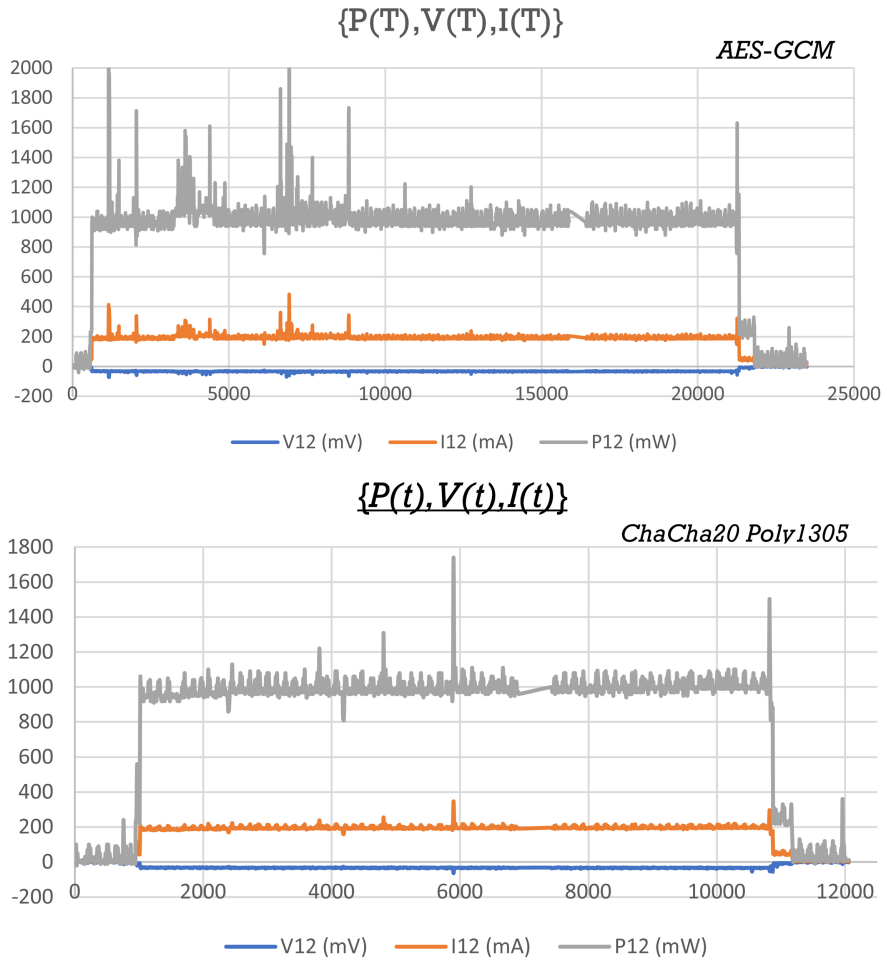


Figure 9. Power, intensity and voltage for the both ciphers.

analyze is the total execution time kept back to one cipher block execution.

The data extracted with the P12 parameters configuration are shown in **Figure 10** where x axis is the time in ms and the y axis is the integrated power over time expressed as energy in Wh. This representation is convenient to model the global energy consumption over time and isolate the noise. Some artifacts appear at regular intervals, they have been identified as task interrupts to handle other processes.

Linear modeling can be employed to characterize the ciphers task behavior. Modeling represent AES curve with $Y_p(\text{AES}) = 0.0026 \cdot X_t$ and Chacha20 curve with $Y_P(\text{ChaCha}) = 2.79E^{-4} \cdot X_t$ with Y the energy en Wh and X the time in milliseconds.

When comparing together the AES-128-GCM and the Chacha20-Poly1305 ciphers in **Figure 11**, AES-128-GCM is found to be more energy intensive than the latter as it is about half as efficient. As for example, with the c12 pair, AES encryption consumed 6 Watts in 20 s, while Chacha consumed 3 Watts in 9.3 s. These results should therefore be borne in mind when selecting an encryption block for the symmetrical end-state encryption process.

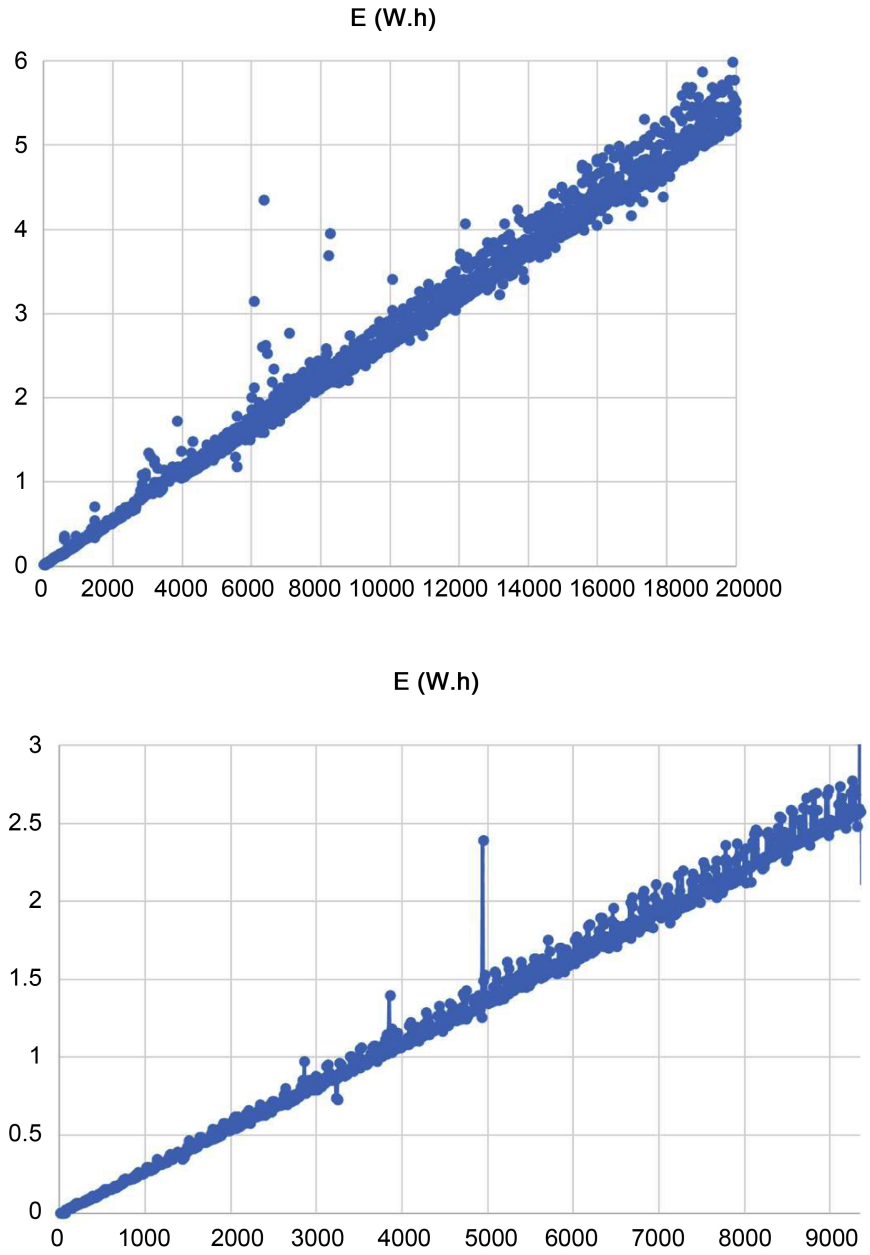


Figure 10. Extract analysis of data collected for P12 (AES & Chacha: 128; 10 k).

7. Synthesis and Discussion

The results of the experiment in Table 3 show that Chacha20-Poly1305 outperforms AES-GCM, while consuming less energy. In terms of security and robustness, the experiment revealed the existence of vulnerabilities for hardware implementations in both ciphers.

The three competitors have advantages and drawbacks in Table 4. From the confidentiality point of view, all rely on AES for strong cryptography or the recent Chacha20 for lightweight cryptography. It's not possible at this stage to draw any conclusions about the robustness of the latter two, as they can both be

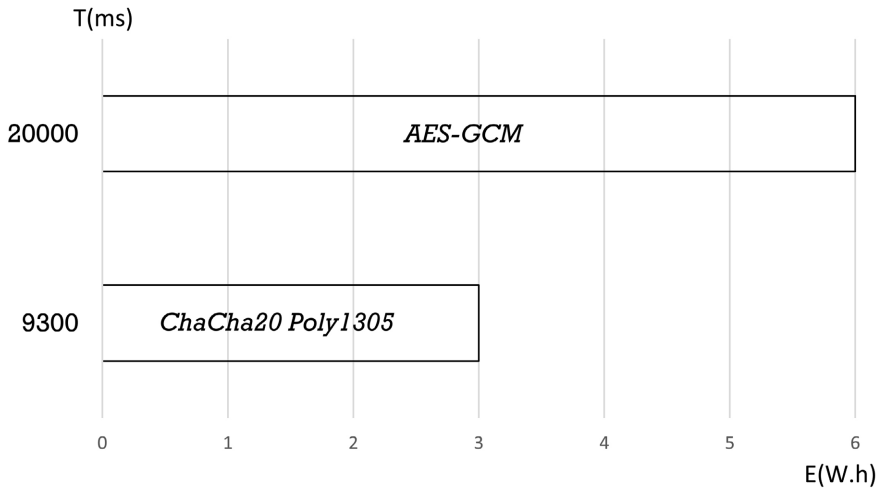


Figure 11. The performance of the ciphers combined with their energy consumption for parameter (P12). AES is nearly twice the power consumption of Chacha.

Table 3. Syntesis results for the power robustness and performance criterions.

	Performance	Robustness	Consumption
AES-128-GCM	1.59 ms	Fault injections	6 Wh
Chacha20-Poly1305	1.17 ms	EMP Probes [58] [59]	3 Wh

attacked by side-channel analysis, and no papers have been found that have successfully cryptanalyzed them to date. On the integrity side, GCM combines counter mode with Galois mode of authentication; it's well-suited for performance and parallelism optimization. For lightweight encryption Poly1305 offers similar function but with less overhead and timing attacks surface.

One of the main benefits is to simplify key generation and exchange. In MACsec, there are lots of keys to deal with: the master key MSK, the KEK, the ICV, CAKs, and the SAKs. Each machine must have one Tx and one Rx bidirectional communications channels with each other machine. And each channel has at least two secret-keys SAKs for handling the packet counter overlap. This led to a lot of key profusion and handling at hardware level. This complexity is transparent for users, at the moment they have compatible machines, and switches supporting MACsec. In practice, no PLCs have support for MACsec for now.

At the Authentication level, MACsec relies on RADIUS with EAP and EAP-AKA for key's agreement and distribution. EAP-TLS must be used to enable certificate-based authentication, which is more secure for machine network access. With the counterpart of managing certificates and a certificate authority at the factory level.

On the other side, OPC-UA embedded the latest technologies in security, with TLS, but all machines are not compatible with the last TLS v1.3, and v1.2 (some

Table 4. Comparison features between the Key Renewal (Proposition, MACsec, OPC-UA).

	Proposition	MACsec	OPC-UA (OPC - gateway)
Confidentiality	Chacha20/AES-GCM	AES-GCM	Basic, AES
Integrity	Poly1305/GCM	GCM + ICV	SHA256 RSA Sign
Keys	Certificates MSK SK + N	PSK (CAK, CKN) KEK + ICV SAK	Certificates + Master Key
Authentication	Radius EAP-TLS Certificates	Radius EAP-AKA	TLS Anonym/User/ Certificate
Key Derivation	scrypt (robust but slow)	AES-ECB => (KEK, ICV) AES-CMAC KDF AES Key Wrap	PSK/xxDH(E)
Performance	Software I0 not measured	Software/Hardware I0 = 30 ms	Software I0 = 100 - 300 ms
Cost (with HW upgrade)	++	++(+++)	++(++)
Security	Light/Strong	Strong	Light (Basic)/ Strong (AES)
Certified	No	Yes	Yes

old v1.1) keeps the norm for many old and inefficient security machines. For key exchange TLS guarantees perfect forward secrecy (v1.2+) by using the Elliptic Curves or "Standard" Diffie-Hellman Ephemeral-variant key exchange. Once again, not so many PLC support these features. Our proposition uses the double RSA ciphering to guarantee confidentiality and proof of authenticity for the secret key exchange. This can be costly in performance implementation (relatively) but efficient as certificates are already into concern. The global performance is crucial since encryption adds overhead to process communications. Most heavily embedded dedicated hardware has ASIC circuit or hardware acceleration to increase performance. Even if the proposed solution is currently purely software, one can imagine hardware acceleration on the same approach.

MACsec and OPC-UA are standardized and certified, they have a community interest to support them. The final element is the cost, and it is very important. Because when dealing with MACsec machines need to be upgraded and reloaded to handle it. It can be used in transparent mode until reaching the switch, but direct access on the same (only one) switch won't benefit from the protection except within the switch. Thus, industries need to change machines, hardware modules, network switches, and all together is a very expensive upgrade for

the return of interest. On the other hand, OPC-UA gateways can be used in front-end of machines to collect data and secure the communications to an historian. But be careful of timing constraints, as a complete negotiation of the start transaction is important (100 to 300 ms) for TLS v1.3 and token-based 0-RTT session restart is fast but considered insecure.

Moreover, PLC like Siemens have OPC-UA performance limitations depending on the PLC level. Most of them are limited to 200 or 100 ms for the minimum sampling rate, and only heavy models (e.i. 1517/1518) can achieve 50 and 10 ms of sampling rate. Massive use of arrays or structs can reduce the read overhead. Thus, OPC-UA protocol must be adopted with these limitations in mind.

To synthesize, MACsec is probably the most achieved solution for industrial protection of LAN level networks and is directly embedded in switches compatible with standard authentication mechanisms, but at the cost of changing or renewing the materials. MACSec can also be joined together with TSN for Time-sensitive Networking. But in practice, our advices is to avoid mixing real-time OT networks with IT streams, and keep applying segregation of networks.

On the other side OPC-UA is the norm for industry 4.0 interoperability, the drawback could be the performance on some real-time or field-level systems. In practice, most specific industrial field protocols like EtherCat, Profinet RT… still have a role to play.

As factories shift into the 4.0 and 5.0 industrial paradigm in the future, they will need to offer security for machine interoperability. Business performance and sustainability could depend on the creation of secure groups that cover most common PLC attack vectors.

Protection against external threats has many facets. A company has several key components, such as industrial control systems, industrial networks, SCADA, assets and cyber-assets, monitoring stations, data historians, dashboards etc. Industrial network design and architecture is essential for load balancing and network isolation. Performance considerations must also be considered in terms of latency, bandwidth, topology, and security control elements. The industry is rich in suppliers and there are a multitude of industrial protocols: fieldbus protocols, backend protocols, monitoring and security protocols. Hacking of an industrial control system has many consequences and drawbacks starting with financial losses, production stoppages and company's reputation etc.

8. Conclusions

This paper proposes a global approach to put corporate sustainability back at the center while improving the global company performance. A new sustainable digital methodology combines performance, sustainability, and the safety of the production by enforcing cybersecurity. This paper contributes on the renewal key generation problem for machines secure communications. And more precisely, on its integration in a coherent cybersecurity approach that involves a

centralized process security supervision, closely linked to the overall network architecture, its segregation zones and authorizations, right down to authenticated and protect groups of machines. The paper assesses the robustness, performance and power consumption of the final ciphers for practical implementation. In particular, this study confirms the performance difference between AES-GCM and Chacha20-Poly1305 where the last one performs faster at equivalent hardware. The power consumption is almost half that of AES. This study reveals a potential hole in robustness for both encryption algorithms face to side channels analysis on eaves-droppable hardware. In this work, the key recovery on AES has been carried out successfully, while the literature confirms us that the same attacks has been successfully performed on Chacha20. To mitigate the risk, in practice this requires access to the PLCs hardware with special equipment/probes, and it's definitely not a mathematical cryptanalysis of these algorithms.

Currently, the key renewal proposal was implemented between a Raspberry Pi front-end module, a Siemens S7-1200 PLC and a certification authority server. For the proof of concept, only key regeneration and frame generation were developed for the experiment. Next step is to realize completely transparent machine exchanges. Several possibilities are now being considered, such as designing specific optimized front-end hardware, or developing a MACsec profile specific to factory use case.

Last but not least, sustainability is enhanced by the protection of machine groups, which can work without downtime or external disturbances. Machine management and safety remain a priority to maintain the company's competitiveness. Human intervention is essential to orchestrate and streamline all these factory processes in a world where society will need to move towards greater sustainability and integral ecology for its industry.

Acknowledgements

Thanks to Group API for providing the Supervision materials, and the Lina Pro MES software used in conjunction with OPC-UA for data gathering.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Lang, J., Burian, J., Cooke, J., Crook, S., Dialani, M., Eriksen, L., Filkins, P., Finalle, P. and Krishnan, S. (2021) IDC FutureScape: Worldwide IT/OT Convergence 2022 Predictions, Oct 2021—Doc Document number: # US47131521.

[2] Mueller, P. and Yadegari, B. (2012) The Stuxnet Worm. University of Arizona, Tucson.

[3] Sen, R., Verma, A. and Heim, G.R. (2020) Impact of Cyberattacks by Malicious Hackers on the Competition in Software Markets. *Journal of Management Informa-*

tion Systems, **37**, 191-216. https://doi.org/10.1080/07421222.2019.1705511

[4] Knaap, E.D. and Langill, J.T. (2015) Industrial Network Security. 2nd Edition, Springer, Berlin. https://doi.org/10.1016/B978-0-12-420114-9.00006-X

[5] Adams, C. and Lloyd, S. (2003) Understanding PKI: Concepts, Standards and Deployment Considerations. 2nd Edition, Addison Wesley, Boston.

[6] Rijmen, V. and Daemen, J. (2002) The Design of Rijndael: AES—The Advanced Encryption Standard.

[7] National Institute of Standards and Technology (2001) Advanced Encryption Standard. Federal Information Processing Standard (FIPS) Publication 197.

[8] Bernstein, D.J. (2008) ChaCha, a Variant of Salsa20.

[9] Adomnicai, A., Fournier, J.J.A. and Masson, L. (2018) Masking the Lightweight Authenticated Ciphers ACORN and Ascon in Software, IACR Cryptol. ePrint Archive 2018/708.

[10] Adomnicai, A. (2019) Cryptographie légère pour l'internet des objets: Implémentations et intégrations sécurisées. Université de Lyon, Lyon.

[11] Da Silveira, G., Borenstein, D. and Fogliatto, F.S. (2001) Mass Customization: Literature Review and Research Directions. *International Journal of Production Economics*, **72**, 1-13. https://doi.org/10.1016/S0925-5273(00)00079-7

[12] Hankel, M. and Rexroth, B. (2015) The Reference Architectural Model Industries 4.0 (RAMI 4.0).

[13] Stock, T. and Seliger, G. (2016) Opportunities of Sustainable Manufacturing in Industry 4.0. *Procedia CIRP*, **40**, 536-541. https://doi.org/10.1016/j.procir.2016.01.129

[14] Vial, G. (2019) Understanding Digital Transformation: A Review and a Research Agenda. *The Journal of Strategic Information Systems*, **28**, 118-144. https://doi.org/10.1016/j.jsis.2019.01.003

[15] Wagner, T., Herrmann, C. and Tiede, S. (2017) Industry 4.0 Impacts on Lean Production Systems. *Procedia CIRP*, **63**, 125-131. https://doi.org/10.1016/j.procir.2017.02.041

[16] Nandakumar, N., Saleeshya, P.G. and Harikumar, P. (2020) Bottleneck Identification and Process Improvement by Lean Six Sigma DMAIC Methodology. *Materials Today: Proceedings*, **24**, 1217-1224. https://doi.org/10.1016/j.matpr.2020.04.436

[17] Lee, B.C.Y., Mahtab, M.S., Neo, T.H., Farooqi, I.H. and Khursheed, A. (2022) Comprehensive Review of Design of Experiment (DOE) for Water and Wastewater Treatment Application—Key Concepts, Methodology and Contextualized Application. *Journal of Water Processing Engineering*, **47**, Article ID: 102673. https://doi.org/10.1016/j.jwpe.2022.102673

[18] Chen, D., Vallespir, B. and Doumeingts, G. (1997) GRAI Integrated Methodology and Its Mapping on to Generic Enterprise Reference Architecture and Methodology. *Computers in Industry*, **33**, 387-394. https://doi.org/10.1016/S0166-3615(97)00043-2

[19] Tang, C. and Tang, C. (2017) Key Performance Indicators for Process Control System Cybersecurity Performance Analysis. US Department of Commerce, National Institute of Standards and Technology, Washington DC. https://doi.org/10.6028/NIST.IR.8188

[20] Ebert, C. and Duarte, C.H.C. (2018) Digital Transformation. *IEEE Software*, **35**, 16-21. https://doi.org/10.1109/MS.2018.2801537

[21] Soori, M., Behrooz, A. and Dastre, R. (2023) Machine Learning and Artificial Intelligence in CNC Machine Tools: A Review. *Sustainable Manufacturing and Service Economics*, **2**, Article ID: 100009. https://doi.org/10.1016/j.smse.2023.100009

[22] Ong, P., Lee, W.K. and Lau, R.J.H. (2019) Tool Condition Monitoring in CNC end Milling Using Wavelet Neural Network Based on Machine Vision. *The International Journal of Advanced Manufacturing Technology*, **104**, 1369-1379. https://doi.org/10.1007/s00170-019-04020-6

[23] Wen, Y., Rahman, M.F., Xu, H. and Tseng, T.-L.B. (2022) Recent Advances and Trends of Predictive Maintenance from Data-Driven Machine Prognostics Perspective. *Measurement*, **187**, Article ID: 110276. https://doi.org/10.1016/j.measurement.2021.110276

[24] Li, C., Zheng, P., Yin, Y., Wang, B. and Wang, L. (2023) Deep Reinforcement Learning in Smart Manufacturing: A Review and Prospects. *CIRP Journal of Manufacturing Science and Technology*, **40**, 75-101. https://doi.org/10.1016/j.cirpj.2022.11.003

[25] Chen, X., Yao, L., McAuley, J., Zhou, G. and Wang, X. (2023) Deep Reinforcement Learning in Recommender Systems: A Survey and New Perspectives. *Knowledge-Based Systems*, **264**, Article ID: 110335. https://doi.org/10.1016/j.knosys.2023.110335

[26] Mughees, H.A. and Rahimi, A. (2023) Deep Learning Methods for Object Detection in Smart Manufacturing. *The Journal of Manufacturing Systems*, **64**, 181-196. https://doi.org/10.1016/j.jmsy.2022.06.011

[27] Tao, F., Qi, Q., Wang, L. and Nee, A. (2019) Digital Twins and Cyber-Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. *Engineering*, **5**, 653-661. https://doi.org/10.1016/j.eng.2019.01.014

[28] La, H.J. and Kim, S.D. (2010) A Service-Based Approach to Designing Cyber Physical Systems. *IEEE/ACIS 9th International Conference on Computer and Information Science*, Kaminoyama, 18-20 August 2010, 895-900. https://doi.org/10.1109/ICIS.2010.73

[29] Zayat, W., Kilic, H.S., Yalcin, S., Zaim, S. and Delen, D. (2023) Application of MADM Methods in Industry 4.0: A Literature Review. *Computers & Industrial Engineering*, **177**, Article ID: 109075. https://doi.org/10.1016/j.cie.2023.109075

[30] Martell, F., López, J.M., Sánchez, I.Y., Paredes, C.A. and Pisano, E. (2023) Evaluation of the Degree of Automation and Digitalization Using a Diagnostic and Analysis Tool for a Methodological Implementation of Industry 4.0. *Computers & Industrial Engineering*, **177**, Article ID: 109097. https://doi.org/10.1016/j.cie.2023.109097

[31] Brundtland, G.H. (1987) Our Common Future World Commission on Environment and Development. https://doi.org/10.1017/S0376892900016805

[32] European Commission. Directorate General for Research and Innovation (2021) Industry 5.0, a Transformative Vision for Europe: Governing Systemic Transformations towards a Sustainable Industry. LU: Publications Office.

[33] Golovianko, M., Terziyan, V., Branytskyi, V. and Malyk, D. (2023) Industry 4.0 vs. Industry 5.0: Co-Existence, Transition, or a Hybrid. *Procedia Computer Science*, **217**, 102-113. https://doi.org/10.1016/j.procs.2022.12.206

[34] Dadhich, M. and Hiran, K.K. (2022) Empirical Investigation of Extended TOE Model on Corporate Environment Sustainability and Dimensions of Operating Performance of SMEs: A High Order PLS-ANN Approach. *Journal of Cleaner Pro-*

duction, **363**, Article ID: 132309. https://doi.org/10.1016/j.jclepro.2022.132309

[35] Yang, L., Zou, H., Shang, C., Ye, X. and Rani, P. (2023) Adoption of Information and Digital Technologies Sustainable Smart Manufacturing Systems for Industry 4.0 in Small, Medium and Micro Enterprises. *Technological Forecasting and Social Change*, **188**, Article ID: 122308. https://doi.org/10.1016/j.techfore.2022.122308

[36] Ndubisi, N.O., Zhai, X.A. and Lai, K.H. (2021) Small and Medium Manufacturing Enterprises and Asia's Sustainable Economic Development. *International Journal of Production Economics*, **233**, Article ID: 107971. https://doi.org/10.1016/j.ijpe.2020.107971

[37] Mahmoodi, E., Fathi, M. and Ghobakhloo, M. (2022) The Impact of Industry 4.0 on Bottleneck Analysis in Production and Manufacturing: Current Trends and Future Perspectives. *Computers & Industrial Engineering*, **174**, Article ID: 108801. https://doi.org/10.1016/j.cie.2022.108801

[38] Mahdiraji, H.A., Yaftiyan, F., Abbasi-Kamardi, A. and Garza-Reyes, J.A. (2022) Investigating Potential Interventions on Disruptive Impacts of Industry 4.0 Technologies in Circular Supply Chains: Evidence from SMEs on an Emerging Economy. *Computers & Industrial Engineering*, **174**, Article ID: 108753. https://doi.org/10.1016/j.cie.2022.108753

[39] Cezarino, L.O., Liboni, L.B., Stefanelli, N.O., Oliveira, B.G. and Stocco, L.C. (2019) Diving into Emerging Economies Bottleneck: Industry 4.0 and Implications for a Circular Economy. *Management Decision*, **59**, 1841-1862. https://doi.org/10.1108/MD-10-2018-1084

[40] De Paula Ferreira, W. Armellini, F., De Santa Eulalia, L.A. and Thomasset-Laperrière, V. (2022) A Framework for Identifying and Analyzing Industry 4.0 Scenarios. *The Journal of Manufacturing Systems*, **65**, 192-207. https://doi.org/10.1016/j.jmsy.2022.09.002

[41] Torbacki, W. (2021) A Hybrid MCDM Model Combining DANP and PROMETHEE II Methods for the Assessment of Cybersecurity in Industry 4.0. *Sustainability*, **13**, Article No. 8833. https://doi.org/10.3390/su13168833

[42] Sadik, S., Ahmed, M., Sikos, L.F. and Islam, A.N. (2020) Toward a Sustainable Cybersecurity Ecosystem. *Computers*, **9**, Article No. 74. https://doi.org/10.3390/computers9030074

[43] Lee, I. (2021) Cybersecurity: Risk Management Framework and Investment Cost Analysis. *Business Horizons*, **64**, 659-671. https://doi.org/10.1016/j.bushor.2021.02.022

[44] Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J. and Zema, T. (2021) Cybersecurity and Sustainable Development. *Procedia Computer Science*, **192**, 20-28. https://doi.org/10.1016/j.procs.2021.08.003

[45] AL-Dosari, K., Fetais, N. and Kucukvar, M. (2023) A Shift to Green Cybersecurity Sustainability Development: Using Triple Bottom-Line Sustainability Assessment in Qatar Transportation Sector. *International Journal of Sustainable Transportation*, **17**, 1287-1301. https://doi.org/10.1080/15568318.2023.2171321

[46] Vrchota, J., Pech, M., Rolinek, L. and Bednář, J. (2020) Sustainability Outcomes of Green Processes in Relation to Industry 4.0 in Manufacturing: Systematic Review. *Sustainability*, **12**, Article No. 5968. https://doi.org/10.3390/su12155968

[47] Rodger, J.A. and George, J.A. (2017) Triple Bottom Line Accounting for Optimizing Natural Gas Sustainability: A Statistical Linear Programming Fuzzy ILOWA Optimized Sustainment Model Approach to Reducing Supply Chain Global Cybersecurity Vulnerability through Information and Communications Technology. *Journal of*

Cleaner Production, **142**, 1931-1949. https://doi.org/10.1016/j.jclepro.2016.11.089

[48] Knaap, E.D. and Langill, J.T. (2014) Industrial Network Security, Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2nd Edition.

[49] Mantravadi, S., Schnyder, R., Møller, C. and Brunoe, T.D. (2020) Securing IT/OT Links for Low Power IIoT Devices: Design Considerations for Industry 4.0. *IEEE Access*, **8**, 200305-200321. https://doi.org/10.1109/ACCESS.2020.3035963

[50] Banga, A.O., Rao, U.P., Visconti, A., Brighente, A. and Conti, M. (2022) An IoT Inventory before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research Directions. *Computers & Security*, **123**, Article ID: 102914. https://doi.org/10.1016/j.cose.2022.102914

[51] Mantravadi, S., Schnyder, R., Møller, C. and Brunoe, T.D. (2020) Securing IT/OT Links for Low Power IIoT Devices: Design Considerations for Industry 4.0. *IEEE Access*, **8**, 200305-200321. https://doi.org/10.1109/ACCESS.2020.3035963

[52] Rezaeibagha, F., Mu, Y., Huang, X.Y., *et al.* (2019) Fully Secure Lightweight Certificateless Signature Scheme for IIoT. *IEEE Access*, **7**, 144433-144443. https://doi.org/10.1109/ACCESS.2019.2944631

[53] Lackorzyński, T. (2022) Practical Encryption Gateways to Integrate Legacy Industrial Machinery. Dissertation.

[54] Dubroca, S. (2016) MACsec: Encryption for the Wired LAN. *Proceedings of NETDEV* 1.1, Seville, 10-12 February 2016, 1-5. https://legacy.netdevconf.info/1.1/proceedings/papers/MACsec-Encryption-for-the-wired-LAN.pdf

[55] Bogdanov, A., Khovratovich, D. and Rechberger, C. (2011) Biclique Cryptanalysis of the Full AES. 17*th International Conference on the Theory and Application of Cryptology and Information Security*, Seoul, 4-8 December 2011, 344-371. https://doi.org/10.1007/978-3-642-25385-0_19

[56] Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D. and Shamir, A. (2010) Key Recovery Attack of Practical Complexity on AES-256 Variants with up to 10 Rounds. 29*th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, French Riviera, 30 May-3 June 2010, 299-319. https://doi.org/10.1007/978-3-642-13190-5_15

[57] Kamucheka, T., Fahr, M., Teague, T., Nelson, A., Andrews, D. and Huang, M.Q. (2021) Power-Based Side Channel Attack Analysis on PQC Algorithms, Department of Computer Science and Computer Engineering, University of Arkansas. 3*rd NIST PQC Standardization Conference*, 7-9 June 2021, 1-9.

[58] Jungk, B. and Bhasin, S. (2017) Don't Fall into a Trap: Physical Side-Channel Analysis of ChaCha20-Poly1305. *Design, Automation & Test in Europe Conference & Exhibition* (*DATE*), Lausanne, 27-31 March 2017, 1110-1115. https://doi.org/10.23919/DATE.2017.7927155

[59] Alexandre, A., Jacques, F. and Laurent, M. (2017) Bricklayer Attack: A Side-Channel Analysis on the ChaCha Quarter Round. 18*th International Conference on Cryptology*, Chennai, 10-13 December 2017, 65-84. https://doi.org/10.1007/978-3-319-71667-1_4