Privacy Recommendations for Future Distributed Control Systems

Wasfi Momen
Department of Computer Science
Georgia State University
Atlanta, GA 30303
Email: wmomen1@student.gsu.edu

Clarify

***Abstract*—As the role of privacy becomes more established in research, new questions and implementations trickle into the Distributed Control Systems (DCS) space focusing on privacy-preserving tools. In the near future, standards will have to include measures to protect the privacy of various objects, people, and systems in DCS plants. Building a privacy framework capable of meeting the needs of DCS applications and compatible with current standards to protect against intellectual theft and ~~sabotage is the primary aspect for DCS.~~ By identifying the lack of privacy protections in the current standards, detailing requirements for the privacy, and proposing suitable technologies we can provide guidelines for the next set of standards for DCS protections.**

Change structure of sentences, reverse order

Fix

I. Introduction

Distributed Control Systems (DCS) ~~are~~ plays a significant part in the daily lives of citizens ~~across~~ around the world. DCS handles the such as production and consumption of wastewater treatment, electricity generation, manufacturing, and other large-scale processes. Across decades of technological improvements, the scalability of DCS ~~went~~ grew from ~~large city production to~~ regional distribution [20]. However, the computers and machines ~~over the years of progress~~ were not replaced ~~every time~~ with up-to-date security improvements, resulting in long-term infrastructure vulnerabilities.

• specify processes are

• give more background on DCS functions

MORE ON IMPORTANCE OF DCS

In the post-cloud era, companies managing DCS now have incentives to replace outdated hardware to connect devices within the Internet of Things. Holes in network security are filled with new updates, and a greater importance ~~on~~ is placed cybersecurity ~~in DCS plants.~~ Typically, data in DCS is stored on the data historian—a computer that records all processes occurring within a plant. While the historian is kept under tight network security, the data must be transmitted throughout the plant for operations and in the cloud for performance analysis.

reword s.t. data vulnerabilities not motive

Data transmissions can be intercepted or changed within the ~~plant~~ to play a larger role for espionage and sabotage of operations via control security faults. Data historians store time, pressure, ~~temperature and other~~ statistics about the industrial ~~process between~~ different machines, therefore one can reverse engineer the process by knowing this information.

The attack ~~scenario~~ follows ~~above is~~ exactly illustrates what happened to a plant in Morgan County, Alabama owned by Toray Industries. The plant in question produced military-grade carbon fiber that is put on watch-lists for export by the United States to prevent terrorists and foreign entities from reverse engineering and selling copies. The Yokogawa data historian, Exaquantum, used ~~on~~ in the plant had known vulnerabilities that were exploited to gain access to the manufacturers data housed in the facility. The Department of Homeland Security notified the company, and the relevant notice ~~was~~ issued in 2014 ~~resulting~~ resulted in Yokogawa Electric applying patches to the vulnerable software.

The Toray plant ~~gives~~ represents an example of information espionage in the DCS field ~~today.~~ Software vulnerabilities will always be abundant, but ~~managed~~ manageable with the adoption of reportable notices like Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). However, the data retained in these systems will ~~exponentially grow~~ in the future. Research into the security of DCS environments are still in the early stages of development and ~~have yet~~ has yet to touch on the topic of *data privacy*. Soon, the ~~past~~ current standards such as NIST SP-800-82, IEC 62443/ISA 99 and industry specific standards like ISA 88 ~~will be~~ should be re-contextualized within a privacy-protected world.

Why? control security vuln...

needs to be managed, secured, further protection.

By analyzing the standards and current technologies of privacy-protection algorithms, we create framework recommendations that can obfuscate, disclose, or otherwise protect the data within industry requirements ~~that would represent a crucial step in protecting against industry theft or sabotage.~~

II. Background and Related Work

A. Current Specifications

Historically, the demand for security in DCS did not come from ~~the~~ system designers ~~of systems for DCS~~ but instead arose as a natural consequence from the business interests of reducing risk. As DCS plants grew larger and spread worldwide, businesses required a standard of the different relations and objectives in order to provide interoperability, reliability, and security.

These standards analyzed for the scope of this paper are summarized in Table I, ~~but~~ a survey paper concerning the frequency of the standards in literature and the context of each can be found in [13].

For most of these standards, the focus is on the *control layer* with the formal definitions of DCS operations. Many devices such as PLCs (Programmable Logic Controllers) ship with compatibility to these standards. The fundamental standards of IEC 62443/ISA99 or ISA99 that make up the interfaces of DCS do not mention any security considerations since they were created 30 years ago with a ”design first, secure

Designation	Title	Description
IEC 62443 / ISA99	Operations	Specifies the various relations and operations of a DCS. This includes the relationship of business to manufacturing, formal nomenclature, and the DCS as a 4-layer model.
ISA 88		Specifically relates to batch processing models. Mentions a hierarchical model for reporting data from different modules representing the device.
NIST SP 800-82 [19]	guideline for ICS	One of the most followed guidelines for DCS security. Shows in-depth known general protection practices, protection of vulnerable protocols, and gives measures for mitigation via control structures.
IEC 62541		Specifies the OPC-UA architecture, the most widely used protocol for modeling relationships within a DCS. Matches a server-client model with standard headers and fields for device interoperability.
NISTIR 7268 [4]		A three-paper set of guidelines in cybersecurity for critical infrastructure made in 2014. Specifically has a whole section devoted to privacy, but mainly in a Smart Grid context. Defines privacy only as it ”relates to individuals” through 4 social dimensions. Data ”in-transit” and ”at-rest” are discussed as part of Category PR.DS-P ”Data Security” in [1], a 2018 report detailing improvements to the initial privacy specification.
CIS CSC 13, 14 [15],[18]		The Center for Internet Security (CIS) Critical Security Controls (CSC) provide a technical framework that relates to NIST standard principles. CSC 13 and 14 specify control access and data protection by minimizing and authorizing control interfaces.

TABLE I
STANDARDS OF DCS SECURITY AND PRIVACY

later” approach. NIST SP 800-82 guidelines ~~create~~ describe the majority fundamental control layer security mechanics, including encryption and access control.

For ~~mentions~~ any mention of privacy protections, the draft guidelines for NISTR 7268 and CIS CSCs 13 and 14 ~~are playing the significant role of developing privacy frameworks for DCS. These are all established references, but also have current drafts for several NIST special working groups.~~ However, privacy in these three documents are defined only as it relates to individuals with personal information, persons, behavior, and communications within the ”Smart Grid” context [4].

Furthermore, these privacy considerations are happening at the *control layer* instead of the *data layer*. This is due in part to the reduced, manageable scope of relating privacy to individual persons mentioned in references by NIST SP 800-82. However, today’s research and technology requires an expansion of this scope from individual persons to machines and systems within a DCS ~~as well.~~ While the control layer was the best place to protect ~~the human interface~~ individual persons of DCS, the data layer will be the place where privacy is protected for machines.

network systems want to protected data layer

While the philosophical, legal, and social questions ~~and theories~~ surrounding the nature of privacy are outside of the scope of this paper, DCS requires a model similar to IEC 62443/ISA99’s Purdue Hierarchy Model (Fig. 1) in order to organize the methodology and tools for privacy protections. Separation of different principles with respect to the control and data layers is important for standard recommendations to protect privacy.

? New Word ?

B. The Separation of Security and Privacy

In past research, DCS security is based on the fundamental security principles of *confidentiality, integrity,* and *availability*. In 1988, these principles originated in [17] as the **CIA triad** which dominates computer security research and education ~~today~~. Within a DCS, each of these principles relate to physical computers and trust relationships in both the standards and in operation. [12] provides a comprehensive overview of the

?

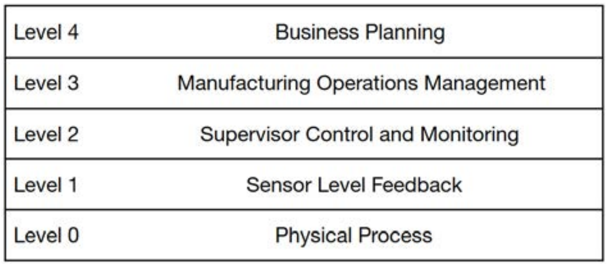

Fig. 1. ISA99 Model of DCS Operations

security principles in control systems and ~~providing~~ exemplary mitigation against security attacks based on these principles.

As research into privacy for computers continues to grow, there is still a need to ~~define~~ relate privacy ~~as it relates to other~~ to the concepts ~~like~~ of security and policy. While the nature of privacy ~~can be questioned, it is clear it represents a different field of information assurance separate from security.~~ Luckily, two years after the development of the CIA triad, [16] presented the **McCumber Cube** (Fig. 2) to ~~relate the~~ synergize principles of security, privacy, and policy. On one side of the cube the original CIA triad is present, while the principles of privacy are represented as data *transmission, storage,* and *processing*. on another side The last side promotes the interests of policy, education, and standardization. Fig 2

In this model, ~~the~~ security, privacy, and policy can be related ~~to a system like DCS by the past standards presented~~ as policy, the current adoption of security principles, ~~and the future development of privacy principles.~~ The separation of security and privacy principles can correlate to network principles of the *control plane* and *data plane*. Focusing on the data plane manages a scope that privacy can act on and thus provide protections in a system like DCS.

To be clear, the separation of privacy and security should not be confused as a ”zero-sum” scenario where gaining privacy comes at the cost of security or results [2]. Some of tools to be mentioned do have trade-offs, but should be compatible within a DCS for ”real, practical results”.

By addressing security and privacy separately, research can focus on ~~different~~ solutions specifically targeting each aspect. For DCS, control plane security ~~is~~ has been researched thoroughly with ~~many different~~ various implementations and ideas being presented [12], but insights into data plane privacy leave a lot to be desired. As such, this paper will focus on looking at current ~~frameworks~~ around DCS and ~~looking~~ into implementations ~~for~~ privacy considerations ~~within the~~ standards.

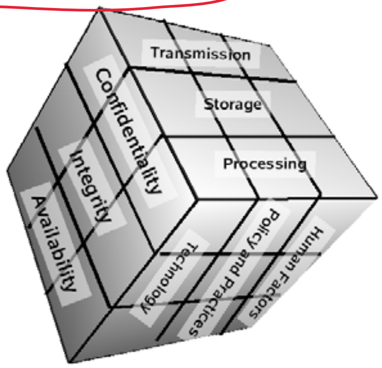

Fig. 2. Model for DCS Information Assurance: The McCumber Cube

III. Privacy Preserving Technologies for DCS Contexts

With the establishment of privacy, the identification and development of several tools suitable for ~~use~~ within a DCS have become available. We suggest these tools ~~as~~ potential privacy implementations ~~of a~~ for general privacy framework for DCS.

Within a DCS, *devices* and *modules* communicate with one another to provide information about certain industrial processes. Such an example of a relationship includes a device such as temperature sensor and a module such as an ~~OPC-UA~~ server to which data is reported. From this data, adversaries can ~~learn~~ steal information ~~about a process in attempts~~ to recreate or sabotage ~~a~~ that process. Other examples modules may ~~be~~ include the Safety Instrumented Systems (SIS) or Manufacturing Execution System (MES), which need to transfer, process, and store data from devices.

ADD MODEL OF PRIVACY

A. Differential Privacy

Differential privacy attempts to add noise to data so an adversary will not be able to identify whether an ~~output record of data~~ data record belongs to one database or another with high confidence. The corresponding mechanism ~~in which it does so is using~~ uses some randomized function K to manipulate every data point within the two databases, D_1 and D_2 [8]. The function takes input parameters of the two databases as well as a *privacy budget* ϵ to spread across all data points. The goal of differential privacy is protect individual data points yet disclose enough information that can be used for general conclusions of the dataset (i.e. utility).

Many ~~different~~ research papers focusing on differential privacy ~~are~~ do so within the Smart Grid context. The Smart Grid ~~will~~ processes inputs from the *Advanced Metering Infrastructure (AMI)* ~~of homes and~~ businesses that transmits time-series data on power consumption for processing at Level 2. From the power consumption data, decisions will ~~have to~~ need to be made ~~to~~ in order to produce more or less power ~~at the physical plant~~. Therefore, the data processed ~~must include measures of~~ privacy ~~for the individual homes and businesses~~. [7] explores privacy preservation of solar power generation and [14] creates a privacy-preserving protocol to obfuscate queries and receive fine-grained results of power consumption. [11] compiles an in-depth view of three privacy-preserving protocols of data minimization.

Why do I care?

~~For use of Level 2 and below~~, the same measure of privacy preservation occurs on the plant between ~~the~~ many sensor devices and a controller commanding inputs required to change the amount of production. With differential privacy, there is a sacrifice of accuracy of data returned ~~from a query in~~ order to preserve privacy of the actual data inputs, so the question is ~~whether the trade~~-off is accurate enough or worth the cost.

[10] provides a general framework to gauge the privacy ~~costs of a DCS with a number of agents that practice a differential private protocol~~. A *closed-loop* state model of a DCS is used to see the cost if an agent (i.e. device) can communicate feedback on the state of a process while giving noisy data values and then also determine an agents preferred next state to control the process. Such a framework can be used to verify differential private protocols or algorithms across agents for the purposes of standardization for different industries and data sets.

Unfortunately, differential privacy may not be the solution for every DCS since data points must be manipulated to gain privacy. While this trade-off is controlled by the privacy budget ϵ, not all industries may be able to cope with the loss. For example, in Emerson’s DeltaV PLC operation, there is the *Statistical Process Monitoring* module that alarms and acts based on thresholds set by plant operators [5]. These thresholds can be any range of ”engineering units” such as voltage, gallons, or grams per mole. Since differential privacy requires some randomized mechanism to work, the amount of noise ~~added may~~ exceed engineering units that have a low tolerance ~~of threshold~~. ~~As such~~, industries like pharmaceuticals or chemicals might have a harder time adopting differential privacy than electricity or water.

~~Also~~, current research ~~for differential privacy have various attack models for the various~~ ways of adding noise via a randomized noise mechanism. Specifically to DCS contexts, [9] provides an attack model in which an adversary can manipulate a differential private DCS by injecting false data ~~while having~~ with the same probability as triggering a false alarm. Under these conditions, integrity and privacy of data becomes disrupted in the system and result in an overall loss in stable state of the DCS.

Go through each ¶ & distill points & rewrite

is if

B. Private Information Retrieval

For differential privacy, the problem ~~relies on not disclosing~~ ~~if~~ the *data record* was from one database or another. For **private information retrieval** (PIR), the problem ~~relies on not~~ is disclosing whether the *query* of the data record was requested from one database or another. As such, PIR requires different ~~mathematics~~ and challenges in order to ~~satisfy its query-based privacy role separate from differential privacy~~. PIR was popularized in [3] with a more efficient scheme.

protect ???

Clean up difference of PPL & PIR

For PIR, randomness is injected into queries for data in the goal of sending multiple queries to the database in order to gain the sought answer without the database or adversary knowing. Suppose we have non-communicating databases D_k with k number of databases that hold a x_n string of data n number of bits. A user will be interested in find i index of the data, so x_i, but queries all the databases independently with random queries to obfuscate the queries. In this way, the index i that the user is looking for is never disclosed. Protocols for PIR dealing with a single database are *information-theoretic*, meaning that even with infinite computational power an adversary would not be able to retrieve the data.

In the protocols discussed in research, the databases returns a single bit of data for each query where all queries can be XOR'd by the user to gain the entire true value. Most research seeks to reduce the communication complexity of bits sent vs bits received between a user and many databases. Cooperating databases might also present a problem, since cooperating databases will be able to disclose the index of sought for data based on their queries to the user. However, [3] and [6] provide protocols that computationally bounded adversaries with control of up to an upper bound of compromised, cooperating databases.

In DCS, PIR would be very useful in gathering data from either sensors from Level 1 or from multiple site historians from Level 2. Queries for the data running through a PIR scheme would be to retrieve time-series data, recover from privacy or security losses, and transfer large data sets without adversary knowledge if combined with codes such as those generated by hash functions. While research for practical PIR needs to enter industries, it can provide guarantees for privacy protections that do not alter data records.

IV. Towards a General Privacy Framework for DCS

Of the given standards, there are two to be ignored entirely —IEC 62443/ISA 99 and ISA 88. While these standards are still being updated, they consider mainly the policy side specified in the McCumber Cube and thus will only include security considerations via policy means. Including protections for security and privacy for these two standards means the implementation of training programs, workforces, and groups that need to be backwards compatible for plants conforming to the original standard. Since the workforce for enforcing security is still in development and the privacy aspects not ~~addressed, recommendations to these standards can only be~~ done after research in both areas come to conclusions of best practices.

?

basically, research has yet to catch up so some procedures for privacy might have to wait

From the above technological solutions, we integrate potential recommendations for current standards to adopt mechanics to protect privacy.

- What needs to be done?
- Why does it matter?
  - practical & why
  - value

A. Recommendations for Standards

IEC 62541 The OPC-UA architecture must include any new privacy protocols that result from research and implementation since it is the baseline for communications in DCS. These new privacy protocols might utilize the same cryptographic concepts used in tools like encryption, so extending those object hierarchies might be possible. The current object primitives such as VariableNode carry the necessary inputs required for passing privacy parameters and MethodNode can handle response outputs for privacy protocols. There is no need to remove the client-server or publisher-subscribe relationships for OPC-UA unless the privacy protocol requires ~~it~~, such as non-cooperation for PIR.

Why do I care about these changes?

How do I implement?

NIST SP 800-82 Since privacy protocols will be added to IEC 62541, it is necessary to append a correlating privacy architecture section and application section for NIST SP 800-82. The architecture section must include key principles of privacy and a model of privacy-preserving systems as detailed in Section II. The application section should relate to the concepts of privacy described in the McCumber Cube—data transmission, processing, and storage.

NISTIR 7268 Volume 2 of NISTIR 7268 concerning the privacy of DCS must expand the scope of protecting privacy to machines and devices, not only persons. Volume 2 shall include the privacy use cases as given in Section IV. Additional discussion of privacy should include mention of the McCumber cube or some other framework of providing privacy.

Same?

CIS CSC 13, 14 Volume 2 of NISTIR 7268 concerning the privacy of DCS must expand the scope of protecting privacy to machines and devices, not only persons. Volume 2 shall include the privacy use cases as given in Section IV. Additional discussion of privacy should include mention of the McCumber cube or some other framework of providing privacy.

e.g.

NISTIR 7268 A new CSC document must be created in order to address privacy concerns. This new CSC document should be titled "Data Privacy" and must include subcategories of the different methods of privacy protections such as data minimization or obfuscation mentioned in [11].

technical spec for privacy

B. Privacy Use Cases

As identified by other standards such as NISTIR 7268, use cases play a pivotal role to attaining a possible scenario where technology can be seen as necessarily integrated factor. As such, we have identified some possible scenarios in which privacy can protect against adversary models exploiting control security faults or data privacy.

1) Power Plant Load Estimation: An attacker using a botnet of smart meters within the AMI tries to inject false data to cause the control algorithm of a power plant to overestimate the power consumption of several neighborhoods. Smart meters protected with differential privacy algorithms that fail to provide valid responses to new privacy parameters will be ousted from load estimation calculations.

2) Nuclear Power Plant Deflagration: Deflagration is the simple event of heating a substance to its flash point—the temperature at which it ignites. Typically, fires can be contained and handled on their own, but in certain situations may lead to *detonation* of products or components in the environment with explosive force. In nuclear power plants, shutdown of cooling mechanisms can allow for accumulation of hydrogen steam within the containment vessel. With enough pressure, the cooling pipes carrying water can rupture and react with the hydrogen violently and lead to detonation.

An adversary sniffing the data of sensors within the plant will be able to simulate a model of the plant and be able to trigger a deflagration event. A PIR scheme implemented within a nuclear DCS will be able to query and respond data without giving away the true output values necessary to simulate the plant's processes.

C.

V. Conclusion

In this paper, we discussed the role of privacy within DCS, examined the various standards that provided DCS security, and recommended privacy protections that can be implemented through the use of current research. By calling back to the original paper where security controls were discussed for security, we were able to glean information to be used in the discussion of creating a framework of privacy as well. We also explained the drawbacks each privacy-preserving technology had and the potential fixes that will be available for future standards. For the DCS standards, we propose these amendments that are acceptable to the other two sides of protecting DCS plants and compatible with current specifications.

References

[1] Matthew P Barrett. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*. Tech. rep. 2018. URL: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11.

[2] Ann Cavoukian et al. "Privacy by design: The 7 foundational principles". In: (). URL: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

[3] Benny Chor et al. "Private information retrieval". In: *Proceedings of IEEE 36th Annual Foundations of Computer Science*. IEEE. 1995, pp. 41–50. URL: https://www.cs.umd.edu/~gasarch/TOPICS/pir/first.pdf.

[4] The Smart Grid Interoperability Panel - Smart Grid Cybersecurity Committee. *NISTIR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity*. Tech. rep. 2014. URL: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final.

[5] *DeltaV Statistical Process Monitoring Whitepaper*. Tech. rep. 2016. URL: https://www.emerson.com/documents/automation/white-paper-statistical-process-monitoring-deltav-en-56970.pdf.

[6] Casey Devet and Ian Goldberg. "The best of both worlds: Combining information-theoretic and computational PIR for communication efficiency". In: *International Symposium on Privacy Enhancing Technologies Symposium*. Springer. 2014, pp. 63–82. URL: https://petsymposium.org/2014/papers/Devet.pdf.

[7] Jin Dong et al. "Privacy-Preserving Aggregation of Controllable Loads to Compensate Fluctuations in Solar Power". In: *2018 IEEE Electronic Power Grid (eGrid)*. IEEE. 2018, pp. 1–5. URL: https://www.osti.gov/biblio/1494017.

[8] Cynthia Dwork. "Differential Privacy: A Survey of Results". In: vol. 4978. Apr. 2008, pp. 1–19. DOI: 10.1007/978-3-540-79228-4_1. URL: https://web.cs.ucdavis.edu/~franklin/ecs289/2010/dwork_2008.pdf.

[9] Jairo Giraldo, Alvaro A Cardenas, and Murat Kantarcioglu. "Security vs. privacy: How integrity attacks can be masked by the noise of differential privacy". In: *2017 American Control Conference (ACC)*. IEEE. 2017, pp. 1679–1684. URL: https://ieeexplore.ieee.org/document/7963194.

[10] Zhenqi Huang et al. "On the cost of differential privacy in distributed control systems". In: *Proceedings of the 3rd international conference on High confidence networked systems*. ACM. 2014, pp. 105–114. URL: https://dl.acm.org/citation.cfm?id=2566468.2566474.

[11] Marek Jawurek. "Privacy in Smart Grids". In: (2013). URL: https://pdfs.semanticscholar.org/ad88/78fd6897bcf5106ee777cbe13a1b08b2696e.pdf.

[12] Roger A Kisner et al. "Cybersecurity through real-time distributed control systems". In: *Oak Ridge National Laboratory, Technical Report ORNL/TM-2010/30* (2010).

[13] Rafal Leszczyna. "Cybersecurity and privacy in standards for smart grids - A comprehensive survey". In: *Computer Standards & Interfaces* 56 (2018), pp. 62–73. ISSN: 0920-5489. DOI: https://doi.org/10.1016/j.csi.2017.09.005. URL: http://www.sciencedirect.com/science/article/pii/S0920548917301277.

[14] Xiaojing Liao et al. "Di-prida: differentially private distributed load balancing control for the smart grid". In: *IEEE Transactions on Dependable and Secure Computing* (2017). URL: https://ieeexplore.ieee.org/document/7954704.

[15] *List of Critical Security Controls by the Center of Internet Security*. Tech. rep. 2016. URL: https://learn.cisecurity.org/control-download.

[16] John R. McCumber. "Information Systems Security: A Comprehensive Model". In: *Proceedings of the 14th National Computer Security Conference: Information Systems Security: Requirements and Practices*. NIST. 1991, pp. 328. URL: https://csrc.nist.gov/CSRC/

media / Publications / conference - paper / 1991 / 10 / 01 / proceedings - 14th - national - computer - security - conference - 1991 / documents / 1991 - 14th - NCSC - proceedings-vol-1.pdf.

[17] Charles P. Pfleeger. *Security in Computing*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1989. ISBN: 0-13-798943-1.

[18] *Poster of all Critical Security Controls by the Center of Internet Security*. Tech. rep. 2016. URL: https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf.

[19] Keith Stouffer et al. "Guide to Industrial Control Systems (ICS) Security". In: *NIST Special Publication* 800 (), p. 82. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final.

[20] Alexandru Ujvarosi. "Evolution Of Scada Systems". In: *Bulletin of the Transilvania University of Brasov. Engineering Sciences. Series I* 9.1 (2016), p. 63. URL: http://webbut.unitbv.ro/BU2016/Series%20I/2016/BULETIN%20I%20PDF/Ujvarosi_Al.pdf.