FACTA UNIVERSITATIS
Series: **Automatic Control and Robotics** Vol. 20, Nº 2, 2021, pp. 123 - 134
https://doi.org/10.22190/FUACR210417010D

Survey Paper

CURRENT TRENDS AND CHALLENGES IN DISTRIBUTED CONTROL SYSTEMS – AN OVERVIEW

UDC ((004.3/.4:0.034.2)+004.78)

Anđela Đorđević, Zoran Jovanović

University of Niš, Faculty of Electronic Engineering, Department of Control Systems, Republic of Serbia

Abstract. *In this paper, innovations in the field of distributed control systems have been considered. Without any claim for completeness, a short summary on current trends in this area has been provided. A special attention is paid to application of blockchain technologies in distributed control systems, game theoretical approach for distributed control applications, and advantages of distributed control for power systems. Also, one of the main issues of modern distributed control systems – cybersecurity has been considered.*

Key words: *Distributed control systems, blockchain technology, game theory, power systems, cybersecurity*

1. INTRODUCTION

With the evolution of industry, one of the main requirements modern industrial control systems meet is increased flexibility. Therefore, distributed control techniques are becoming more and more prominent due to many advantages over centralized control systems which lack both flexibility and scalability. In the last decade, a great deal of research in this field has been done. In [1] a basic structure of a distributed control system has been given, while Poștovei *et al.* considered the evolution of modern distributed control systems (DCS) and some of the challenges they face [2]. Advantages of distributed over centralized systems can also be found in [3]. Many authors considered implementation of distributed control techniques for large-scale systems. Some of the work on this topic can be found in [4]-[6].

A great number of papers consider the advantages of implementing distributed control in power systems [7]-[9]. Schneider *et al.* in [7] proposed the coordination of distributed

Received April 17, 2021 / Accepted August 03, 2021
Corresponding author: Anđela Đorđević
University of Niš, Faculty of Electronic Engineering, Department of Control Systems, Aleksandra Medvedeva 14, 18000 Niš, Republic of Serbia
E-mail: andjela.djordjevic@elfak.ni.ac.rs

and centralized control by implementing laminar control architecture for a better reliability and resiliency of a power system. The advantages of distributed control, cooperative multiagent control technique and the use of neural networks for adaptive distributed control has been considered in [8].

Another interesting approach to the problem of large-scale control can be found in [9], where the principles of game theory have been used in distributed control. Quijano *et al.* in [9] explored the idea of using evolutionary game theory in overcoming frequent problems in large-scale systems. Problems occurring in smart cities, as well as the control of urban drainage systems and microgrids have been addressed from the game theoretical perspective [9].

The 21st century is the time when disruptive technologies, such as blockchain, have emerged. Several authors showed interest in application and implementation of blockchain technologies for distributed control [10]-[12]. The application of blockchain technology in industrial control systems with a goal of better cybersecurity has been considered in [10], while the authors in [11] gave a useful insight into the use of blockchain technology for distributed control and cooperative robotics. Stanciu *et al.* proposed the implementation of blockchain technology in the highest control level of a hierarchical DCS [12]. The system in [12] was based on IEC 61499 standard [13].

With the development of Industry 4.0 and Internet of Things, the question of cybersecurity and privacy becomes more prominent. Distributed systems usually consist of a large number of connected heterogenous devices and are therefore vulnerable to security attacks. A considerable effort to ensure cybersecurity in distributed systems has been made. Some of the research on this topic can be found in [14]-[16]. Pasqualetti *et al.* focused their research on detection and identification of intentional attacks and proposed mathematical models of a system under attack [14]. The work [15] extends some of the results of [14]. Weerakkody *et al.* considered the mechanisms which can be used to prevent perfect attacks and therefore, make the design of a DCS robust and immune to such intrusions. Another work focusing on cybersecurity and privacy of distributed systems can be found in [16], where the differential privacy in DCS has been studied. The authors proposed adding Laplace noise to the signal sent between agents in order to ensure the compromise between providing privacy of data and optimal performance of the system.

This paper is organized as follows. In Section 2, a basic structure of a DCS is given, along with a brief overview of several papers focusing on modern distributed control. The application of distributed control in power systems is presented in Section 3. Section 4 considers implementation of the game theory in distributed control. The application of blockchain technologies in DCS is considered in Section 5, while the issue of cybersecurity in DCS is considered in Section 6. The authors discuss future direction of DCS development and give concluding remarks in the last section.

2. MODERN DISTRIBUTED CONTROL SYSTEMS

The early development of DCS started in the 70s, and since then, these systems have developed significantly. Bangemann *et al.* described the structure of modern DCS using functional blocks such as "*Server"*, "*Engineering Tool"*, "*Human-Machine Interface"*, "*Controller"*, "*Safety Controller"* and "*Field Devices"* [1]. According to [1], high speed networks should be used as a medium of communication between functional blocks in

modern DCS. The highest level in modern DCS systems according to [1], consists of "*Server"*, "*Engineering Tool"*, and "*Human-Machine Interface HMI"* block. These blocks are usually connected via Redundant Ethernet network. Essential information about the system such as configurations, alarm lists, data history and interfaces to other systems, are contained in the "*Server"*. The "*HMI"* blocks provide graphical user interface. The HMI displays, along with network definitions and controller applications, are part of the "*Engineering Tools"* block. One of the most important blocks is the "*Controller"*, in charge of the control logic and algorithms. Distributed systems consist of several controllers, connected with sensors and actuators which are spatially distributed. The communication between the controllers is usually peer-to-peer. It is extremely important that the deterministic behavior is obtained in the system. This is ensured by communication protocols, but the problem arises when wireless devices are integrated in the system. When wireless communication is present, it is harder to maintain the deterministic behavior. The information about the process is acquired via sensors and sent to control logic which determines adequate actions. Human, environment and plant safety are ensured by "*Safety Controller"* [1].

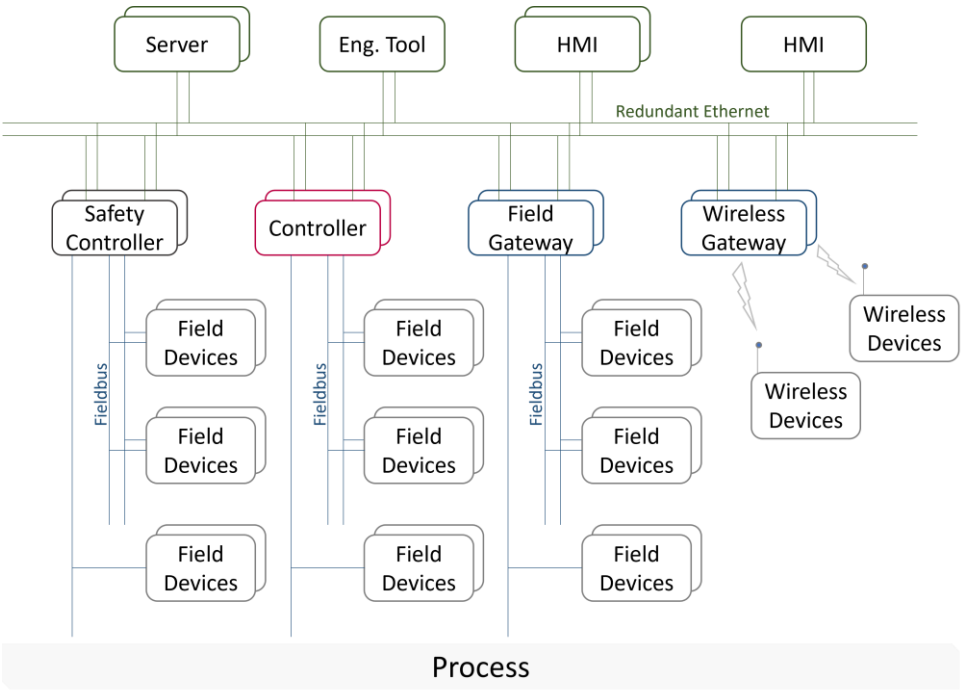

Fig. 1 Modern DCS structure presented in [1, p. 7]

Poștovei *et al.* stated some of the main characteristics of modern DSC in [2]. According to [2], modern DCS is a scalable and modular system that can be easily integrated with other systems. In order to ensure better optimization, the supervision of the control process is centralized. The authors in [2] considered cybersecurity, cloud computing and server virtualization in DCS, along with the integration of DCS into Enterprise Resource Planning

"ERP" and ensuring high availability to be the main challenges of modern DCS. Some of the main characteristics of modern DCS according to [2] are shown in Fig. 2.

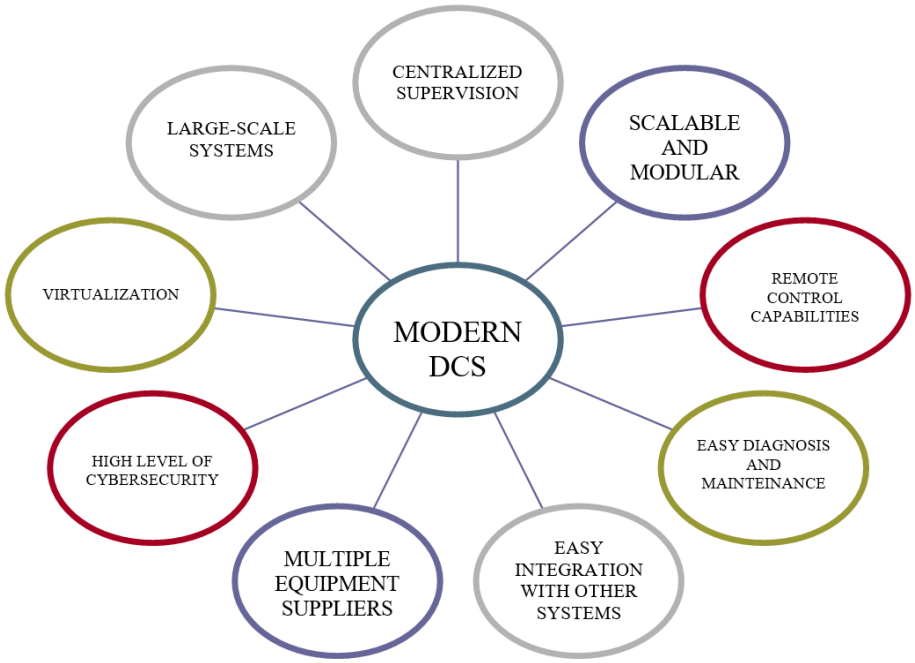

Fig. 2 Characteristics of modern DCS [2]

In [2] the implementation of redundant architecture is proposed in order to achieve the high availability. The authors stated that the aim of this architecture is providing alternative means of communication. Along with an overview of distributed systems' evolution and challenges, the authors have also provided a useful insight on the implementation of modern DCS in Electrical Power Systems: EPS. In order to ensure redundancy, authors considered two common architectures for DCS in EPS: a combination of "Rapid Spanning Tree Protocol" (RSTP) and "Link Aggregate", or a combination of "Parallel Redundancy Protocol" (PRP) and "Link Aggregate" [2].

The distribution of controllers and monitoring elements over the plant area is one of the most important advantages of DCS compared to centralized control where a single controller has a central role in managing all components of a system [3]. Therefore, a single controller gets the information about the whole process and provides adequate actions as an answer. On the other hand, a role of a controller in DCS is not managing a whole process, but only some segments. Bearing that in mind, it can easily be concluded that a failure of one element in a distributed system does not result in the failure of system operation, which is not the case in centralized control systems [3]. Therefore, it is common to describe a large-scale problem as a composition of several smaller problems. Also, a great issue when the centralized controller is applied is the need for high-bandwidth communication and complex architecture when the number of components in the system is large. Still, centralized control provides a higher level optimization of system operation.

3. DISTRIBUTED CONTROL IN POWER SYSTEMS

The advantages of implementing distributed control in power systems have been considered in many papers [7]-[9]. Schneider *et al.* in [7] stated few advantages of distributed versus centralized control for power systems such as better scalability and interoperability, spreading computational burden across the platform, better data communication accessibility, lower cost, etc. Still, the authors did not ignore the fact that centralized control gives the opportunity of better process optimization. Therefore, the authors presented the implementation of the laminar control for distributed power systems. The laminar architecture is hierarchical with constrained interactions between layers. This ensures interoperability in case when large numbers of devices are connected to the system. As it was stated in [7, p. 9963]: "The constraints on interactions between layers take two forms: the layering of controls, and the decomposition of objectives into sub-objectives, or sub-problems, with constraints coupled between layers." Each layer operates with respect to imposed constraints to achieve its goals. The laminar architecture scheme described in [7] is presented in Fig.3. The first layer consists of local (edge) devices. In this layer operations are pre-programmed and based on the information acquired by sensors. The second layer provides distributed coordination of grouped first layer devices. This level provides peer-to-peer communication, and therefore minimizes the need to communicate directly with the central node. The highest layer represents the central unit which uses all available resources in order to achieve a high level of optimization for system operation. If a solution is not time critical, it is obtained by intensive computations and optimizations executed in the central node [7].

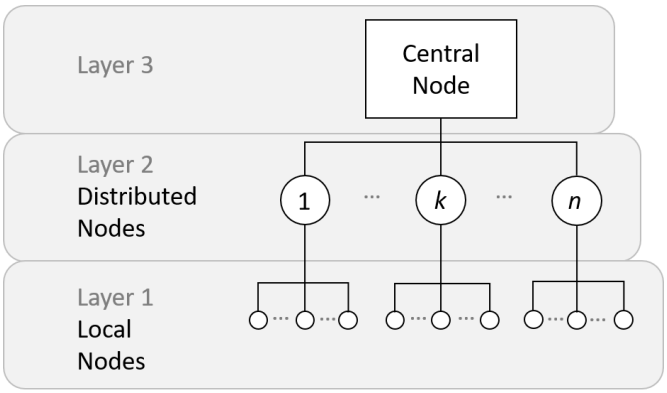

Fig. 3 Laminar control scheme [7]

This architecture enabled the coordination of distributed and centralized control. Consequently, the operational flexibility was increased, and this solution led to the improvement of resiliency and reliability of distributed power systems [7]. The main focus of the authors in [7] was on implementing the laminar control architecture to provide a better coordination of utility and non-utility assets.

Another interesting research in this field can be found in [8]. Bidram *et al.* considered the distributed generators' coordination using microgrids. According to [8], the control strategy in microgrids can be divided into a primary, secondary and tertiary control. The main focus of the authors was on the secondary control level, essential for the power

quality and maintaining optimal operation of the system. The authors considered the advantages of the application of a distributed communication network instead of a centralized structure for this layer. A solution where the cyberinformation flow layer is used as a distributed communication network has been considered. This layer determines the communication links between distributed generators. The authors considered the implementation of cooperative multiagent control techniques in the secondary control layer [8]. According to [8], this technique gives neighbouring agents the opportunity to exchange information in order to achieve a common goal. Each agent can exchange information only with its neighbours. The authors applied the input-output feedback linearization method for the transformation of distributed generators' dynamics. In [8], the authors have also considered the use of neural networks in order to implement the adaptive distributed control. They stated that the application of neural networks had made the system robust to changes of distributed generators parameters.

The dispatch problem in power systems was considered in [9]. The approach proposed in [9] will be further explained in the next chapter.

4. GAME THEORETICAL APPROACH FOR DISTRIBUTED CONTROL

Distributed control from game-theoretical perspective has been considered in [9]. In work by Quijano *et al.* the application of game theory, concretely the evolutionary game theory (EGT) in overcoming large-scale system challenges has been considered. The paper focused on some of the prominent problems in smart cities. The authors explored problems of optimal economic dispatch in microgrids, smart lighting and control of urban drainage systems. According to Quijano *et al.* there are three main challenges common in large-scale systems [9]:

1) information needed for proper operation of the system;
2) the architecture of the system and communication structure involve certain economic costs;
3) expensive computation for the control inputs.

If a large-scale system consists of many agents, EGT strategies, especially the evolutionary game dynamics, can be used to model interactions between agents. The authors stated three advantages of EGT application in control systems: parallel between engineering problems and games, game solutions obtained using Nash equilibrium and optimization solutions are related, and the last advantage lays in the fact that local information can be used to find the solution of a game [9]. The authors stated that if an engineering problem is addressed by applying game framework, centralized coordination of a process can be easily avoided.

The authors have proposed population dynamics approach for the dispatch problem in power systems. Two approaches were proposed in [9]: one where central controller executes the dispatch algorithm, and second with the distributed algorithm. As it has been mentioned earlier, the main problem with the centralized controller is the need for high-bandwidth communication and complex architecture when the number of components in the system is large. Therefore, the authors proposed the distributed replicator dynamics to address the optimal dispatch problem [9].

One of the smart city problems the authors considered in their work was the problem of smart lighting. The application of distributed replicator dynamics was again proposed

as control strategy since it supports efficient use of energy resources. As much as low energy consumption is important, it is also crucial to provide adequate lightning levels for the smart-city residents. Large urban systems, buildings for example, are usually divided in areas supervised by local controllers [9]. According to [9], in this kind of environment it would be ineffective to apply centralized control techniques because of the large number of devices. Therefore, the implementation of distributed techniques is advisable due to the low computational burden and robustness to packet loss. Quijano *et al.* proposed a resource-allocation strategy to address the problem of illumination control. The authors based this strategy on distributed replicator dynamics to achieve desired illumination while taking care that both the energy consumption and network structure are adequate. The authors stated that the main difficulty which occurs when this strategy is applied is the fact that the illumination of one area is dependent on the voltages of all lamps. Therefore, the authors have defined voltage vectors as the population state, illumination areas as the strategy set and limited voltage available in the system as the population mass. To address the issue of constraints on the voltage vector and inability to reach the setpoints, the authors introduced a fictious area acting as a surplus variable. The strategy designed in [9] was tested in two environments: "*divided environment*" where the areas were separated by half sized walls, and "*open environment*" where the areas were open. The results showed that the desired illumination was achieved in all areas in the "*divided environment*", while this was not the case in the "*open environment*". This problem occurred because of the truncation in certain areas in the "*open environment*".

Another application of game-theoretical strategies in smart cities, which was the research subject of Quijano *et al.* in [9], is for solving the problems occurring in urban drainage systems (UDS). The authors consider computational burden to be one of the main issues in UDS control. This problem occurs due to the significant number of control signals and states to be estimated. Again, Quijano *et al*. have proposed minimizing overflows by solving resource-allocation problem. A decentralized population-games-based controller has been suggested for this purpose. The authors modeled the system using the hydrological model. The effects of heavy rain as disturbances were considered. The division of the system into several subsystems which are controlled independently was proposed. For the purpose of the research, a case study of stormwater UDS in Bogotá, Columbia was performed. It has been demonstrated that the overflows in case of an abrupt rain can be avoided by using decentralized population-games-based technique [9].

5. Application of Blockchain Technology in Distributed Control Systems

Blockchain technology is a new disruptive technology mostly known for its application in cryptofinance. However, the use of blockchain technology can be far broader beyond Bitcoin. Several authors explored the application of blockchain technologies in industrial control [10]-[12]. For example, implementation of blockchain techniques for better cybersecurity of industrial systems was considered in [10]. In [11], Khan *et al.* give an overview of blockchain applications in control systems as well as some of its main advantages and disadvantages. According to the authors, one of the main advantages of blockchain technology implementation in DCS is the prevention of unauthorized access to a system, unauthorized data alteration, etc. The authors stated that decentralization, as one of the most prominent characteristics of this technology, plays a major part in preventing security problems and

solving the issue of interruption and interception. According to [11], third-party interference is prevented because all the nodes in the network have the original copy of the data, so when one copy is changed, the rest of the nodes still have the original one. Another issue considered in [11] is unauthorized data addition made to look legitimate. The authors stated that this problem can be solved by applying blockchain technology, since it is impossible to make data alterations inside one block and to maintain the valid hash which is contained in the next block. Bearing this in mind, it can be concluded that implementation of blockchain technologies can be greatly beneficial in data misuse prevention. Even though the application of blockchain technologies in DCS can have many advantages, the authors also pointed out some of its disadvantages and limitations. One of the main limitations would be the time required for transaction validation. Long validation time is the cause of latency in data transactions. This is a big issue especially for systems that require fast response. Another problem considered in [11] is the problem of "51% attack", referring to the hypothetical situation where the system security is threatened if 51% of nodes decide to attack the system and modify the data. Finally, the authors also raised the question of privacy of DCS with implemented blockchain technology since the main book by default is always public.

Stanciu in [12] explored the implementation of blockchain technology for hierarchical DCS. Blockchain solution suggested by Stanciu was Hyperledger Fabric. The author proposed applying blockchain technology as a platform for edge computing, a modern method used to ensure that the latency requirements are met, especially when huge volume of data should be processed. Also, the author stated the advantage of using edge computing when it is desirable that data processing is executed as close as possible to end devices. The author concluded that the implementation of this technique can be beneficial for DCS because of its capability to reduce large data transfers and increase responsiveness. In [12] hierarchical structure has been considered. The DCS was based on IEC 61499 standard. The advantages of IEC 61499 architecture have been considered in [13], where Vyatkin presented a survey on the development of this standard and its applications. The strategic role in the structure is given to a central automation system with implemented blockchain technology [12]. This is the highest level of the structure where validation of smart contracts is executed. The medium layer consists of distributed control nodes in charge of the management of field devices.

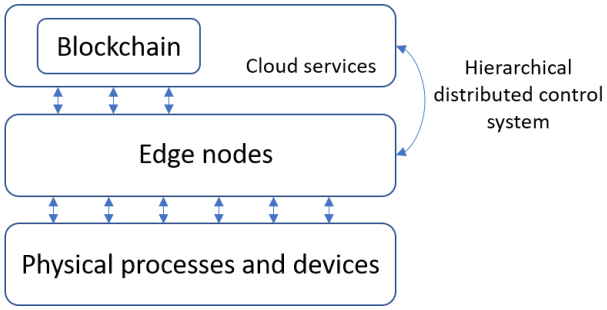

Fig. 4 Control scheme with implemented blockchain technology proposed in [12, p. 668]

The major problem the author noticed is the fact that smart contracts within the system are not capable of accessing outside data. Stanciu proposed implementation of

specialized decentralized blockchain. This way, the data is provided into the blockchain and then consumed by smart contracts. According to the author, another advantage of this solution is the possibility of data transfer to remote devices. The results of the research also showed that the capacity of the highest layer, where blockchain technology was implemented, to process data in real time is limited. However, Stanciu supposed that the data processed by this layer is not of large volume since its main role is strategic and mainly involves supervising the lower layer which has direct control over field devices [12].

6. CYBERSECURITY OF DISTRIBUTED CONTROL SYSTEMS

Distributed systems are vulnerable to cyberattacks mainly due to their dependance on communication networks and large number of components they consist of. In particular, large-scale systems consist of a considerable number of heterogenous components and are therefore notably exposed to numerous attacks. The issue of cybersecurity in DCS has been considered in many papers, some of which can be found in [14]-[16]. The focus of Pasqualetti *et al.* in [14] was on the detection and identification of attacks in cyber-physical systems. The authors proposed a mathematical formulation of a system under attack, modeled based on known attack scenarios, such as "false data injection", "stealth", "replay attacks", "deterministic static detection problem" and "covert attacks". In [14], mathematical definitions of "*detectability*" and "*identifiability*" have been given. Pasqualetti *et al*. stated that "An attack is undetectable (respectively unidentifiable) if no measurements due to the attack coincide with the measurements due to some nominal operating condition." [14, p. 2712]. The authors have analyzed circumstances under which undetectable attacks may take place, determined by the system interconnection structure. This work also provided characterization of an undetectable attack from a graph-theoretical perspective. As defined in [14, p. 2718], "Analogous to detectability, the identifiability of an attack is the possibility to distinguish from measurements between the action of two distinct attacks." Pasqualetti *et al.* also considered capabilities of different types of monitors from graph-theoretical and system-theoretical perspective. Centralized and distributed monitors designed to recognize attacks have been recommended.

Procedures to prevent perfect attacks have been considered in [15], where some of the results of [14] have been extended. Three main contributions have been provided: extending the concept of structural left invertibility to the concept of vertex separators, formulating and solving sensing and communication optimization problems while providing perfect attack resilience, and, in the end, minimizing communication networks for a constrained optimization problem. The design of robust system immune to perfect attacks has been considered. Weerakkody *et al*. also considered the case where constraints on communication between components were imposed. The authors focused on distributed systems with p as a maximum number of agents which could be threatened by an attack. Any atypical behaviour of the system is recognized by a centralized anomaly detector. The main assumption in [15] was that the attacker's objective is to disrupt the distributed system without being noticed by the anomaly detector. This way, the system could be under the attack for a long time without the appropriate defence. The additional attack nodes were introduced to describe malicious inputs. The authors proved

that the size of minimal vertex separators between additional node and each agent influences the system's vulnerability to perfect attacks. According to Weerakkody *et al.* "If an attack is perfect, both measurement and residues of the DCS are unaffected by the adversary's actions. As a result, the adversary is able to bias the state away from the region of desired operation without incurring detection" [15, p. 63]. It is also stated in [15, p. 64] that "In order to design a system that ensures deterministic detection of an adversary, more sensors are required than potential attack inputs". Weerakkody *et al.* noted that "In order to verify that a system is robust to perfect attacks we must ensure the size of the minimum vertex separator for each agent of the system is at least p (equals to the number of sensors and agents that can potentially be compromised)" [15, p. 64]. The authors concluded that attack detection is possible if the system is structurally left invertible for all feasible attacks.

An interesting research concerning differential privacy in DCS can be found in [16], where Wang *et al.* studied the issue of compromise between optimal performance and data privacy. Information exchange always involves a certain risk of privacy abuse. The authors stated that it is not possible to achieve both optimal privacy and optimal performance [16]. If optimal privacy is to be achieved, the agents would have to act without exchanging any information. On the other hand, if optimal performance is the goal, it would likely be obtained if agents exchanged all the information, but that would carry a great risk of data misuse. In order to solve the issue of differential privacy, the authors have proposed adding Laplace noise to the information exchanged between agents. The point of applying Laplace mechanism is preventing third party to determine the aggregate state of the system [16]. The authors gave the following definition of differential private mechanisms "By definition, differentially private mechanisms ensure that two alternative values of the private data set cannot be distinguished by any sequence of reported states with significant probability, therefore, it obstructs accurate estimation on the private data set for an observer" [16, p. 119]. However, this rises a possible problem of non-optimal performance since estimation of the system state is not precise. The authors have shown that when Laplace mechanism is applied, the performance cost for stable systems grows as $O(T3/N\varepsilon 2)$. The authors used ε to denote privacy parameter (with the increase of ε, the strength of privacy mechanism rises), while T denotes time horizon. On the other hand, if a system is unstable, the cost could grow exponentially. According to the authors, the entropy of an unbiased estimator of the private dataset is affected by the number of agents, dimension of each agent's state and time horizon. Differential privacy was ensured, and the entropy was minimized using Laplace mechanism [16].

7. CONCLUSION

In this paper, the authors presented a brief overview of current trends in distributed control systems. The authors specially focused on advantages of distributed control for power systems, distributed control from game-theoretical perspective and application and implementation of blockchain technologies in DCS. Distributed control techniques are superior to centralized techniques when it comes to flexibility, scalability and interoperability, but the advantages of the centralized control should not be denied. Having in mind the fact that the centralized control offers a superior operation optimization, applying a hierarchical structure which embeds the best features of the distributed and centralized control is

frequently proposed for some processes. Applying the principles of game theory in DCS can be beneficial, especially for large-scale systems. The authors believe that implementation of game theoretical principles, as well as blockchain technology, in DCS present an interesting possible direction of distributed control development. Benefits, application and full potential of blockchain implementation in distributed control are yet to be explored. This is an intriguing topic to be explored in the future.

Another important question has also been covered in this paper: the issue of cybersecurity in DCS. Bearing in mind the fact that distributed systems are usually large-scale and, therefore, consist of a considerable number of devices, it can easily be concluded how exposed and sensitive they can be to cyberattacks. The development of Industry 4.0 and IoT carries a great deal of risk from data misuse and third-party attacks. Therefore, providing adequate mechanisms to detect, identify and prevent cyberattacks is crucial. The question of cybersecurity and data privacy is not to be neglected and should be approached seriously and consciously.

Acknowledgement: *This work has been supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia. This paper was realized as a part of the projects III 43007 and TR 35005, funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia.*

REFERENCES

[1] T. Bangemann, S. Karnouskos, R. Camp, O. Carlsson, M. Riedl, S. McLeod, R. Harrison, A. W. Colombo and P. Stluka, “Chapter 2 State of the Art in Industrial Automation.” (2015).

[2] D. A. Poștovei, C. Bulac, I. Triștiu and B. Camachi, "The evolution and challenges of modern Distributed Control Systems," *2020 IEEE 14th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania, 2020, pp. 000089-000094, doi: 10.1109/SACI49304.2020.9118829.

[3] “What is Distributed Control System (DCS)?”, [Online]. Available: www.electricaltechnology.org/2016/08/distributed-control-system-dcs.html

[4] D. Zhang, P. Shi and Q. G. Wang, "Energy-efficient distributed control of large-scale systems: a switched system approach," *International Journal of Robust and Nonlinear Control*, vol. 26 no. 14, pp. 3101-3117, December 2015, doi: 10.1002/rnc.3494.

[5] D. Zhang, S. K. Nguang and L. Yu, "Distributed control of large-scale networked control systems with communication constraints and topology switching," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 47, no. 7, pp. 1746-1757, July 2017, doi: 10.1109/TSMC.2017.2681702.

[6] T. Koponen et al., "Onix: A distributed control platform for large-scale production networks", *OSDI'10: Proceedings of the 9th USENIX conference on Operating systems design and implementation*, vol. 10, pp. 351-364, October 2010, doi: 10.5555/1924943.1924968.

[7] K. P. Schneider et al., "A Distributed Power System Control Architecture for Improved Distribution System Resiliency", *IEEE Access*, vol. 7, pp. 9957-9970, 2019, doi: 10.1109/ACCESS.2019.2891368.

[8] A. Bidram, F. L. Lewis and A. Davoudi, "Distributed Control Systems for Small-Scale Power Networks: Using Multiagent Cooperative Control Theory," *IEEE Control Systems Magazine*, vol. 34, no. 6, pp. 56-77, Dec. 2014, doi: 10.1109/MCS.2014.2350571.

[9] N. Quijano, C. Ocampo-Martinez, J. Barreiro-Gomez, G. Obando, A. Pantoja and E. Mojica-Nava, "The Role of Population Games and Evolutionary Dynamics in Distributed Control Systems: The Advantages of Evolutionary Game Theory," *IEEE Control Systems Magazine*, vol. 37, no. 1, pp. 70-97, Feb. 2017, doi: 10.1109/MCS.2016.2621479.

[10] M. Mao and H. Xiao, “Blockchain-based Technology for Industrial Control System CyperSecurity”, *2018 International Conference on Network, Communication, Computer Engineering (NCCE 2018)*. Atlantis Press, pp. 903-907, May 2018, doi: 10.2991/ncce-18.2018.151.

[11] A. T. Khan, X. Cao, S. Li and Z. Milosevic, “Blockchain Technology Applications to Distributed Control and Cooperative Robotics: A Survey”, *International Jurnal of Robotics and Control* vol. 2, no. 1, pp. 36-48, January 2019, doi: 10.5430/ijrc.v2n1p36.

[12] A. Stanciu, “Blockchain Based Distributed Control System for Edge Computing”, 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, 2017, pp. 667-671, doi: 10.1109/CSCS.2017.102.

[13] V. Vyatkin, "IEC 61499 as Enabler of Distributed and Intelligent Automation: State-of-the-Art Review," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 768-781, Nov. 2011, doi: 10.1109/TII.2011.2166785.

[14] F. Pasqualetti, F. Dörfler and F. Bullo, "Attack Detection and Identification in Cyber-Physical Systems," IEEE Transactions on Automatic Control, vol. 58, no. 11, pp. 2715-2729, Nov. 2013, doi: 10.1109/TAC.2013.2266831.

[15] S. Weerakkody, X. Liu, S. H. Son and B. Sinpoli, “A Graph-Theoretic Characterization of Perfect Attackability for Secure Design of Distributed Control Systems”, IEEE Transactions on Control of Network Systems vol. 4, no. 1, pp. 60-70, March 2017, doi: 10.1109/TCNS.2016.2573741.

[16] Y. Wang, Z. Huang, S. Mitra and G. E. Dullerud, "Differential Privacy in Linear Distributed Control Systems: Entropy Minimizing Mechanisms and Performance Tradeoffs", IEEE Transactions on Control of Network Systems, vol. 4, no. 1, pp. 118-130, March 2017, doi: 10.1109/TCNS.2017.2658190.