An approach for providing industrial control system sustainability in the age of digital transformation

An approach for providing industrial control system sustainability in the age of digital transformation

Andrey Dakhnovich [1*], Dmitriy Moskvin [1] and Dmitriy Zeghzda [1]

[1] Peter the Great St. Petersburg Polytechnic University, Politechnicheskaya str., 29, Saint Petersburg, 195251, Russia

* E-mail: add@ibks.spbstu.ru

Abstract. The specifics and challenges of securing Industrial Control Systems (ICS) in the age of Digital Transformation are proposed in the paper. Providing sustainability is considered as the main safety challenge while securing ICS systems. Secure information sharing between participants of Digital Manufacturing process and their segments is considered as the main information security challenge of a new production paradigm. Available technics and the drawbacks thereof to provide ICS security in the context of sustainability are mentioned. To meet the challenges an approach based on garlic routing principals is proposed to secure communications and provide stable manufacturing process due to providing information flaws availability and integrity in between different segments.

1. Introduction

In the industrial context Digital Transformation is a process that brings new abilities to manufacturers from Information Technologies (IT) which aim is to make production smarter and cheaper. So after that manufacturing is called Smart Manufacturing, Digital Manufacturing, Connected Factory etc. Also Industry 4.0 is applied to name this transformation to underline that today we live in the age of the Fourth Industrial Revolution. In this paper the Digital Manufacturing term is used to consider evolution Industrial Control Systems (ICS) as a result of Digital Transformation. That means that new abilities such as planning, prognosis and automation could be utilized in production. These abilities are available due to the appliance of IT-systems in ICS production systems [1]. But such convergence of two different systems brings new security challenges. The NIST SP 800-82 standard [2] describes differences between IT and ICS systems. For instance, the ICS system requires real-time data processing while IT-system permits some data transferring delay. So, the availability and integrity of data are more prioritized over confidentiality security property for ICS system. Another consideration is that the ICS system is always maintained by a one vendor while IT is maintained by many.

The IT system that is utilized as a main driver of the manufacturing Digital Transformation is an appliance of Cyber-Physical Systems (CPS) in production and the Internet of Thing (IoT) concept as its main implementation. The IoT generates the Big Data, which is transferred via network, and sometimes via Internet, to be processed in the main segment of production.

As a result, ICS systems cannot slightly utilize IT technologies in the production processes because they consider specifics of IT segment but not Cyber-Physical and ICS. It brings new attack vectors that can endanger physical safety [3–5].

The purpose of this paper is to analyze security challenges of Digital Manufacturing while applying the IoT technologies in the production systems. Section 2 considers main security challenges and attacks vectors while building Digital Manufacturing process. Section 3 describes main principals and application of garlic routing today. The appliance of garlic routing to secure information sharing secure between different segments of Digital Manufacturing in Section 4. Section 5 describes related works that also consider security challenges in Digital Manufacturing. Section 6 presents summaries of the paper and gives an overview of future works.

2. Security challenges of digital manufacturing

The vast majority of the Industrial Control Systems (ICS) are isolated today and feature underlying hierarchical model, which is mostly based on the Purdue five-level model. This architecture is recommended by US CERT (figure 1) [6], SANS Institute [7] and others as secure for building the ICS systems. There are also some modifications of such architecture, e.g., Cisco and Rockwell Automation proposed Converged Plantwide Ethernet (CPwE) architecture [8], or an IoT World Forum Reference Model [9].

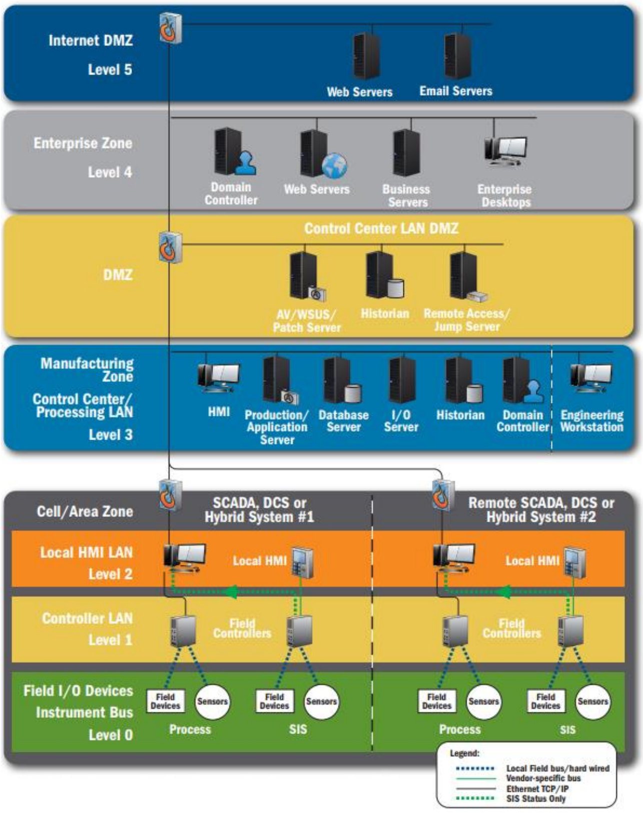

Figure 1. US CERT proposed secure ICS architecture.

These models implement Defence-in-Depth strategy, which means that every level of model provide security methods against types of attacks that can be performed at this level. This approach reduces risks while preserving information availability and integrity in the ICS processes. The Defence-in-Depth strategy protects when ICS system remains isolated and does not need communications and data transition through the public untrusted channels such as Internet [1, 4, 6]. However, new systems, which utilize IoT in the production edge (Industrial Internet of Things, IIoT) become network-open [10, 11]. There is no standard so far for the IIoT manufacturing systems. The main challenge when providing security in Digital Manufacturing is to remain production sustainable while using IoT and other IT technologies in production. The Industrial Internet Consortium (IIC) proposed a three-tier architecture pattern for the IIoT-enterprise (figure 2). The Edge Tier is the one, where IoT devices are used to perform production operation [12] and are supposed to be autonomous utilizing different communication protocols, topologies and can be also geographically distributed.

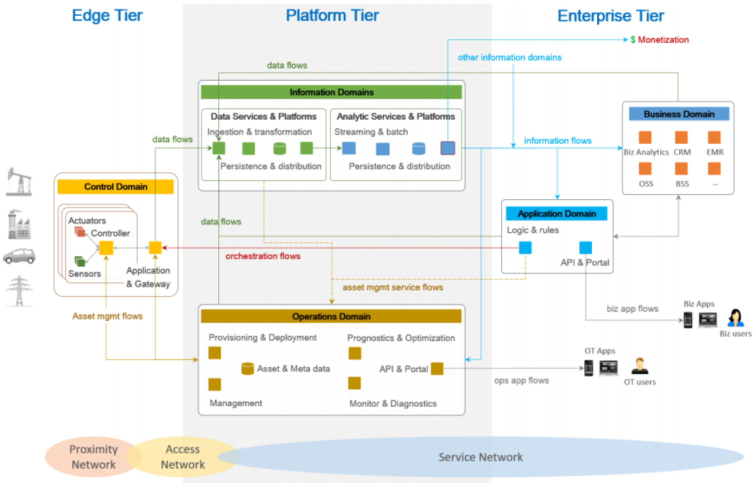

Figure 2. IIC three-tier architecture pattern.

Thus, communications for now go through the Internet as the main communication channel. For instance, not every enterprise can provide Big Data management, so a Cloud provider will be in use. But transferring sensitive data between company's edge and Cloud edge must be secured. Another example is described by Ulltveit-Moe et al: IIoT platforms use a huge amount of different "smart devices", they should be maintained and expertized by a service provider or a vendor. But, as it was stated in the Introduction, not the only vendor was usually used in IT, so access should be granted to different third parties and only to the devices and data they need without information leakage about business processes. The authors provide data sharing between stakeholders, external vendors, suppliers, security services as the Intrusion Detection Systems as an example of necessary data exchange with the third-party segments [5].

As a result of IoT appliance in the ICS new security issues become relevant:

- availability and identification of production equipment from the Internet;
- weak authorization, authentication and accounting (AAA) methods while granting access to the IoT-devices (usually authentication data is stored on the devices in an opened manner or hardcoded, default passwords are not changed);
- lack of data encryption in the industrial communication protocols (MODBus, S7comm etc.);
- lack of access control between devices and different segments [5].

Thus, new attack vectors are the most critical for production (figure 3):

- attacks on services and platforms, that administrate CPS segments;
- attacks against smart devices, such as sensors and actuators, to control data at the lowest level;
- data spoofing and availability violation while transferring between segments and inside them;
- channel eavesdropping and hijacking to collect data about internal processes and communications.

The ENISA agency provides the holistic view on the new attack vectors on IoT devices [13].

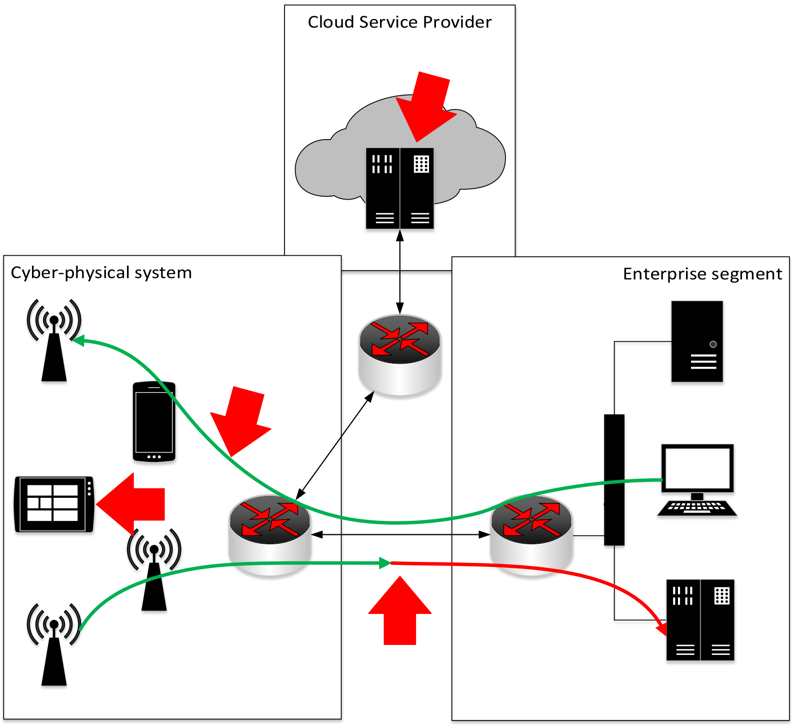

Figure 3. Main attack vectors in digital manufacturing.

The sustainability of CPS is the availability of the system to perform its functions in the context of external influence. There are some works where authors are trying to solve the problem of evaluating sustainability of the system [14]. The sustainability of the system can be gained by providing its information security and physical safety [12]. The physical safety usually gained by controlling physical access and data analysis of significant information values that can indicate the production process is not going according to the right scenarios. In order to provide information security in the context of sustainability, the information availability and integrity is prioritized over confidentiality.

The information availability and integrity can be provided in Digital Manufacturing while securing according assets:

1. Secure communication channels between segments and IoT devices to provide availability, integrity and confidentiality.

2. Fine-grained access control and authentication between IoT devices and CPS segments.

The information security is provided now in CPS segments and communications between them with the security technics, that are also mentioned in IIC and ENISA frameworks [12, 13]. They are also positioned as requirements for providing ICS security in recommendation documents such as NIST SP 800-82, SANS etc. [6, 7]:

- industrial network gateways that can process industrial protocols;
- cryptography methods to secure information sharing;
- communication channels redundancy to provide data availability, if one of the channels is down.

These technics have come from the IT-world. The gateways are used to separate network to independent zones (figure 1) in the course of cryptography methods to encrypt any data transferring between two remote segments.

The gateways are used in ICS systems for the same purpose and can provide:

- unauthorized data filtering to prevent attacks from the external network;
- prevent compromised devices from participating in distributed attacks and botnets;
- check data integrity before transferring it from devices and to devices on the edge tier [15].

An example from IIC IIRA model for Edge Tier is depicted in figure 4. The gateway is used here to build communications between Platform Tier and IoT devices, actuators and sensors.

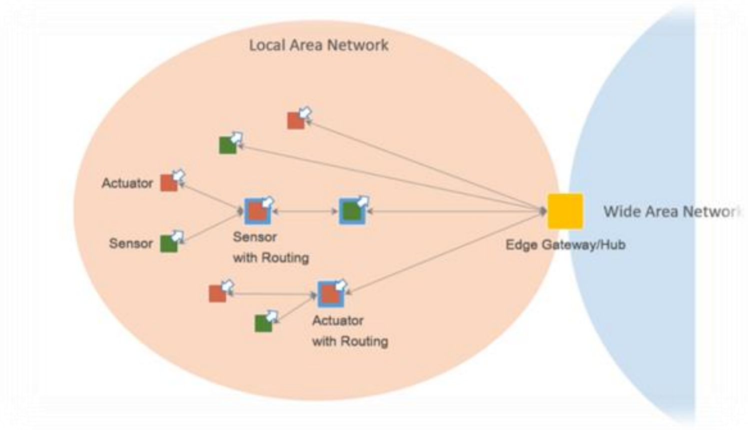

Figure 4. Edge tier leveraging edge gateway to communicate with platform tier.

However, the network gateways feature same drawbacks:

- data availability can not be guaranteed because gateway is a single point of failure;
- defense against internal adversary is not provided as data can be modified on the devices;
- gateways do not provide fine-grained access to the third parties.

The cryptography methods to secure data transfer are used to build secure communication channels. Nowadays vendor solutions can encrypt data through VPN and/or TLS tunnels. Despite the fact that the encrypted channels can provide data integrity and confidentiality, it can only be used to secure channels between two segments, but not between the particular devices, because connection of every device to VPN network is a hardly scalable solution and not each device can support such cryptography operations that VPN protocols require. Furthermore, the VPN channels can not provide security against internal adversary.

3. Garlic routing and garlic encryption

The terms “Garlic Routing” and “Garlic Encryption” were described by mathematician Michael Freedman in the year 2000 [18]. The Garlic encryption is built on an Onion routing principals, where the receiving node only can decrypt packets addressed to it, thus, unchaining one layer of the onion packet [19]. However, the main difference is that all packets in the garlic routing, called “cloves”, are encrypted separately by each sender and then packed in one with a fixed size, called “garlic”, while sending between nodes. Then “garlic” packet is encrypted entirely by each node as in the Onion routing scheme. Every clove message is unpacked and decrypted only on the receiving node so it cannot be read by any other participant, they can only retranslate it to the next hop of the network. The main appliance of Garlic routing is an I2P overlay network for now, where this technique provides anonymity of any clients and servers (in terms of I2P called nodes), as well as defense from traffic analysis (figure 4).

Thus, to secure communications between to clients and servers I2P network leverages information security methods listed below:

1. Appliance of public key cryptography for data encryption and signing node data (every node has its own two pairs of public and private keys).

2. Appliance of multi-layered onion-like encryption for outgoing and ingoing tunnels, where every node can decrypt only its own layer.

3. Different tunnels for outgoing and ingoing channels are utilized, where the second one is used for notifications about delivery status of messages sent through the outgoing tunnel. Every tunnel has its own life time.

4. Every packet, called “garlic” transferred between nodes through tunnels, consist of multiple messages, called “cloves”.

Thus, I2P network mitigates cyber attacks:

1. Man-in-the-Middle by data encryption and signing.

2. Attacks concerned with the data amount analysis techniques and timing attacks, as every “clove” has its own addressee and is transferred via temporary tunnels that have short living time.

The connection setup process between two remote nodes is depicted in figure 5.

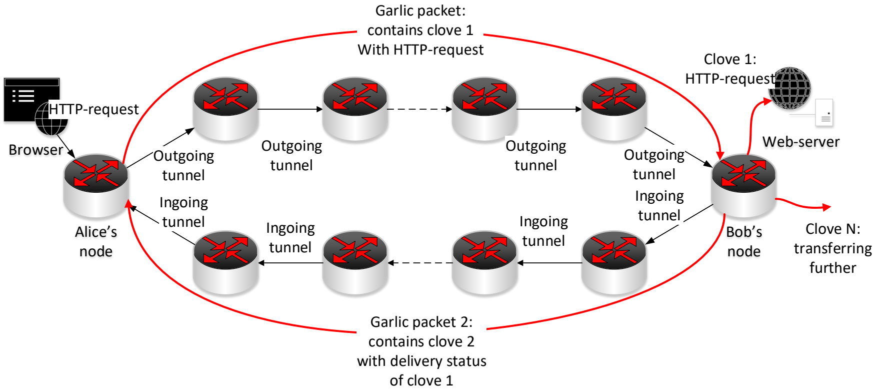

Figure 5. Example of connection setup in I2P Network.

4. Garlic routing appliance to provide digital manufacturing sustainability

The information security and control to provide sustainability of Digital Manufacturing processes in the IoT edge is considered in the paper. The garlic routing and garlic encryption can be slightly used for that purposes.

The garlic routing security measures are matched in table 1 with information security issues that should be mitigated for providing sustainability of Digital Manufacturing processes that go through the IoT segments connected to the third-party tiers.

Table 1. Appliance of garlic routing security measures for securing digital manufacturing processes.

Security measure	Security issue
End-to-end encryption between communicating nodes	Confidential data transferring via Internet or other untrusted channels
Nodes’ authentication	Mitigation of MiTM-attacks and IoT devices tampering
Digital signature	Data integrity assurance
Multiple tunnels for outgoing and ingoing channels	Secure against data interception, thus, data availability
Message delivery status notification	Data availability. If message has not been transferred and notification has not been received, message can be sent via another outgoing channel.
“Garlic” packet and message “cloves”	Mitigation of internal data analysis by the third parties

Furthermore, the I2P network is an overlay. That means that it does not depend on the protocols used on the network layer such as IP. Proceeding from the fact that there is a wide plenty of industrial communication protocols this issue could be solved by the overlay network such as I2P.

However, the garlic routing cannot be applied as it is applied to the IIoT segments. Some additional systems should be deployed to address Digital Manufacturing specifics. The specific routing tables should be used on each segment tier to control communications and provide fine-grained access between segments. Every segment *i* should control two tables for each communication list to another segment *j*:

1. Outbound table is a list of remote segment *j* nodes addresses that current segment *i* can communicate with. This table must be synchronized with the corresponding inbound table of the remote segment *j*.
2. Inbound table is a list of current segment *i* nodes that the remote segment *j* can communicate with. This table must be synchronized with the corresponding outbound table of segment *i*.

The address in any table is the match between the network address (e.g. IP-address) and two public keys. If node *k* of segment *i* can send data to the node *l* of the remote segment *j*, then table of segment *i* in routing will have two entry public keys: PK_{jl} and PK_{ik} . Key PK_{ik} is the public ciphering key of the node *l* from segment *j* and is used for data encryption sent to node *l* only. Key PK_{ik} is the public signing key of node *k* from segment *i* and is used for signature verification when data is transferred from node *k* to the current node. E.g., the outbound routing table of segment *i* will contain such entry:

$$RA_{jlik} = (PK_{jl}, PK_{ik}), \tag{1}$$

where, RA_{jlik} is a remote address of node *l* from segment *j* that node *i* from segment *k* can send information to;
PK_{jl} and PK_{ik} are the public keys, the first one is the public key of node *l* from segment *l* for data encryption, the second is the public key for signature of node *k* from segment *k* verification.

PK_{jl} and PK_{ik} should be synchronized with the remote Inbound table entry in segment *j* for correct integrity checking and data decryption. Thus, the corresponding Inbound table of segment *j* will have the same entry:

$$RA_{jlik} = (PK_{jl}, PK_{ik}) \ , \tag{2}$$

where, RA_{ikjl} is the address of node *l* from current segment *j* that node *i* from the remote segment *k* can send information to.

The example of data transferring between nodes in different segments that could participate in Digital Manufacturing processes is shown in figure 6.

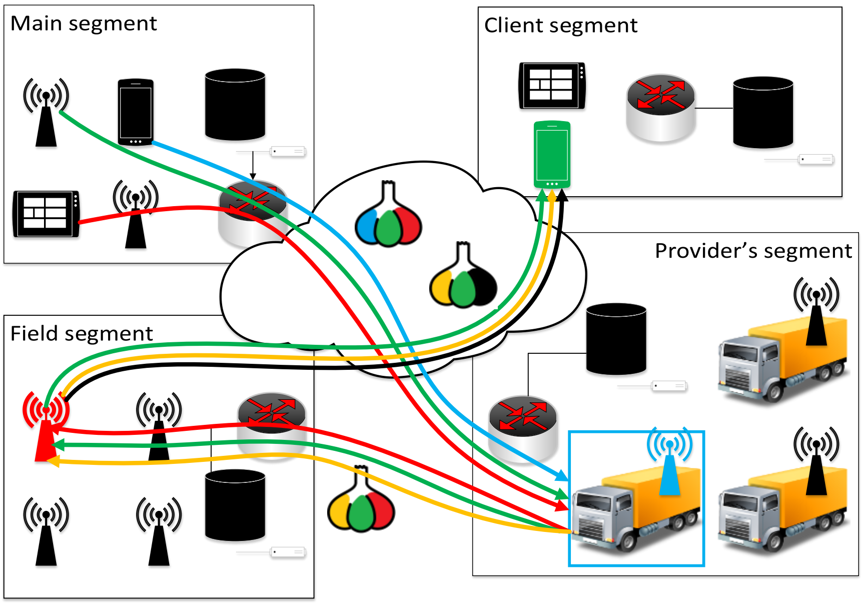

Figure 6. Example of garlic routing in the context of digital manufacturing segments communication.

The main drawback of the proposed method is that nodes participating in Digital Manufacturing are usually the IoT devices that are the low-energy ones featuring some energy constraints. The vast majority of these devices have no cryptography functions implementations on their edge so far. However, this missing should be eliminated in the nearest future. For instance, ENISA document contains technical measures chapter with recommendations that should mitigate attacks on IoT devices. One of them is to build devices that are compatible with the lightweight encryption [14].

5. Related works

As the Internet of Things becomes the main conception of Digital Manufacturing deployment, there are several research works around IoT security challenges. Sadeghi et al. describe new attack vectors in the Industrial Internet of Things and the main security challenges building secure architecture in CPS provide integrity verification of CPS and secure IoT device management [1]. Varga et al. give a comprehensive list of security issues in automation of IoT and propose a new layered approach to address attacks at each level in a research [16].

Some researchers also consider a necessity of a new secure architecture as IoT segments require to exchange information through boundaries. Sajid et al. describe security issues in utilization of SCADA systems based on IoT segment and backed with Cloud services and give some methods to mitigate these issues in the research [10]. Ulltveit-Moe et al. also consider problems of secure information sharing caused by collaboration between stakeholders, integrators and developers of IoT devices [5]. Xu et al. provide a view on a current state of the IoT in the Industry context, where a challenge of providing Quality of Service on a network layer of IoT systems takes place [5].

6. Conclusion and future works

The Garlic routing techniques for securing data communications could be used to build secure information sharing between different segments that need to grant fine-grained access to their manufacturing equipment such as IoT devices used in the industrial context. Secure information sharing between segments is one of the main issues that should be tackled to build manufacturing that will use all advantages of digital IT-technologies and Industry 4.0 paradigm [20].

Further works involve research on more detailed comparison with the existing tools, developing PKI key management and evaluating appliance of proposed method in the context of current government requirements for Critical Information Infrastructure and in the context of technical implementation by modelling on the existing examples of Digital Manufacturing segments communications.

Acknowledgment

The reported study was funded by RFBR according to the research project №18-29-03102.

References

[1] Security and Privacy Challenges in Industrial Internet of Things, http://www.academia.edu/23878296/Security_and_Privacy_Challenges_in_Industrial_Internet_of_Things

[2] Guide to Industrial Control Systems (ICS) Security, https://www.jpcert.or.jp/research/2016/NISTSP800-82r2_20160314.pdf

[3] Vasiliev U S, Zeghzda P D and Zeghzda D P 2016 *News of the Russian Academy of Science. Power Engineering* **3** 49–61

[4] Zeghzda D P 2016 *Problems of Information Security* **2** 13–18

[5] *Secure Information Sharing in an Industrial Internet of Things*, https://pdfs.semanticscholar.org/e6e5/e4de44a552a81ba5faa516f7cf1678a69a66.pdf

[6] Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICSCERT_Defense_in_Depth_2016_S508C.pdf

[7] Converged Plantwide Ethernet (CPwE) Design and Implementation Guide, https://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
[8] A Proposed Internet of Things Reference Model, http://cdn.iotwf.com/resources/ 72/IoT_Reference_Model_04_June_2014.pdf
[9] Secure Architecture for Industrial Control Systems, https://www.sans.org/reading-room/whitepapers/ICS/paper/36327
[10] Anam S, Haider A and Kashif S 2016 *Review of the State of the Art and Future Challenges* **4** 1375–1384
[11] Secure and trusted inter-cloud communications in the arrowhead framework, https://ieeexplore.ieee.org/document/8390802
[12] The Industrial Internet of Things Volume G1: Reference Architecture, https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf
[13] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, https://www.enisa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport
[14] Sustainability of cyber-physical systems in the context of targeted destructive influences, https://ieeexplore.ieee.org/document/8390814
[15] Securing the Industrial Internet of Things, www.redhat.com/cms/managed-files/rh-industrial-internet-of-things-iot-iiot-security-intelligent-gateway-whitepaper-f6951kc- 201706-en.pdf.
[16] Security Threats and Issues in Automation IoT, https://www.researchgate.net/ publication/317003655_Security_Threats_and_Issues_in_Automation_IoT/download
[17] Li Da Xu, Wu He, Shancang Li. 2014 IEEE Transactions on Industrial Informatics **10** (4) 2233–2243
[18] Garlic Routing and “Garlic” Terminology, https://geti2p.net/en/docs/how/garlic-routing
[19] Design and Deployment of an Anonymous Secure Data Haven, https://webcache. googleusercontent.com/search?q=cache:aGeFnbk2NGsJ:https://www.freehaven.net/doc/free haven.ps+&cd=1&hl=ru&ct=clnk&gl=ru
[20] Digital manufacturing-driven transformations of service supply chains for complex products, https://www.emeraldinsight.com/doi/pdfplus/10.1108/SCM-10-2013-0387