9th International Conference on Through-life Engineering Service
3-4 November 2020, Cranfield UK

Manufacturing Process Control Through a Digital Twin: Encoding Issues

Alexios Papacharalampopoulos[a], Christos Michail[a], Panagiotis Stavropoulos[a,*]

[a]*Laboratory for Manufacturing Systems and Automation, Department of Mechanical Engineering and Aeronautics, University of Patras, Patras 265 04, Greece*

** Corresponding author. Tel.: +30 2610 910 160; fax: +30 2610 997 314. E-mail address: pstavr@lms.mech.upatras.gr*

Abstract

A Manufacturing Process Digital Twin is highly useful in Process Control, since it shows adaptiveness and near-real-time responsivity. However, cloud architectures are in place, or more commonly, CPS-based modules communicate through IoT technology, implicating security (data-related) and safety (concerning proper control enforcement). With respect to Thermal Processes, and in particular Laser Welding, this work studies the effect of encoding on Process Control efficiency. More specifically, compression and encryption are applied to control signals and the process control efficiency is studied. The simulations used to this end are considered to be part of a digital twin.

Keywords: Process control; Digital Twin; Cryptosystem; Manufacturing processes

1. Introduction

Process control in laser welding is a fundamental property to succeed in producing high quality products. As a matter of fact, the emergence of Cyber-Physical-System (CPS) in laser-based processes can play an important role in addressing the issue of real-time communication under the context of Digital Twin (DT) [1]. The role of the digital twin would be to be used as means of control and/or optimization of the process itself. Integrating Control theory, it would be robust and adaptive enough to capture uncertainty in real time and be able to provide the physical system (process) with feedback.

Recently, a considerable part of literature has grown around the communications through wireless networks and have been addressing challenges around the security enhancement and delay-prone communications in the context of Cyber-Physical Systems [2–4]. Furthermore, the trend of Big Data on industrial scale manufacturing processes, such laser welding, needs the appropriate development for the aforementioned demands [5]. Thus, delays from IoT devices through Networked Control System (NCS) could lead to undesirable performance leading to out-of-tolerance product. Several studies suggest robust controllers addressing time-varying (or dead-time) delays [6, 7] or simulate packet dropouts [8]. Another approach to overtake time-delays is utilizing the switched or hybrid systems [9–11].

On the other hand, the communication of machines could implicate cyber threading during that time. Hence, the outcome of a corrupted control signal may cause a physical damage and so the awareness of such threats should be addressed in the context of Cyber-Physical Systems [12].

Traditionally, source and channel coding are encountered, implying compression and error correction, respectively. The first one reduces the data size, whilst the second one increases it [13]. Examples of such algorithms families are Lempel-Ziv and Hamming, respectively. Encryption (in terms of cryptography) is also considered on top of those two [14].

In this research work, being an application of encryption and decryption conducted to control signals, one set of encryption-decryption is performed each time the signal is transmitted through the Networked Control System. In Figure 1, a Digital Twin Controller with the adoption of a cryptosystem is depicted. Recently, researchers computed the encrypted controller with homomorphism attribute in which the parameters of controller compute from the encrypted reference feedback and control signals over the communication links [15–19].

Also, under the concept of utilizing Cyber Physical System (the new trend of current status of industry towards smart manufacturing) and cloud-based manufacturing processes, it seems that there is lack for authentication of data while attackers may find easy vulnerable access and especially in process control of laser welding [20].

Laser-based manufacturing processes, such as welding, require transmitting through Internet of Things (IoT) devices vast amount of data, (leading to need Big Data techniques [21]) and the need of

cryptography architectures would be crucial to the integrity of data.

In literature, process control could be enhanced with respect to security through adopting cryptography methods such as Rivest–Shamir–Adleman (RSA) [22], ElGamal [16], Advanced Encryption Standard (AES), Data Encryption Standard (DES), Paillier [15, 23–25] algorithms or with validation of the audits through the current trend of blockchain [26, 27].

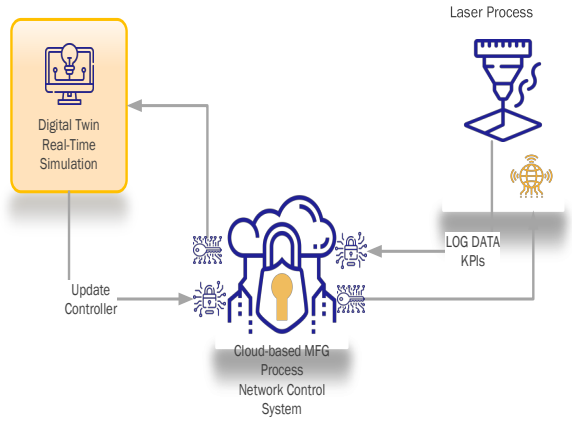

Figure 1 Digital Twin Controller

In the current work, process models are used to design a proper controller able to manipulate the delays introduced by coding-related modules such as cryptography encryption/decryption. Then, the efficiency of the controller is studied.

2. Approach

A laser process model was developed through (Finite Element Method) FEM commercial software in order to obtain via system identification techniques the dynamical system under an empirical heat flux profile. It is worth mentioning that previous research has attempted either Proportional-Integral-Differential (PID) family controller for the linear system [12, 22, 28] or Model Predictive Control (MPC) synthesis [24, 29].

In the current paper, an observer-based controller has been implemented with the H∞ state-feedback from [30] for the controller gain K in terms of Linear Matrix Inequalities (LMIs) while an observer L was assumed to the purpose of the process control. This robust controller should maintain the designed control performance within certain bounds of disturbances / delays / uncertainties [31]. This paper aims to highlight the importance of security of control signal against attackers / threads with RSA technique as a proof of concept with a robust controller to obtain the desired temperature within adequately fast settling time.

The following discrete-time time-invariant linear system is considered where $x \in \Re^n$ is the state vector, $y \in \Re^m$ the controlled output, z the performance output and w the exogenous input. All the matrices have the appropriate dimensions.

$$\begin{aligned} x(k+1) &= Ax(k) + B_w w(k) + B_u u(k) \\ z(k) &= C_z x(k) + D_{zw} w(k) + D_{zu} u(k) \\ y(k) &= C_y x(k) \end{aligned} \quad (1)$$

Theorem: A controller in the form (3) exists if and only if the matrices X, L and P exist such that the objective function value μ is minimized in the following LMI [30]:

$$\begin{bmatrix} P & AX + B_u L & B_w & \mathbf{0} \\ (\cdot)^T & X + X^T - P & \mathbf{0} & X^T C_z^T + L^T D_{zu}^T \\ (\cdot)^T & (\cdot)^T & \mathbf{I} & D_{zw}^T \\ (\cdot)^T & (\cdot)^T & (\cdot)^T & \mu \mathbf{I} \end{bmatrix} > 0 \quad (2)$$

where X, L and P are the variables.

The control-law of a linear static state-feedback system is:

$$u(k) = Kx(k) \quad (3)$$

where K equals to the static gain

$$K = LX^{-1} \quad (4)$$

Figure 2 depicts the possible three positions of coding modules in the generic feedback scheme.

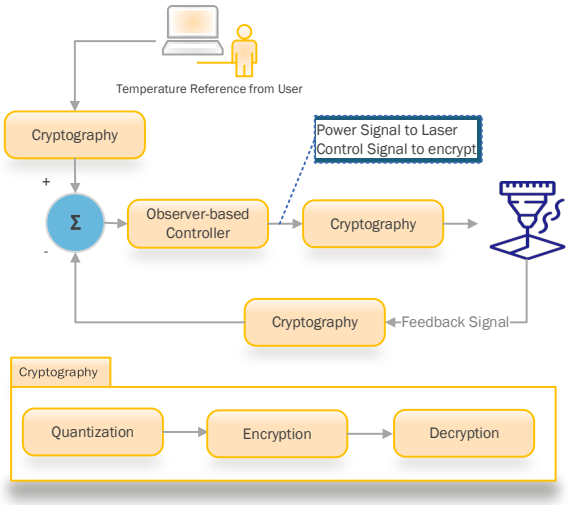

Figure 2 Cryptography-based Process Control System for Thermal Process

For the case of studying the encryption of controller, saturation filters have not been considered.

It is noted here that in terms of services, the digital twin can be considered to augment the part

and/or the process towards an enhanced system that can provide feedback to the operator be self-adjusted. This is highly profitable for the manufacturing phase as well as the whole product lifecycle, as concepts realized from circular economy, such as remanufacturing or even recycling would be rendered possible [32]. Quality assessment is also implementable in the context of this Digital Twin, however, this exceeds the purpose of the current work. It is worth mentioning, though, that the concept of Product-Service System [33] is very useful from business point of view to supporting the aforementioned augmentation.

3. Case Study: Process Control of Laser Welding

3.1 Process control efficiency

The case of heating up with laser source is considered here as per previous literature. The performance of a controller based on cryptography algorithms should not deteriorate the initial measurements. The received signals (input signal to encryption) have to be the same when the decryption (output signal) is completed and the pass from the communication network via the IoT devices. The implementation of RSA cryptosystem was selected for the control and feedback signal and a Personal Computer was used to this end.

Below, in the following two diagrams, the evolution of heat flux and temperature signals is depicted, comparing their initial and decrypted states, which coincide, as well as their encrypted state for reference. It is noted that the encrypted state has no physical interpretation and has only data related value.

It's clearly observed that the RSA algorithm has been utilized successfully for both control and feedback signals as shown in Figure 3 while the computational time for control signal is depicted in Figure 4. The encryption/decryption of control and feedback are performed as expected with the input signal to be ciphered correctly and the decryption to be identical to the actual signal. This technique provides end-to-end encryption throughout the operation while the crucial data e.g. in case of laser welding the desired attributes are temperature, power of laser, welding speed and many other Key Performance Indicators (KPIs).

Next, what has been depicted in Figure 4, is the delay of coding the samples. It has been measured in terms of computational time. Overlooking the high initial delays, probably due to some ramp-up procedure caused by initialization of variables, it is observed that the delays are comparable to the sampling rate of the discrete system used. Thus, the delay can be considered to be discrete. This can be further engineered by the fact that additional delay can be added so that is rendered steady. However, in the next sections a robust controller is designed and studied.

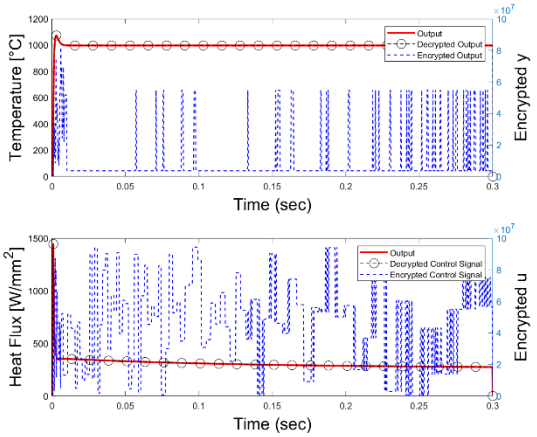

Figure 3 Encrypted/Decrypted Feedback Signal (upper), Encrypted/Decrypted Control Signal (lower)

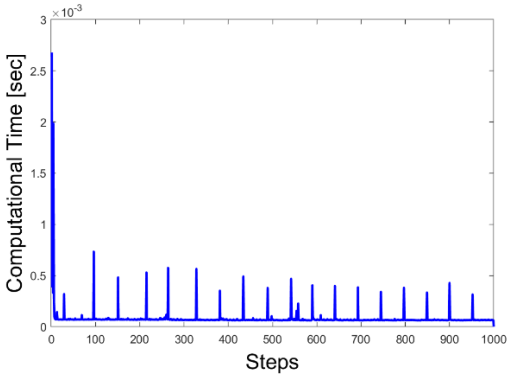

Figure 4 Computational Time of Control Signal to Quantized-Encrypted-Decrypted

3.2 Effect of time-varying delay system

In this section, an investigation of the controller's efficiency is conducted. The delay of computational time assumed as a single timestep k in the differential equations of state-space model. The transfer function of delay in the control theory is described by z^{-d}, where d takes non-negative integer numbers. For the current simulation, it is assumed to be a varying delay between the values of 0 and d_{max}. The schematic depicts in Figure 5.

The implementation in the Simulink environment is convenient as the delay extent can be controlled in many ways. In the current implementation, the delay is stochastic. Furthermore, the position of the controller implies temperature tracking. No phase change is involved, however, the temperature range covered renders the system rather complicated, due to change of dynamics as temperature increases and conduction / convection / imposing laser

characteristics change with respect to each other. The controller in this case is designed only using the initial system. It is worth noting that throughout this work, the controller has been modified to include also the observer, minimizing the connectivity requirements in the schematics. It is noted here that it would be of high importance to check the non-negativity of the flux used as a control signal, since the laser machines do not have the capability of cooling locally the part. So, a limitation in flux should be taken into account.

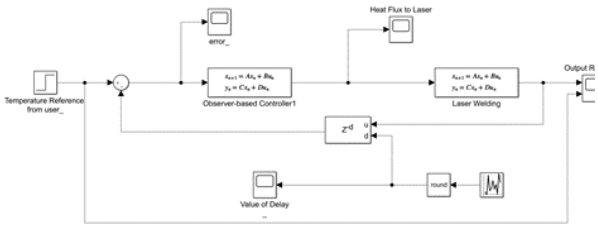

Figure 5 Time-varying delay schematic

3.3 Utilizing a robust controller

Finally, a switched system among the whole ensemble of systems is regarded, taking into account initial system (delay-free) and the delayed with dmax. The delay z^{-d} increase the order of plant by the delay value. For this reason, an augmentation sliding matrix implemented in order to coincide the size of matrices. The simulation was conducted in Simulink with a random switching rule and then the gain of the controller is tailored accordingly. In this case the controller has been designed for all the systems with delays between 0 and d_{max}. The overall maximum value for dmax has been considered to be equal to three samples, since, as aforementioned, three stages of encryption are required: cryptography, compression and error correction and one sample could be adequate for each one of them.

4. Results & Discussion

4.1 Addressing delays from Cryptography

The following diagram (Fig. 6) depicts the responses of a closed loop system in two variants: without and with stochastic delay.

Both systems seem to converge to the tracking temperature and reaching a steady-state within an acceptable time interval. The value of delay which derives from ciphering the signal does not alter settling time or overshoot. The latter is a special characteristic of the process because of the outcome that has to the product, for instance the dynamic overshoot may cause over-melting and modify the desirable melt-pool dimensions such as width and depth, or even affect the material structure [34].

Next, an accumulation of time-delays derives from cryptography and signal transmission in/out to network was considered. The varying values of delay range from 1 to 3 samples controlled by an integer random source. The network-based control system guarantees the stability of such time-delays and the performance is shown in Figure 7.

The congested delays in the control system influence only the overshoot while the steady-state agrees with the initial system. For short lags the developed controller operates with the desirable performance. In order to tackle longer delays, more sophisticated time-varying delays based on network control system could be implemented.

The normal encryption method responded as expected corresponding to the signals of the experiment while the computational cost remains close to zero. The effect of delay while varying between 0 and 1 shows the robustness of controller under the interval delays in the system and even between 1 and 3. Hence the acceptance of such controllers may be a considerable step to laser-welding industry.

The third part of simulations examines the performance of switched system under a random rule and utilizing the robust controller that is intended to handle potential delays between zero and one samples. The performance of the closed loop system is depicted in Fig. 8.

The performance has not been improved, however, this may be due to a lot of factors, namely:

- Controllability may be computationally stiff. The condition number of the controllability matrix increases 15 orders of magnitude if one delay is added, one more order is added by the second delay, and one more by the next one.
- The controller may be insufficient as it is static, while it is also robust towards input uncertainties, due to robust modelling.
- Controllability may be affected by augmentation also.

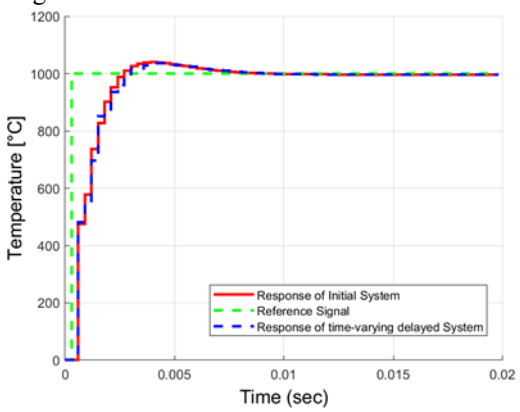

Figure 6 Response of closed loop system with time-varying delay system {0,1} and simple Hinf Controller

To check if this the case, the Controller has been designed also for delays 0 to 3. The results have been

promising, as the overshoot duration seems to be enhanced. However, the overshoot itself has not been reduced.

As a result, it seems that no direct conclusion can be drawn at this moment, and further elaboration has to be made on the causes that may affect the performance of the closed loop system.

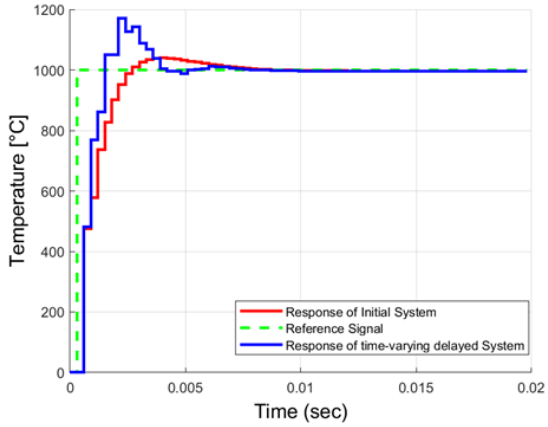

Figure 7 Response of closed loop system with time-varying delay system {0,..,3} and simple Hinf Controller

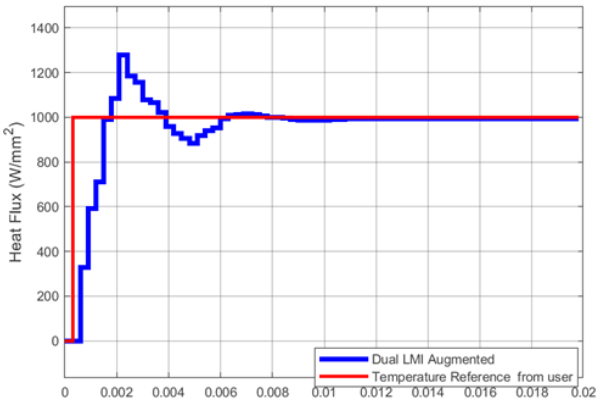

Figure 8 Response of closed loop system with time-varying delay system {0,..,3} and $H_{infinity}$ Controller for {0,1}

4.2 Cryptography efficiency

Another issue to be tackled is the cryptography efficiency itself. Normally, algorithms have been checked with respect to changing characteristics of the message, however, herein it is signals that have to be encrypted. So, for the case of Fig. 3, which may be characterized more predictable situation, the histograms of the involved signals are given in Fig. 9.

It is apparent that the statistical description of the signal has completely changed with encryption. This renders the decryption process hard and the digital twin utilizing such a technique safe. Of course further investigation is needed to formally prove such a declaration, but the first indications are apparent.

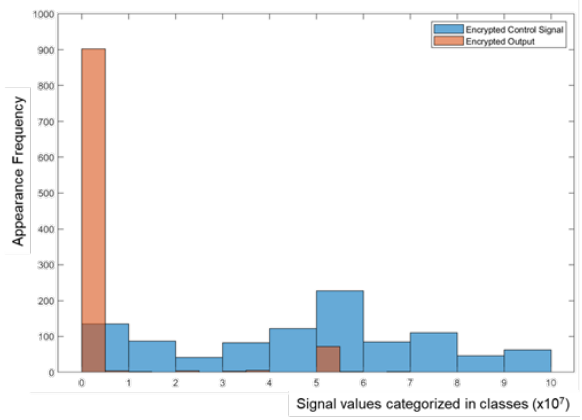

Figure 9 Histogram of signals of Fig. 4 with 10 defined classes

Conclusions & Future Outlook

This work addressed the challenge of ciphered signals while maintaining the expected efficiency. The performance of controller (e.g. in tracking or stability) has been proved to be appropriate even in the case of short lags to the network system. The use of a simple H-infinity controller is proved adequate (depending on the requirements on the overshoot). The use of a robust controller seems to slightly deteriorate the performance.

Regarding future applicability and challenges, a dynamic switched system involving encrypted signals may constitute a safe solution to the three phases (heating, melting and cooling-down) of laser welding since each one of them has different dynamic characteristics with the other. All the computed controllers should be a part of Digital Twin and NCS could be considered with stochastically varying delays. However, it is pending to check the use of a dynamic controller, or alternative techniques to sliding matrix, in order to study the performance computationally in these cases.

Acknowledgement

This work is under the framework of EU Project AVANGARD. This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 869986. The dissemination of results herein reflects only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.

References

1] Papacharalampopoulos A, Stavridis J, Stavropoulos P, Chryssolouris G. Cloud-based Control of Thermal Based Manufacturing Processes. Procedia CIRP 2016; 55:254–9.

[2] Mourtzis D, Vlachou E, Milas N, Tapoglou N, Mehnen J. A cloud-based, knowledge-enriched framework for increasing machining efficiency based on machine tool monitoring. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture 2019; 233(1):278–92.

[3] Mourtzis D, Vlachou E, Boli N, Gravias L, Giannoulis C. Manufacturing Networks Design through Smart Decision Making towards Frugal Innovation. Procedia CIRP 2016; 50:354–9.

[4] Li X, Di Li, Wan J, Vasilakos AV, Lai C-F, Wang S. A review of industrial wireless networks in the context of Industry 4.0. Wireless Netw 2017; 23(1):23–41.

[5] Mourtzis D, Vlachou E, Milas N. Industrial Big Data as a Result of IoT Adoption in Manufacturing. Procedia CIRP 2016; 55:290–5.

[6] Mubeen S, Nikolaidis P, Didic A, Pei-Breivold H, Sandstrom K, Behnam M. Delay Mitigation in Offloaded Cloud Controllers in Industrial IoT. IEEE Access 2017; 5:4418–30.

[7] Gao H, Chen T, Lam J. A new delay system approach to network-based control. Automatica 2008; 44(1):39–52.

[8] Papacharalampopoulos A, Stavropoulos P, Stavridis J, Chryssolouris G. The Effect of Communications on Networked Monitoring and Control of Manufacturing Processes. Procedia CIRP 2016; 41:723–8.

[9] Papacharalampopoulos A, Stavropoulos P. Towards a Digital Twin for Thermal Processes: Control-centric approach. Procedia CIRP 2019; 86:110–5.

[10] Du D. filter for discrete-time switched systems with time-varying delays. Nonlinear Analysis: Hybrid Systems 2010; 4(4):782–90.

[11] Sun YG, Wang L, Xie G. Delay-dependent robust stability and H∞ control for uncertain discrete-time switched systems with mode-dependent time delays. Applied Mathematics and Computation 2007; 187(2):1228–37.

[12] D. Martynova, P. Zhang. An Approach to Encrypted Fault Detection of Cyber-Physical Systems. In: 2019 12th Asian Control Conference (ASCC); 2019. p. 1501–6.

[13] S. DeCelles, M. Stamm, N. Kandasamy. Data Reduction, Compression, and Recovery for Online Performance Monitoring. In: 2019 IEEE 12th International Conference on Cloud Computing (CLOUD); 2019. p. 256–63.

[14] R. Yegireddi, R. K. Kumar. A survey on conventional encryption algorithms of Cryptography. In: 2016 International Conference on ICT in Business Industry Government (ICTBIG); 2016. p. 1–4.

[15] Tran J, Farokhi F, Cantoni M, Shames I. Implementing homomorphic encryption based secure feedback control. Control Engineering Practice 2020; 97:104350.

[16] Kogiso K, Fujita T. Cyber-security enhancement of networked control systems using homomorphic encryption 2015:6836–43.

[17] Jung Hee Cheon, Kyoohyung Han, Seong-Min Hong, Hyoun Jin Kim, Junsoo Kim, Suseong Kim et al. Toward a Secure Drone System: Flying With Real-Time Homomorphic Authenticated Encryption.

[18] Kim J, Lee C, Shim H, Cheon JH, Kim A, Kim M et al. Encrypting controller using fully homomorphic encryption for security of cyber-physical systems. IFAC-PapersOnLine 2016; 49(22):175–80.

[19] Yankai Lin, Farhad Farokhi, Iman Shames, Dragan Nesic. Secure Control of Nonlinear Systems Using Semi-Homomorphic Encryption 2018.

[20] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, W. Li. SecSDN-Cloud: Defeating Vulnerable Attacks Through Secure Software-Defined Networks. IEEE Access 2018; 6:8292–301.

[21] K. Gai, M. Qiu, H. Zhao. Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing. IEEE Transactions on Big Data 2017:1.

[22] Fujita T, Kogiso K, Sawada K, Shin S. Security enhancements of networked control systems using RSA public-key cryptosystem 2015:1–6.

[23] Y. Lin, F. Farokhi, I. Shames, D. Nešić. Secure Control of Nonlinear Systems Using Semi-Homomorphic Encryption. In: 2018 IEEE Conference on Decision and Control (CDC); 2018. p. 5002–7.

[24] Darup MS, Redder A, Quevedo DE. Encrypted cloud-based MPC for linear systems with input constraints. IFAC-PapersOnLine 2018; 51(20):535–42.

[25] Kishida M. Encrypted control system with quantiser. IET Control Theory & Applications 2019; 13(1):146–51.

[26] Y. Rahulamathavan, R. C. -. Phan, M. Rajarajan, S. Misra, A. Kondoz. Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption. In: 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS); 2017. p. 1–6.

[27] Huang S, Wang G, Yan Y, Fang X. Blockchain-based data management for digital twin of product. Journal of Manufacturing Systems 2020; 54:361–71.

[28] Alexandru AB, Morari M, Pappas GJ. Cloud-based MPC with encrypted data. In2018 IEEE Conference on Decision and Control (CDC) 2018 Dec 17 (pp. 5014-5019). IEEE.

[29] Schulze Darup M, Redder A, Shames I, Farokhi F, Quevedo D. Towards Encrypted MPC for Linear Constrained Systems. IEEE Control Syst. Lett. 2018; 2(2):195–200.

[30] Oliveira MC de, Geromel JC, Bernussou J. Extended H 2 and H norm characterizations and controller parametrizations for discrete-time systems. International Journal of Control 2002; 75(9):666–79.

[31] Papacharalampopoulos A, Stavropoulos P, Stavridis J. Adaptive Control of Thermal Processes: Laser Welding and Additive Manufacturing Paradigms. Procedia CIRP 2018; 67:233–7.

[32] Stavropoulos P, Spetsieris A, Papacharalampopoulos A. A Circular Economy based Decision Support System for the Assembly/Disassembly of Multi-Material Components. Procedia 2019;85:49-54.

[33] Athanasopoulou L, Papacharalampopoulos A, Stavropoulos P, Mourtzis D. Design and manufacturing of a smart mobility platform's context awareness and path planning module: A PSS approach. Presented in 30th International Conference on Flexible Automation and Intelligent Manufacturing (FAIM2020). 15-18 June 2020, Athens, Greece.

[34] Stavridis J, Papacharalampopoulos A, Stavropoulos P. Quality assessment in laser welding: a critical review. Int J Adv Manuf Technol 2018; 94(5-8):1825–47.