8-13-2019

Privacy Recommendations for Future Distributed Control Systems

Wasfi Momen

PRIVACY RECOMMENDATIONS FOR FUTURE DISTRIBUTED CONTROL SYSTEMS

by

WASFI MOMEN

Under the Direction of Anu Bourgeois, Ph.D.

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.

INDEX WORDS: Privacy, Differential Privacy, Distributed Control Systems, Smart Grid

PRIVACY RECOMMENDATIONS FOR FUTURE DISTRIBUTED CONTROL SYSTEMS

by

WASFI MOMEN

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science

in the College of Arts and Sciences

Georgia State University

2019

PRIVACY RECOMMENDATIONS FOR FUTURE DISTRIBUTED CONTROL SYSTEMS

by

WASFI MOMEN

Committee Chair: Anu Bourgeois

Committee: Ashwin Ashok

Yubao Wu

Electronic Version Approved:

Office of Graduate Studies

College of Arts and Sciences

Georgia State University

August 2019

DEDICATION

I dedicate this work to my father (Abdul Momen), my mother (Masuma Momen), and my sister (Akeafa Momen). Without their help and support, my journey at Georgia State University would have never even begun.

ACKNOWLEDGEMENTS

Georgia State is full of many people who supported me with the knowledge and motivation to get me this far. I would like to thank Dr. Anu Bourgeois for her incredible guidance from the very start of my graduate degree and the conversations of words that expanded my worldview. And her husband, Doug Bourgeois, whose vast knowledge about DCS and willingness to bounce ideas around helped make this paper's foundations.

I'd also like to thank the committee members for their time, patience, and consideration for the ideas presented.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

- AMI – Advanced Metering Infrastructure
- CERT – Community Emergency Response Team
- CSC – Critical Security Controls
- DCS – Distributed Control System
- IEC – International Electrotechnical Commission
- ICS – Industrial Control Systems
- ISA – International Society of Automation
- NIST – National Institute of Standards and Technology
- NISTIR – National Institute of Standards and Technology Interagency Report
- OPC – Open Platform Communications
- PIR – Private Information Retrieval
- SIS – Safety Instrumented System
- SP – Special Publications

1 INTRODUCTION

Distributed Control Systems (DCS) play significant part in the daily lives of citizens around the world. DCS handles the production and consumption of wastewater treatment, electricity generation, manufacturing, and other large-scale processes. Across decades of technological improvements, the scalability of DCS grew from large city production to regional distribution [1]. 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.

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 is placed on cybersecurity. Typically, data in DCS is stored on the data historian—a computer that records all processes occurring within a plant. The data must be transmitted throughout the plant for operations and in the cloud for performance analysis.

Due to control security faults, espionage and sabotage of operations occur via intercepted or altered data transmissions. Data historians store environmental data such as time, pressure, temperature and various other statistics for operations. Knowledge of this information can be used to reverse engineer industrial processes or to sabotage vulnerable equipment.

One attack scenario illustrates a security failure 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 in the plant had known vulnerabilities that were exploited to gain access to the manufacturing data

housed in the facility. The Department of Homeland Security notified the company and the relevant notice was issued in 2014 resulted in Yokogawa Electric applying patches to the vulnerable software.

The Toray plant represents an example of information espionage through control security faults. Software vulnerabilities will always be abundant, but 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 need further protection. Research into the security of DCS environments are still in the early stages of development and has yet to touch on the topic of *data privacy*. Soon, the current standards such as NIST SP-800-82, IEC 62443/ISA 99 and industry specific standards like ISA 88 should be re-contextualized within a privacy-protected world.

By analyzing the current standards and technologies of privacy-protection algorithms, we recommend standard modifications to create a framework that can obfuscate, disclose, or otherwise protect the data within industry requirements.

1.1 Cybersecurity in Distributed Control Systems

DCS traditionally started as a singular, physical plant that hosted all the necessary components for processing hardwired to one another via copper wiring. As time grew on, it grew necessary to have multiple sites all reporting back statistics to corporate offices and integrate new technology such as mainframes. Thus, IEC 62443/ISA 99's predecessor, ISA 95, was created.

Level 4	Business Planning
Level 3	Manufacturing Operations Management
Level 2	Supervisor Control and Monitoring
Level 1	Sensor Level Feedback
Level 0	Physical Process

Figure 1 Purdue Hierarchy Model

ISA 95 provided a baseline standard for companies to follow in order to communicate with multiple plants, set up new infrastructure, and manage roles within a DCS. Each level was designed to maintain a different aspect of plant production with data moving between each layer. Developing technologies were integrated to form the functions required of the standard. For example, Level 2 Supervisor Control and Monitoring saw the creation the "Data Historian", a computer that keeps a record of all time-series data for every device within a DCS plant.

In the post-2010 "cloud era", DCS plants were now connected to internet with vast data passed from Level 2 to Level 3 and 4 via cloud-based systems and data stores. As such, more cybersecurity control was implemented to provide authentication and integrity with tools like logins, access portals, and firewalls. Currently, these security practices are being implemented into the new version of standards for DCS, IEC 62443 / ISA 99.

1.2 Adversary Models

Adversaries throughout most DCS models are never omnipresent unless they access oracles responsible for controlling randomization mechanisms. Adversary goals include to either infiltrate, sabotage, or leave backdoors within DCS. Most of the standards around DCS look at the same adversary models presented in research.

[3] provides the most detailed look into adversary models for Smart Grid privacy that can be extracted to provide general guidelines for other time-series dependent DCS. One of the primary attacks in the Smart Grid includes the “Non-intrusive appliance load monitoring attack”, or NALM, for short. According to [3], NALM is “to detect appliance usage in households” with the use to inexpensive sensors that can be attached to the main smart meter. The sensor can be used to sniff data off the smart meter or try to gain more granular data such as electromagnetic interference to guess what kind of devices are inside the home. Current research focusing on adversarial examples tries to leverage the data gained by NALM and the predicted output of the load monitoring algorithm which controls power production to create an attack with the same probability as a false alarm. Therefore, the DCS will infer the behavior as normal, create false conclusions about power consumption, and lead to power production increase or decrease not in phase with the actual data values.

2 LITERATURE REVIEW

2.1 Current Specifications

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

The standards analyzed for the scope of this paper are summarized in Table 1. A survey paper concerning the frequency of the standards in literature and the context of each can be found in [1].

Table 1 Standards for DCS Security and Privacy

Designation	Title	Description
IEC 62443 / ISA99	Security for Industrial Automation and Control Systems	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	Batch Control	Specifically relates to batch processing models. Mentions a hierarchical model for reporting data from different modules representing the device.
NIST SP 800-82[21]	Guide to Industrial Control Systems (ICS) Security	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	OPC Unified Architecture	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. The OPC-UA archtiecture manifests the logical and physical relationships established by IEC 62443/ISA 99.
NISTIR 7268 [5]	Guidelines for Smart Grid Cybersecurity	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 [16],[20]	Critical Security Controls	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.

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

For any mentions of privacy, the guidelines of NISTR 7268 and CIS CSCs 13 and 14 try to integrate privacy considerations into DCS protections. 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 effort of making a reduced, manageable scope of relating privacy to individual persons. However, today's research and technology requires an expansion of this scope from individual persons to machines and systems within a DCS. While the control layer was the best place to protect individual persons of DCS, the data layer will be the place where privacy is protected for machines.

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

2.2 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 [5] as the **CIA triad**, which dominates computer security research and education today. Within a DCS, each of these principles relate to physical computers and relationships in both the standards and in operation. [6] provides a comprehensive overview of the security principles in control systems and exemplary mitigations against security attacks based on these principles.

As research into privacy for computers continues to grow, there is still a need to relate privacy to other concepts of control security and business policy. The principles of privacy differ from those of security and policy which indicates a need to make privacy an separate field of study. Luckily, two years after the development of the CIA triad, [7] presented the McCumber Cube (Fig. 2) synonymous to the 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 the other side. The last side promotes the interests of policy through education, and standardization.

In the McCumber Cube model, the past standards of policy, the current adoption of security principles, and the future development of privacy principles are combined to promote the creation of effective protections for DCS. 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 solutions specifically targeting each concept. For DCS, control plane security has been researched thoroughly with various implementations and ideas being presented [6], but insights into data plane privacy leave a lot to be desired. As such, this paper will focus on looking at current standards around DCS and into implementations for privacy considerations.

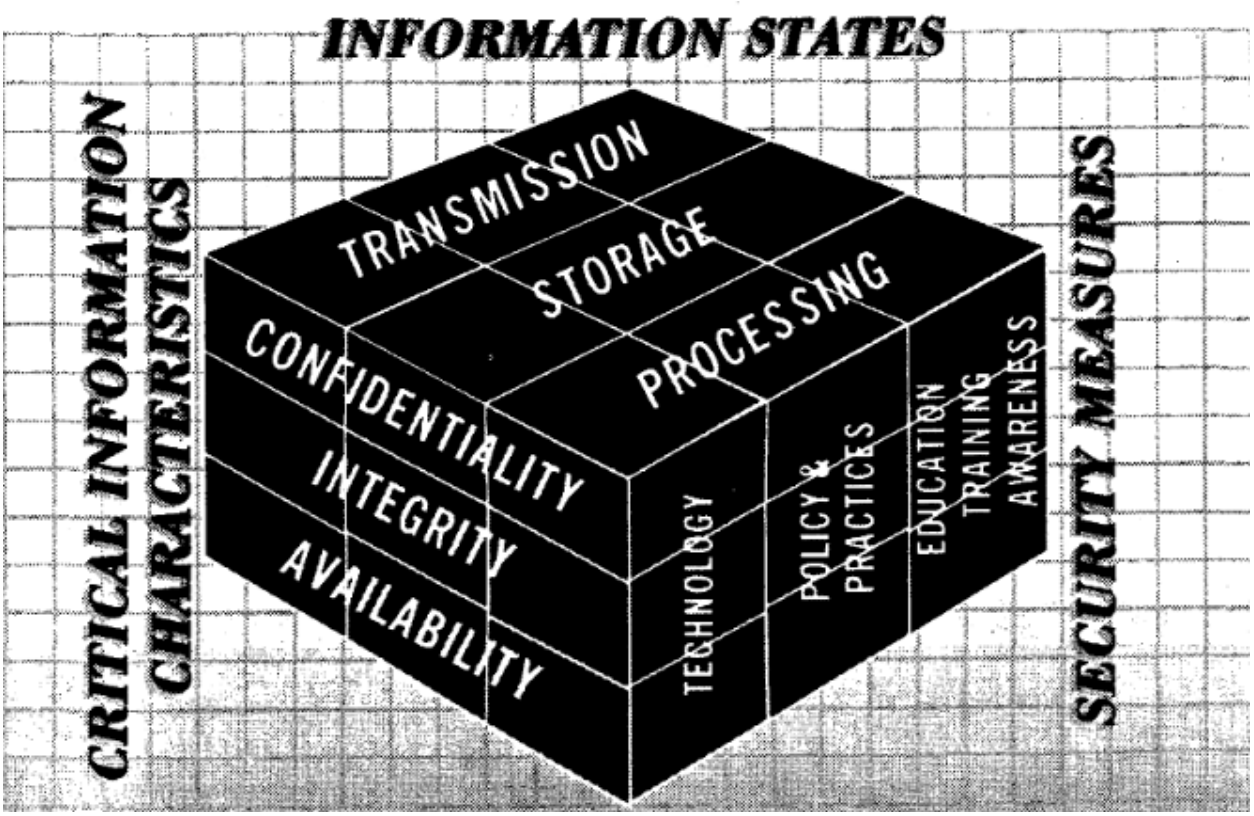

Figure 2 The McCumber Cube

3 PRIVACY PRESERVING TECHNOLOGIES FOR DCS CONTEXTS

With the establishment of privacy in the McCumber Cube model, the identification and development of several tools suitable for use within a DCS have become available. We suggest these tools as potential privacy implementations for a 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 a server to which data is reported. From this data, adversaries can steal information that attempt to recreate or sabotage that process. Other examples of modules may include the Safety Instrumented Systems (SIS) or Manufacturing Execution System (MES), which need to transfer, process, and store data from devices.

3.1 Differential Privacy

Differential privacy attempts to add noise to data so an adversary will not be able to identify whether a *data record* belongs to one database or another with high confidence. The corresponding mechanism 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 to inject noise in order to protect individual data points yet disclose enough information that can be used for the general conclusions of the dataset (i.e. utility).

Many research papers focusing on differential privacy do so within the Smart Grid context. The Smart Grid processes inputs from the Advanced Metering Infrastructure (AMI) that transmits time-series data on power consumption for processing at Level 2. From the power consumption data, decisions need to be made in order to produce more or less power. To protect against false data injection, the data processed must include measures of privacy. [9] explores

privacy preservation of solar power generation and [10] creates a privacy-preserving protocol to obfuscate queries and receive fine-grained results of power consumption. [3] compiles an in-depth view of three privacy-preserving protocols of data minimization.

For use of Level 2 and below, the same measure of privacy preservation occurs on the plant between 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 to preserve privacy of the actual data inputs, so the question is whether the trade-off is accurate enough or worth the cost.

[11] 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 [12]. 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 exceed engineering units that have a low tolerance of modification. Sensitive industries may not be able to adopt differential privacy

protections as readily as other industries such as electricity or water. Therefore, it is not recommended to include differential privacy for those specialized industry standards.

Current research include various attack models for the ways of adding noise via a randomized noise mechanism. Specifically to DCS contexts, [13] provides an attack model in which an adversary can manipulate a differential private DCS by injecting false data with having 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.

3.2 Private Information Retrieval

For differential privacy, the problem is if the *data record* was from one database or another. For *private information retrieval* (PIR), the problem is on not disclosing whether the *query* of the data record was requested from one database or another. As such, PIR requires different challenges in order to satisfy its query-based privacy role separate from differential privacy. PIR was popularized in [14] with a more efficient scheme.

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, [14] and [15] 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.

4 TOWARDS A GENERAL PRIVACY FRAMEWORK FOR DCS

For every standard presented in Table 1, we present recommendations to provide privacy protections for DCS. Each standards' existing security and policy attributes are examined in the McCumber Cube model. For each standards' scope and objectives, the recommendations create new requirements for privacy protection using the technologies specified in Section 3.

Of the given standards, there are two to be ignored: IEC 62443/ISA 99 and ISA 88. These two standards mainly consider the policy procedures and processes in order for a DCS to function. Matured security concepts such as the CIA triad are currently in the working drafts for these standards, so recommendations for privacy considerations are too early to recognize with current research. "Best practices" similar to principles detailed in [2] are currently being discussed in research like [16] for DCS in Europe due to General Data Protection Regulation (GDPR).

4.1 Recommendations for Standards

From the technological solutions in Section 3, we integrate potential recommendations for current standards to adopt mechanics to protect privacy. The recommendations are given keywords where 'must' is a requirement and 'should' is a recommendation as in IEEE standards:

IEC 62541

Rationale: For OPC-UA, machine-to-machine communications are represented by relations between object models. Objects can be given access, modifications, and request services. In part 7 of the standard, profiles for the interaction of UA Servers and Clients are specified which can include security protocols. Secure communications over profiles include sending encryption parameters, algorithm names, and public keys.

Recommendation: A privacy protocol must be implemented to carry the necessary inputs required for passing privacy parameters and handle responses. 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.

NIST NP-800-82

*Rationale***:** NIST SP-800-82 summarizes items for all security-related concerns for a wide variety of protocols and concepts. Both security and policy are mentioned in the guidelines with in-depth suggestions. If IEC 62541 adds privacy protocols, then it is necessary to append a correlating privacy architecture section and application section for NIST SP 800-82.

Recommendation: 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

Rationale: NISTIR 7268 is a step ahead of other standards by addressing all sides of the McCumber Cube model, however the privacy section only focuses on protecting individual persons. The Smart Grid privacy archetype can be expanded to other industries that utilize DCS.

Recommendation: 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 must include privacy use cases as those given in Section IV. Additional discussion of privacy should include mention of the McCumber cube or some other framework of providing

privacy. In section 5.7.3 "Recommended Privacy Practices", there should be inclusion of the technologies given in Section 3. For differential privacy and PIR, the recommended titles should be similar to section 5.4 of [3] as *perturbation* and *trusted computation*, respectively.

CIS CSC 13, 14

Rationale: The CIS organization gives various compliance tools from its CSC documents. Providing a document and compliance tool for privacy can be included to give protections for DCS plants.

Recommendation: 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 mentioned in section 5.4 of [3].

4.2 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.

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.

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.

5 DISCUSSION

With the realization of a general privacy framework, we can discuss the benefits, costs, and limitations to the amended standards and the overall goal for privacy's inclusion.

In the event of control security failures, a DCS plant loses its integrity, and also requires all industrial processes to be validated in an audit for compliance, quality, and recovery. With data privacy protections, the process for returning to continuity of operations should be drastically reduced with the knowledge that the data retained in the plant has a measure of information assurance.

DCS plants might also employ statistical-based *Intrusion Detection Systems* (IDS) to look for outlier behavior of operating machine. By having more statistical data to work with, an IDS practicing both security and privacy based protocols would have more information to make decisions of whether to trust values outputted from a certain machine.

However, the costs of privacy must also be understood for practical implementation. With the technologies given in Section 3 there is clear research showing differential privacy costs in the quality of data, while private information retrieval costs in the number of queries for the data. We support that these costs to be acceptable for DCS. The tolerance of data changes are already present with the use of engineering units and models for controlling the outputs of processes for DCS.

While we did not present simulations or models to gauge privacy costs, there are paths to simulating practical results using the technologies presented in Section 3. For the analysis of cybersecurity, NIST provided a testbed for design in [17] where privacy protections could also be implemented.

However, the theoretical framework of privacy presented contributes a better, holistic view of protections for DCS. The current implementation of security in the standards will not be enough to cover the protection of data for machines, humans, and systems in DCS. We propose that the tools provided will be part of the answer for protecting the data in ways that do not compromise security, the required functions of DCS, and the business interests present.

In future adversary models where privacy and security are acting together, we hope that it will be harder to gain enough information to steal process details or destroy plant equipment.

6 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] R. Leszczyna, "Cybersecurity and privacy in standards for smart grids - A comprehensive survey," *Computer Standards & Interfaces,* vol. 56, pp. 62-73, 2018.

[2] A. Cavoukian and others, "Privacy by design: The 7 foundational principles".

[3] M. Jawurek, "Privacy in Smart Grids," 2013.

[4] T. S. G. I. P. S. G. C. Committee, "NISTIR 7628 Rev. 1 Guidelines for Smart Grid Cybersecurity," 2014.

[5] C. P. Pfleeger, Security in Computing, Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1989.

[6] R. A. Kisner, W. W. Manges, L. P. MacIntyre, J. J. Nutaro, J. K. Munro, P. D. Ewing, M. Howlader, P. T. Kuruganti, R. M. Wallace and M. M. Olama, "Cybersecurity through real-time distributed control systems," *Oak Ridge National Laboratory, Technical Report ORNL/TM-2010/30,* 2010.

[7] J. R. McCumber, "Information Systems Security: A Comprehensive Model," in *Proceedings of the 14th National Computer Security Conference: Information Systems Security: Requirements and Practices,* 1991.

[8] C. Dwork, "Differential Privacy: A Survey of Results," 2008.

[9] J. Dong, T. Kuruganti, S. Djouadi, M. Olama and Y. Xue, "Privacy-Preserving Aggregation of Controllable Loads to Compensate Fluctuations in Solar Power," in *2018 IEEE Electronic Power Grid (eGrid)*, 2018.

[10] X. Liao, P. Srinivasan, D. Formby and A. R. Beyah, "Di-prida: differentially private distributed load balancing control for the smart grid," *IEEE Transactions on Dependable and Secure Computing*, 2017.

[11] Z. Huang, Y. Wang, S. Mitra and G. E. Dullerud, "On the cost of differential privacy in distributed control systems," in *Proceedings of the 3rd international conference on High confidence networked systems*, 2014.

[12] "DeltaV Statistical Process Monitoring Whitepaper," 2016.

[13] J. Giraldo, A. A. Cardenas and M. Kantarcioglu, "Security vs. privacy: How integrity attacks can be masked by the noise of differential privacy," in *2017 American Control Conference (ACC)*, 2017.

[14] B. Chor, O. Goldreich, E. Kushilevitz and M. Sudan, "Private information retrieval," in *Proceedings of IEEE 36th Annual Foundations of Computer Science*, 1995.

[15] C. Devet and I. Goldberg, "The best of both worlds: Combining information-theoretic and computational PIR for communication efficiency," in *International Symposium on Privacy Enhancing Technologies Symposium*, 2014.

[16] F. Mannhardt, S. A. Petersen and M. F. Oliveira, "Privacy challenges for process mining in human-centered industrial environments," in *2018 14th International Conference on Intelligent Environments (IE)*, 2018.

[17] R. Candell, T. Zimmerman and K. Stouffer, "An industrial control system cybersecurity performance testbed," *National Institute of Standards and Technology. NISTIR,* vol. 8089, 2015.

[18] A. Ujvarosi, "Evolution Of Scada Systems," *Bulletin of the Transilvania University of Brasov. Engineering Sciences. Series I,* vol. 9, p. 63, 2016.

[19] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," *NIST Special Publication,* vol. 800, p. 82.

[20] C. Barreto, J. Giraldo, A. A. Cardenas, E. Mojica-Nava and N. Quijano, "red Control systems for the power grid and their resiliency to attacks," *IEEE Security & Privacy,* vol. 12, pp. 15-23, 2014.

[21] "Poster of all Critical Security Controls by the Center of Internet Security," 2016.

[22] "List of Critical Security Controls by the Center of Internet Security," 2016.