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

Copyright by

Wasfi Momen

2019

PRIVACY RECOMMENDATIONS FOR FUTURE DISTRIBUTED CONTROL SYSTEMS

by

WASFI MOMEN

Committee Chair: Anu Bourgeois

Committee: Ashwin Ashok

TBD

Electronic Version Approved:

Office of Graduate Studies

College of Arts and Sciences

Georgia State University

July 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**

[ACKNOWLEDGEMENTS v](#_Toc13683386)

[LIST OF TABLES viii](#_Toc13683387)

[LIST OF FIGURES ix](#_Toc13683388)

[LIST OF ABBREVIATIONS x](#_Toc13683389)

[1 INTRODUCTION 1](#_Toc13683390)

[1.1 Structure of Distributed Control Systems 2](#_Toc13683391)

[1.2 Review of Privacy 2](#_Toc13683392)

[1.3 2](#_Toc13683393)

[2 Literature review 3](#_Toc13683394)

[2.1 Current Specifications 3](#_Toc13683395)

[2.2 Separation of Security and Privacy 4](#_Toc13683396)

[3 privacy preserving technologies for dcs contexts 6](#_Toc13683397)

[3.1 Differential Privacy 6](#_Toc13683398)

[3.2 Private Information Retrieval 6](#_Toc13683399)

[4 towards a general privacy framework for dcs 8](#_Toc13683400)

[4.1 Recommendations for Standards 8](#_Toc13683401)

[4.2 Privacy Use Cases 8](#_Toc13683402)

[5 conclusion 10](#_Toc13683403)

[REFERENCES 11](#_Toc13683404)

[APPENDICES 12](#_Toc13683405)

[Appendix A 12](#_Toc13683406)

[Appendix A.1 12](#_Toc13683407)

[Appendix A.2 12](#_Toc13683408)

[Appendix B 12](#_Toc13683409)

[Appendix C 12](#_Toc13683410)

# LIST OF TABLES

[Table 1 Standards of DCS Security and Privacy 3](#_Toc13677709)

# LIST OF FIGURES

[Figure 3.1 You're Almost Ready to Graduate! 3](#_Toc410652167)

# 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
* SP – Special Publications

# INTRODUCTION

Distributed Control Systems (DCS) are a significant part in the daily lives of citizens across the world. DCS handles the production and consumption of wastewater treatment, electricity generation, and other large-scale processes. Across decades of technological improvements, the scalability of DCS went from large city production to regional distribution. 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 greater importance on 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 moved around throughout the plant for operations and in the cloud for performance analysis.

Unfortunately, the data inside the data historian holds key aspects of production processes that business would want to protect against intellectual theft through business espionage. 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 scenario above is exactly 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 the plant had known vulnerabilities that were exploited to gain access to the data housed in the facility. The Department of Homeland Security notified the company and the relevant notice was issued in 2014 resulting in Yokogawa Electric applying patches to the vulnerable software.

The Toray plant gives an example of information espionage in the DCS field today. Software vulnerabilities will be abundant, but managed with the adoption of reportable notices like ICS-CERT and improving technologies. 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 to touch on the topic of \textit{data privacy}. Soon, the past standards such as

NIST SP-800-82, ISA 99/IEC 62443 and industry specific standards like ISA 88 and IEC 61580 will be re-contextualized within a privacy-protected world.

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.

## Structure of Distributed Control Systems

## Review of Privacy

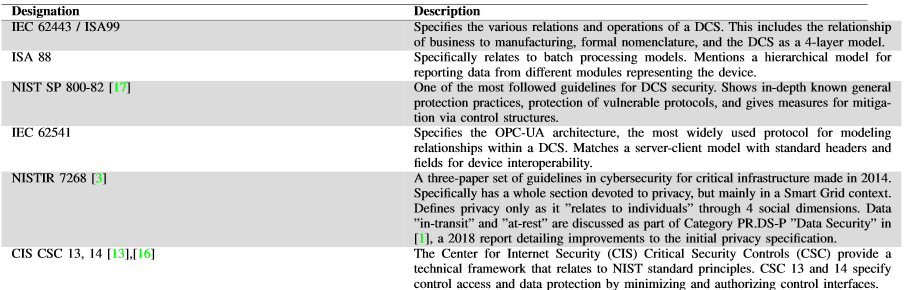
## Adversary Models

# Literature review

Historically, the demand for security in DCS did not come from the designers of systems for DCS but instead arose as a natural consequence from 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.

## Current Specifications

Table 1 Standards of DCS Security and Privacy



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 create the majority fundamental control layer security mechanics, including encryption and access control.

For mentions 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.

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 of DCS, the data layer will be the place where privacy is protected for machines.

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 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.

## 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 \cite{Pfleeger\_1988\_ciainception} 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. \cite{kisner\_2010\_oakridge} provides a comprehensive overview of the security principles in control systems and providing mitigation against security attacks based on these principles.

As research into privacy for computers continues to grow, there is still a need to define privacy as it relates to other concepts like 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, \cite{mccumber\_1991\_megacites} presented the McCumber Cube to relate 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. The last side promotes the interests of policy, education, and standardization.

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 \cite{cavoukian2009privacy}. 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 researched thoroughly with many different implementations and ideas being presented \cite{kisner\_2010\_oakridge}, 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.

# privacy preserving technologies for dcs contexts

With the establishment of privacy, the identification and development of several tools suitable for us within a DCS have become available. We suggest these tools as potential privacy implementations of 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 an OPC-UA server to which data is reported. From this data, adversaries can learn information about a process in attempts to recreate or sabotage a process. Other modules may be the Safety Instrumented Systems (SIS) or Manufacturing Execution System (MES) which both need to transfer, process, and store data from devices.

## Differential Privacy

Differential privacy attempts to add noise to data such that an adversary will not be able to identify whether an output record of data belongs to one database or another with high confidence. The mechanism in which it does so is using some randomized function K to manipulate every data point within the two databases, D1 and D\_2 \cite{dwork\_2008\_goodintroforstandardsofprivacy}. The function takes input parameters of the two databases as well as a privacy budget epsilon 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 (i.e. utility).

## Private Information Retrieval

For differential privacy, the problem relied on not disclosing if a data record was in one databases or another. For private information retrieval (PIR), the problem relies on not disclosing the query of the data record requested from one database or another. As such, PIR requires different mathematics in order to satisfy its query-based privacy role separate from differential privacy.

# towards a general privacy framework for dcs

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

## Recommendations for Standards

Of the given standards, there are a couple of recommendations to be given to some, but also ignoring others entirely. The ones to be ignored entirely are the ones that built DCS in the first place, 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 for most countries 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.

## Privacy Use Cases

As identified by other standards such as NIST SP-800, 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* With previous research on Smart Grid privacy, individual person privacy and systems privacy must both play a vital role to protecting the DCS of a power plant. 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.

*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.

# conclusion

From the specifications provided, we created a

# REFERENCES

# APPENDICES

## Appendix A

### Appendix A.1

### Appendix A.2

## Appendix B

## Appendix C