Institute of Technology Management and Entrepreneurship

A MODEL OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY OF SCADA TO ENHANCE PUBLIC SAFETY IN UAE

Omar Alhashmi

Doctor of Philosophy

2023

A MODEL OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY OF SCADA TO ENHANCE PUBLIC SAFETY IN UAE

OMAR ALHASHMI

A thesis submitted
in fulfilment of the requirements for the degree
of Doctor of Philosophy

Institute of Technology Management and Entrepreneurship

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DEDICATION

To my beloved mother and father

ABSTRACT

The dependence of industrial systems, including Supervisory Control and Data Acquisition (SCADA) systems, on AI technology is growing rapidly. Given the mandate of AI to achieve efficient and effective industrial supervisory systems, the pertinent threats resulting from both internal malfunctions and external cyber sabotage, and the defence mechanisms often installed internal and external to the systems, the time seems right for an all-inclusive model of AI critical evaluation threat-resilience model. This futuristic model places AI as the main actor and regresses the role of humans into a supportive position. The aim of the study is to critically examine the threat-resilience of AI-SCADA systems in ensuring improved public safety to arrive at critical implications to UAE cybersecurity governance. To address the research questions outlined, the study employs an explanatory sequential mixed methods design (Creswell & Plano Clark, 2011). The explanatory sequential mixed methods design encompasses the collection and analysis of quantitative data followed by qualitative data. The first stage of the study involves qualitative research, The first stage of this study involves a qualitative exploration followed by Qualitative findings informed the development of a survey instrument that was used to collect data from a larger population. The qualitative survey research employed empirical data from the three main groups of stakeholders: the regulators of key SCADA sectors, SCADA operators in the UAE, and clients of SCADA Systems. Critical attention is paid to the utility and oil and gas sectors as central to the use of SCADA systems in a context where public safety is most vulnerable. A sample of 380 SCADA-related project managers is considered sufficient to generalise the results to the study population, even though 219 were considered useful for empirical analysis after data cleansing. While for the Qualitative research, data were collected with the help of interviews, document analysis and observation. This phase involved the top 2 SCADA operators who control approximately 60% of all non-law enforcement-related systems and their respective clients. The Qualitative research was implemented in a leading role, whilst the qualitative survey research was applied to support the study findings in this regard. Findings from the Qualitative study and survey research are largely complementary. Exploratory evidence revealed three key security operationalisation areas: risk management, physical and environmental management, and user access management. Findings show that risk management of AI-based SCADA systems is optimal in both the utility and oil and gas sectors. However, physical and environmental management in the utility sector is at optimal levels even though the oil and gas sector is mainly lagging in system governance. Also, user access management in both the utility and oil and gas sectors is lagging in terms of governance and external defence systems. As part of the survey, findings reveal that human governance is a valid mediator of the model, whilst defence systems also significantly moderate the relationship between attack resilience and public safety. Evidence also shows that the utility and oil and gas sectors differ significantly in the operationalisation of the research model; moreover, the AI threat-resilience model was validated among the operational levels of the sector organisations. It is recommended that cybersecurity

governance be made a mandatory policy for oil and gas companies, utility companies, and organisations that use AI-based SCADA systems.

.

MODEL KECERDASAN TIRUAN DALAM KESELAMATAN SIBER SCADA UNTUK MENINGKATKAN KESELAMATAN AWAM DI UAE

ABSTRAK

Kebergantungan sistem perindustrian pada teknologi kecerdasan buatan (AI) berkembang pesat, termasuk juga Sistem Kawalan Penyeliaan dan Pemerolehan Data (SCADA). Memandangkan tanggungjawab AI untuk mencapai sistem penyeliaan industri yang cekap dan berkesan, ancaman berkaitan yang berpunca daripada kerosakan dalaman, sabotaj siber luaran, dan mekanisme pertahanan sering dipasang secara dalaman dan luaran pada sistem, dan keperluan sekarang untuk model yang merangkumi semua seperti model penilaian kritikal ketahanan ancaman AI. Model futuristik ini meletakkan AI sebagai pelakon utama dan meletakkan peranan manusia sebagai sokongan. Matlamat kajian adalah untuk mengkaji secara kritis ketahanan ancaman sistem AI-SCADA dalam memastikan keselamatan awam yang telah dipertingkatkan untuk mencapai implikasi kritikal kepada tadbir urus keselamatan siber UAE. Untuk menangani persoalan kajian yang digariskan, kajian ini menggunakan penjelasan reka bentuk kaedah campuran berjujukan. Penjelasan reka bentuk kaedah campuran berurutan merangkumi pengumpulan dan analisis data kuantitatif diikuti oleh data kualitatif. Peringkat pertama kajian melibatkan penyelidikan kualitatif. Peringkat pertama kajian ini melibatkan penerokaan kualitatif diikuti dengan hasil dapatan kualitatif ini akan terlibat di dalam pembangunan tinjauan instrumen yang digunakan untuk mengumpul data daripada populasi yang lebih besar. Penyelidikan tinjauan kualitatif menggunakan data empirikal daripada tiga kumpulan utama: pengawal selia sektor utama SCADA, pengendali SCADA di UAE dan pelanggan Sistem SCADA. Perhatian kritikal diberikan kepada sektor utiliti dan sektor minyak dan gas kerana keselamatan awam paling terdedah pada sector ini dari konteks penggunaan sistem SCADA. Seramai 380 sampel pengurus projek berkaitan SCADA telah diperolehi dan ianya dianggap mencukupi untuk menyamaratakan keputusan kepada populasi kajian, walaupun 219 sampel dianggap mencukupi untuk analisis empirikal selepas proses pembersihan data. Manakala bagi kajian Kualitatif pula, data dikumpul secara temu bual, analisis dokumen dan pemerhatian. Fasa ini melibatkan 2 pengendali SCADA teratas yang mengawal kira-kira 60% daripada semua sistem bukannya berkaitan dengan penguatkuasaan undang-undang dan klien masing-masing. Kajian kualitatif merupakan kajian utama, manakala kajian tinjauan kualitatif digunakan untuk menyokong dapatan kajian ini. Penemuan daripada kajian Kualitatif dan kajian tinjauan sebahagian besarnya adalah saling melengkapi antara satu sama lain. Bukti penerokaan kajian mendedahkan tiga kunci utama di dalam bidang operasi keselamatan: pengurusan risiko, pengurusan fizikal dan alam sekitar, dan pengurusan akses pengguna. Penemuan menunjukkan bahawa pengurusan risiko sistem SCADA berasaskan AI adalah optimum dalam kedua-dua sektor utiliti dan sektor minyak dan gas. Walaubagaimanapun, pengurusan fizikal dan alam sekitar dalam sektor utiliti berada pada tahap optimum walaupun sektor minyak dan gas kebanyakannya ketinggalan dalam tadbir urus sistem. Selain itu, pengurusan akses pengguna dalam kedua-dua sektor utiliti dan sektor minyak dan gas adalah ketinggalan dari segi tadbir urus dan

sistem pertahanan luar. Sebagai sebahagian daripada tinjauan, penemuan mendedahkan bahawa tadbir urus manusia adalah pengantara yang sah bagi model tersebut, manakala sistem pertahanan juga menunjukkan signifikasi secara sederhana bagi perhubungan di antara daya tahan serangan dan keselamatan awam. Bukti juga menunjukkan bahawa sektor utiliti dan sektor minyak dan gas berbeza dengan ketara dalam pengoperasian model kajian; tambahan pula model ketahanan ancaman AI ini telah disahkan dalam kalangan peringkat operasi organisasi sektor. Adalah disyorkan agar tadbir urus keselamatan siber dijadikan dasar mandatori untuk syarikat minyak dan gas, syarikat utiliti dan organisasi yang menggunakan sistem SCADA berasaskan AI.

ACKNOWLEDGMENTS

In the name of Allah, the Most Gracious and the Most Merciful. Alhamdulillah, I praise and thank Allah SWT for His greatness and for giving me the strength and courage to complete this thesis.

First and foremost, I would like to express my deepest gratitude to my supervisor, Associate Professor Ts. Dr. Mohd Faizal Abdollah for his endless support and guidance throughout the period of my research.

I am grateful to all those who supported me in any way or form in the course of my research. I am most grateful to the case study organisations who granted me access to their premisses and other persons who broke protocol to let me on critical insight necessary for my study completion. Without them, the study could not have been completed successfully.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATION

ADNOC	-	Abu Dhabi National Oil Company (ADNOC)
ADWEA	-	Abu Dhabi Water and Electricity Authority
AI	-	Artificial Intelligence
CCTV	-	Closed-circuit television
CFA	-	Confirmation Factor Analysis
DELIA	-	Deep Learning Interface for Accounting
DEWA	-	Dubai Electricity and Water Authority
EAR	-	External Attack Resilience
EDS	-	External Defense System
EFA	-	Exploratory Factor Analysis
ENEC	-	Emirates Nuclear Energy Corporation
FAHR	-	Federal Authority for Government Human Resources
FEWA	-	Federal Electricity and Water Authority
GCC	-	Gulf Corporation Council
GDP	-	Gross Domestic Product
GOV	-	System Governance
IAR	-	Internal Attack Resilience
ICT	-	Information Communication Technology
IDS	-	Internal Defense System

IP	-	Internet Protocol
ISC	-	Industrial Systems Control
MOE	-	Ministry of Energy
NCW	-	Network-Centric Warfare
NESA	-	Emirates National Electronic Security Authority
NGO	-	Non-Governmental Organisation
PS	-	Public Safety
SCADA	-	Supervisory Control and Data Acquisition
SD	-	Standard deviation
SEWA	-	Sharjah Electricity and Water Authority
UAE	-	United Arab Emirate
UK	-	United Kingdom
US	-	United States

LIST OF PUBLICATIONS

1. Alhashmi, O. A. R and Abdollah, M. F., 2019. Critical evidence on the implementation of SCADA in the UAE: Artificial Intelligence Mandate Vulnerability, and public safety. *International Conference in Management and Technology, Kuala Lumpur.* (Best Paper Award)

2. Alhashmi, O. A. R and Abdollah, M. F., 2020. Critical evidence on the implementation of SCADA in the UAE: Artificial Intelligence Mandate Vulnerability, and public safety. *TEST Engineering and Management*, 83 (March - April 2020), pp. 931- 937.

3. Alhashmi, O.A.R., Abdullah, M.F., Kamalrudin, M., 2022. The threat-resilience of AI-SCADA for improved public safety in UAE: The Moderating and Mediation Roles of Cyber-Defence and Governance. *NEUROQUANTOLOGY*, 20(11), pp. 4519-4536.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Many of today's ICSs derive from the application of IT methods into existing physical systems, often replacing or integrating physical control mechanisms. For example, the built-in digital controls replaced the analog mechanical controls in rotating machines and motors. Both the cost and the performance improvements have encouraged this evolution, resulting in the introduction of many of today's "smart" technologies such as smart grids, smart transportation, smart buildings, and smart manufacturing. While on the one hand, this evolution increases the connectivity and criticality of these systems, on the other hand, it creates a greater need for their adaptability, resilience, security, and protection. Engineering models are evolving to address these emerging properties including safety, protection, privacy, and interdependencies on the environmental impact. However, the full understanding of SCADA systems, their structure, as well as their functionality is fundamental for the management of their security. SCADA systems are essential components of the production processes used in several sectors, from the control of machinery in nuclear power plants to the management of traffic lights and cameras in cities. Since SCADA systems are involved in very critical processes, any kind of vulnerability, if exploited, could have serious repercussions not only within the critical infrastructures themselves but also across the whole region. The introduction of IT capabilities into physical systems involves a change in the structure and behavior of those systems, with implications

for their security. These systems are constantly evolving, acquiring new functionalities in response to the new requirements of an increasingly connected world.

According to Patel and Sanyal (2008), *"SCADA system is a computer-based process control system used by a nation's infrastructure utility systems, that permits control and monitoring of utilities by gathering field data from sensors and instruments located at remote sites, transmitting and displaying these data at a central site, and enabling engineers to send control commands to the field instruments".*

These systems help control industrial machinery in charge of water supply, electric power generation and distribution, mass transportation, and oil and gas production and distribution systems (Patel and Sanyal, 2008). Control commands are sent to field instruments through information communication technology (ICT), usually over web-based systems that operate over the internet (Patel and Sanyal, 2008). Using these systems, a technician can control the traffic signal, water and gas pumps, among other industrial gadgets, from a distant location. With growing significance in today's national economies, the global SCADA market is estimated to reach 40.18 billion United States Dollars by 2024 (Research and Markets, 2018).

As the delivery of public service is automated using SCADA systems, artificial intelligence (AI) help expand the functionalities of these systems to improve their overall capabilities (Kadar et al., 1999). This leads to what Lange (2007) terms "intelligent SCADA systems". Industrial systems are becoming larger and complex, and AI is considered the best tool to conduct supervisor and control tasks efficiently and effectively possible. Incorporating AI expert systems with high operational capabilities, industrial plants are able to make up for personnel shortage, identify flaws in a system and fix these flaws automatically, manage information overload and manage plat interface, all in a combined interrelated attempt beyond what humans could ever accomplish.

On an elaborate background on the increasing role of AI in massive industry control systems in utilities, transportation, oil and gas and other critical infrastructure, their exposure to cyber threat remains an area of concern to public safety (Nicholson et al., 2012; Research and Markets, 2018). A number of global incidents and case studies have revealed that the threat to SCADA systems to create unthinkable damage to humans and infrastructure is real (Williams, 2007). Considering Mateski et al. (2012) and Duggan et al. (2007) generic threat matrix of cybersecurity, attacks on SCADA systems remain a level 1 threat with the highest level of intensity, stealth and time dedication to achieve threat outcome (Figure 1.1). Under human control, such a threat may take years to a decade to execute and require an enormous amount of knowledge on cyber, kinetic and access; however, with AI mounting these attacks, such threats are no longer superficial.

Table 1.1: The generic threat matrix (Duggan et al., 2007; Mateski et al., 2012)

THREAT LEVEL	THREAT PROFILE						
	COMMITMENT			RESOURCES			
	INTENSITY	STEALTH	TIME	TECHNICAL PERSONNEL	KNOWLEDGE		ACCESS
					CYBER	KINETIC	
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L