Array 15 (2022) 100238

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/locate/array

Application of Artificial Immune Systems in Advanced Manufacturing ☆

Rui Pinto *, Gil Gonçalves

SYSTEC - Research Center for Systems and Technologies, Rua Dr. Roberto Frias, s/n, office i219, 4200-465, Porto, Portugal
Faculty of Engineering, University of Porto, Rua Dr. Roberto Frias, s/n 4200-465, Porto, Portugal

ARTICLE INFO

Keywords:
Artificial Immune Systems
Autonomic Computing
Advanced Manufacturing Systems

ABSTRACT

In recent years, the application of Advanced Manufacturing Technologies (AMT) in industrial processes represents the introduction of different Advanced Manufacturing Systems (AMS), which encourage enterprises to improve their core competitiveness and maintain sustainable development when facing the increasing demand for personalized product customization. More recently, AMT led to a new Internet revolution, mostly known as 4th Industrial Revolution. Considering the development and deployment of Artificial Intelligence to enable smart and self-behaving industrial systems, autonomic approaches allow the system to adapt itself, eliminating the need for human intervention for management. This paper presents a systematic literature review regarding Artificial Immune Systems (AIS) approaches to tackle multiple AMS problems requiring levels of autonomy. First, a systematic review of current industrial AIS applications in manufacturing environments is presented. Then, a conceptual framework is proposed to bridge the gap between research in the AIS field and the manufacturing industry while discussing key challenges and opportunities to be addressed by future research. This study aims to build a body of knowledge for researchers and manufacturers regarding AIS solutions under Advanced Manufacturing while suggesting directions for understanding the requirements for designing and managing autonomic industry applications supported by AIS.

1. Introduction

The high global competitiveness between companies characterizes the 21st century industry. Constant changes in demand by the consumer side lead to a shorter lifetime of products. To remain competitive, companies must be able to respond quickly to this rapid demand. The big challenge is implementing new methodologies that allow system adaptability and flexibility to mass production methods to obtain a high product variability and, at the same time, large production volumes. Since the beginning of industrialization, there has been considerable interest from the industry side to innovate their production systems and develop new ideas. The applicability of new technologies in the industry, which lead to paradigm changes by allowing increased revenues at lower costs, are usually known as industrial revolutions, and the current one is the 4th Industrial Revolution or *Industry 4.0* (I4.0) [1].

I4.0 is based on the idea of converging the real and virtual worlds by connecting every physical object to each other, to identify themselves with other devices and communicate with each other. This is highly motivated by the Advanced Manufacturing Technology (AMT) progress application in industrial scenarios, such as in Multi-Agent Systems (MAS), the Internet of Things (IoT) and Cyber–Physical Systems (CPS). Also, based on Artificial Intelligent (AI) principles, such as Machine Learning (ML) and bio-inspired methods, it is emphasized the creation of autonomic systems, which are smart and autonomic systems that make decisions, react and adapt in real-time to changes during the manufacturing process as human operators do. All these ideas paved the way for Advanced Manufacturing Systems (AMS), which are supported by intelligent and autonomic (Self-*) properties [2].

According to Qu et al. [3], extensive effort has been made to enable autonomic proprieties in AMS. The research community's increasing attention is on using Information and Communication Technologies (ICT), such as cognitive agents, swarm intelligence, and Cloud computing, to integrate, organize, and allocate machine resources. On the other hand, adaptive and intelligent manufacturing control is another crucial area due to the emergence of self-organizing MAS. This level of autonomy is only possible due to data-driven approaches and

☆ This work was financially supported by: INDTECH 4.0 (SP4) - POCI-01-0247-FEDER-026653, co-funded by European Regional Development Fund (FEDER), through Competitiveness and Internationalization Operational Program (POCI) and Base Funding - UIDB/00147/2020 of the Systems and Technologies Center – SYSTEC – funded by national funds through the FCT/MCTES, and was part of the project "RECLAIM- RE-manufaCturing and Refurbishment LArge Industrial equipMent" and received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 869884.

* Corresponding author at: Faculty of Engineering, University of Porto, Rua Dr. Roberto Frias, s/n 4200-465, Porto, Portugal.
E-mail addresses: rpinto@fe.up.pt (R. Pinto), gil@fe.up.pt (G. Gonçalves).

https://doi.org/10.1016/j.array.2022.100238
Received 20 October 2021; Received in revised form 19 July 2022; Accepted 19 July 2022
Available online 25 July 2022

AI-supported decision-making and continuous improvement strategies since they enable predictive product status awareness, manufacturing process monitoring and prognostics, equipment prognostics, health management and predictive maintenance.

However, the adoption of such properties by industry is still relatively poor compared to academic research since the application of proper solutions and technologies in real environments is complex, i.e., there are unique and difficult challenges that may not exist in controlled environments. Also, despite the interest from the industry to update their production systems considering I4.0 principles, and increase revenues at lower costs, the technology acceptance is still slow. This is mainly because these are emergent technologies with low Technology Readiness Level (TRL), sometimes still immature and lacking proper integration and validation among real industrial situations.

Machine intelligence has become the basis for executing manufacturing processes, which requires close integration of process intelligence and machine controls. Allied with the introduction of autonomic proprieties to these systems, it is expected that further inspirations taken from biological systems are adopted for designing and maintaining their operation. Thus, this biological transformation of manufacturing systems induces cognition, learning capabilities, intelligence and self-healing and self-organization capabilities into AMS [4]. Artificial Immune Systems (AIS) are one of the most popular categories of bio-inspired techniques. These approaches are inspired by the Biologic Immune System (BIS), a remarkable information processing and self-learning system. Thus, the AIS research field has gained popularity over the years as one successful branch of AI [5].

For this purpose, this paper presents a Systematic Literature Review (SLR) on AIS applications in AMS. The objective is two-fold. On the one hand, the study collects and analysis the scientific contributions that report industrial AIS applications in multiple research areas to tackle different problems. On the other hand, these applications are assessed based on the Level of Autonomy (LOA) introduced to the system, considering a taxonomy of system autonomy presented by Peres et al. [6]. To this end, the following research questions were formulated:

RQ 1. What is the research trend of AIS applications in AMS?
RQ 2. What is the status of AIS applications in AMS?
RQ 3. What are the main motivations for using AIS in AMS?
RQ 4. What are the research gaps and future areas within AMS based on AIS solutions?

The paper is organized into five additional sections. In Section 2 the main concepts addressed in this paper are introduced, namely AMS, Autonomic Computing and the AIS field. It also presented existing literature reviews on these topics and popular AIS applications in non-industrial-related scenarios. Section 3 provides a detailed description of the SLR methodology undertaken and subsequent assessment of the selected body of literature. Section 4 characterizes the main results of the SLR and tries to find answers to the research questions related to the research trend, AIS applications status (research fields), AIS usage motivation (conceptualization) and existing research gaps. Section 5 provides a detailed characterization of a proposed conceptual framework regarding AIS applicability in AMS, based on the analysis of the SLR results. Finally, Section 6 concludes the paper with final remarks about the work presented, such as challenges and opportunities for future research, considering autonomy maturity and AIS application potential, main strengths and limitations of the SLR.

2. Related work

This section has a twofold objective. First, it starts by addressing important theoretical concepts used in the SLR, namely the development process of AMS and Advanced Manufacturing Technology (AMT), Autonomic Computing, Biologic Inspired Computation, and the AIS field (main techniques and widespread applications in non-industrial related scenarios). Second, it presents the main existing literature reviews on one or more of these topics. The analysis of the existing literature reviews and identified limitations leads to the justification of development of this SLR, which focus in the merger of all the addressed topics.

2.1. Advanced manufacturing

AMT [7] has been studied since the 1960s, when there was a move from mechanical technology to digital circuits and systems as a result of the introduction of Programmable Logical Controllers (PLC) and computer numerically controlled (CNC) machine tools on the shop floor. This was the start of the Third Industrial Revolution. Indeed, AMT has always significantly impacted the growing process of manufacturing paradigms ranging from craft production to mass production to mass customization and personalization. Before the 1960s, with the development and deployment of early factory automation technologies and related automated production equipment, manufacturing shop floors were progressively changed from the original craft production manual workshop into rigid automated production lines. It helped manufacturing enterprises achieve mass production and lower costs since increasing affluent customers and matching personalized requests required mass production. Numerous AMT were created and are still widely used today, leading to the development of several AMS, including Flexible Manufacturing, Computer Integrated Manufacturing, Lean Production, among others. [8].

Along the way, these AMS supported the transition of manufacturing from mass production to mass customization by encouraging enterprise information and process integration. Other related AMT have been developed rapidly due to the increasing personalized demand, enhancing manufacturing processes' agility, globalization, and intelligence. More recently, in the *Industrie 4.0* era, networked devices enable unprecedented data and information exchange by applying typical IoT scenarios, Service-Oriented Architectures (SOA), and CPS to industrial contexts. This can be explained by the remarkable progress in the technological capability of computational (embedded) devices and networks. These technologies were developed in parallel with the general emergence of AMT, which helped deploy the personalization paradigm [9].

As a result, AMS represent non-traditional manufacturing technologies that enterprises may employ to preserve or increase their competitiveness. These technologies incorporate all of the benefits of industrial automation (CNC, Robot, and Automated Guided Vehicles (AGVs), integrated and computerized control, Industrial Local Area Network (LAN), distributed architecture (MAS, and holonic manufacturing), and distributed AI techniques.

Germany has one of the most competitive manufacturing industries in the world. Because of its vital machinery and plant manufacturing industry, its global significance of ICT competencies and its know-how in embedded systems and automation engineering, Germany has the advantage of being the leader in the research, development and production of innovative manufacturing technologies. Also, they already followed a structured and integrative approach for the AMT implementation to take advantage of all their individual and systemic benefits [10]. So, in 2011, the *Industrie 4.0* term was first used at the Hannover Fair, and, in 2013, the Industrie 4.0 Working Group presented a final report [11], stating that I4.0 is the strategic initiative to secure the future of the German manufacturing industry.

However, Germany was not the only country that have recognized the trend to deploy AMS into the manufacturing industry. Similar initiatives are also found, such as the U.S. *Smart Manufacturing Leadership Coalition* (SMLC) [12], the Chinese *Made In China 2025* (MIC25) [13], the French *Usine du Futur* [14], the British *Catapult* [15], the Korean *Industry Innovation 3.0* [16], etc.

Meanwhile, in 2015, at the World Economic Forum in Davos, the German chancellor Angela Merkel urged all of Europe to embrace I4.0

[17]. With this it was introduced to European industries the urgency to deal with the fusion of the online world and the world of industrial production. The paradigm is changing, and those who are the leaders in the digital domain will take the lead in industrial production. The support for research in this area increased dramatically over the years, and I4.0 became a hot topic among practitioners and academics in Europe and one of the top priorities for research centres, universities and companies. For the first time in the history of the industrial revolution, a revolution was announced before it actually happened [18]. This provided various opportunities for companies and research institutes to shape the future of I4.0 actively.

Most AMT nowadays relates to integrating computational and physical processes and connecting billions of objects over the internet. This is often addressed by modern CPS, IoT, and other similar technologies. Many conventional terminologies, such as Manufacturing and Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), Robotics, among others, are commonly used to refer to the same AMT. This ambiguity is especially apparent in the AMS paradigm when numerous other technologies and concepts overlap, such as embedded systems, IoT, MAS, CPS, industrial networks, Wireless Sensor & Actuator Networks, *Digital Twin* (DT), among others.

This makes defining AMS and AMT difficult, especially when considering all of the application scenarios and research fields. Furthermore, because research in some of these technologies is so vast and may encompass multiple disciplines of knowledge, they eventually become their own research domains. Next, it is presented a description of the core AMT, which are paving the way for the development of recent AMS and Industry 4.0-related application scenarios.

CPS CPS are a new generation of systems that have integrated computational and physical capabilities and can interact with humans via various procedures. A CPS is generally a networked computation and physical process-integrated system with cooperating computational elements and controlling physical entities. Its roots are frequently seen as embedded systems, objects with specialized sensing and processing capabilities. Because a CPS is a network of interacting embedded devices, it is feasible to process data locally such that valuable information or abstracted data may be transmitted through the network. CPS implementation in industrial contexts is commonly referred to as Cyber–Physical Production Systems (CPPS) or Industrial CPS [19,20].

SCADA/ICS SCADA/ICS play a vital role in managing and controlling critical infrastructure. These are frequently defined as infrastructures that offer essential services and serve as the foundation for a country's security, economic, and healthcare systems. They can include sectors such as agriculture, healthcare, nuclear reactors, transportation, the energy industry, civil and chemical engineering, water plants, research, and so on. Technological improvements have resulted in the SCADA/ICS evolution to modern systems such as CPS [21].

IoT Because of the fast expansion of Internet technology, many physical objects may now be linked to the Internet via embedded electronics, software, sensors, and network devices. IoT often refers to scenarios in which network connection is extended to everyday physical things. The fundamental idea behind IoT is to link devices to each other over the Internet, thanks to recent developments in wireless technology. The Internet, in this scenario, symbolizes the worldwide networking of linked devices – or Things – that allow them to communicate with one another by sharing and transforming information. In industry, IoT is commonly referred to as the Industrial Internet of Things (IIoT). By connecting all industrial systems and shop-floor equipment to the Internet, a production manager or executive may readily obtain production information from any location with an Internet connection. Furthermore, they may remotely control the events of production equipment [22–24].

Industrial LAN In a traditional industrial context, there are primarily two communication levels: process and control. Each has unique network needs, such as round-trip time, determinism, dependability, and the severity of failures, requiring different communication methods. Thus, IP networks are often employed at the process level, whereas field networks are used at the control level. Field networks, namely fieldbus protocols, have been utilized in industrial applications for some time. Industrial Ethernet protocols were developed to bridge the gap between fieldbus systems and IP networks [25,26].

MAS MAS is based on a society of intelligent, cooperative, proactive, and autonomous entities called agents that represent physical or logical things in the system. It is derived from the field of distributed AI. The agents are dispersed across the environment, interacting with one another and with the environment to achieve a specific or common objective, sharing information, making choices, and modifying their behaviour as conditions change [27].

DT To accomplish digitalization, a more significant effort in standardization is necessary to develop consistent interfaces. This will foster open communication among a diverse set of entities. This standardization is frequently achieved through the notion of DT, which is often viewed as a wrapper used to connect any device or process into a network where information can be readily accessed, processed, and shared. In the industrial environment, the DT may be viewed as a software wrapper of physical equipment or information systems, offering autonomous decision making, standardized communication, sensorisation as a plug & play approach, and smart control [28–30].

AI Manufacturing processes should employ a computationally processable model, such as data-based, physical-based, numerical-based, or discrete-based, to realize the full potential of decision support. Data-driven models involve the analysis of sensor data to discover hidden patterns in the data. This is referred to as data mining, and it can employ one or more AI algorithms to extract relevant information from data. These approaches may be based on hard computing, such as Machine Learning methods, or on soft computing, such as Biologic Inspired Computation [6,31,32].

WSAN Sensors are used to acquire data about physical processes to monitor them. This data is then analysed and used to regulate physical processes via actuators, resulting in the optimization of a manufacturing process. WSAN has recently enabled sensors and actuators using wireless communication. Sensor motes can be utilized if industrial needs require the deployment of a large number of sensors where the primary aim is to gather sensor data at a reasonable cost or if sensor integration has proven challenging because of the lack of accessibility to remote physical places. Motes are tiny devices commonly used to develop WSAN and are equipped with a microcontroller, battery, radio, Analog to Digital Converter (ADC), and some sensors [33–35].

Cloud/Edge Computing Because of advancements in Cloud computing, IoT has become appealing. Wireless devices are distinguished by their mobility and battery power, which present several constraints for data process and storage needs for running algorithms. This means that these capabilities can be relocated out of the constrained devices to powerful remote servers as long as a network connection is available (for information exchange). Cloud computing refers to the ability of hardware and software systems to deliver data services over the Internet. Data collected from the sensorisation layer can be further processed remotely on the Cloud or the Fog. On the other hand, Fog

and Edge computing are characterized by an intermediate layer between the end devices and the Cloud, which can be seen as an extension of the Cloud. These layers are responsible for providing computation, storage and networking services at the edge of the network since sometimes the Cloud is not prepared to provide mobility support, geo-distribution, local awareness or low latency to end devices [36–39].

Big Data As more things, or smart devices, are linked to the Internet of Things, more data is collected from them to perform analytics to identify trends and relationships that lead to insights. Big Data refers to the challenge of gathering, storing, querying, analysing, and managing a massive volume of heterogeneous data generated by many devices with different time and location signatures [40,41].

Industrial Robots An industrial robot is a self-contained, reprogrammable, multifunctional manipulator with three or more axes that can be stationary or mobile, used in industrial automation applications. An industrial robot generally comprises a manipulator that moves an end-effector to accomplish the intended duties, a controller that actuates and regulates the manipulator, and a teach pendant that programmes and supervises the operations. There are also Automated Guided Vehicles (AGV), which are robots that transport goods in facilities. More recently, collaborative robots emerged. Cobots are designed to work safely alongside human workers in a shared, collaborative workspace [42,43].

Despite this difficulty for many people and companies when it comes to identifying and implementing AMS, which can be seen currently as I4.0 scenarios, right now, the concept is more transparent. All the implemented I4.0 scenarios converge to very similar requirements and goals to achieve added value in different manufacturing applications, based on ICT technological advances, such as IoT, AI, Cloud/Edge, and CPS. Oztemel and Gursev [1] presents 12 goals to achieve I4.0, namely:

- **Standardization** [*STD*] - Standardization of systems and creation of a reference architecture;
- **Optimized Management** [*OM*] - Performing optimized management of complex systems;
- **Communication Network Infrastructure** [*NET*] - Manage industrial network infrastructure for communication reliability;
- **Safety & Security** [*SS*] - On one hand, setting a safe and secure environment to human operator. On the other hand, enable system protection against misuse and unauthorized access;
- **Human Management** [*HM*] - Organizing and managing the workplace in a human-centred way, by considering processes, human, automation and environmental changes;
- **Upskilling** [*UP*] - Personnel training for upskilling the workforce and management (Education 4.0);
- **Regulatory Framework** [*RF*]- Creating an organizational framework for data organization, to ensure new technology is compliant with the law;
- **Resource Efficiency** [*RE*] - Increasing the efficiency of resource utilization (Green Manufacturing);
- **Autonomy** [*AU*] - Self-behaving systems (Self-*), where minimum human interaction is required;
- **Process Efficiency & Product Quality** [*PEQ*] - Product an Process interaction (due to autonomy behaviour);
- **Data Analytics** [*DA*] - Big data analysis, for data-driven autonomic decision-making;
- **Adaptability** [*AD*] - Adaptability and flexibility, for responsiveness to changes in real time.

2.2. Autonomic computing

Computer systems have reached a level of complexity where human intervention for operation and control is becoming increasingly difficult. In the IoT paradigm, the visions of ubiquitous and pervasive computing will become true by surrounding us with embedded technology and transforming every physical object into a CPS. These CPS are connected to sensors and actuators to maintain communication between physical and virtual worlds and are interconnected to other CPS using communication systems. How can such a complex system be managed in this scenario, considering all the actively interacting heterogeneous devices and uncertainty involved? In 2001, the International Business Machines Corporation (IBM) suggested the concept of Autonomic Computing, referring to the need for new methods to manage and control the behaviour of complex systems, where these systems should be able to adapt themselves, eliminating the need for human intervention [44].

According to IBM [44], a system is autonomic only if: (1) it knows itself in terms of what resources it has access to, what are its capabilities and limitations and how and why it is connected to other systems; (2) it can automatically configure and reconfigure itself depending on the changing computing environment; (3) can optimize its performance to ensure the most efficient computing process; (4) can work around encountered problems by either repairing itself or routing functions away from the trouble; (5) can detect, identify and protect itself against various types of attacks to maintain overall system security and integrity; (6) can adapt to its environment as it changes, interacting with neighbouring systems and establishing communication protocols; (7) relies on open standards and cannot exist in a proprietary environment; (8) anticipates the demand on its resources while keeping transparent to users.

The Autonomic Computing concept, later extended to Organic Computing [45], has been inspired by the human autonomic nervous system [46], which removes from the consciousness the tasks of coordinating all our bodily functions (for regular maintenance and optimization) by taking care of most of them. Kephart and Chess [47] warn that system managers cannot anticipate, design and maintain the complexity of the interactions among devices and computer systems, especially in CPS. For this reason, computer systems should constantly adapt themselves to changing environmental conditions in a logic loop that monitors the context of execution. Such dynamics can be realized by a Monitor–Analyse–Plan–Execute (MAPE) loop or a Monitor–Analyse–Plan–Execute–Knowledge (MAPE-K) loop architecture [44,47], which is illustrated in Fig. 1.

The essence of Autonomic Computing is the system capacity of Self-Management, which, according to Ganek and Corbi [48], includes the so-called Self-x, Self-* (Self-star) or Self-CHOP properties. According to Berns and Ghosh [49], Self-Managing systems are systems that maintain, improve and restore their functionality or properties without external actions on the system. Self-Management is the generic property that encompasses the various Self-* properties, which relies on Zadeh's concept of adaptivity [50]. Essential Self-* properties are:

- Self-configuration [*SC*]
- Self-optimizing [*SOP*]
- Self-healing [*SH*]
- Self-organizing [*SOR*]
- Self-awareness [*SAW*]
- Self-adaptive [*SAD*]
- Self-immunity [*SI*]

As seen before, one of the main goals of AMS is to target the implementation of autonomic and collaborative manufacturing assets with advanced self-capabilities [4]. With this in mind, and taking into account the heterogeneous nature of industrial systems and their applications, Peres et al. [6] presents a taxonomy of manufacturing

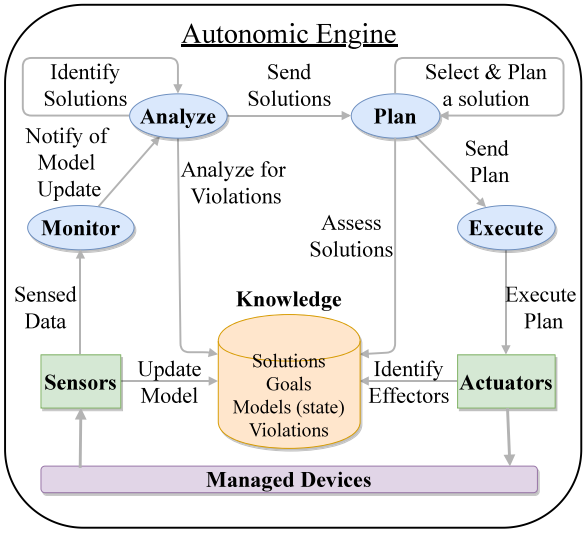

Fig. 1. MAPE-K model for autonomic systems [47].

system autonomy, defining a six-level model of automated decision-making based on industrial processes. The model contextualized with industrial scenarios for each Level of Autonomy (LOA) is:

- Level 0: No autonomy. Human operators have complete control without any assistance from an AI system.
- Level 1: Assistance with respect to select functions. Human operators have full responsibility and make all decisions.
- Level 2: Partial autonomy. Human operators have full responsibility in clearly defined areas and define (some) goals.
- Level 3: Delimited autonomy. In larger sub-areas, the AI system warns if problems occur, and human beings validate the solutions recommended by the system.
- Level 4: Adaptability and autonomic functions. Human operators can supervise or intervene in emergency situations within defined system boundaries.
- Level 5: Full autonomy. The AI system operates autonomously in all areas, including cooperation and fluctuating system boundaries. Human operators do not need to be present.

In this work, we seek to study the introduction of Self- * properties in AMS, thanks to the implementation and application of techniques that follow *Autonomic Computing* principles, such as AIS. AIS belong to the broader paradigm of *Biologic Inspired Computation* [51] and will be described next.

2.3. Biologic inspired computation

Biologic Inspired Computation refers to the study of biologically motivated computation, which belongs to the field of *Natural Computing* and a sub-field of *Computational Intelligence*. *Biologic Inspired Computation* main goal is to solve engineering and computation problems by generating solutions inspired by different biological processes from the natural world. Several sub-disciplines focus on adaptive and intelligent systems, such as *Evolutionary Computation*, *Swarm Intelligence*, *Fuzzy Systems*, Artificial Neural Networks (ANN), and AIS.

Regarding AIS, they are a category of biology-inspired computational methods that emerged in the '90s, bridging different areas such as immunology, computer science and engineering. AIS have been developed by computationally modelling biological immune processes, abstracting those models into algorithms and implementing them in the context of engineering. The BIS is an immensely rich system, and many immune processes are not well understood yet, generating discussion and little agreement among immunologists. This leads to a lack of clarity of the functioning of immune processes and, regarding AIS practitioners, a difficulty in properly model a computational system.

2.3.1. Biological immune system

The BIS is a robust and self-organized system with remarkable abilities, such as recognition and discrimination, maintenance, inference from danger/context and memory. To maintain a healthy state, the BIS processes the state of the body and takes action accordingly through healing processes [52,53]. The BIS is a multilayer system wherein different types of defence mechanisms are active in each layer. There are three main lines of defence: the anatomic barrier, innate immunity and adaptive immunity. The anatomic barrier is constituted by physical obstacles, such as skin, mucous membranes and skin secretions, to prevent pathogens such as bacteria and viruses from entering the organism. If a pathogen breaches the first line of defence, innate immunity provides an immediate but non-specific response, such as inflammatory response and antimicrobial proteins. If pathogens successfully evade the innate response, it will activate the adaptive immunity, which adapts its response during an infection to improve its recognition skills and kill the pathogen.

The BIS consists of a set of organs (central and peripheral lymphoid organs), cells (lymphocytes or white blood cells and granulocytes) and molecules (immunoglobulins or antibodies) [54,55]. The central lymphoid organs, such as bone marrow and the thymus, are responsible for producing and assisting lymphocytes. The purpose of peripheral lymphoid organs, such as lymph nodes, spleen and mucosal tissues, is to facilitate the interaction between lymphocytes and antigens.

An antigen is a molecule capable of inducing an immune response on the part of the host organism, though sometimes antigens can be part of the host itself. The lymphocyte population is constituted mainly of B and *T* cells. B cells are responsible for recognizing particular antigens and producing antibodies, which will bind to antigens. B cells are activated in the presence of antigens, and the maturation process begins. B cell maturation consists of becoming plasma cells or memory cells. Plasma cells are the ones that actively secrete antibodies.

Antigens are characterized by bounding molecules called epitopes, which are the part of an antigen that is recognized by B and *T* cells. In the recognition process, the epitope bonds to the lymphocytes using the paratope, which is the bonding molecule of the lymphocyte. Antibodies are a particular type of molecule. They are the paratopes of the B cells and are responsible for binding to the antigen. Antigens are mostly known as non-self cells, while the host body cells are known as self-cells. Epitopes are usually non-self if they are part of antigens, or self since some proteins of the host body could be recognized by lymphocytes.

2.3.2. Artificial immune systems

As mentioned before, AIS were created to computationally simulate immunologic processes in the BIS, abstracting the concepts into algorithms and implementing them in engineering settings. Pinto et al. [56] presents a deep review of AIS, focusing on anomaly detection applications in CPS. As described next, four main immune mechanisms have inspired most standard AIS techniques [5]. However, there are ensemble methods, which represent approaches that combine more than one basic technique. Finally, there are immune-inspired methods, which do not follow exactly a specific immune model but use immune principles.

Negative Selection Algorithms (NSA) [57] The main characteristics of the NSA are described by Forrest et al. [57]. NSA rely on the *Self/Nonself theory* existing in the BIS. The main goal is for *T* cells to detect foreign and potentially dangerous pathogens and respond adequately, ignoring harmless substances and their own body cells. This can be done by only enabling cells that distinguish between self and non-self cells. Different variations

of NSA have been proposed [5]. The algorithm generically consists of 3 main steps: (a) Immature *T* cells with various antigen receptors are produced in the bone marrow and migrate to the thymus; (b) In the thymus, *T* cells that recognize self-antigens undergo a programmed cell death process. On the other hand, *T* cells that do not recognize any self-antigen are allowed to live; (c) Mature *T* cells that do not recognize self-antigens are now used to recognize any non-self antigen invading the body, such as virus and bacteria.

Artificial Immune Network Models (AIN) [58,59] Jerne [60] proposed the immune network theory, also known as idiotypic network theory, in 1974, which suggests that the immune system maintains an idiotypic network of interconnected B cells for antigen recognition and immunological memory. An idiotype is a group of antibodies that share a common characteristic. This algorithm investigates the interconnectivity of different immune cells, i.e., cell populations linked over successive generations, to stimulate or suppress immune responses. The Artificial Immune Network algorithm (aiNet) [61] is a well-known approach inspired by the AIN. In this technique, antibodies stimulate and suppress each other to stabilize the network and the memory. An idiotype is stimulated when the antibodies from the group bind to idiotopes of other groups of antibodies. This results in the increase of the concentration of antibodies from the idiotype, and the concentration of antibodies from the recognized group decreases, leading to the stimulation or suppression of a given immune response.

Clonal Selection Algorithms (CSA) [62] The clonal selection theory tries to explain how B and *T* cells improve their response in the presence of antigens based on the antigen–antibody affinity. This affinity is based on the binding level between a B cell and an antigen. When a B cell is activated by the presence of an antigen, the B cell matures into plasma cells and secretes antibodies. The created antibodies with higher affinities are cloned, and a mutation process differentiates the clones. If the new antibodies react to self cells, then they are eliminated. In these situations, the concentration of B cells with an improved affinity builds up. Some B cells are retained as memory cells to make a more effective immune response to antigens encountered previously. The created antibodies bind to antigens to tag and inactivate them. A well know technique of CSA is the CLONal selection ALGorithm (CLONALG) [62,63]. Other theories were proposed, such as Artificial Immune Recognition System (AIRS) [64] and The B-Cell Algorithm (BCA) [65]. Haktanirlar Ulutas et al. [66] summarizes the basic features of the CSA and its variants and reviews the corresponding application areas.

Danger Theory (DT) [67] Matzinger [68] explains how an immune response is initiated. She states that, contrary to the previous theories, the 'foreignness' of a pathogen is not the important feature that triggers a response, and 'selfness' is no guarantee of tolerance. The immune response is initiated by a co-stimulatory signal from specific Dendritic Cells (DCs). Injured cells, such as those exposed to pathogens, emit danger/alarm signals that activate DCs. These signals should not be emitted by healthy cells or cells undergoing normal physiological death. Once activated, they provide a co-stimulatory signal to exhibit an immune response in the danger zone around the injured cell. The most notorious DT-based algorithm is the Dendritic Cell Algorithm (DCA) [69], which captures the function of DCs [70], first identified by Steinman and Cohn [71]. In the tissue, when antigens stimulate DCs, they mature and differentiate accordingly to the specific danger context collected. The level of maturation of a DC is facilitated by the detection of signals within the tissue, namely danger signals (caused by damage to tissue cells), pathogenic associated molecular patterns (pre-defines bacterial signatures), safe signals (caused by regulated cell deaths) and inflammatory signals (general tissue distress). After maturing, DCs migrate to local lymphoid nodes, where they stimulate or tolerate an immune response according to the danger context.

2.3.3. AIS applications

Considering the nature of AIS techniques, they have already proven to be suitable for solving real-world problems in computer science and engineering. They can be found in different fields, such as machine learning, pattern recognition and classification, computer virus detection, anomaly detection, optimization, robotics, etc. Aldhaheri et al. [72] proposes six different properties of the AIS approaches:

1. **Adaptive** [*AD*]: has the ability to learn over time and develop adaptive behaviours.
2. **Robust** [*RO*]: has the ability to process under imprecise and uncertain data circumstances.
3. **Resiliency** [*RES*]: the immune system created with a bottom-up approach of Agent based paradigm, to realize dynamic, heterogeneous and distributed environment.
4. **Self-tolerance** [*ST*]: has the ability to prevent the response to self against a particular antigen.
5. **Lightweight** [*LH*]: has the ability to process with low computational complexity.
6. **Distributed** [*DS*]: has the ability to process in a distributed manner not centralized.

This SLR focuses on the collection and analysis of AIS applications in AMS scenarios. Some non-industrial scenario applications are described next. Since detecting anomalies in computer systems greatly resembles the BIS's functionality, most AIS techniques applications are found in computer security, namely virus detection, network security and intrusion/anomaly detection systems. Greensmith et al. [73] used the DT concept, namely the DCA, to develop an Intrusion Detection System (IDS). The authors assessed the IDS in the port scan detection problem. Later, the same DCA technique was applied in the bot detection problem [74], online break-in fraud for an Online Video on Demand System [75] and Deny of Service Detection Problem in IEEE 802.11 Networks [76]. More recently, Alsulami and Zein-Sabatto [77,78] applied AIS techniques, namely the NSA, to CPS in the Aviation industry to detect false data injection and sensor spoofing attacks.

The second great AIS application field is regarding optimization problems. Cayzer and Aickelin [79] presents an AIS approach applied to the task of film recommendation. Zand et al. [80] demonstrates how the CSA can be used to solve the File Transfer Scheduling optimization problem. A traffic signal control system was developed based on AIS to supervise an isolated intersection and build a regulation strategy as soon as a disturbance (such as congestion or an accident) is detected [81]. Also, Chen and Zhang [82] presented an AIS approach for scheduling wireless access networks in a 5G message service system.

Other proposals are more related to machine learning, pattern recognition and classification problems. Takeda et al. [83] proposes a biometric personal authentication method using the CSA as a classifier training method. Xu et al. [84] used AIS for GPS data processing to solve the nonlinear models and avoid the ill-conditions (single-frequency precise point positioning). Finally, in wireless multimedia sensor networks, AIS was used for energy-efficient, distributed and collaborative image pattern recognition on camera sensors [85].

2.4. Comparison of the related work

To emphasize the need for this SLR, this section explores the previous literature review of both AMS and AIS approaches. Table 1 present a comparison of the related work.

Regarding AMS, there are some review-type articles investigating different perspectives of I4.0 already published. Zhong et al. [94] provide a survey of I4.0-related worldwide movements and governmental

Table 1
Comparison of the related work.

Work	Year	Study type	AMS	Self-*	AIS	Purpose
Timmis [86]	2007	Position	✗	✗	✓	Immune models
Shafi and Abbass [87]	2007	Survey	✗	✓	✓	Bio-inspired IDS
Timmis et al. [88]	2008	Survey	✗	✗	✓	Immune models
Zheng et al. [89]	2010	Survey	✗	✗	✓	AIS applications
Dasgupta et al. [5]	2011	Survey	✗	✗	✓	Immune models
Haktanirlar Ulutas et al. [66]	2011	Literature review	✗	✗	✓	CSA
Muhamad and Deris [90]	2013	Survey	✓	✗	✓	AIS in job-shop scheduling
Bayar et al. [91]	2015	Survey	✗	✗	✓	AIS in FDDR
Bere and Muyingi [92]	2015	Survey	✓	✗	✓	AIS for ICS security
Raza and Fernandez [93]	2015	Literature review	✓	✗	✓	AIS in robotics
Zhong et al. [94]	2017	Literature review	✓	✗	✗	Generic I4.0
Oztemel and Gursev [1]	2018	Literature review	✓	✗	✗	Generic I4.0
Qu et al. [3]	2019	Survey	✓	✓	✗	Smart manufacturing
Aldhaheri et al. [72]	2020	SLR	✗	✗	✓	AIS for IoT security
Al-Khatib and Doush [95]	2020	Survey	✗	✗	✓	AIS applications
Peres et al. [6]	2020	SLR	✓	✓	✗	AI in I4.0
Radanliev et al. [96]	2020	SLR	✓	✓	✗	AI in CPS
Stock et al. [2]	2020	Survey	✓	✓	✗	Self-* CPS
Alrubayyi et al. [97]	2021	Survey	✗	✗	✓	AIS for IoT security
This study	2022	SLR	✓	✓	✓	AIS in AMS

strategies while describing associated topics and critical technologies, such as the IoT, CPS, Cloud Computing, Big Data and ICT, which are used to enable AMS. This survey was performed at a time when the I4.0 concept was still very immature. Later, Oztemel and Gursev [1] provide a comprehensive review of I4.0 and related technologies by defining clearly the concept and providing a taxonomy of I4.0, which can be used to support the implementation of I4.0 design principles. Also, Qu et al. [3] present a comprehensive study of the recent trend of Smart Manufacturing Systems (SMS), which represent an AMS that explores data-driven decision making, collaborative intelligence and system autonomy. The authors summarize the evolution, definition, objectives, functional requirements, business requirements, technical requirements, and components of SMS. More recently, Stock et al. [2] discuss how modern IT architectures and infrastructure for industrial CPS can enable their inherent Self-* capabilities to pave the road towards higher levels of autonomy facilitated by data-driven technologies.

Considering AMS-related SLRs, Peres et al. [6] present a systematic review of current Industrial AI literature, focusing on its application in real-world manufacturing environments. On the other hand, Radanliev et al. [96] provide a literature review of current and future challenges in using AI in CPS, and present a new conceptual framework for analysing the evolution of AI decision-making in these type of systems.

Moreover, thus far, several review-type articles deserve attention in the AIS field. To review available immune models and related inspired methods, Timmis [86] survey the current state of the AIS approaches and reflect on the field roadblocks for future development. In this work, Timmis et al. [88] analyse AIS in a broader context of interdisciplinary research, based on an established conceptual framework that encapsulates mathematical and computational modelling of immunology, abstraction and then the development of engineered systems. Finally, Dasgupta et al. [5] survey the significant works in the AIS field and, in particular, it explores up-to-date advances in applied AIS during the last few years.

Other proposals focus specifically on AIS application scenarios. Zheng et al. [89] review immune applications of the AIS approach and propose several suggestions to the AIS community that can be undertaken to help move the area forward. On the other hand, Haktanirlar Ulutas et al. [66] presents a literature review of the CSA, its variants (basic and hybrid approaches), and the main applications. More recently, Al-Khatib and Doush [95] extensively summarize research of AIS and categorize them based on the application problem to understand the current trend of the usage of this category of algorithms.

Related to the security field, there are several AIS review papers. Shafi and Abbass [87] survey some key work in the Complex Adaptive Systems field, with the primary focus on biologically-inspired adaptive approaches, including AIS, to the Network Intrusion Detection problem. Bayar et al. [91] provide a survey on biological immunity and highlight the main concepts and mechanisms that are particularly relevant to fault detection, diagnosis and recovery (FDDR) problems. More recently, Aldhaheri et al. [72] and Alrubayyi et al. [97] present an SLR and a survey with a comprehensive study of empirical research on AIS approaches to secure IoT environments. Moreover, and also related to AMS, Bere and Muyingi [92] presents an analysis of AIS solutions to secure Industrial Control Systems (ICS) from persistent threats. Finally, Muhamad and Deris [90] review the production scheduling problems, focusing on ways AIS can be used to solve job-shop and flexible job-shop scheduling problems. On the other hand, Raza and Fernandez [93] present a detailed review of immuno-inspired robotic applications.

To the best of our knowledge, none of the previously identified reviews formed insights into applying AIS approaches in AMS. Generally, we find studies focusing only on the AMS domain or the AIS domain. Some AMS-domain reviews also address autonomy in industrial systems (Self-*), but do not include directly in the study AIS applications. On the other hand, AIS-domain reviews have the purpose of surveying the main immune models or specific AIS applications. However, these application scenarios are not related to the industry.

Nevertheless, we encountered three reviews similar reviews, which merge both AIS and AMS domains [90,92,93]. However, these reviews are limited to specific application contexts and/or research categories, such as ICT security, job-shop scheduling and robotics. Thus, there is a need for this systematic review. The main contribution is a comprehensive study of AIS models applied to different application contexts and research categories within AMS. This will provide readers with a complete understanding of the role of AIS in industrial scenarios.

3. SLR methodology

An SLR was conducted following the guidelines outlined in the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) statement. The PRISMA flow chart reporting the different phases of the systematic review is shown in Fig. 2.

In the *Identification* stage, a search string was constructed based on the core concepts associated with AIS and AMS. Two groups of keywords were defined, and at least one element of each of the groups was present in the search string, using a combination of OR and AND operators. More detail about the groups of keywords can be found in Appendix A. The search string was then adapted to each electronic database included in this study. In this case, they were:

- IEEE Xplore

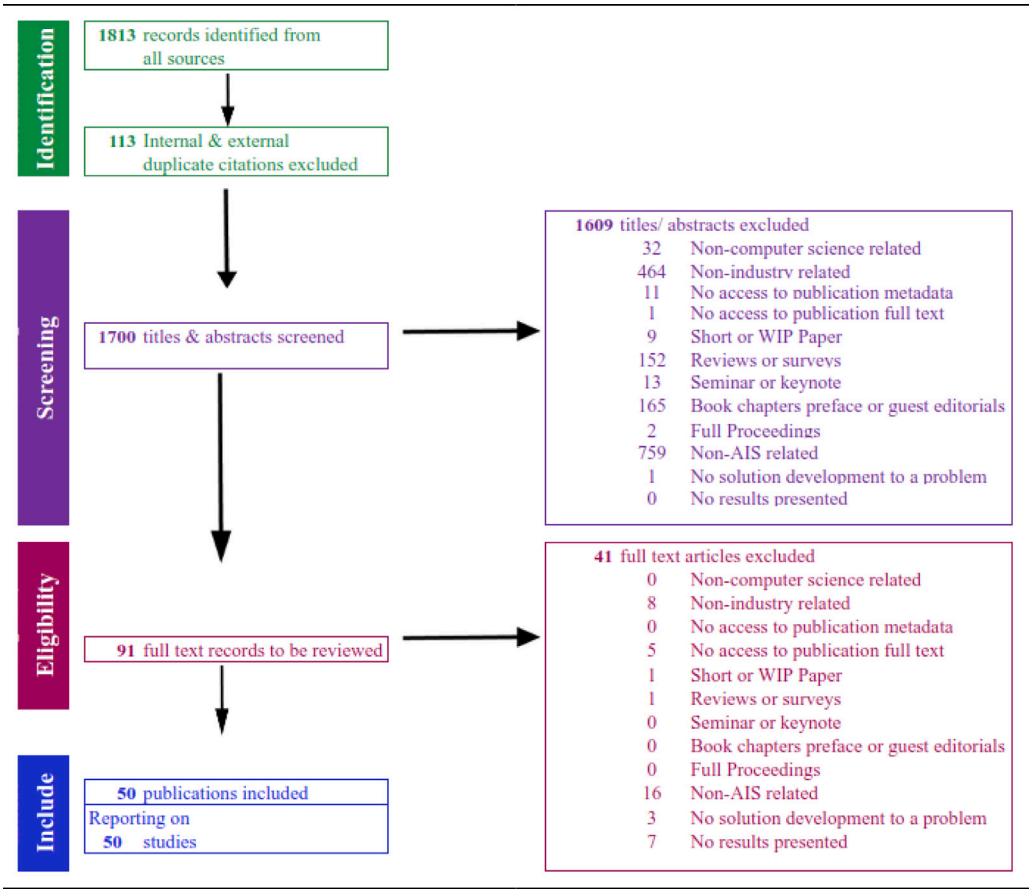

Fig. 2. PRISMA flowchart of study inclusions and exclusions for the SLR.

- Elsevier Scopus
- Elsevier ScienceDirect
- Springer
- ACM Digital Library
- Engineering Village (Inspec & Knovel)
- ISI Web of Knowledge

More information regarding the search strategy, i.e., the electronic database search strings used, can be found in Appendix B. The search was conducted between July and October 2021 and then updated in July 2022. In both phases, it included academic research that: (i) contained at least one term from each group (see Appendix A) in either the abstract, title or keywords; (ii) published in peer-reviewed journals, conference proceedings or book chapters; (iii) written in the English language.

In the *Screening* stage, the records that resulted from the search were aggregated, and the duplicated work was removed. Next, one independent reviewer carried out a screening process, following the criteria represented in Fig. 2 and Appendix C. First, the screening process was performed based only on the publication metadata, i.e., title, abstract and keywords. Next, in the *Eligibility* stage, all remaining articles from the initial screening had their full text analysed in further detail, based on the eligibility criteria represented in Fig. 2 and Appendix C. Finally, in the *Include* stage, each of the articles eligible to be included in the study, considering the screening results, were analysed based on the research questions defined in Section 1.

4. Characterization of AIS applications in AMS

In this section, the results of the literature review are analysed according to the research questions defined previously in Section 1. The research questions are:

RQ 1. What is the research trend of AIS applications in AMS?
RQ 2. What is the status of AIS applications in AMS?
RQ 3. What are the main motivations for using AIS in AMS?
RQ 4. What are the research gaps and future areas within AMS based on AIS solutions?

Following the PRISMA guidelines and the steps described in Section 3, a total of 1813 items were identified from database searches. Of those, 113 internal & external duplicate items were excluded, resulting in 1700 unique records. Those 1700 items were screened based on the exclusion criteria represented in Fig. 2 and Appendix C. While screening only titles/abstracts, 1609 items were excluded, resulting in 91 full-text records to be reviewed. After the full-text screening, 41 items were excluded, resulting in 50 publications included in this study. Table 2 summarizes the findings from this assessment, extracting from each included publication the critical information required to address the research questions defined previously.

4.1. Research trends

This section tries to answer the *RQ 1. What is the research trend of AIS applications in AMS?* by presenting the analysis results of the papers included in the SLR regarding year-wise publications, contributions by publishers, high-contributing authors, contributions by country, keywords statistics, contributions per research category, application context and immune model.

4.1.1. Year-wise publication analysis

In order to achieve a general view of the literature work analysed, we mapped the publications based on a year-wise analysis, as represented in Fig. 3.

Table 2
Overview of publications included in the SLR.

ID	Authors	Application context	Research category	TRL	LOA	Algorithms
P01	Pinto et al. [98]	Manufacturing	Intrusion Detection	3–4	0	DT
P02	Rocha et al. [99]	Manufacturing	Autonomic Systems	3–4	3	NSA CSA; AIN
P03	Lokesh and Kumaraswamy [100]	CPS	Anomaly Detection	3–4	0	DT
P04	Xu et al. [101]	Robotics	Operations Research	4–5	4	CSA
P05	Igbe et al. [102]	Electric Power Industry	Intrusion Detection	3–4	0	DT
P06	Samigulina and Samigulina [103]	SCADA/ICS	Control Systems	–	–	CSA
P07	Lokesh et al. [104]	CPS	Autonomic Systems	3–4	0	Ensemble
P08	Lokesh and Kumaraswamy [105]	CPS	Autonomic Systems	3–4	0	Ensemble
P09	Lima et al. [106]	Electric Power Industry	Anomaly Detection	3–4	2	NSA
P10	Li and Cai [107]	Manufacturing	Operations Research	5–6	3	Ensemble
P11	Lima et al. [108]	Electric Power Industry	Fault Diagnosis	3–4	2	NSA
P12	Ieao et al. [109]	Electric Power Industry	Anomaly Detection	4–5	2	CSA
P13	Ko et al. [110]	Robotics	Control Systems	5	4	Immune inspired
P14	Rammig et al. [111]	CPS	Autonomic Systems	3–4	3	DT
P15	Degeler et al. [112]	Robotics	Intrusion Detection	3–4	2	Ensemble
P16	Pinto et al. [113]	Manufacturing	Intrusion Detection	3–4	0	DT
P17	Clotet et al. [114]	Manufacturing	Intrusion Detection	4–5	0	NSA
P18	Guerrero et al. [115]	Electric Power Industry	Control Systems	3–4	3	CSA
P19	Guo and Yang [116]	Manufacturing	Anomaly Detection	5–6	1	Ensemble
P20	Semwal and Nair [117]	CPS	Operations Research	4–5	3–4	Ensemble
P21	Zhu et al. [118]	CPS	Fault Diagnosis	4–5	1–2	Ensemble
P22	Zhao et al. [119]	SCADA/ICS	Fault Diagnosis	4–5	1–2	Ensemble
P23	Kim [120]	SCADA/ICS	Control Systems	3–4	3	AIN
P24	Li et al. [121]	Electric Power Industry	Autonomic Systems	3–4	3	Immune inspired
P25	Aghaebrahimi et al. [122]	Electric Power Industry	Operations Research	4–5	2	CSA
P26	Lizondo et al. [123]	Electric Power Industry	Control Systems	3–4	3	AIN
P27	Kayama et al. [124]	SCADA/ICS	Fault Diagnosis	3–4	2	Ensemble
P28	Wang et al. [125]	SCADA/ICS	Control Systems	3–4	3	AIN
P29	Jun et al. [126]	Robotics	Control Systems	3–4	4	AIN
P30	Jin et al. [127]	Electric Power Industry	Control Systems	3–4	3	Immune inspired
P31	Huang [128]	Robotics	Control Systems	5	4	Ensemble
P32	Lau and Wong [129]	Robotics	Control Systems	3–4	4	Immune inspired
P33	Xiaobo and Guoqing [130]	Electric Power Industry	Operations Research	4–5	2	Ensemble
P34	Lee and Sim [131]	Robotics	Control Systems	3–4	4	Ensemble
P35	Lau and Ng [132]	Robotics	Control Systems	3–4	4	CSA
P36	Yin [133]	Electric Power Industry	Islanding Detection	3–4	1	Immune inspired
P37	Bhuvaneswari et al. [134]	Electric Power Industry	Control Systems	3–4	3	CSA
P38	Yuan et al. [135]	Electric Power Industry	Operations Research	3–4	1–2	Immune inspired
P39	Lau and Wong [136]	Robotics	Control Systems	3–4	4	Immune inspired
P40	Michelan and Von Zuben [137]	Robotics	Control Systems	3–4	4	AIN
P41	Hanumantha Rao and Sivanagaraju [138]	Electric Power Industry	Operations Research	3–4	2	CSA
P42	Gao and Luo [139]	Robotics	Operations Research	3–4	3–4	AIN
P43	Sun et al. [140]	Robotics	Control Systems	3–4	4	Ensemble
P44	Rimal and Belkacemi [141]	Electric Power Industry	Control Systems	3–4	3	Immune inspired
P45	Diez-Olivan et al. [142]	CPS	Anomaly Detection	4–5	0	Ensemble
P46	Khoie et al. [143]	SCADA/ICS	Control Systems	3–4	3	Ensemble
P47	Pinto et al. [56]	CPS	Anomaly Detection	3–4	0	Ensemble
P48	Pinto et al. [144]	CPS	Intrusion Detection	4–5	0	DT
P49	Kim et al. [145]	Manufacturing	Anomaly Detection	3–4	0	Ensemble
P50	Outa et al. [146]	Manufacturing	Fault Diagnosis	4–5	0	NSA

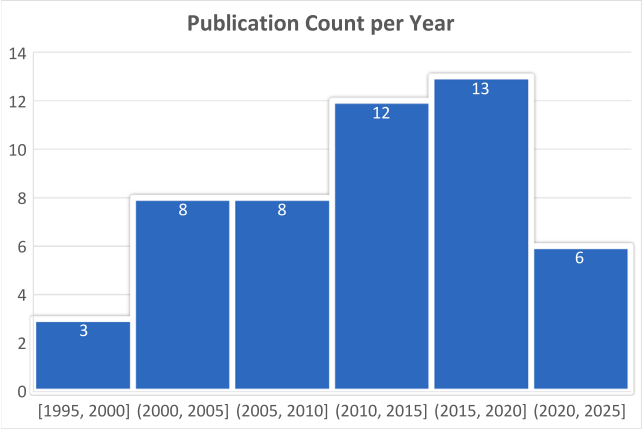

Fig. 3. Year-wise publications.

The analysis shows a stable trend of published papers between 2000 and 2010, while there was an increasing number of publications after 2010 throughout recent years, especially in the range from 2015 and 2020. Between 1995 and 2010, there was a mean of 1 publication per year, while from 2010 forward, until 2022, there was a mean of 3 publications per year. The AIS research field emerged in the '90s, so it is natural to find studies in the area since 1995. The academic community was more active after 2010 because the emergence of the Industry 4.0 happened in 2011 and other national initiatives in the following years. This implies that the topic of AIS applications in AMS is attracting more and more attention from the academic community.

4.1.2. Contributions from publishers

Fig. 4 presents the distribution of contributions from different publishers. The Institute of Electrical and Electronics Engineers (IEEE) is the most contributing publisher, with a 66% share. This can be explained since IEEE is currently one of the largest associations of technical professionals in electrical and electronic engineering, telecommunications, computer engineering and similar disciplines. Next, we can find Elsevier (14%) and Springer (10%) since they publish several articles in multiple journals and conferences in engineering-related fields

Table 3
Journals encompassed in the study.

Journal	SCImago classification
Journal of Intelligent Manufacturing	Q1
IEEE Transactions on Industrial Informatics	Q1
Electric Power Systems Research	Q1
IET Generation, Transmission & Distribution	Q1
IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans	Q1
IEEE Transactions on Industrial Electronics	Q1
Industrial & Engineering Chemistry Research	Q1
Journal of Loss Prevention in the Process Industries	Q1
Computers in Industry	Q1
Cybersecurity	Q1
Applied Soft Computing	Q1
Electric Power Systems Research	Q1
International Journal of Critical Infrastructure Protection	Q2
Algorithms	Q2
Lecture Notes in Networks and Systems	Q4
Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering	Q4
Acta Scientiarum. Technology	Q4

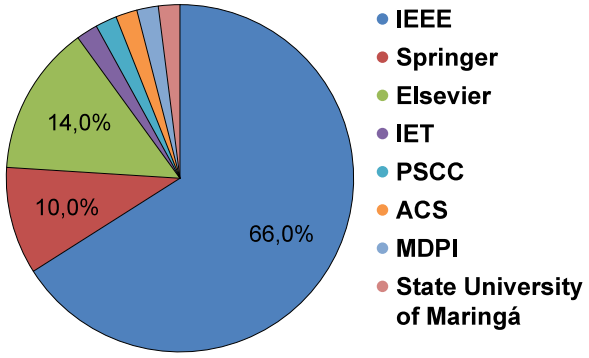

Fig. 4. Contributions from publishers.

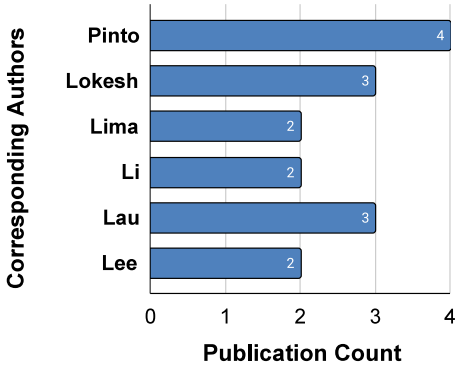

Fig. 5. Contributing authors.

every year. Out of the top three, we can find contributions published in the Institution of Engineering and Technology (IET), Power Systems Computation Conference (PSCC), American Chemical Society (ACS), and the State University of Maringá.

To ensure a comprehensive collection and analysis of publications while understanding the article publication trend, both journal and proceedings articles were considered. In this case, 62% of the paper were published in conference proceedings, while 38% were published in scientific journals. Considering the journals, according to SCImago, 73.6% are classified as Q1, 10.5% Q2 and 15.8% Q4. Table 3 presents the journals considered and the SCImago classification. On the other hand, conferences are rated using the H-Index metric, according to SCImago, ranging from 2 to 71.

4.1.3. Affiliation-wise publication analysis

Fig. 5 presents the top contributing authors. The analysis consider only two or more publications where the author is the corresponding author. In this case, the most contributing author is *Pinto*, with 4 publications. The other top contributing authors are *Lokesh* and *Lau*, with 3 publications each, and *Lima*, *Li* and *Lee* with 2 publications each.

On the other hand, considering authors' contributions by country, the analysis shows that the top five contributing countries are China (40 authors), Brazil (19 authors), Portugal (16 authors) India (14 authors), and South Korea (12 authors), as represented in Fig. 6.

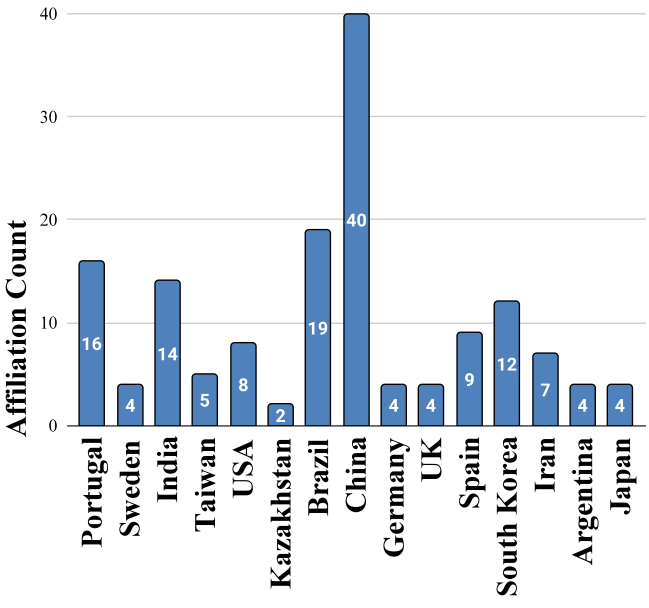

Fig. 6. Contributions by country.

4.1.4. Frequent keywords analysis

Keywords are used to classify the related literature. Fig. 7 represents the distribution of top-rated keywords used in the selected publications. Based on the keyword analysis, the top five frequent keyword encountered in the publications included in this study are *Artificial Immune Systems* (20.6%), *Distributed Control* (9.9%), *Multi-Agent Systems* (9%), *Cyber–Physical Systems* (9%) and *Robot Systems* (6.6%).

4.2. Research fields

This section tries to answer the *RQ 2. What is the status of AIS applications in AMS?* by collecting and analysing data, such as the main research categories and application areas found in selected papers, as

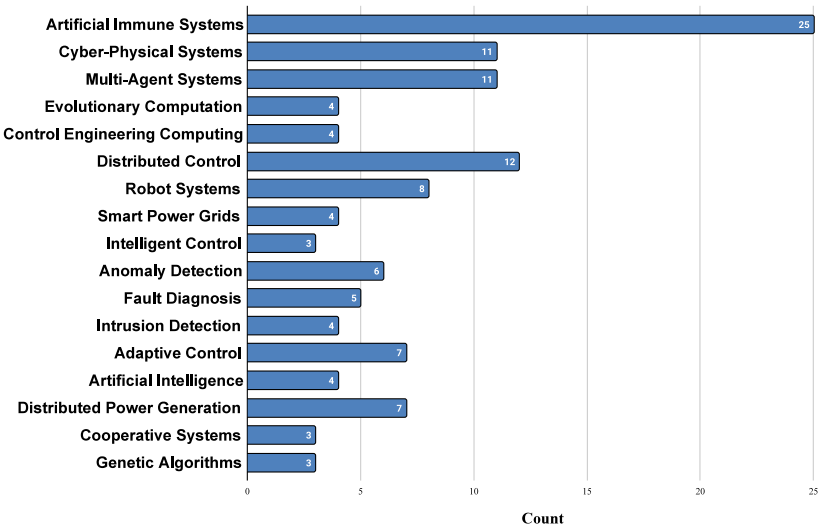

Fig. 7. Frequently used keywords.

well as the work TRL and LOA introduced by the immune model to the system.

Every paper selected in this SLR identifies a problem on a specific research field and proposes a solution based on immune mechanisms. This solution is also developed and/or validated in a given application scenario. Thus, each paper was further categorized based on the research field, application area and immune mechanisms, as shown in Fig. 8. The characterization matrix displays data relationships between research areas and application fields. These relationships consist mainly in immune-based approaches. The research areas considered in the selected papers are *Autonomic Systems*, *Control Systems*, *Islanding*, *IDS*, *Anomaly Detection*, *Fault Diagnosis* and *Operations Research*. On the other hand, the solutions application fields are *Electric Power Industry*, *SCADA/ICS*, *Manufacturing*, *Robotics* and *CPPS*. Finally, each solution can be categorized based on the immune model used, i.e., *DT*, *CSA*, *NSA*, *AIN*, *Immune Inspired* or *Ensemble*.

By inspecting Fig. 8 regarding the overall categorization of the five application fields, it is possible to conclude that more attention has been paid to the Electrical Power Industry (30% share) in comparison to the other application areas. Selected research in this field includes network communication protocol in Smart Grids, electrical distribution systems, Distribution Management Systems (DMS), Distributed Generation (DG), power optimization and management. This is followed by studies in the Robotics field (24% share), which includes mobile robots, Autonomous Guided Vehicles (AGVs), robot manipulators and distributed multi-robot systems. The third place belongs to the CPS field (18% share), which includes different problems in cyber–physical processes. Next, with a share of 16% and 12% are the Manufacturing and Supervisory Control and Data Acquisition (SCADA) fields, which include problems primarily at the industrial process level and control.

On the other hand, there are seven research categories tackled by the different contributions by inspecting Fig. 8 regarding the overall categorization of the research fields. Most of the AIS applications were used to develop Control Systems (38% share), such as overall distributed and cooperative system control and Proportional Integral Derivative (PID) controller tuning. Next, several topics within Operations Research (16% share) are addressed, such as meta-heuristic, optimization, planning and scheduling. Anomaly/Intrusion Detection (14% and 12% share) and Fault Diagnosis (10% share) are very similar research categories since they all rely on similar solutions to detect and analyse system attacks and/or failures. These can be used for system state awareness, online diagnosis, and prognosis. Autonomic Systems (10.% share) refer to the introduction of Self-* properties in industrial systems (as discussed in Section 2.2). Finally, Islanding Detection presents a 2% share only in the Electrical Power Industry.

Finally, inspecting the actual immune mechanisms used to develop solutions in these different research categories and application areas, most of the contributions follow an ensemble method (32.7%), which consists in using multiple learning algorithms to obtain better performance when compared with the learning algorithms alone. In this case, the ensemble methods can be a combination of two or more different AIS techniques or with other Machine Learning or bio-inspired techniques. The four main immune inspired mechanisms are used (both basic or variants), namely Clonal Selection (CSA) - 17.3%, Immune Network (AIN) - 13.5%, Danger Theory (DT) - 11.5% and Negative Selection (NSA) - 9.6%. Finally, there are several immune-inspired solutions (15.4%), i.e., solutions that follow one or more immune principles but do not follow exactly the general guidelines of a specific immune model.

4.2.1. Autonomic systems

As mentioned before, Autonomic Systems refer to the introduction of Self-* properties in industrial systems (as discussed in Section 2.2). The main applications areas found are CPS, Electric Power Industry and Manufacturing. Overall, all the proposals were validated with datasets for proof of concept, or small lab testbeds, achieving a TRL of 3–4. On the other hand, the LOA of most proposals (dataset validated) is 0 since the proposed solution is demonstrated in a simulated dataset (no system autonomy achieved). Considering the work validated on testbeds, it is possible to find LOA of 3, i.e., despite the predominant pre-programmed functionality, the system is capable of self-adjusting its own behaviour (within specific boundaries) considering the perceived environment state.

Regarding the CPS application area, Rammig et al. [111] (P14) proposed an online model checking technique that can be applied to identify needs and adapt the currently running software system proactively. In this case, a DT-based approach is used for continuous system supervision. This way, achieving a lightweight solution for Self-adaptation in Real-Time Operating Systems (RTOS) is possible. The proposed solution is demonstrated in a paravirtualization context (virtual machines) and tested in an abstracted emulation framework. On the other hand, Lokesh et al. [104] (P07) propose a MAS-CPS model-based integrated with an ensemble immune model (combination of DT and AIN). This model introduces resiliency and self-adaptation to the system by enabling state awareness, self-tolerance and self-healing. The proposed solution is demonstrated as a generic framework and applied to a simulated dataset containing data from several CPS layers, such as monitor & actuator, communication and computation & control. The authors propose a similar solution to the same problem [105]

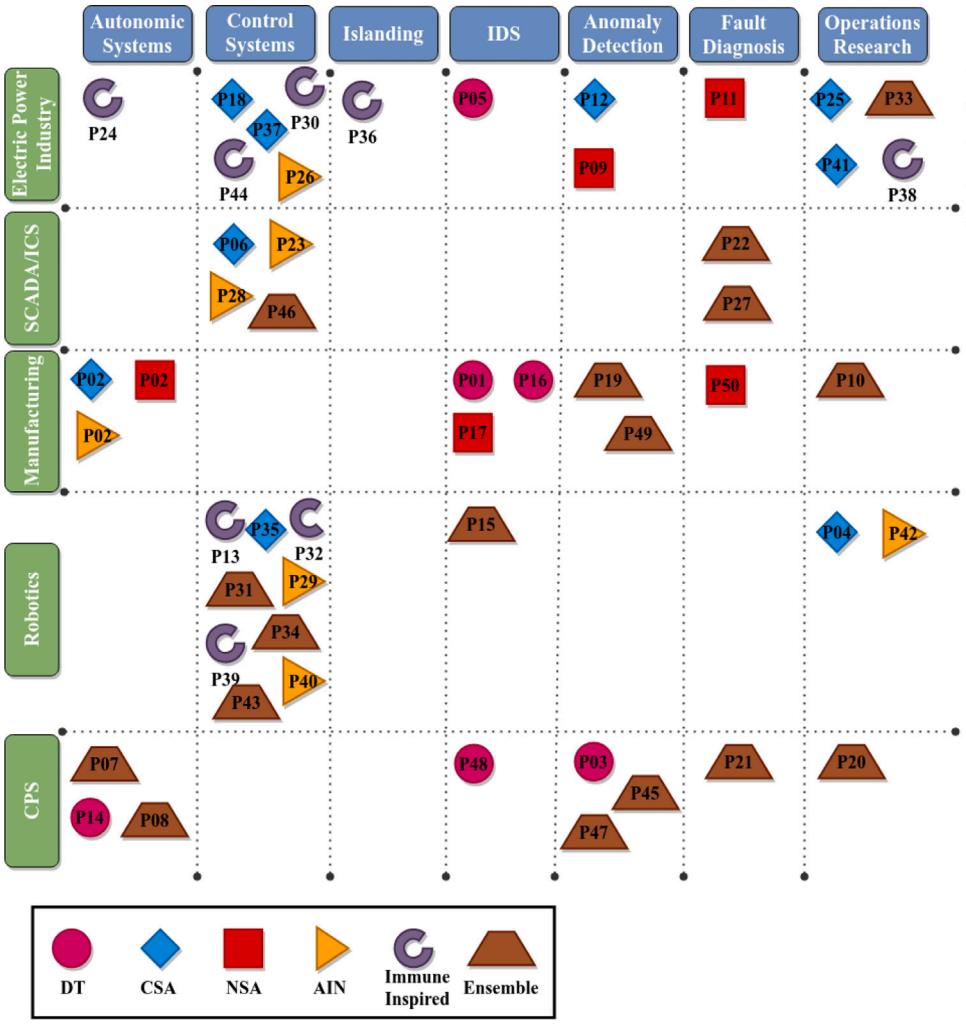

Fig. 8. Characterization matrix of the studies selected.

(P08). However, in this case, the ensemble immune model used was a combination of DT and Artificial Immune Recognition System V2 (AIRS2), a technique from the CSA family.

In the Electric Power Industry, Li et al. [121] (P24) address the distribution service restoration problem, in the event of a large-scale blackout in a power distribution network with DGs, by proposing a generic immune-inspired MAS, designated Multi-agent Immune Algorithm (MIA). This solution introduces adaptability, resiliency, Self-tolerance and Self-healing properties to the power system. The solution is demonstrated using a power flow analysis software of a simulated scenario with real-world conditions. More recently, but in the Manufacturing application area, Rocha et al. [99] (P2) studied industrial approaches to distributed machine diagnosis, using a MAS paradigm combined with AIS. For this work, lightweight NSA, AIN and CSA models are developed based on fuzzy logic, enabling distributed system adaptability, resiliency and Self-tolerance. The models were demonstrated and validated in simulation environments.

4.2.2. Control systems

Control systems manage the behaviour of other system devices using control loops. In this case, it can be found mainly in Robotics, SCADA/ICS, and the Electric Power Industry. Overall, most work is validated in lab environments (mostly simulations) for proof of concept, achieving a TRL of 3–4. However, two proposals in the robotics field were validated in real industrial relevant environments, achieving a TRL of 5. Regarding LOA, all robotics-related work achieve an LOA of 4 since the robot system can behave as an adaptive and autonomic system and continuously self-learn within known system boundaries. However, proposals related to SCADA/ICS and Electric Power Industry achieve LOA of 3 since the system can self-adjust its own behaviour. However, a human is responsible for overseeing system decisions.

Robotic immuno-based control systems are very popular. In the early years, Lee and Sim [131], Jun et al. [126] and Sun et al. [140] (P34, P29, P43) were already proposing an ensemble method, combining CSA and AIN and achieving cooperative control in a distributed autonomic robotic system. Based on the MAS paradigm, the proposed solution enables adaptive group control as a swarm strategy, where robots can find and execute tasks that are spread out in the environment. Validation is performed in a simulated environment regarding a collaborative robot search problem. On the other hand, Michelan and Von Zuben [137] (P40) investigates an autonomic control system of a mobile robot based (in this work, non-distributed), using an AIN model. The robot navigates to solve a multi-objective task, namely, garbage collection, while it adapts to environmental conditions to establish a trajectory without colliding with obstacles. The authors used simulation to validate the solution.

Moreover, considering mobile robots, Lau and Wong [129] (P32) present a fully distributed and adaptive control framework, based on generic immune theories, to manage, coordinate and schedule a fleet of agents employed in an AGV system. The framework was validated in a simulation study of an intelligent transport system operated by a fleet of AIS agents in a warehousing environment. Later, the authors presented a mathematical model of the control framework [136] (P39).

On the other hand, Lau and Ng [132] (P35) reports the development of the MAS-based control paradigm, inspired by the CSA, for the distributive trajectory control of a robot manipulator. Authors tried to enable cobot capabilities, such as adaptive, resiliency and robustness. They validated the solution in a MATLAB simulation of the Whole Arm Manipulator (WAM) system, a four degrees-of-freedom robot installed at the Intelligent Systems Laboratory of the University of Hong Kong. Ko et al. [110] (P13) propose a distributed control system, based on the immuno-suppression theory, for a Modular Self-Reconfigurable (MSR) robot arm. The proposed framework, designated General Suppression Framework, is adaptive, resilient, robust and Self-tolerance since it enables robot modules to generate emergent group behaviours by exhibiting aggressive or tolerant behaviour based on environmental changes. The framework is validated through computer simulation (MATLAB) and in a hardware implementation of a seven-module MSR manipulator. More recently, Huang [128] (P31) proposed an online motion control of four-wheeled redundant Swedish mobile robots by using a fuzzy system incorporated with the Bacterial Foraging Optimization (BFO) metaheuristic technique and AIS, designated FS-PBFOAIS. The solution was validated in an experimental four-wheeled redundant mobile robot, with one FPGA, to self-adjust the polar-space trajectory tracking. Results show Self-tolerance and robustness.

Considering the SCADA/ICS application area, Kim [120] (P23) and Khoie et al. [143] (P46) proposed tuning approaches for PID controllers. The first approach uses AIN to make the system adaptive and Self-tolerant to its external environment while allowing a strong parallel distributed processing network to complete patterns against the environmental situation. The approach is validated in a simulated power plant system. The second approach proposes a Genetic-AIS algorithm using multi-objective optimization for PID tuning. The system was also evaluated via simulation control test scenarios. Moreover, Wang et al. [125] (P28) propose a distributed AIN-based algorithm for complex industrial processes control. The algorithm can learn the control knowledge of different operators and optimize the existing control knowledge in an online fashion. Validation is performed in a simulated environment (a beer fermentation process). More recently, Samigulina and Samigulina [103] (P06) uses the CSA and the MAS paradigm to develop distributed and Self-adaptive complex object control capabilities in Honeywell Distributed Control Systems. However, it is not clear in what conditions solution experimentation and validation were performed.

Finally, there is also some control-related work in the Electric Power Industry. Considering distributed generators, Jin et al. [127] (P30) propose an immune-inspired method for power system damping control in DG systems. The solution was validated in a simulated example of a power system with large-scale integration of distributed generation. On the other hand, Bhuvaneswari et al. [134] (P37) presents the implementation of a MAS distributed control system in a microgrid operation to optimize local DG systems' production. This control system is based on the CSA and is validated in a simulated scenario by mimicking realistic market prices for power and distributed generator bids reflecting realistic operational costs. Rimal and Belkacemi [141] (P44) propose an immune-inspired approach to model the automatic generation control in a two-area power system. The idea is to introduce system adaptability and self-tolerance to reduce the system's mechanical oscillations. The solution was validated in a simulated scenario. More recently, Guerrero et al. [115] (P18) proposed a CSA for optimal real-time solution of the Coordinated Volt/VAr Control (CVVC) problem in distribution networks composed of multiple control equipment. The solution was validated in a simulated scenario, which emulated the interoperability actions commonly established among the main functions of a modern DMS during the real-time operation of a CVVC. Finally, Lizondo et al. [123] (P26) tackles the Peak Load problem in Smart Grid environments by proposing a MAS distributed control system based on AIN. A simulated case (Air Conditioner devices) is used to validate the solution.

4.2.3. Islanding

Islanding Detection is a common research category in the Electrical Power Industry, since it tries to detect islanding situations (a condition in which a distributed generator continues to power a location even though external electrical grid power is no longer present). Yin [133] (P36) proposes a robust immune-inspired approach to detect islanding of DG, based on digital signal processing and harmonic signature recognition. The approach was validated in a simulated grid-connected inverter based on a digital signal processor, achieving a TRL of 3–4 and LOA of 1, i.e., the system may suggest goal-oriented improvements, but a human always approves them in order to take effect.

4.2.4. Anomaly detection

Anomaly Detection is used to identify a system's bad behaviour compared to a predefined intended behaviour, which is considered normal or baseline. The assumption is that anomalies, or faults, are outliers in the dataset, which always differ from the ordinary behaviour of a standard dataset. Anomaly Detection studies can be found in CPS, Manufacturing, and the Electric Power Industry. Overall, TRLs are relatively high when compared to other research areas since it is possible to find several proposals validated and demonstrated in relevant environments. However, some proposals are only validated in lab scenarios (both dataset and simulation). On the other hand, the overall LOA is relatively low. One can find work in the CPS field without achieving system autonomy (LOA = 0). Also, the manufacturing-related proposal achieves an LOA of 1 (system decision-support, while in the Electric Power Industry, it is found presented partial system autonomy (LOA = 2).

Regarding CPS applications, Lokesh and Kumaraswamy [100] (P03) propose a DCA approach for anomaly detection towards CPS state awareness. The main contribution was to model system resiliency using a MAS paradigm on CPS (together with the DCA). Diez-Olivan et al. [142] (P45) tackles industrial prognosis, i.e., the prediction of failures of an industrial asset, by proposing an adaptive learning approach based on an ensemble method (DCA for drift detection and a Deep Neural Network — DNN that dynamically adapts to new operational conditions). The solution is validated in a dataset containing operational data from an experimental benchmark comprising a real-world industrial problem. Finally, Pinto et al. [56] (P47) propose an ensemble approach, the Cursory Dendritic Cell Algorithm (CDCA), which merges the DCA with a clustering algorithm for flexible monitoring and anomaly detection in industrial processes. The CDCA tackles some DCA original problems, such as manual characterization of signals (using a K-Means approach), and online data analysis and classification. The approach was validated in two industrial-oriented datasets regarding physical and network-related data.

On the other hand, in manufacturing applications, Guo and Yang [116] (P19) proposes an anti-jamming ensemble approach that combines DT with AIN for distributed machine energy leakage diagnosis in complex environments such as parallel-machine job shops. In order to evaluate the proposed approach, several experiments were performed on a tyre vulcanization shop floor in China to diagnose the steam leakage of steam traps. Results show that the lightweight immune approach introduces robustness and Self-tolerance. Moreover, Kim et al. [145] (P49) propose an ensemble approach, merging the NSA with the CSA, to enable a multiclass anomaly detection algorithm. The proposed algorithm was validated using an intelligent maintenance bearing dataset and a vacuum deposition equipment dataset.

In the Electric Power Industry, Ieao et al. [109] (P12) propose an ensemble methodology based on the unconstrained binary programming (UBP) model and the CSA to estimate fault sections in electric power systems. The proposed methodology is tested in a simulated environment, using part of the South-Brazilian electric power system. On the other hand, mainly used in Smart Grid environments, Lima et al. [106] (P09) propose a method of using a voltage and current abnormality detector filter in electrical distribution systems based on the NSA. The solution was validated in two simulated distribution systems.

4.2.5. Intrusion detection system

An IDS is a malicious activity monitoring software application. The goal of an IDS is to detect intrusions by collecting and analysing data. A generic IDS collects and analyses system data and then responds to the results. The analysis, in this case, is performed using AIS methods. Also, the approach to the detection analysis is anomaly-based (Anomaly-IDS). This way, it is possible to say that intrusion detection, in this context, is a sub-category of anomaly detection, where the anomalies are triggered by malicious activity, such as cyber and physical attacks on the system. IDS are used in Manufacturing, CPS, Robotics, and the Electric Power Industry. Overall, most of the proposals were validated with datasets for proof of concept, or small lab testbeds (sometimes data collected from real industrial scenarios), achieving a TRL of 3–4 and 4–5. On the other hand, the LOA of most proposals (dataset validated) is 0 since no system autonomy was achieved. Considering the work validated on lab testbeds (in the robot field), it is possible to find LOA of 2, i.e., the system is capable of self-adjusting its own behaviour (limited boundaries), but the human retains all decision-making power.

In manufacturing, Pinto et al. [98] (P01) presents an IDS approach based on the deterministic version of the DCA (dDCA). To evaluate the dDCA effectiveness, a testing dataset was generated by implementing and injecting various attacks on an OPC UA-based CPS testbed. The properties introduced by the immune model are adaptive, robustness and Self-tolerance. Later, Pinto et al. [113] (P16) propose the Incremental Dendritic Cell Algorithm (iDCA) for online incremental detection in an unsupervised manner. The iDCA was also validated using datasets. Moreover, Clotet et al. [114] (P17) propose a MAS real-time IDS, based on the NSA, to detect attacks targeting physical components at the industrial process level. The solution was validated using a dataset from a water treatment plant laboratory.

Regarding CPS applications, Pinto et al. [144] propose a Model-based Engineering (MBE) approach to enable security-by-design during the development of CPS, using the IEC 61499 standard. The security features introduced rely on an IDS based on the iDCA. The authors used a CPS testbed to validate the proposed approach. Results show that the solution is very lightweight and can dramatically reduce design and code complexity while improving application maintainability.

In the robotics field, Degeler et al. [112] (P15) propose a DT-based IDS to protect AGVs against cyber-attacks that can cause severe physical damage to the manufacturing system. The solution is validated in a simulated factory floor with a distributed scenario (three AGVs operating simultaneously). Finally, related to the Electric Power Industry, Igbe et al. [102] (P05) propose an IDS in industrial communication scenarios based on the dDCA. In this case, the authors used the DNP3 protocol and proposed a dataset for a Smart Grid scenario to validate the solution.

4.2.6. Fault diagnosis

Fault Diagnosis, or fault isolation, refers to the system monitoring and identifying faults when they occur, and pinpointing the type of fault and its location, along with one or more root causes of problems, to the point where corrective action can be taken. Typically, Fault Diagnosis includes anomaly detection. One can find Fault Diagnosis in Electric Power Industry applications, SCADA/ICS, Manufacturing and CPS. Overall, the LOA is 2, meaning that the proposals introduce partial autonomy to the system, but humans are responsible for the decision-making. On the other hand, one can find work validated in lab scenarios (mostly simulations in SCADA/ICS and Electric Power Industry applications for proof of concept), achieving a TRL of 3–4, and validation in partially relevant environments (SCADA/ICS and CPS), achieving a TRL of 4–5.

On SCADA/IDS applications, Kayama et al. [124] (P27) propose an ensemble (combining AIN with Learning Vector Quantization — LVQ) for distributed detection and diagnosis of faulty sensor outputs in control plants. The solution is validated in a simulation environment (temperature sensors for a heating furnace plant of a hot strip mill line). On the other hand, Zhao et al. [119] (P22) propose an online fault diagnosis system for safety in chemical processes by combining Artificial Neural Networks (ANN) with an immune-inspired model. The solution was developed for a lab-scale distillation process, achieving adaptive, robust and Self-tolerance properties. Moreover, in CPS application scenarios, Zhu et al. [118] (P21) also propose an artificial immune system-based fault diagnosis, designated AISFD, combined with Bayesian estimation, for controlling alarm floods during transitions of chemical processes. A pilot-scale distillation process was used to validate the solution.

On Manufacturing applications, Outa et al. [146] propose the NSA for failure detection during the maintenance of pressure vessels. Detection relies on the recognition of vibration signals. The approach was validated in a small lab testbed that represents the behaviour of the flow of a fluid and the respective vibration of the system. Experimental results show that the approach is robust in precision and signal recognition and for classifying the degree of severity and probability of failure. Finally, regarding Fault Diagnosis in Electric Power Industry, Lima et al. [108] (P11) propose a new approach to detecting and classifying voltage disturbances in electrical distribution systems based on a combination of wavelet transform and NSA. Two distribution systems were simulated to evaluate the proposed method's performance.

4.2.7. Operations research

Operations Research deals with developing and applying advanced analytical methods to improve decision-making in complex problems, where optimal or near-optimal solutions are typically found. In this SLR context, Operations Research can be found in several applications, mainly for optimization and scheduling problems. The AIS model is used as a meta-heuristic method, such as in the Electric Power Industry, Robotics, Manufacturing and CPS. Regarding TRL achievement, one can find good results (TRL = 4–5 or 5–6) since most of the work is validated and demonstrated in real relevant environments. However, some proposals in the Electric Power Industry and Robotics fields were validated in simulation environments for proof of concept (TRL = 3–4). On the other hand, one can find very low and also very high LOA. For example, the maximum LOA found in the Electric Power Industry was 2 since systems present only partial autonomy. In both manufacturing and robotics fields, one can find LOA of 3 and 4 since the system already presents several autonomic capabilities, including most of the decision-making on its own.

In the Electric Power Industry, several optimization types of problems exist. Aghaebrahimi et al. [122] (P25) proposed an optimization approach for solving the DG placement problem. The approach is based on the CSA and validated in Tehran's Khoda-Bande-Loo distribution test feeder. Xiaobo and Guoqing [130] (P33) focused on the distribution network multi-objective planning that takes into account minimizing the investment cost of DG and the power loss of the distribution network. The approach is based on the Particle Swarm Optimization (PSO) combined with immune principles, designated IPSO algorithm. Validation is performed in a distribution network. On the other hand, Hanumantha Rao and Sivanagaraju [138] (P41) investigates the problem of multiple DG unit placement. A CSA-based model is proposed to determine the optimal DG-unit size and location. The solution is validated in a simulated scenario. More recently, Yuan et al. [135] (P38) proposed a multi-objective optimization immune-inspired algorithm to coordinate the parameters of a distributed static synchronous series compensator controller in power grids. The solution is validated in a simulated scenario.

In the manufacturing field, Li and Cai [107] (10) propose an ensemble solution (ANN combined with DT), designated Intelligent Immune System (I^2S), used to achieve optimized sustainability in manufacturing systems. This sustainability optimization refers to optimizing manufacturing lifecycles for global energy consumption reduction, based on adaptive re-scheduling of jobs. The (I^2S) system has been validated

through real-world industrial deployment in some companies in Sweden, the U.K. and Spain. More recently, considering now the CPS field, Semwal and Nair [117] (P20) presented a decentralized mechanism, based on the combination of CSA, AIN and DT, applicable to multiple distributed problems in CPS. Although being developed for CPS, the solution is validated in both emulated (CPS) and real (robot) scenarios. In this case, robots must discover the best path to follow in a real mobile multi-robot system.

Finally, considering the robotics topic, Gao and Luo [139] (P42) proposed an AIN model for efficient cooperative task allocation in a multi-robot system with autonomously distributed architecture. The dynamic allocation method for cooperative robots was demonstrated and analysed in the simulation of emergency handling. On the other hand, Xu et al. [101] (P04) proposed an AIS-fuzzy method (fuzzy systems combined with CSA model) for a hybrid optimization technique in order to accomplish distributed formation control. The System-on-a-programmable-chip (SoPC) methodology is adopted for the solution validation, where each robot is realized as an independent CPS in one FPGA chip.

4.3. AIS conceptualization

This section tries to answer the *RQ 3. What are the main motivations for using AIS in AMS?*, by collecting from the selected papers all the Self-* and specific AIS properties (see more in Sections 2.2 and 2.3.3) introduced by the implemented immune-models. This data is analysed and correlated considering the primary AMS requirements (see more in Section 2.1). This way, it is possible to understand if the desired AMS requirements are met and what the introduced properties that make it possible. Table 4 presents a summary of the AIS conceptualization.

In a previous review work, Oztemel and Gursev [1] presents 12 main goals to achieve I4.0 (see more detail in Section 2.1). From the selected papers in this SLR, the most relevant goals addressed are: *Data Analytics* (25.5%), *Adaptability* (19.4%), *Autonomy* (18.9%), *Optimized Management* (14.3%) and *Process Efficiency & Product Quality* (10.2%). In this context, *Data Analytics* refers to the capability to handle a big amount of data and perform well-defined analyses to manage the system and achieve target goals. This includes a strong system sensorisation for continuous data collection. On the other hand, *Autonomy* and *Adaptability* refer to generating Self-behaving systems (minimum human interaction) and system responsiveness to the changes. These goals are correlated since *Adaptability* is only possible by analysing Big Data. Also, system adaptability is one of the most important properties when trying to reach a Self-behaving system, which is the desired approach to managing complex systems (*Optimized Management*). Finally, *Process Efficiency & Product Quality* refers to the dynamic interaction that may exist between devices involved in the process, in a Machine-to-Machine (M2M) communication scenario (for process optimization) or between equipment and product (for product quality control). This can only be achieved with a strong digitalization component, mainly by enabling MAS architectures.

A Self-behaving system consist of a system that implements one or more Self-* properties, in order to achieve a certain LOA (see more detail in Section 2.2). The top Self-* properties found in the selected papers are *Self-awareness* (35.6%) and *Self-adaptive* (28.1%). Other less popular properties are *Self-healing* (9.6%), *Self-configuration* (8.9%), *Self-optimization* (6.7%), *Self-immunity* (5.9%) and *Self-organizing* (5.2%). All these Self-* properties aim at introducing a certain level of autonomy to the system, which is compliant with the *Autonomy* AMS goal.

Self-awareness refers to the system's awareness of its state and surrounding environmental conditions to adjust and adapt to changes and external actions. The *Self-awareness* property is introduced and motivated by the *Data Analytics* AMS goal since sensor data is always available and continuous system monitoring is possible. On the other hand, *Self-adaptive* refers to a property where the system reacts to environmental changes by changing its internal properties accordingly. This presents a strong synergy with the *Adaptability* AMS goal. Finally, the other Self-* properties refer, in general, to systems that, when facing a set of external actions, can change their configurations and/or system topology to restore or improve their global state. These behaviours are aligned with both *Optimized Management* and *Process Efficiency & Product Quality* AMS goals since the management of complex systems, specially MAS-related, require a high level of adaptation (configuration and settings update) to achieve an optimum global state. The relationship between AIS approaches following MAS architectures is common due to their similarities.

Looking closer to the main AIS properties ((see more detail in Section 2.3.3)) found in all the immune models implemented, one can find in the top-3, *Self-tolerance* (27.7%), *Adaptive* (23.5%) and *Robust* (18.7%). In the BIS, *Self-tolerance* refers to eliminating auto-reactive immune cells, ensuring that the immune system does not attack its own body cells. In engineering scenarios, this property means that the system clearly distinguishes what a normal system behaviour/state/conditions is and what is abnormal while reacting only to the abnormalities. Since human supervision and decision-making are minimum, this property is essential to meet the AMS goal *Autonomy*. On the other hand, the *Adaptive* AIS property refers to continuous learning to develop adaptive behaviours, lining up with the *Adaptability* AMS goal. Finally, the AIS *Robust* property refers to the capability of system operation with data shortage or poor quality. This property is critical to meet the AMS goal *Data Analytics* since the data collection process may be imprecise in certain circumstances.

Based on the analysis, it is safe to say that the primary motivation for using immune models is because they provide flexible decision-making mechanisms for dynamic and complex environments such as AMS. Considering the main AIS properties introduced and the Self-* properties achieved, it is clear that there is a direct cause–effect between the immune models and system autonomy. Most of this autonomy is found in state awareness and adaptability scenarios, which are very aligned with the AMS goals *Autonomy* and *Adaptability*. Also, since immune models provide Self-tolerance and robustness, they are a good match with AMS applications. On the one hand, the desired capability of no human intervention and supervision is only possible if the system decision-making process is reliable by tolerating good conditions and reacting to bad ones. Finally, data analysis results are only as good as the data collected in the first place. So, a robust system operating normally with uncertain data is an advantage for a systematic system monitoring process.

4.4. Research gaps

This section tries to answer to the *RQ 4. What are the research gaps and future areas within AMS based on AIS solutions?*, by analysing the correlated data between Self-* and AIS properties, and AMS goals. Considering Table 4 and continuing with the analysis provided in Section 4.3, it is possible to identify research gaps, in terms of less addressed AMS goals. The AMS requirements with less research work, considering the application of AIS approaches, are *Safety & Security* (6.1%), *Resource Efficiency* (2.6%), *Communication Network Infrastructure* (2%), *Standardization* (1%), *Human Management* (0.5%), *Regulatory Framework* and *Upskilling* (both with 0%).

4.4.1. Safety & security

Safety refers to the absence of threats to human operators, i.e., to the fact that machines, production facilities or products should not pose a danger to people or the environment. On the other hand, Security (IT security or cyber-security) refers to the protection of digital systems, i.e., the system itself needs to be protected against misuse and cyber-attacks.

Most of the approaches that tackle the security topic of this goal are in the IDS and/or anomaly detection research fields, i.e., the problem

Table 4
AIS conceptualization (*STD* = Standardization, *OM* = Optimized Management, *NET* = Communication Network Infrastructure, *SS* = Safety & Security, *HM* = Human Management, *UP* = Upskilling, *RF* = Regulatory Framework, *RE* = Resource Efficiency, *AU* = Autonomy, *PEQ* = Process Efficiency & Product Quality, *DA* = Data Analytics, *AD* = Adaptability | *SAD* = Self-adaptive, *SH* = Self-healing, *SAW* = Self-awareness, = *SI* = Self-immunity, *SOR* = Self-organizing, *SC* = Self-configuration, *SOP* = Self-optimizing | *AD* = Adaptive, *RO* = Robust, *RES* = Resiliency, *ST* = Self-tolerance, *LH* = Lightweight, *DS* = Distributed).

ID	AMS requirements												Self-* properties							AIS properties					
	STD	*OM*	*NET*	*SS*	*HM*	*UP*	*RF*	*RE*	*AU*	*PEQ*	*DA*	*AD*	*SAD*	*SH*	*SAW*	*SI*	*SOR*	*SC*	*SOP*	*AD*	*RO*	*RES*	*ST*	*LH*	*DS*
P01	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗
P02	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓
P03	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗
P04	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓
P05	✓	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗
P06	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✗	✗	✓
P07	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗
P08	✗	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗
P09	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
P10	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗	✗	✓	✗
P11	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✓	✗	✓	✗	✓	✗	✗
P12	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗
P13	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
P14	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗
P15	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	✗	✓
P16	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗
P17	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
P18	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓	✗	✗
P19	✗	✓	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓
P20	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓
P21	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗
P22	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗
P23	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗
P24	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗
P25	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓	✗	✓	✗	✓
P26	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✗	✓	✓	✗	✓
P27	✗	✓	✗	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	✓	✗	✓
P28	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓	✗	✓
P29	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓
P30	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓	✗	✓
P31	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓	✓	✗
P32	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓
P33	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✓	✗	✗
P34	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓
P35	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗
P36	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗
P37	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓	✓	✗	✓	✓	✗	✓
P38	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗
P39	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✓	✗	✓
P40	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	✗	✗
P41	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓	✗	✓	✗	✗
P42	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓
P43	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✓	✗	✓	✗	✗	✓	✗	✓	✓	✗	✓
P44	✗	✓	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✗	✓	✗
P45	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓	✗	✓	✗	✗
P46	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗
P47	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗
P48	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	✓	✗
P49	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗
P50	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗

of protecting a system by detecting attacks against it, usually by using anomaly-based techniques. Pinto et al. [98] (P01), Pinto et al. [113] (P16), Pinto et al. [144] (P48), and Igbe et al. [102] (P05) propose network-based IDS (NIDS), i.e., the detection is performed based on the network data analysis, in order to detect network attacks. On the other hand, Clotet et al. [114] (P17), Degeler et al. [112] (P15) and Pinto et al. [56] (P47) propose host-based IDS (HIDS), i.e., detection focus on attacks targeting physical components at the industrial process level, by analysing host data. Regarding the safe topic of this goal, Yin [133] (P36) proposes a robust immune-inspired approach to detect islanding scenarios that threaten people and the environment.

The tendency to use immune-related approaches for Safety & Security targets the detection instead of classical methods to preserve the integrity of the equipment and assets (data encryption, digital signatures, password authentication, public keys encryption, etc.). An autonomic and adaptive attack/intrusion detection is crucial when considering the complexity of AMS architectures and the global connectivity of shop-floor systems, exposing these types of systems to much more vulnerabilities than the already existing systems. Also, considering the similarities that the BIS functionalities have with the problem of detecting attacks/intrusion in computer systems, AIS has incredible potential to be used for autonomic IDS. However, this research is still in its infancy. More detail about bio-inspired IDS and AIS-related security in AMS enabler technologies, such as IoT and CPS, can be found in previous work [72,87,92,147].

4.4.2. Resource efficiency

Resource utilization efficiency refers to the usage of new materials, new processes, new technologies, and other measures that may improve resource utilization efficiency while reducing and balancing environmental pollution. Some work can be found regarding AIS application for resource utilization efficiency in AMS, especially in Manufacturing and Electric Power Industry application contexts.

In the Manufacturing application area, Li and Cai [107] (10) proposes the I^2S solution to achieve optimized sustainability, i.e., optimization of manufacturing lifecycles for global energy consumption reduction. On the other hand, Guo and Yang [116] (P19) proposes an approach for machine energy leakage diagnosis in complex environments. Considering the resource utilization goal, both proposals tackle the global energy consumption reduction (job re-scheduling or energy leakage detection).

Regarding the Electric Power Industry application area, Bhuvaneswari et al. [134] (P37), and Lizondo et al. [123] (P26) propose control solutions. The first work, the control of a microgrid operation, aims to optimize the power production of local DG systems. The second work proposes a control system to tackle the Peak Load problem. Both proposals focused on energy demand management, which dictates correct resource usage in different periods, such as the size of generators, transmission lines, transformers and circuit breakers. On the other hand, and also related, Xiaobo and Guoqing [130] (P33) focused on planning distribution networks by considering the cost minimization of DGs and the power losses.

Despite the previous work, more research is needed since the industrial sector is still among the top contributors to greenhouse gas emissions worldwide. Developing lean/green approaches will allow manufacturing companies to cut energy costs, enhance process efficiency, and even provide a safer working environment for employees. Also, by introducing immune approaches, it is possible to enable the adaptation of resource usage considering energy consumption. More detail about lean-green manufacturing can be found in previous work [148–150].

4.4.3. Communication network infrastructure

Communication Network Infrastructure refer to the needed infrastructure that enables a higher volume or quality data exchange provided by communication networks. Overall, challenges associated with this goal are related to (i) scalability, (ii) security and (iii) availability. In the AMS context, all industrial assets are connected via the Internet, according to IoT principles. Thus, wireless communication technologies play a significant role since they allow ubiquitous internet access and increased interaction (availability). Also, as the number of networked connected devices increases, the network infrastructure should be scalable. Finally, the increased number of connections opens the surface of harmful cyber-attacks to be deployed in the system (security).

In this SLR, four publications tackled network-related issues, namely NIDS [98,102,113,144] (P01, P16, P05 and P48), focusing only on the security aspects of the network infrastructure. This research work is not enough to impact this AMS goal. Also, other approaches may be needed for the other two challenges.

4.4.4. Standardization

Standardization and open standards for a reference architecture refer to the normalization of cooperation mechanisms and information exchange between system devices. Reference architectures are helpful for the development, integration and operation of the technological innovations introduced to the AMS. A common standardization effort exists in networked devices in a manufacturing system, such as Edge devices, related to the Communication Network Infrastructure AMS goal.

In this SLR, [102] (P16) and [144] (P48) tackle standardization goals. On the one hand, [102] focus on the HIDS on networks using the Distributed Network Protocol 3 (DNP3) communication protocol, which is part of the IEEE Standard for Electric Power Systems Communications. On the other hand, [144] uses the IEC 61499 standard to provide security-be-design features during the development of a CPS.

Moreover, Pinto et al. [98],Pinto et al. [113] (P01 and P16) provide detection in field networks using OPC UA. Although having continuous specification work, strong user support and implementations, and considerable marketing efforts to support its adoption, OPC UA may be considered a standardization attempt rather than an established standard at this stage.

4.4.5. Human management

Human management refers to the work organization and design, considering the role of employees. AMS transformation should not focus only on the innovation and implementation of technology. One should also consider how employees will be part of the AMS transformation and how the presence of technology in the work environment will impact employees' work processes, especially considering new scenarios such as Human–Machine Interaction (HMI). This paradigm is also known as Human-Centred Manufacturing [151] or Operator 4.0 [152].

Bio-inspired Human-Centred Manufacturing was the potential to be a hot topic since there are several challenges regarding complex system design (considering the human operator), or even the HMI scenarios for collaborative tasks, where robots need to learn and adapt their own task execution considering the operator work profile and task performance within the overall collaboration.

4.4.6. Upskilling

Workforce and managers of manufacturing companies, such as professionals and executives, need to develop high-demanding skills in new transforming technologies within the AMS paradigm. These systems are changing the job requirements for several positions within manufacturing companies. So, several manufacturing processes and tasks are being adjusted to include this new paradigm's demands. This means that the existing workforce and management must face new challenges regarding new skills development. Thus, the implementation of AMS poses new challenges for new skills and academic training for continuing professional development and upskilling, also known as Education 4.0 [153].

4.4.7. Regulatory framework

Regulatory framework refers to the need for regulating new technology to be implemented in AMS. This regulation considers the legality of a new technology or the associated liability and data protection issues that could inhibit its acceptance and slow the innovation process.

5. Conceptual framework for industrial AIS applications

Despite the rich research efforts and numerous implementations of existing AIS models, its actual prevalence in AMS is still relatively low. The results of this study suggest that most of the performed research is implemented and validated as a proof of concept, using datasets, simulation environments or, at most, demonstrated in laboratory environments since the average TRL is between 3 and 4. The impact of such technologies on system autonomy is also disappointing since the average LOA is between 2 and 3 (partially/limited autonomy).

On the one hand, over the last few years, some researchers claim that AIS have not experienced the success of other bio-inspired approaches [154]. This explains why there are so many ensemble models compared to basic models. Also, the strong stochastic aspect of immune mechanisms makes them hard to explain and evaluate, which poses a difficulty to the research field since it is hard to use these models outside the field. This is not the case with several classical Machine Learning techniques, especially the ones related to Explainable Artificial Intelligence (XAI) [155]. On the other hand, implementing AIS in AMS scenarios may require a significant digital transformation in the manufacturing industry, which involve time and money to deploy several changes to existing systems. Those changes may be related to the technological implementation of CPS, Edge devices manipulation, embedded systems (SoPC FPGAs) and Big Data analysis for data-driven scenarios, according to AMS vision. This may not even be possible in some systems, such as Electrical Power Systems. That is the reason why simulation and emulation are such essential technologies when it comes to validating implementations.

Due to the lack of solid evidence of successful AIS applications in AMS, the industrial adoption of the technology is thus very slow. However, there is an enormous potential for the impact that such

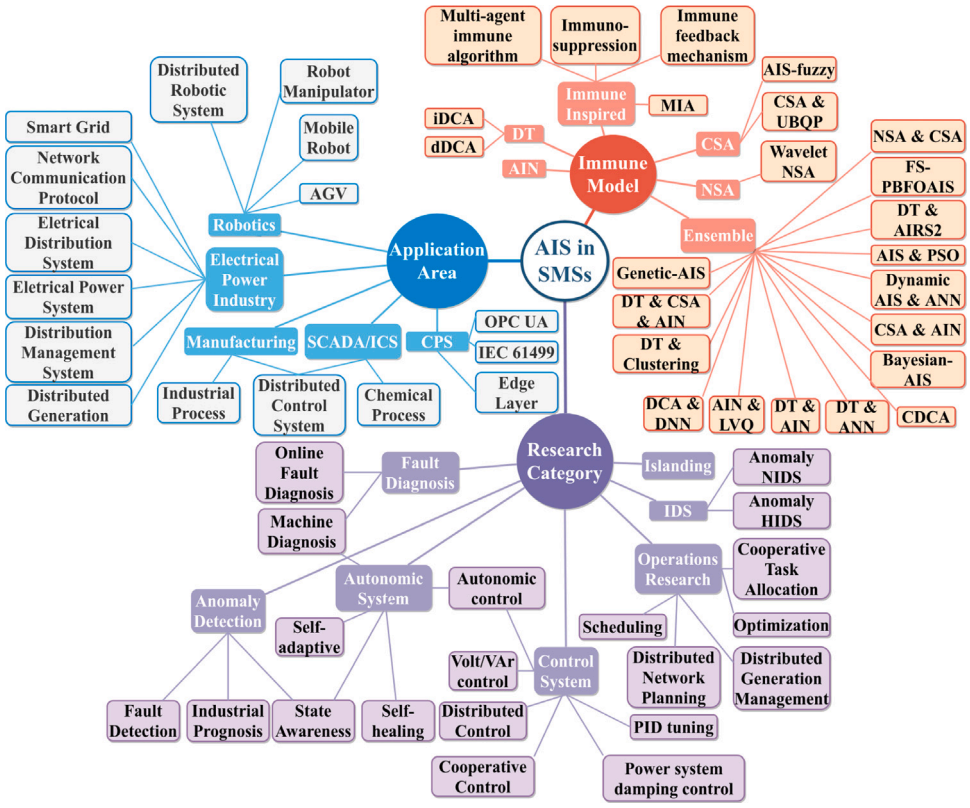

Fig. 9. Industrial AIS applications conceptual framework.

bio-inspired technologies may have on the AMS paradigm. Industrial companies must understand the enabling technologies of AIS implementation and deployment and the operational and organizational requirements to realize the full autonomy vision in AMS. Thus, Fig. 9 represents a conceptual framework of industrial AIs applications, providing some guidelines for manufacturers to adapt AIS in their own manufacturing applications to solve different problems. The authors propose the conceptual framework by collecting the findings from the study performed in this SLR in terms of the application areas, research categories and immune models that drive AIS in AMS. Moreover, the leading enabling technologies found in the literature review behind the industrial application of AIS are described next:

- **MAS**: A Multi-Agent System is, by nature, a system that presents autonomic behaviours by manifesting one or more Self-* properties. These type of systems consist of multiple interacting intelligent software agents, which develop complex behaviours even when each agent have a simple individual strategy (like a swarm). Essential characteristics of such agents are the autonomy level (self-aware), the knowledge of local views only and distributed control. These characteristics greatly resemble the properties of immune models, so the application development usage of both technologies is widespread.
- **Edge Devices**: The Edge computing paradigm brings computation and data processing together to the edge device level, i.e., devices that collect sensor data. This way, achieving real-time processing of real-time data generated by sensors is possible. In Edge computing scenarios, data may travel between different distributed nodes connected through the Internet, such as an IoT scenario. These nodes may also be resource-constrained devices, like a typical embedded system. Considering the AIS applications, Edge Devices are found in the lab or relevant environment validation scenarios. They work great together because immune models are lightweight, robust, and distributed. This means they can be executed in decentralized resource-constrained devices, where real-time raw data needs to be analysed with low latency.
- **Simulation/Emulation**: Simulation models are representations of the real physical systems, representing the key characteristics or behaviours of the selected system or process. In the AIS context, simulation was widely used to validate immune applications in AMS (especially in Electric Power systems) since the real system cannot be engaged because it may not be accessible, or it may be dangerous or unacceptable to engage. These models simulate data sources with specific behaviours, while the data is the main input of immune models for analysis. Also, some immune proposals may use their outputs to inject back into the simulation model to determine the eventual real effects of alternative conditions and courses of action. Finally, simulations may also be used to model the immune model itself (as a natural system) and gain insight into its functioning.
- **Big Data**: Big data refers to solutions for collecting and analysing large and complex datasets. As mentioned before, if this collection and analysis are performed at the Edge level, “instant data” is generated by sensors, so real-time processing scenarios are required. Typical solutions that address big data problems may have a multiple-layer and distributed architecture. These properties are shared with some immune models, making them suitable for big data scenarios.

Finally, and since several proposals are validated using datasets, the main datasets found in the literature review for application validation are:

- *M2M using OPC UA* [98,113,156]: This dataset was generated by implementing and injecting various attacks on an OPC UA-based CPPS testbed, and it aims to enable users to evaluate the effectiveness of different techniques for developed IDS in the manufacturing context. The dDCA and the iDCA models were validated using this dataset.

- *Random number dataset* [100,104,105]: This dataset contains status monitoring measurements of different CPS layers within specific periods for anomaly detection purposes. The dDCA model was validated using this dataset.
- *DNP3 smart grid dataset* [102]: Dataset generated after implementing several security threats to the DNP3 communication protocol for Smart Grids. The dDCA model was validated using this dataset.
- *KDD Cup99* [113,157]: This dataset is used for IDS purposes and contains a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment. The dDCA and the iDCA models were validated using this dataset.
- *Secure Water Treatment (SWaT) testbed* [114,158]: SWaT represents a scaled-down version of a real-world industrial water treatment plant. The dataset contains network and physical (process) data on the different number of sensors and actuators in all stages of the SWaT testbed for anomaly-IDS purposes. The NSA model was validated using this dataset.
- *Skoltech Anomaly Benchmark (SKAB) Dataset* [56,159]: The development of *SKAB* is based on sensor readings deployed in a water circulation system from an IoT testbed, located in the Skolkovo Institute of Science and Technology (Skoltech). Anomalies are introduced by inserting different physical faults in the system, such as closing valves, increases in temperature, and rotor imbalances. The CDCA model was validated using this dataset.

6. Conclusion

This study comprises a systematic literature review, restricted to journal and related conference papers in Artificial Immune Systems and Advanced Manufacturing Systems fields. By characterizing previous surveys and reviews in terms of their purpose and topics addressed (AMS, Self-* and AIS), the authors identified the need for this study. The systematic review was conducted following PRISMA guidelines, and the publications considered are indexed in the IEEE Xplore, Scopus, ScienceDirect, Springer, ACM, Inspec, Knovel and Web of Science databases.

This review has a few limitations considering the exclusion criteria, i.e., some relevant publications might have been left out of the study. First, limiting the inclusion to English language articles naturally implies the exclusion of non-English documents. Secondly, some publications were not included because authors could not access the necessary metadata and/or the full text. Thirdly, and maybe the most important reason, there were several publication exclusions because the work was not directly industry-related. However, the work was related (to some extent) to industrial enable technologies and/or other research fields that were not applied in industrial contexts. Some examples are identified in Section 2.3.3. Fourth, some publications were left out simply because the paper did not show results, despite having solution proposals. Finally, the general string queries for each database search may limit the results achieved.

This study results in a comprehensive characterization of AIS applications in AMS. We start by analysing the research trend considering these topics and then assess the status of such work. With this analysis, it was possible to define the main motivations for using AIS in AMS and identify the research gaps while commenting on possible future research trends in these topics. Finally, based on the systematic review of existing AIS in AMS literature and empirical evidence, a conceptual framework is proposed, providing a holistic view of the core elements of applying AIS in AMS, such as application areas, research categories, and immune models developed.

CRediT authorship contribution statement

Rui Pinto: Methodology, Data collection, Formal analysis, Investigation, Writing – original draft, Writing – review & editing, Project administration, Validation, Visualization. **Gil Gonçalves:** Supervision, Validation, Project administration, Resources, Writing – review & editing.

Declaration of competing interest

No author associated with this paper has disclosed any potential orpertinent conflicts which may be perceived to have impending conflictwith this work.

Appendix A. General string queries

Group 1. :

```
Artificial Immune System, AIS,
Dendritic Cell Algorithm, DCA
```

Group 2. :

```
Cyber-Physical System, Cyber-Physical Systems,
CPS, Cyber-Physical Production System, CPPS,
Cyber-Physical Production Systems,
Industrial Cyber-Physical System,
Industrial Cyber-Physical Systems,
Supervisory Control and Data Acquisition,
SCADA, Distributed Control System,
Distributed Control Systems,
Industrial Internet of Things,
Internet of Industrial Things,
IIoT, Industry, Industry 4.0, I4.0,
Manufacturing, Manufacturing System
Manufacturing Systems, AVM
Added Value Manufacturing
```

Appendix B. Database search inputs

- IEEE Xplore:

```
("Document Title":"Artificial Immune Systems"
OR "Document Title":"AIS" OR "Document Title":
"Dendritic Cell Algorithm" OR "Document Title":
"DCA") AND ("Document Title":"Cyber-Physical System"
OR "Document Title":"Cyber-Physical Systems" OR
"Document Title":"CPS" OR "Document Title":
"Cyber-Physical Production System" OR "Document Title":
"Cyber-Physical Production Systems" OR
"Document Title":"CPPS" OR "Document Title":
"Industrial Cyber-Physical System" OR "Document Title":
"Industrial Cyber-Physical Systems" OR "Document Title":
"Supervisory Control and Data Acquisition" OR
"Document Title":"SCADA" OR "Document Title":
"Distributed Control System" OR "Document Title":
"Distributed Control Systems" OR "Document Title":
"Industrial Internet of Things" OR "Document Title":
"IIoT" OR "Document Title":
"Internet of Industrial Things") OR ("Abstract":
"Artificial Immune Systems" OR "Abstract":"AIS" OR
"Abstract":"Dendritic Cell Algorithm" OR "Abstract":
"DCA") AND ("Abstract":"Cyber-Physical System" OR
"Abstract":"Cyber-Physical Systems" OR
"Abstract":"CPS" OR "Abstract":
"Cyber-Physical Production System" OR "Abstract":
"Cyber-Physical Production Systems" OR
"Abstract":"CPPS" OR "Abstract":
"Industrial Cyber-Physical System" OR "Abstract":
"Industrial Cyber-Physical Systems" OR "Abstract":
"Supervisory Control and Data Acquisition" OR
```

"Abstract": "SCADA" OR
"Abstract": "Distributed Control System" OR "Abstract":
"Distributed Control Systems" OR "Abstract":
"Industrial Internet of Things" OR "Abstract":
"IIoT" OR "Abstract": "Internet of Industrial Things")
OR ("Index Terms": "Artificial Immune Systems" OR
"Index Terms": "AIS" OR "Index Terms":
"Dendritic Cell Algorithm" OR "Index Terms":
"DCA") AND ("Index Terms": "Cyber-Physical System"
OR "Index Terms": "Cyber-Physical Systems" OR
"Index Terms": "CPS" OR "Index Terms":
"Cyber-Physical Production System" OR
"Index Terms": "Cyber-Physical Production Systems"
OR "Index Terms": "CPPS" OR "Index Terms":
"Industrial Cyber-Physical System" OR
"Index Terms": "Industrial Cyber-Physical Systems"
OR "Index Terms": "Supervisory Control and Data Acquisition"
OR "Index Terms": "SCADA" OR "Index Terms":
"Distributed Control System" OR "Index Terms":
"Distributed Control Systems" OR "Index Terms":
"Industrial Internet of Things" OR
"Index Terms": "IIoT" OR "Index Terms":
"Internet of Industrial Things")

- Scopus:

(Artificial Immune Systems OR AIS OR
Dendritic Cell Algorithm OR DCA) AND
(Cyber-Physical System OR Cyber-Physical Systems OR
CPS OR Cyber-Physical Production System OR
Cyber-Physical Production Systems OR CPPS OR
Industrial Cyber-Physical System OR
Industrial Cyber-Physical Systems OR
Supervisory Control and Data Acquisition OR SCADA OR
Distributed Control System OR
Distributed Control Systems OR
Industrial Internet of Things OR IIoT OR
Internet of Industrial Things)

- ScienceDirect:

("Artificial Immune Systems" OR "Dendritic Cell Algorithm")
AND ("Cyber-Physical System" OR
"Cyber-Physical Production System" OR
"Industrial Cyber-Physical System" OR SCADA OR
"Distributed Control System" OR
"Industrial Internet of Things" OR IIoT)

- Springer:

(Artificial Immune Systems OR AIS OR
Dendritic Cell Algorithm OR DCA) AND
(Cyber-Physical System OR Cyber-Physical Systems OR
CPS OR Cyber-Physical Production System OR
Cyber-Physical Production Systems OR CPPS OR
Industrial Cyber-Physical System OR
Industrial Cyber-Physical Systems OR
Supervisory Control and Data Acquisition OR
SCADA OR Distributed Control System OR
Distributed Control Systems OR
Industrial Internet of Things OR IIoT OR
Internet of Industrial Things)

- ACM:

[[[Publication Title: "artificial immune systems"]
OR [Publication Title: "ais"] OR [Publication Title:
"dendritic cell algorithm"] OR [Publication Title: "dca"]]
AND [[Publication Title: "cyber-physical system"] OR
[Publication Title: "cyber-physical systems"] OR
[Publication Title: "cps"] OR [Publication Title:
"cyber-physical production system"] OR [Publication Title:
"cyber-physical production systems"] OR
[Publication Title: "cpps"] OR [Publication Title:
"industrial cyber-physical system"] OR
[Publication Title: "industrial cyber-physical systems"]
OR [Publication Title:
"supervisory control and data acquisition"] OR
[Publication Title: "scada"] OR [Publication Title:
"distributed control system"] OR [Publication Title:
"distributed control systems"] OR [Publication Title:
"industrial internet of things"] OR [Publication Title:
"iiot"] OR [Publication Title:
"internet of industrial things"]]] OR [[[Abstract:
"artificial immune systems"] OR [Abstract: "ais"] OR
[Abstract: "dendritic cell algorithm"] OR [Abstract:
"dca"]] AND [[Abstract: "cyber-physical system"] OR
[Abstract: "cyber-physical systems"] OR [Abstract:
"cps"] OR [Abstract: "cyber-physical production system"]
OR [Abstract: "cyber-physical production systems"] OR
[Abstract: "cpps"] OR [Abstract:
"industrial cyber-physical system"] OR [Abstract:
"industrial cyber-physical systems"] OR [Abstract:
"supervisory control and data acquisition"] OR
[Abstract: "scada"] OR [Abstract:
"distributed control system"] OR [Abstract:
"distributed control systems"] OR [Abstract:
"industrial internet of things"] OR [Abstract:
"iiot"] OR [Abstract: "internet of industrial things"]]]
OR [[[Keywords: "artificial immune systems"] OR
[Keywords: "ais"] OR [Keywords:
"dendritic cell algorithm"] OR [Keywords: "dca"]]
AND [[Keywords: "cyber-physical system"] OR
[Keywords: "cyber-physical systems"] OR [Keywords:
"cps"] OR [Keywords: "cyber-physical production system"]
OR [Keywords: "cyber-physical production systems"]
OR [Keywords: "cpps"] OR [Keywords:
"industrial cyber-physical system"] OR [Keywords:
"industrial cyber-physical systems"] OR [Keywords:
"supervisory control and data acquisition"] OR
[Keywords: "scada"] OR [Keywords:
"distributed control system"] OR [Keywords:
"distributed control systems"] OR [Keywords:
"industrial internet of things"] OR [Keywords:
"iiot"] OR [Keywords: "internet of industrial things"]]]

- Engineering Village:

("Artificial Immune Systems" OR "AIS" OR
"Dendritic Cell Algorithm" OR "DCA") AND
("Cyber-Physical System" OR "Cyber-Physical Systems"
OR "CPS" OR "Cyber-Physical Production System" OR
"Cyber-Physical Production Systems" OR "CPPS" OR
"Industrial Cyber-Physical System" OR
"Industrial Cyber-Physical Systems" OR
"Supervisory Control and Data Acquisition" OR
"SCADA" OR "Distributed Control System" OR
"Distributed Control Systems" OR
"Industrial Internet of Things" OR "IIoT" OR
"Internet of Industrial Things")

- ISI Web of Knowledge:

(ALL=("Artificial Immune Systems" OR "AIS" OR
"Dendritic Cell Algorithm" OR "DCA")) AND
ALL=("Cyber-Physical System" OR
"Cyber-Physical Systems" OR "CPS" OR
"Cyber-Physical Production System" OR
"Cyber-Physical Production Systems" OR "CPPS"
OR "Industrial Cyber-Physical System" OR
"Industrial Cyber-Physical Systems" OR
"Supervisory Control and Data Acquisition"
OR "SCADA" OR "Distributed Control System"
OR "Distributed Control Systems" OR
"Industrial Internet of Things" OR "IIoT"
OR "Internet of Industrial Things")

Appendix C. Exclusion criteria

EC 1. Non-computer science related
EC 2. Non-industry related
EC 3. No access to publication metadata
EC 4. No access to publication full text
EC 5. Short or WIP Paper
EC 6. Reviews or surveys
EC 7. Seminar or keynote
EC 8. Book chapters preface or guest editorials
EC 9. Full Proceedings
EC 10. Non-AIS related
EC 11. No solution development to a problem
EC 12. No results presented

References

[1] Oztemel E, Gursev S. Literature review of industry 4.0 and related technologies. J Intell Manuf 2018;31(1):127–82. http://dx.doi.org/10.1007/S10845-018-1433-8, 2018 31:1. URL: https://link.springer.com/article/10.1007/s10845-018-1433-8.

[2] Stock D, Bauernhansl T, Weyrich M, Feurer M, Wutzke R. System architectures for cyber-physical production systems enabling self-x and autonomy. In: IEEE symposium on emerging technologies and factory automation, ETFA, Vol. 2020-Septe. 2020, p. 148–55. http://dx.doi.org/10.1109/ETFA46521.2020.9212182, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85093364574&doi=10.1109%2FETFA46521.2020.9212182&partnerID=40&md5=c28471c7815e33fb58c4ee7c2f4f8c1b.

[3] Qu YJ, Ming XG, Liu ZW, Zhang XY, Hou ZT. Smart manufacturing systems: state of the art and future trends. Int J Adv Manuf Technol 2019;103(9–12):3751–68. http://dx.doi.org/10.1007/s00170-019-03754-7, URL: http://link.springer.com/10.1007/s00170-019-03754-7.

[4] Wegener K, Gittler T, Weiss L. Dawn of new machining concepts: Compensated, intelligent, bioinspired. In: Procedia CIRP, Vol. 77. 2018, p. 1–17. http://dx.doi.org/10.1016/j.procir.2018.08.194, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85057394514&doi=10.1016%2Fj.procir.2018.08.194&partnerID=40&md5=8764e8ffa84b47a5246b2cc7e8c928be.

[5] Dasgupta D, Yu S, Nino F. Recent advances in artificial immune systems: models and applications. Appl Soft Comput 2011;11(2):1574–87.

[6] Peres RS, Jia X, Lee J, Sun K, Colombo AW, Barata J. Industrial artificial intelligence in industry 4.0 -systematic review, challenges and outlook. IEEE Access 2020. http://dx.doi.org/10.1109/ACCESS.2020.3042874, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85097938680&doi=10.1109%2FACCESS.2020.3042874&partnerID=40&md5=fbff910a5e850300f34de6960330a155.

[7] Gunawardana K. Introduction of advanced manufacturing technology: a literature review. Sabaragamuwa Univ J 2006;6(1):116–34.

[8] Tao F, Cheng Y, Zhang L, Nee AYC. Advanced manufacturing systems: socialization characteristics and trends. J Intell Manuf 2017;28(5):1079–94. http://dx.doi.org/10.1007/s10845-015-1042-8.

[9] Huang Z, Jowers C, Kent D, Dehghan-Manshadi A, Dargusch MS. The implementation of industry 4.0 in manufacturing: from lean manufacturing to product design. Int J Adv Manuf Technol 2022;121(5):3351–67. http://dx.doi.org/10.1007/s00170-022-09511-7.

[10] da Rosa Cardoso R, Pinheiro de Lima E, Gouvea da Costa SE. Identifying organizational requirements for the implementation of advanced manufacturing technologies (AMT). J Manuf Syst 2012;31(3):367–78. http://dx.doi.org/10.1016/j.jmsy.2012.04.003, URL: https://www.sciencedirect.com/science/article/pii/S0278612512000337.

[11] Kagermann H, Helbig J, Hellinger A, Wahlster W. Recommendations for implementing the strategic initiative industrie 4.0: securing the future of German manufacturing industry. Final report of the industrie 4.0 working group, Forschungsunion; 2013.

[12] Tran J. SMLC - smart manufacturing leadership coalition. 2016, https://www.smartmanufacturingcoalition.org/.

[13] Li L. China's manufacturing locus in 2025: With a comparison of "made-in-China 2025" and "industry 4.0". Technol Forecast Soc Change 2018;135:66–74. http://dx.doi.org/10.1016/j.techfore.2017.05.028, URL: https://www.sciencedirect.com/science/article/pii/S0040162517307254.

[14] Athimon M. Usine du futur. 2016, http://industriedufutur.fim.net/.

[15] McKernan R. How catapults can help your business innovate. 2016, https://www.catapult.org.uk/wp-content/uploads/2016/04/How-Catapults-can-help-your-business-innovate-2016.pdf.

[16] Kim M. Innovation in manufacturing 3.0 strategy needs better focus with clearer direction. 2015, http://www.businesskorea.co.kr/english/features/special-reports/13060-smart-factory-innovation-manufacturing-30-strategy-needs-better-focus.

[17] Zaske S. Germany's vision for industrie 4.0: The revolution will be digitised. 2015, http://www.zdnet.com/article/germanys-vision-for-industrie-4-0-the-revolution-will-be-digitised/.

[18] Drath R, Horch A. Industrie 4.0: Hit or hype?[industry forum]. IEEE Ind Electron Mag 2014;8(2):56–8.

[19] Liu Y, Peng Y, Wang B, Yao S, Liu Z. Review on cyber-physical systems. IEEE/CAA J Autom Sin 2017;4(1):27–40. http://dx.doi.org/10.1109/JAS.2017.7510349.

[20] Sharma N, Awasthi LK, Mangla M, Sharma KP, Kumar R. Cyber-physical systems: a comprehensive guide. CRC Press; 2022.

[21] Boyer SA. SCADA: Supervisory control and data acquisition. International Society of Automation; 2009.

[22] Yang H, Kumara S, Bukkapatnam ST, Tsung F. The internet of things for smart manufacturing: A review. IISE Trans 2019;51(11):1190–216. http://dx.doi.org/10.1080/24725854.2018.1555383, arXiv:https://doi.org/10.1080/24725854.2018.1555383.

[23] Asghari P, Rahmani AM, Javadi HHS. Internet of things applications: A systematic review. Comput Netw 2019;148:241–61. http://dx.doi.org/10.1016/j.comnet.2018.12.008, URL: https://www.sciencedirect.com/science/article/pii/S1389128618305127.

[24] Antão L, Pinto R, Reis J, Gonçalves G. Requirements for testing and validating the industrial internet of things. In: 2018 IEEE international conference on software testing, verification and validation workshops (ICSTW). 2018, p. 110–5. http://dx.doi.org/10.1109/ICSTW.2018.00036.

[25] Valenzuela-Valdés JF, Triantafyllou A, Sarigiannidis P, Lagkas TD. Network protocols, schemes, and mechanisms for internet of things (IoT): Features, open challenges, and trends. Wirel Commun Mob Comput 2018;2018:5349894. http://dx.doi.org/10.1155/2018/5349894.

[26] Galloway B, Hancke GP. Introduction to industrial control networks. IEEE Commun Surv Tutor 2013;15(2):860–80. http://dx.doi.org/10.1109/SURV.2012.071812.00124.

[27] Dorri A, Kanhere SS, Jurdak R. Multi-agent systems: A survey. IEEE Access 2018;6:28573–93. http://dx.doi.org/10.1109/ACCESS.2018.2831228.

[28] da Silva Mendonça R, de Oliveira Lins S, de Bessa IV, de Carvalho Ayres FA, de Medeiros RLP, de Lucena VF. Digital twin applications: A survey of recent advances and challenges. Processes 2022;10(4). http://dx.doi.org/10.3390/pr10040744, URL: https://www.mdpi.com/2227-9717/10/4/744.

[29] Semeraro C, Lezoche M, Panetto H, Dassisti M. Digital twin paradigm: A systematic literature review. Comput Ind 2021;130:103469. http://dx.doi.org/10.1016/j.compind.2021.103469, URL: https://www.sciencedirect.com/science/article/pii/S0166361521000762.

[30] Liu M, Fang S, Dong H, Xu C. Review of digital twin about concepts, technologies, and industrial applications. J Manuf Syst 2021;58:346–61. http://dx.doi.org/10.1016/j.jmsy.2020.06.017, URL: https://www.sciencedirect.com/science/article/pii/S0278612520301072. Digital Twin towards Smart Manufacturing and Industry 4.0.

[31] Arinez JF, Chang Q, Gao RX, Xu C, Zhang J. Artificial intelligence in advanced manufacturing: Current status and future outlook. J Manuf Sci Eng 2020;142(11). http://dx.doi.org/10.1115/1.4047855, 110804. arXiv:https://asmedigitalcollection.asme.org/manufacturingscience/article-pdf/142/11/110804/6594922/manu_142_11_110804.pdf.

[32] Javaid M, Haleem A, Singh RP, Suman R. Artificial intelligence applications for industry 4.0: A literature-based study. J Ind Integr Manage 2022;07(01):83–111. http://dx.doi.org/10.1142/S2424862221300040, arXiv:https://doi.org/10.1142/S2424862221300040.

[33] Majid M, Habib S, Javed AR, Rizwan M, Srivastava G, Gadekallu TR, Lin JC-W. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors 2022;22(6). http://dx.doi.org/10.3390/s22062087, URL: https://www.mdpi.com/1424-8220/22/6/2087.

[34] Ali A, Ming Y, Chakraborty S, Iram S. A comprehensive survey on real-time applications of WSN. Future Internet 2017;9(4). http://dx.doi.org/10.3390/fi9040077, URL: https://www.mdpi.com/1999-5903/9/4/77.

[35] Queiroz DV, Alencar MS, Gomes RD, Fonseca IE, Benavente-Peces C. Survey and systematic mapping of industrial wireless sensor networks. J Netw Comput Appl 2017;97:96–125. http://dx.doi.org/10.1016/j.jnca.2017.08.019, URL: https://www.sciencedirect.com/science/article/pii/S1084804517302771.

[36] Durao F, Carvalho JFS, Fonseka A, Garcia VC. A systematic review on cloud computing. J Supercomput 2014;68(3):1321–46. http://dx.doi.org/10.1007/s11227-014-1089-x.

[37] Askary Z, Kumar R. Cloud computing in industries: A review. In: Kumar H, Jain PK, editors. Recent advances in mechanical engineering. Singapore: Springer Singapore; 2020, p. 107–16.

[38] Cao K, Liu Y, Meng G, Sun Q. An overview on edge computing research. IEEE Access 2020;8:85714–28. http://dx.doi.org/10.1109/ACCESS.2020.2991734.

[39] Laghari AA, Jumani AK, Laghari RA. Review and state of art of fog computing. Arch Comput Methods Eng 2021;28(5):3631–43. http://dx.doi.org/10.1007/s11831-020-09517-y.

[40] Chong D, Shi H. Big data analytics: a literature review. J Manage Anal 2015;2(3):175–201. http://dx.doi.org/10.1080/23270012.2015.1082449, arXiv:https://doi.org/10.1080/23270012.2015.1082449.

[41] Günther WA, Rezazade Mehrizi MH, Huysman M, Feldberg F. Debating big data: A literature review on realizing value from big data. J Strat Inf Syst 2017;26(3):191–209. http://dx.doi.org/10.1016/j.jsis.2017.07.003, URL: https://www.sciencedirect.com/science/article/pii/S0963868717302615.

[42] Lynch KM, Park FC. Modern robotics. Cambridge University Press; 2017.

[43] Siciliano B, Khatib O. Robotics and the handbook. In: Springer handbook of robotics. Cham: Springer International Publishing; 2016, p. 1–6. http://dx.doi.org/10.1007/978-3-319-32552-1_1.

[44] IBM. Autonomic computing: ibm's perspective on the state of information technology. 2001, http://people.scs.carleton.ca/~soma/biosec/readings/autonomic_computing.pdf.

[45] Würtz RP. Organic computing. Springer Science & Business Media; 2008.

[46] Parashar M, Hariri S. Autonomic computing: An overview. In: Unconventional programming paradigms. Springer; 2005, p. 257–69.

[47] Kephart JO, Chess DM. The vision of autonomic computing. Computer 2003;36(1):41–50.

[48] Ganek AG, Corbi TA. The dawning of the autonomic computing era. IBM Syst J 2003;42(1):5–18.

[49] Berns A, Ghosh S. Dissecting self-* properties. In: 2009 third IEEE international conference on self-adaptive and self-organizing systems. IEEE; 2009, p. 10–9.

[50] Zadeh LA. On the definition of adaptivity. Proc IEEE 1963;51(3):469–70.

[51] Brownlee J. Clever algorithms: Nature-inspired programming recipes. Jason Brownlee; 2011.

[52] Cohen IR. Tending Adam's garden: evolving the cognitive immune self. Academic Press; 2000.

[53] Cohen IR. Immune system computation and the immunological homunculus. In: International conference on model driven engineering languages and systems. Springer; 2006, p. 499–512.

[54] Dasgupta D, Nino F. Immunological computation: theory and applications. CRC Press; 2008.

[55] Janeway CA. How the immune system works to protect the host from infection: a personal view. Proc Natl Acad Sci 2001;98(13):7461–8.

[56] Pinto C, Pinto R, Gon¸calves G. Towards bio-inspired anomaly detection using the cursory dendritic cell algorithm. Algorithms 2022;15(1). http://dx.doi.org/10.3390/a15010001, URL: https://www.mdpi.com/1999-4893/15/1/1.

[57] Forrest S, Perelson AS, Allen L, Cherukuri R, et al. Self-nonself discrimination in a computer. In: IEEE symposium on security and privacy, Oakland. 1994, p. 202–12.

[58] Timmis J, Neal M, Hunt J. An artificial immune system for data analysis. Biosystems 2000;55(1):143–50.

[59] Knight T, Timmis J. AINE: An immunological approach to data mining. In: Proceedings of the 2001 IEEE international conference on data mining. IEEE Computer Society; 2001, p. 297–304.

[60] Jerne NK. Towards a network theory of the immune system. In: Annales d'immunologie. 125, (1–2):1974, p. 373–89.

[61] Nunes de Casto L, Von Zuben F. An evolutionary immune network for data clustering. In: Proceedings. Vol. 1. Sixth Brazilian symposium on neural networks. 2000, p. 84–9. http://dx.doi.org/10.1109/SBRN.2000.889718.

[62] De Castro LN, Von Zuben FJ. The clonal selection algorithm with engineering applications. In: Proceedings of GECCO, Vol. 2000; 2000, p. 36–9.

[63] De Castro LN, Von Zuben FJ. Learning and optimization using the clonal selection principle. IEEE Trans Evol Comput 2002;6(3):239–51.

[64] Watkins A, Timmis J, Boggess L. Artificial immune recognition system (AIRS): An immune-inspired supervised learning algorithm. Genet Program Evol Mach 2004;5(3):291–317.

[65] Kelsey J, Timmis J. Immune inspired somatic contiguous hypermutation for function optimisation. In: Genetic and evolutionary computation conference. Springer; 2003, p. 207–18.

[66] Haktanirlar Ulutas B, Kulturel-Konak S, Ulutas BH, Kulturel-Konak S. A review of clonal selection algorithm and its applications. Artif Intell Rev (Netherlands) 2011;36(2):117–38. http://dx.doi.org/10.1007/s10462-011-9206-1, http://dx.doi.org/10.1007/s10462-011-9206-1https://www.scopus.com/inward/record.uri?eid=2-s2.0-80051553003&doi=10.1007%2Fs10462-011-9206-1&partnerID=40&md5=a20b62e6c246a58caca3718ae8548a93.

[67] Aickelin U, Cayzer S. The danger theory and its application to artificial immune systems. 2008, arXiv preprint arXiv:0801.3549.

[68] Matzinger P. The danger model: a renewed sense of self. Science 2002;296(5566):301–5.

[69] Greensmith J, Aickelin U, Cayzer S. Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection. In: International conference on artificial immune systems. Springer; 2005, p. 153–67.

[70] Greensmith J, Aickelin U, Twycross J. Articulation and clarification of the dendritic cell algorithm. In: International conference on artificial immune systems. Springer; 2006, p. 404–17.

[71] Steinman RM, Cohn ZA. Identification of a novel cell type in peripheral lymphoid organs of mice I. Morphology, quantitation, tissue distribution. J Exp Med 1973;137(5):1142–62.

[72] Aldhaheri S, Alghazzawi D, Cheng L, Barnawi A, Alzahrani BA. Artificial immune systems approaches to secure the internet of things: A systematic review of the literature and recommendations for future research. J Netw Comput Appl 2020;157:102537. http://dx.doi.org/10.1016/j.jnca.2020.102537, URL: https://www.sciencedirect.com/science/article/pii/S1084804520300114.

[73] Greensmith J, Twycross J, Aickelin U. Dendritic cells for anomaly detection. In: 2006 IEEE international conference on evolutionary computation. 2006, p. 664–71. http://dx.doi.org/10.1109/CEC.2006.1688374.

[74] Al-Hammadi Y, Aickelin U, Greensmith J. DCA for bot detection. In: 2008 IEEE congress on evolutionary computation (IEEE world congress on computational intelligence). 2008, p. 1807–16. http://dx.doi.org/10.1109/CEC.2008.4631034.

[75] Huang R, Tawfik H, Nagar AK. Artificial dendritic cells algorithm for online break-in fraud detection. In: 2009 second international conference on developments in esystems engineering. 2009, p. 181–9. http://dx.doi.org/10.1109/DeSE.2009.59.

[76] Danziger M, Lacerda M, de Lima Neto FB. Danger theory and multi-agents applied for addressing the deny of service detection problem in IEEE 802.11 networks. In: 2009 ninth international conference on intelligent systems design and applications. 2009, p. 695–702. http://dx.doi.org/10.1109/ISDA.2009.136.

[77] Alsulami AA, Zein-Sabatto S. Detection and defense from false data injection attacks in aviation cyber-physical systems using artificial immune systems. In: 2020 international conference on computational science and computational intelligence (CSCI). 2020, p. 69–75. http://dx.doi.org/10.1109/CSCI51800.2020.00019.

[78] Alsulami AA, Zein-Sabatto S. Resilient cyber-security approach for aviation cyber-physical systems protection against sensor spoofing attacks. In: 2021 IEEE 11th annual computing and communication workshop and conference (CCWC), Piscataway, NJ, USA. 2021, p. 0565–71, URL: http://dx.doi.org/10.1109/CCWC51732.2021.9376158.

[79] Cayzer S, Aickelin U. A recommender system based on the immune network. In: Proceedings of the 2002 congress on evolutionary computation. CEC'02 (cat. no.02TH8600), Vol. 1. 2002, p. 807–12. http://dx.doi.org/10.1109/CEC.2002.1007029, vol.1.

[80] Zand MD, Kalantari M, Golzari S. File transfer scheduling optimization using artificial immune system. In: 2013 14th ACIS international conference on software engineering, artificial intelligence, networking and parallel/distributed computing. 2013, p. 17–22. http://dx.doi.org/10.1109/SNPD.2013.52.

[81] Moalla D, Elkosantini S, Darmoul S. An artificial immune network to control traffic at a single intersectio. In: Proceedings of 2013 international conference on industrial engineering and systems management (IESM); 2013, p. 1–7.

[82] Chen D, Zhang F. 5G message service system based on artificial immune dynamic adaptive mechanism. IEEE Access 2019;7:91146–59. http://dx.doi.org/10.1109/ACCESS.2019.2927271.

[83] Takeda T, Taniguchi K, Asari K, Kuramoto K, Kobashi S, Hata Y. Biometric personal authentication by one step foot pressure distribution change by fuzzy artificial immune system. In: International conference on fuzzy systems. 2010, p. 1–6. http://dx.doi.org/10.1109/FUZZY.2010.5584216.

[84] Xu C, Xu S, Chen W. Artificial immune system and its applications in gps single frequency precise point positioning. In: 2008 3rd international conference on intelligent system and knowledge engineering, Vol. 1. 2008, p. 180–3. http://dx.doi.org/10.1109/ISKE.2008.4730921.

[85] Wang H, Peng D, Wang W, Sharif H, Wegiel J, Nguyen D, Bowne R, Backhaus C. Artificial immune system based image pattern recognition in energy efficient wireless multimedia sensor networks. In: MILCOM 2008 - 2008 IEEE military communications conference. 2008, p. 1–7. http://dx.doi.org/10.1109/MILCOM.2008.4753651.

[86] Timmis J. Artificial immune systems - today and tomorrow. Nat Comput (Netherlands) 2007;6(1):1–18, URL: http://dx.doi.org/10.1007/s11047-006-9029-1.

[87] Shafi K, Abbass HA. Biologically-inspired complex adaptive systems approaches to network intrusion detection. Inf Secur Tech Rep 2007;12(4):209–17. http://dx.doi.org/10.1016/j.istr.2007.09.001, URL: https://www.sciencedirect.com/science/article/pii/S1363412707000416.

[88] Timmis J, Andrews P, Owens N, Clark E. An interdisciplinary perspective on artificial immune systems. Evol Intell (Netherlands) 2008;1(1):5–26, URL: http://dx.doi.org/10.1007/s12065-007-0004-2.

[89] Zheng J, Chen Y, Zhang W. A survey of artificial immune applications. Artif Intell Rev (Netherlands) 2010;34(1):19–34, URL: http://dx.doi.org/10.1007/s10462-010-9159-9.

[90] Muhamad AS, Deris S. An artificial immune system for solving production scheduling problems: a review. Artif Intell Rev (Netherlands) 2013;39(2):97–108, URL: http://dx.doi.org/10.1007/s10462-011-9259-1.

[91] Bayar N, Darmoul S, Hajri-Gabouj S, Pierreval H. Fault detection, diagnosis and recovery using artificial immune systems: A review. Eng Appl Artif Intell 2015;46:43–57. http://dx.doi.org/10.1016/j.engappai.2015.08.006, URL: https://www.sciencedirect.com/science/article/pii/S0952197615001840.

[92] Bere M, Muyingi H. Initial investigation of industrial control system (ICS) security using artificial immune system (AIS). In: 2015 international conference on emerging trends in networks and computer communications (ETNCC). Proceedings, Piscataway, NJ, USA. 2015, p. 79–84, URL: http://dx.doi.org/10.1109/ETNCC.2015.7184812.

[93] Raza A, Fernandez BR. Immuno-inspired robotic applications: A review. Appl Soft Comput (Netherlands) 2015;37:490–505, URL: http://dx.doi.org/10.1016/j.asoc.2015.08.050.

[94] Zhong RY, Xu X, Klotz E, Newman ST. Intelligent manufacturing in the context of industry 4.0: A review. Engineering 2017;3(5):616–30. http://dx.doi.org/10.1016/J.ENG.2017.05.015, URL: https://www.sciencedirect.com/science/article/pii/S2095809917307130.

[95] Al-Khatib R, Doush I. A survey for recent applications and variants of nature-inspired immune search algorithm. Int J Comput Appl Technol (Switzerland) 2020;63(4):354–70, URL: http://dx.doi.org/10.1504/IJCAT.2020.110417.

[96] Radanliev P, De Roure D, Van Kleek M, Santos O, Ani U. Artificial intelligence in cyber physical systems. AI Soc 2020. http://dx.doi.org/10.1007/s00146-020-01049-0, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85090061979&doi=10.1007%2Fs00146-020-01049-0&partnerID=40&md5=90c718b0157dc5597a36ff8dbc6059c7.

[97] Alrubayyi H, Goteng G, Jaber M, Kelly J. Challenges of malware detection in the IoT and a review of artificial immune system approaches. J Sens Actuat Netw 2021;10(4). http://dx.doi.org/10.3390/jsan10040061, URL: https://www.mdpi.com/2224-2708/10/4/61.

[98] Pinto R, Gonçalves G, Tovar E, Delsing J. Attack detection in cyber-physical production systems using the deterministic dendritic cell algorithm. In: 2020 25th IEEE international conference on emerging technologies and factory automation (ETFA), Vol. 1. 2020, p. 1552–9.

[99] Rocha AD, Lima-Monteiro P, Parreira-Rocha M, Barata J. Artificial immune systems based multi-agent architecture to perform distributed diagnosis. J Intell Manuf 2019;30(4):2025–37. http://dx.doi.org/10.1007/s10845-017-1370-y.

[100] Lokesh MR, Kumaraswamy YS. State awareness towards resiliency in cyber-physical system: A modified danger theory based deterministic dendritic cell algorithm approach. In: 2015 IEEE international conference on computer graphics, vision and information security (CGVIS). 2015, p. 201–8. http://dx.doi.org/10.1109/CGVIS.2015.7449922.

[101] Xu SS-D, Huang H-C, Kung Y-C, Chu Y-Y. A networked multirobot CPS with artificial immune fuzzy optimization for distributed formation control of embedded mobile robots. IEEE Trans Ind Inf 2020;16(1):414–22. http://dx.doi.org/10.1109/TII.2019.2936045.

[102] Igbe O, Darwish I, Saadawi T. Deterministic dendritic cell algorithm application to smart grid cyber-attack detection. In: 2017 IEEE 4th international conference on cyber security and cloud computing (CSCloud). 2017, p. 199–204. http://dx.doi.org/10.1109/CSCloud.2017.12.

[103] Samigulina GA, Samigulina ZI. Development of smart-technology for complex objects control based on approach of artificial immune systems. In: Proceedings - 2018 global smart industry conference, GloSIC 2018, Piscataway, NJ, USA. 2018, p. 6. http://dx.doi.org/10.1109/GloSIC.2018.8570142, http://dx.doi.org/10.1109/GloSIC.2018.8570142https://www.scopus.com/inward/record.uri?eid=2-s2.0-85060726058&doi=10.1109%2FGloSIC.2018.8570142&partnerID=40&md5=284e30bf2c42e419068f81ae53d5c930.

[104] Lokesh MR, Kumaraswamy YS, R LM, Kumaraswamy YS. Modified danger theory based optimized artificial immune network on resiliency in cyber-physical system. In: 2015 international conference on green computing and internet of things (ICGCIoT). Proceedings, Piscataway, NJ, USA. 2015, p. 1228–35. http://dx.doi.org/10.1109/ICGCIoT.2015.7380651.

[105] Lokesh MR, Kumaraswamy Y. Healing process towards resiliency in cyber-physical system: A modified danger theory based artifical immune recogization2 algorithm approach. In: 2015 IEEE international conference on computer graphics, vision and information security (CGVIS). 2015, p. 226–32. http://dx.doi.org/10.1109/CGVIS.2015.7449926.

[106] Lima FP, Lotufo AD, Minussi CR. Disturbance detection for optimal database storage in electrical distribution systems using artificial immune systems with negative selection. Electr Power Syst Res 2014;109:54–62. http://dx.doi.org/10.1016/j.epsr.2013.12.010, URL: https://www.sciencedirect.com/science/article/pii/S0378779613003398.

[107] Li W, Cai X. Intelligent immune system for sustainable manufacturing. In: 2018 IEEE 22nd international conference on computer supported cooperative work in design ((CSCWD)). 2018, p. 190–5. http://dx.doi.org/10.1109/CSCWD.2018.8465214.

[108] Lima FP, Lotufo ADP, Minussi CR. Wavelet-artificial immune system algorithm applied to voltage disturbance diagnosis in electrical distribution systems. IET Gener Transm Distrib 2015;9(11):1104–11. http://dx.doi.org/10.1049/iet-gtd.2014.1102.

[109] Ieao FB, Pereira RAF, Mantovani JRS, Leão FB, Pereira RAF, Mantovani JRS. Fault section estimation in electric power systems using an artificial immune system algorithm. In: 16th power systems computation conference, PSCC 2008, Strathclyde, UK. 2008, p. 7, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84944097046&partnerID=40&md5=c9465da4ebb5830b12931208567dfa95.

[110] Ko A, Lau HYK, Lau TL. An immuno control framework for decentralized mechatronic control. In: Nicosia G, Cutello V, Bentley PJ, Timmis J, editors. Artificial immune systems. Berlin, Heidelberg: Springer Berlin Heidelberg; 2004, p. 91–105.

[111] Rammig FJ, Grösbrink S, Stahl K, Zhao Y. Designing self-adaptive embedded real-time software – towards system engineering of self-adaptation. In: Proceedings of the 2014 Brazilian symposium on computing systems engineering. SBESC '14, USA: IEEE Computer Society; 2014, p. 37–42. http://dx.doi.org/10.1109/SBESC.2014.15.

[112] Degeler V, French R, Jones K. Combined danger signal and anomaly-based threat detection in cyber-physical systems. In: Lecture notes of the institute for computer sciences, social-informatics and telecommunications engineering. LNICST, vol. 169, Cham: Springer; 2015, p. 27–39. http://dx.doi.org/10.1007/978-3-319-47063-4_3, URL: https://link.springer.com/chapter/10.1007/978-3-319-47063-4_3.

[113] Pinto R, Gonçalves G, Delsing J, Tovar E. Incremental dendritic cell algorithm for intrusion detection in cyber-physical production systems. In: Arai K, editor. Intelligent computing. Cham: Springer International Publishing; 2021, p. 664–80.

[114] Clotet X, Moyano J, León G. A real-time anomaly-based IDS for cyber-attack detection at the industrial process level of critical infrastructures. Int J Crit Infrastruct Prot 2018;23:11–20. http://dx.doi.org/10.1016/j.ijcip.2018.08.002, URL: https://www.sciencedirect.com/science/article/pii/S1874548217300884.

[115] Guerrero CAV, Silveira PM, Filho JMC. Adaptation of the clonal selection algorithm to the real-time coordinated Volt/VAr control through a software-in-the-loop strategy. Electr Power Syst Res 2021;194:107092. http://dx.doi.org/10.1016/j.epsr.2021.107092, URL: https://www.sciencedirect.com/science/article/pii/S0378779621000730.

[116] Guo J, Yang H. An anti-jamming artificial immune approach for energy leakage diagnosis in parallel-machine job shops. Comput Ind 2018;101:13–24. http://dx.doi.org/10.1016/j.compind.2018.05.004, URL: https://www.sciencedirect.com/science/article/pii/S016636151730756X.

[117] Semwal T, Nair SB. A decentralized artificial immune system for solution selection in cyber–physical systems. Appl Soft Comput 2020;86:105920. http://dx.doi.org/10.1016/j.asoc.2019.105920, URL: https://www.sciencedirect.com/science/article/pii/S156849461930701X.

[118] Zhu J, Shu Y, Zhao J, Yang F. A dynamic alarm management strategy for chemical process transitions. J Loss Prev Process Ind 2014;30:207–18. http://dx.doi.org/10.1016/j.jlp.2013.07.008, URL: https://www.sciencedirect.com/science/article/pii/S0950423013001393.

[119] Zhao J, Shu Y, Zhu J, Dai Y. An online fault diagnosis strategy for full operating cycles of chemical processes. Ind Eng Chem Res 2014;53(13):5015–27. http://dx.doi.org/10.1021/ie400660e, URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84897503835&doi=10.1021%2Fie400660e&partnerID=40&md5=fb5a1bb394bf1bcea3590bba40e4d76b.

[120] Kim DH. Tuning of 2-DOF PID controller by immune algorithm. In: Proceedings of the 2002 congress on evolutionary computation. CEC'02 (cat. no.02TH8600), Vol. 1. 2002, p. 675–80. http://dx.doi.org/10.1109/CEC.2002.1007007, vol.1.

[121] Li XD, Xu YQ, Zhang L. Distribution service restoration with DGs based on multi-agent immune algorithm. In: 2009 2nd international conference on power electronics and intelligent transportation system (PEITS), Vol. 1. 2009, p. 1–4. http://dx.doi.org/10.1109/PEITS.2009.5407060.

[122] Aghaebrahimi MR, Amiri M, Zahiri SH. An immune-based optimization method for distributed generation placement in order to minimize power losses. In: 2009 international conference on sustainable power generation and supply. 2009, p. 1–7. http://dx.doi.org/10.1109/SUPERGEN.2009.5348235.

[123] Lizondo D, Araujo P, Will A, Rodriguez S. Multiagent model for distributed peak shaving system with demand-side management approach. In: 2017 first IEEE international conference on robotic computing (IRC). 2017, p. 352–7. http://dx.doi.org/10.1109/IRC.2017.50.

[124] Kayama M, Sugita Y, Morooka Y, Fukuoka S. Distributed diagnosis system combining the immune network and learning vector quantization. In: Proceedings of IECON '95 - 21st annual conference on IEEE industrial electronics, Vol. 2. 1995, p. 1531–6. http://dx.doi.org/10.1109/IECON.1995.484178, vol.2.

[125] Wang B, Wang S-A, Zhuang J. A distributed immune algorithm for learning experience in complex industrial process control. In: Proceedings of the 2003 international conference on machine learning and cybernetics (IEEE cat. no.03EX693), Vol. 4. 2003, p. 2138–41. http://dx.doi.org/10.1109/ICMLC.2003.1259859, Vol.4.

[126] Jun J-H, Lee D-W, Sim K-B. Realization of cooperative strategies and swarm behavior in distributed autonomous robotic systems using artificial immune system. In: IEEE SMC'99 conference proceedings. 1999 IEEE international conference on systems, man, and cybernetics (cat. no.99CH37028), Vol. 6. 1999, p. 614–9. http://dx.doi.org/10.1109/ICSMC.1999.816622, vol.6.

[127] Jin X, Zhao J, Wang HF. On-line stability control of power systems integrated with distributed generation systems. In: Proceedings of the 41st international universities power engineering conference, Vol. 2. 2006, p. 472–6. http://dx.doi.org/10.1109/UPEC.2006.367522.

[128] Huang H-C. An evolutionary optimal fuzzy system with information fusion of heterogeneous distributed computing and polar-space dynamic model for online motion control of Swedish redundant robots. IEEE Trans Ind Electron 2017;64(2):1743–50. http://dx.doi.org/10.1109/TIE.2016.2562613.

[129] Lau HYK, Wong VWK. A strategic behavioral-based intelligent transport system with artificial immune system. In: 2004 IEEE international conference on systems, man and cybernetics (IEEE cat. no.04CH37583), Vol. 4. 2004, p. 3909–14. http://dx.doi.org/10.1109/ICSMC.2004.1400955, vol.4.

[130] Xiaobo T, Guoqing T. Risk distribution network planning including distributed generation based on particle swarm optimization algorithm with immunity. In: 2009 international conference on sustainable power generation and supply. 2009, p. 1–5. http://dx.doi.org/10.1109/SUPERGEN.2009.5348246.

[131] Lee D-W, Sim K-B. Artificial immune network-based cooperative control in collective autonomous mobile robots. In: Proceedings 6th IEEE international workshop on robot and human communication. RO-MAN'97 SENDAI. 1997, p. 58–63. http://dx.doi.org/10.1109/ROMAN.1997.646953.

[132] Lau HYK, Ng AKS. Immunology-based control framework for multi-jointed redundant manipulators. In: IEEE conference on robotics, automation and mechatronics, 2004, Vol. 1. 2004, p. 318–23. http://dx.doi.org/10.1109/RAMECH.2004.1438938, vol.1.

[133] Yin G. A distributed generation islanding detection method based on artificial immune system. In: 2005 IEEE/PES transmission distribution conference exposition: Asia and Pacific. 2005, p. 1–4. http://dx.doi.org/10.1109/TDC.2005.1547072.

[134] Bhuvaneswari R, Srivastava SK, Edrington CS, Cartes DA, Subramanian S. Intelligent agent based auction by economic generation scheduling for microgrid operation. In: 2010 innovative smart grid technologies (ISGT). 2010, p. 1–6. http://dx.doi.org/10.1109/ISGT.2010.5434745.

[135] Yuan J, Tang A, Zhai X, Yan H, Zheng X, Zhao H. Coordination control strategy of DSSC converter based on multi-objective optimal immune algorithms. In: 2019 IEEE 3rd advanced information management, communicates, electronic and automation control conference (IMCEC). 2019, p. 1987–91. http://dx.doi.org/10.1109/IMCEC46724.2019.8983846.

[136] Lau HYK, Wong VWK. An immunity-based distributed multiagent-control framework. IEEE Trans Syst Man Cybern A 2006;36(1):91–108. http://dx.doi.org/10.1109/TSMCA.2005.859103.

[137] Michelan R, Von Zuben FJ. Decentralized control system for autonomous navigation based on an evolved artificial immune network. In: Proceedings of the 2002 congress on evolutionary computation. CEC'02 (cat. no.02TH8600), Vol. 2. 2002, p. 1021–6. http://dx.doi.org/10.1109/CEC.2002.1004383, vol.2.

[138] Hanumantha Rao B, Sivanagaraju S. Optimum allocation and sizing of distributed generations based on clonal selection algorithm for loss reduction and technical benefit of energy savings. In: 2012 international conference on advances in power conversion and energy technologies (APCET). 2012, p. 1–5. http://dx.doi.org/10.1109/APCET.2012.6302004.

[139] Gao Y, Luo Z. Dynamic task allocation method based on immune system for cooperative robots. In: 2008 7th world congress on intelligent control and automation. 2008, p. 1015–20. http://dx.doi.org/10.1109/WCICA.2008.4593060.

[140] Sun S-J, Lee D-W, Sim K-B. Artificial immune-based swarm behaviors of distributed autonomous robotic systems. In: Proceedings 2001 ICRA. IEEE international conference on robotics and automation (cat. no.01CH37164), Vol. 4. 2001, p. 3993–8. http://dx.doi.org/10.1109/ROBOT.2001.933241, vol.4.

[141] Rimal AN, Belkacemi R. CPS compliant adaptive immune based load frequency control with varying wind penetrations. In: 2016 IEEE power energy society innovative smart grid technologies conference (ISGT). 2016, p. 1–5. http://dx.doi.org/10.1109/ISGT.2016.7781032.

[142] Diez-Olivan A, Ortego P, Del Ser J, Landa-Torres I, Galar D, Camacho D, Sierra B. Adaptive dendritic cell-deep learning approach for industrial prognosis under changing conditions. IEEE Trans Ind Inf 2021;1. http://dx.doi.org/10.1109/TII.2021.3058350.

[143] Khoie M, Sedigh AK, Salahshoor K. PID controller tuning using multi-objective optimization based on fused genetic-immune algorithm and immune feedback mechanism. In: 2011 IEEE international conference on mechatronics and automation. 2011, p. 2459–64. http://dx.doi.org/10.1109/ICMA.2011.5986338.

[144] Pinto R, Gonçalves G, Delsing J, Tovar E. Enabling data-driven anomaly detection by design in cyber-physical production systems. Cybersecurity 2022;5(1):9. http://dx.doi.org/10.1186/s42400-022-00114-z.

[145] Kim YJ, Nam W, Lee J. Multiclass anomaly detection for unsupervised and semi-supervised data based on a combination of negative selection and clonal selection algorithms. Appl Soft Comput 2022;122:108838. http://dx.doi.org/10.1016/j.asoc.2022.108838, URL: https://www.sciencedirect.com/science/article/pii/S1568494622002332.

[146] Outa R, Chavarette FR, Gonçalves AC, Silva SLd, Mishra VN, Panosso AR, Mishra LN. Reliability analysis using experimental statistical methods and AIS: application in continuous flow tubes of gaseous medium. Acta Sci Technol 2021;43(1):e55825. http://dx.doi.org/10.4025/actascitechnol.v43i1.55825, URL: https://periodicos.uem.br/ojs/index.php/ActaSciTechnol/article/view/55825.

[147] He H, Maple C, Watson T, Tiwari A, Mehnen J, Jin Y, Gabrys B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In: 2016 IEEE congress on evolutionary computation (CEC). IEEE; 2016, p. 1015–21.

[148] Leong WD, Lam HL, Ng WPQ, Lim CH, Tan CP, Ponnambalam SG. Lean and green manufacturing—a review on its applications and impacts. Process Integr Optim Sustain 2019;3(1):5–23.

[149] Abualfaraa W, Salonitis K, Al-Ashaab A, Ala'raj M. Lean-green manufacturing practices and their link with sustainability: A critical review. Sustainability 2020;12(3):981.

[150] Rajput SP, Datta S. Sustainable and green manufacturing–A narrative literature review. Mater Today Proc 2020;26:2515–20.

[151] Brandt D, Tschiersch I, Henning K. The design of human-centered manufacturing systems. In: The design of manufacturing systems. CRC Press; 2019, 108–163.

[152] Ruppert T, Jaskó S, Holczinger T, Abonyi J. Enabling technologies for operator 4.0: A survey. Appl Sci 2018;8(9):1650.

[153] Hariharasudan A, Kot S. A scoping review on digital english and education 4.0 for industry 4.0. Soc Sci 2018;7(11):227.

[154] Parrend P, Guigou F, Navarro J, Deruyver A, Collet P. For a refoundation of artificial immune system research: AIS is a design pattern. In: 2018 IEEE symposium series on computational intelligence (SSCI). 2018, p. 1122–9. http://dx.doi.org/10.1109/SSCI.2018.8628868.

[155] Adadi A, Berrada M. Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). IEEE Access 2018;6:52138–60. http://dx.doi.org/10.1109/ACCESS.2018.2870052.

[156] Pinto R. M2M using OPC UA. 2020, http://dx.doi.org/10.21227/ychv-6c68.

[157] Bay SD, Kibler D, Pazzani MJ, Smyth P. The UCI KDD archive of large data sets for data mining research and experimentation. ACM SIGKDD Explor Newsl 2000;2(2):81–5.

[158] Goh J, Adepu S, Junejo KN, Mathur A. A dataset to support research in the design of secure water treatment systems. In: International conference on critical information infrastructures security. Springer; 2016, p. 88–99.

[159] Katser ID, Kozitsin VO. Skoltech anomaly benchmark (SKAB). 2020, http://dx.doi.org/10.34740/KAGGLE/DSV/1693952, https://www.kaggle.com/dsv/1693952.