A Model of Artificial Intelligence in Cyber Security of SCADA to Enhance Public Safety in UAE

Omar Abdulrahmanal Alattas Alhashmi[a*], Mohd Faizal Abdullah[b], , Raihana Syahirah Abdullah[b]
oalhashmi@ymail.com, mothman@utem.edu.my, raihana.syahirah@utem.edu.my
[a] Institute of Technology Management and Entrepreneurship, Univesiti Teknikal Malaysia
Abu Dhabi Civil Defence Authority, Abu Dhabi, UAE
[b] Faculty of Information and Communication Technology. Universiti Teknikal mlaysia Melaka

Abstract
The UAE government has set its sights on creating a smart, electronic-based government system that utilizes AI. The country's collaboration with India aims to bring substantial returns through AI innovation, with a target of over $20 billion in the coming years. To achieve this goal, the UAE launched its AI strategy in 2017, focused on improving performance in key sectors and becoming a leader in AI investment. To ensure public safety as the role of AI in government grows, the country is working on developing integrated cyber security solutions for SCADA systems. A questionnaire-based study was conducted, using the AI IQ Threat Scale to measure the variables in the research model. The sample consisted of 200 individuals from the UAE government, private sector, and academia, and data was collected through online surveys and analyzed using descriptive statistics and structural equation modeling. The results indicate that the AI IQ Threat Scale was effective in measuring the four main attacks and defense applications of AI. Additionally, the study reveals that AI governance and cyber defense have a positive impact on the resilience of AI systems. This study makes a valuable contribution to the UAE government's efforts to remain at the forefront of AI and technology exploitation. The results emphasize the need for appropriate evaluation models to ensure a resilient economy and improved public safety in the face of automation. The findings can inform future AI governance and cyber defense strategies for the UAE and other countries.

Keywords:
SCADA systems; Public safety; Artificial intelligence; Cyber sabotage; Cyber defense; Cyber security

1. Introduction

The UAE government is committed to implementing a smart government system where all operations are electronic and automated using AI techniques [1], [2]. This includes key utility services, transportation, and oil and gas facilities, with plans to expand into other sectors for cost savings and increased efficiency. The UAE has also established partnerships with neighboring countries, including India, to promote AI innovation and maximize its impact on the economy. The Minister of State for Artificial Intelligence, Omar Sultan Al Olama, plays a crucial role in these developments. The UAE believes AI can drive innovation and enhance the delivery of government services, as well as boost private sector performance by utilizing AI as a data and processing backbone. The expected returns from these efforts are projected to reach over $20 billion in the coming years [3]. The UAE is partnering with neighboring countries to advance its AI-based economy. One such alliance is the collaboration with India on innovation in AI between the UAE Ministry of Artificial Intelligence and Indian startups. This partnership aims to generate over $20 billion in returns in the coming years, with a significant role being played by Omar Sultan Al Olama, the UAE Minister of State for Artificial Intelligence. The UAE government views AI as a key driver of innovation, enhancing the delivery of government services and boosting private sector efficiency. By harnessing AI to catalyze data processing and drive business growth, the government hopes to improve the effectiveness of service delivery [4]. The UAE Strategy for Artificial intelligence was launched in 2017; this strategy is the first of its kind within the region, with key objectives to be achieved as part of the objectives of the UAE Centennial 2071 [5]. Through this strategy, the government aspires to improve performance at all levels and make the UAE the first in the field of AI investment in various sectors, including the creation of a new vital market with high economic value. The strategy mainly covers the application of Ai to key sectors, including the transportation, healthcare, space, renewable energy, water, technology, education, environment and traffic sectors.

In recent developments, the UAE and neighbouring countries have worked relentlessly on the field of cybersecurity in developing integrated solutions for SCADA. Cassidian is one of the first technology companies to develop the SCADA protection solution that protects industrial control systems (ICS) from outside attacks [6], [7]. Named Cymerius, the system ensures that SCADA systems and businesses are able to continue operations even in times of business interruptions or disasters. The system monitors both ICS and Business IT, with integration into the MOSEO smartphone application, which permits encryption of phone calls and other

Manuscript received February 5, 2023
Manuscript revised February 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.2.19

interactions between business and SCADA operators to secure all access points [8]–[10].

In another application of AI to SCADA systems, the UAE is reported to play an integral role in securing high-level professional cyber defense services to audit security infrastructure architectures and implement control and operational centres with dedicated security supervision in SCADA and other technology systems [10]. Careful vulnerability and security assessments are conducted in all critical infrastructure and government facilities at various levels of violence whilst keeping in mind the equal possibility of terrorism. Entities include public businesses in sensitive economic areas such as ADNOC, airports, seaports, water and power utilities, and the UAE nuclear plants, mainly in the energy, oil and gas and related sectors. Highlights of these developments appeared in the Cyber Warfare Integration and Data Protection section of the Nation Shield Magazine Journal on Military and Strategic Affairs issued by the UAE Armed Forces [11].

An empirically validated model of AI in cybersecurity is lacking but critical now than ever due to the increased dependence of human lives on installed technology systems. The trend towards technology dependence is only going to increase as AI gained an integral role in controlling the day-to-day supplies, safety and livelihood of humans [12]. Technology has not only gained roots in everyday life but has offered autonomous control over industrial and utility systems on which the lives of people depend, SCADA systems. AI is needed to process large information in record time, monitor real-time industrial processes and prompt the need for action when the need arises [13]. From education, entertainment, and industrial machinery to utility systems, AI and technology continue to be offered control over structures which renders significant loss of human lives when compromised [14]. It is of crucial urgency that insight is established into how these technology systems can be resilient to attacks whilst effectively serving the purpose for which they were installed [15]. There is a need to empirically assess threat systems to understand how such evaluation models can be adopted to nullify internal-external threat channels whilst improving internal-external defense mechanisms towards improved public safety.

As the role of AI in government increases, mainly prioritizing areas of SCADA, such technology changes witness continuous security challenges that require constant supervision to ensure that pertinent threats are mitigated and reduced [16]. Their implementation of an appropriate evaluation model is essential for a UAE Smart Government system which seeks to be fully adopted by 2021 and will cover all scopes of government operations, including SCADA systems in utility and sensitive economic sectors [17]. The present study helps conceptualize the threat of automation whilst maintaining the role of automated defensive mechanisms in the face of mediatory regulatory measures. This insight is critical to ensuring a resilient economic system in the wake of the digital economy. The study also contributes to the UAE Government's agenda to remain at the top of AI and technology exploitation within the region and on the global terrain.

2. Materials and Method

The questionnaire was prepared based on the measurement of variables using carefully supported and validated data collection instruments in the literature. The AI IQ Threat Scale was used for the measurement of the four main attacks and defense applications of AI presented in the research model. This scale was originally developed and empirically validated by [18]. AI Governance and Public Safety were measured with the help of [19], and importantly, [20] framework for AI governance. The individual items for the measurement of the items are presented in Table 1. The main items on the questionnaire were 30 in total. These items were measured with the help of the five-point Likert scale. Each of the six constructs within the model was measured using 5 items each adapted from reputable and validated empirical sources. In addition to the demographics, a total of 36 questions were produced on the survey questionnaire. To validate these items, a pilot study and expert review were conducted. These items were presented on the survey questionnaire together with questions on respondents' demographics such as age, gender, institution/company, and level of management. The research model was controlled for the level of management and the company of the respondent since holding these in an unchanging state will permit a better outcome of the empirical results. Using the survey questionnaire is also justified as it helped collect quantitative data in line with the quantitative research method, using mainly a five-point Likert scale to measure the constructs in the research model. The Likert scale help in the measurement of variables as a continuous scale as recommended by [21]; this help conducts the needed forms of inferential statistical analysis as part of the quantitative methods.

Table 1: Measurement items for survey questionnaire

Dimension	Items	Source
Internal Threat Resilience	installed system security infrastructure	
	system security personnel	
	system security architecture	
	internal self-threat checks	
	system culture towards non-technical threats	
External threat resilience	system readiness to fend off external Attacks	[22][18]
	Dedicated internal systems to curb the external cyber threat	
	System internal management structures	
	Special units exist to combat external	

	threat developments	
	Overall external threat resilience	
Internal Defense	Active defense systems	[18], [22]
	Procedures for defense from system attacks	
	Defense of original operational modules	
	Constant monitoring of systems	
	Overall internal threat resilience	
External Defense	The systems service provider collaboration	[18], [22]
	Government support readiness	
	Client system governance	
	Client governance of human roles	
	Overall external defense systems	
Governance	The existence of appropriate policies to govern AI	[19], [20]
	Cyber supervision by government agencies	
	Learning from events	
	Constant evaluation of options to ensure public safety	
	Stakeholder engagement	
Public Safety	public life safety	[20]
	Service continuity	
	Operationalization of safety systems infrastructure	
	Prioritization of public life	
	Overall public safety	

According to Saunders et al. (2012), the survey research strategy permits the collection of data from a large set of participants or audience and assists in efforts to achieve representativeness and generalizability. The survey research strategy is therefore justified to help maintain objectivity and replicability in all areas of data collection administration. Maintaining reliability and validity is vital to help complement research credibility. These observations and a systematic approach are in line with the positivist philosophy in this investigation.

2.1 Instrumentation

Four main data collection instruments are employed in the present investigation. These instruments are divided into two main groups qualitative and qualitative groups, as highlighted in the earlier section.

2.1.1 Instruments for the qualitative research

Three main instruments were used for the qualitative research phase. These tools include an interview guide, an observation guide, and a secondary data collection guide. The interview guide consisted of six main questions. Question one focused on the resilience of SCADA systems to internally generated threats; question 2 focused on systems resilience to the externally generated threat; question 3 looked into internal defense mechanisms; question 4 considered external control mechanisms; question 5 considered the government's role and policy-making behavior; finally, question 6 focused on recommendations to improving public safety by building SCADA system resilience to attack and defense mechanisms.

The second data collection instrument under this group was the observation guide. The guide was prepared based on the observation matrix. The methodology that informs the matrix was originally prepared or submitted in an earlier publication by [23]. The observation focused on the two main actors of businesses within the Utility and Oil and Gas sectors. It collected vital data on the branch and SCADA operator. The observation matrix is built on security policies, mechanisms, and security personnel dimensions integral to the model. These policies and mechanisms were combined to clearly define the safety of SCADA systems as they exist within the scope of the study.

The last data collection instrument considered document analysis, mainly focusing on secondary data documents accessible from the SCADA operators. Secondary data documents were sought from the two main perspectives of (1) oil and gas and (2) utility companies' application of SCADA systems. The qualities of any document received were labelled regarding (1) policy or operational document, (2) confidential or non-confidential nature of the document, and (3) public or non-public. Even though confidential documents may be deemed non-public, not all non-public documents could be classified as confidential; these groups of documents were of particular interest to the present study.

2.1.2 Instruments for the qualitative survey research

The survey questionnaire was used for the qualitative phase of the present investigation. The questionnaire has four demographic questions under biodata; these questions include gender, age, level in the organization, and technology/SCADA-related position in the organization. These questions fell under the demographics of the study. As part of the demographics, a second sub-section of institutional particulars was presented to gather data on the sector of the organization and the level of SCADA adoption.

It also covers the resilience of SCADA systems to internal and external threats; five questions were each allocated to internal and external threat resilience. Another ten questions were asked regarding the internal and external defense systems, using items presented in the earlier section of this material and method – the measurement of variables for SCADA AI defense systems.

3. Result and Discussion

3.1 Overview of data from organisations

The study originally sought to conduct four interviews as part of the action research diagnosis strategy. Two sample respondents were sought from each study organisation. Only one qualitative study provided approval and subsequently made available participants for the research interviews. Specifically, the oil and gas organisation provided one sample for participation in the interview. Two other informal interviews were conducted as reported in [23]; however, these other engagements did not reveal much insight and are therefore not considered.

As part of the diagnosis stage, document analysis was conducted; a one-and-a-half-page policy document on information security was obtained from the utility case study organisation. Following the diagnosis, the observation paves the way for action planning based on the original diagnosis. The observation was conducted to gather numerical data using the observational matrix prepared in the later section of this analysis; both case study organisations provided consent to observe data. These three data collection efforts support the first three stages of action research. Following these stages, the findings are evaluated, and key learnings are specified.

3.2 Interview data analysis

The interview with the respondent from the oil and gas company lasted about 18 minutes. Even though the interview was not recorded, due to a lack of permission to do so, the data was manually documented to capture a good amount of data in the course of the discussions. A total of six main questions were asked, as presented in the interview guide. The vital role of SCADA in operational efficiency and performance of the oil and gas sectors was discussed. Examples were offered on the use of SCADA to oil and gas control gauges, control the flow of fuel in pipelines from offshore to onshore reservoirs, and SCADA to be used as control mechanisms to support workers activities.

The threat of SCADA systems was discussed as both external and internal to the organisation. Internal threats were considered difficult to understand since these threats usually come from unexpected internal sources. Threats are often external as an organisation has to watch out for adversaries outside the organisation. Internal threat sources hold the potential of causing severest damage to the organisation due to direct access to resources, control systems, and how things work within the organisation. In the same manner, as internal human threat poses these challenges, internal AI systems threat also falls within the same category. In the actual words of the respondents:

"Internally, AI systems operate within the organisational environment and humans may have the capability of influencing other systems to malfunction… normal employees would not see this as only the system architect or engineer can identify this problem".

Internal threats may not reveal themselves easily as they may be conceived within some software within the program. They may have different impacts on the system, including slow reaction time, dysfunctional gauges and other on-site instruments, among others. The immediate response may be to replace dysfunctional systems, but the problem may be deeper than that as the dysfunctional system may be caused by the interference of intelligence mechanisms within the network system. Over time, the lags may have serious effects on the organisation as a whole due to accumulated inefficiencies and often productivity halts.

Aside from the threat that gradually inhibits productivity, a threat may appear in a sudden form easily observable by non-professional IT personnel and other system experts alike. Such sudden outburst is easy to spot and may be controlled before any further damage. Nonetheless, the sharp burst has the tendency to cause equal damage as malign systems behaviour that remain hidden over long periods of time.

Elaborating on externally generated threats, it was emphasised that such threats might as well take the form of a slow destroyer or harsh impact depending on the nature of the attack. External attack forms are mainly interested in the network link between the SCADA control centre and the client organisation system. Individually, the SCADA control centre and the client organisation act as closed networks that cannot be easily infiltrated by outsiders. Closed network systems have strong network protocols to guide against outside infiltrations. However, since the client has to offer back-end access to the SCADA operator, this reveals a key vulnerability within the network systems. The respondent in this submission mentioned that:

"Outsiders target this connection since it is the weakest point of the SCADA work system with thin security measures. Also, this connection is usually available on the wider internet system even though encrypted".

Whereas the organisation can work conducted within an intranet, inaccessible from outside sources, the connectivity of SCADA control systems usually happens over the internet. Attackers from all over the world may be able to gain access if they have the right access to network addresses and passcodes used by any of the personnel on the network.

In view of looming internal and external threats, internal defense mechanisms are installed within the SCADA system. These systems work automatically or intuitively, with little to no human intervention. The internal networks reject external access even with correct codes if users are attempting to log in from an unusual location even within the same country. Multiple logins and the use of wrong credentials are also monitored. Systems intelligently

change the access uniform resource locator using verifiable key codes at the client and SCADA control centre. A constant search and monitoring of user patterns are conducted as part of internal defense systems.

Aside from these internal defense mechanisms, some external cyber-defense systems are installed or procured from the network provider to create autonomous defense network systems. Such security solutions are network perimeter-based and mainly exist in the form of load balancers and firewalls. These defense mechanisms are often generic and fend off state-based distributed denial of service (DDoS) attacks. This is not only one of the most common forms of external attacks present on the global cyber network, but most such attacks are directed at SCADA systems with the intent of causing indirect damage caused by network lapses.

On the question pertaining to the governance of the system, the role of humans in the SCADA system cannot be exempted. This originates from the fact that humans are the very architects of the system, and the ability of the system to function properly is equal to the measure of input by the human architects. Human actors mainly act as control parties that frequently check the system to make sure the system functions at an optimal level. In addition, humans within an AI-based system introduce constraints and policies to guide system operability. Even though efficiency and systems effectiveness may be appraised due to the role of AI, the need for limitations on AI powers was highlighted at the final stages of the discussion. AI systems cannot be completely independent and must always be subjected to human control.

On the last question regarding recommendations for improvement, the respondent emphasised that public safety is ensured because SCADA control room personnel are able to initiate action based on AI sensors and other intelligent triggers. These sensors and triggers do not only act as sensors but interpret the behaviour of sensors based on environmental conditions. An instance is that interference in oil and gas flow through existing pipelines may be ignored in the event that such interference is caused by rainy or stormy weather. At the same time, these interferences do not imply that the rapture of an existing pipeline must be over-overlooked. Deafferenting between a pipeline rupture and a mere interference caused by external conditions is critical to saving the lives of the public.

3.3 Document analysis

The one-and-a-half-page document obtained from the utility company mainly entailed non-confidential excerpts from the company's internal policy on information security. The document acknowledged the need to provide policy-level direction for securing industrial control systems (ICS), including SCADA, Distributed Control Systems (DCS), external control networks, controller systems, among others. The document also clearly emphasises that traditional IT systems are different from ICS due to the direct environmental interaction of ICS. The controls exist within the physical space, and the potential impact of ICS may be comparable to any threat within the physical space. The scopes of impact may range from health, safety, environment, and production, among others. The policy document acknowledged that such facilities require extra security features due to the ‘cyber-physical impacts of ICS. Three sub-policy areas are highlighted, with individual objectives analysed as part of this study.

The primary objective of the cybersecurity risk management policy is to manage risk appropriately in three main areas:

- Timely implementation of risk mitigation activities
- Monitoring and reporting of risk-related activities
- Closure of identified control gaps.

To implement these objectives, risk areas are identified and managed appropriately throughout the project life cycle. All gadgets must go through Factor Acceptance Testing (FAT) and Site Acceptance Testing (SAT) before they are commissioned and handed over to these facilities and gadgets for use. Risks are also revisited frequently by an assigned committee, as well as partial assessments during maintenance sessions. The risk policy mainly focuses on the aspects of risk surrounding ICS vulnerability, ICS incidents, and other national threats.

In addition to the risk management policy, the security physical and environmental policy is also directly in tune with the need to ensure public safety. Policy objectives include:

- Ensure ICS assets are physically protected within the ICS facility in order to prevent unauthorized access and damage.
- To mandate appropriate controls based on the asset’s underlying business value and associated risk factors.

The implementation of the security physical and environmental policy takes a variety of forms, including the protection of physical areas that can be physically accessible by adversaries or insurgents. Ultimately, assets are secured based on their classifications; assets that are considered critical, vulnerable, and with the most threat are closely addressed in the physical and environmental policy.

One final policy in this regard is the access control policy. The aim of this policy is to ensure that only authorized users, processes, or devices are permitted access to ICS systems and/or ICS assets. Access points are not only through physical channels but cyber channels. System users and access are categorised into classifications to enable easy implementation of control measures in case of an access breach. Access is, therefore, defined based on the role of the personnel. All user rights are restricted to limit user activity and reduce damage, even in the event of

wrongful access. Role-based accounts offer a technically feasible solution to support the principle of least privilege.

3.4 Action planning (definitions)

At this stage of the research, the evaluation matrix was prepared using relevant cues gathered from the earlier diagnosis. The action planning was undertaken ahead of the observation exercise, drawing on the peculiarities of the research model and findings revealed through the diagnoses.

3.4.1 Security information policies

The scope of attack within the AI-powered SCADA system is defined as P - an AI-based security scope enhancing or degrading public safety. Two main scopes are considered in a mix that affects public safety; these include:

P_1: All attack resilience scenarios that define a scope relevant to public safety.

P_2: All defense scenarios that define a scope relevant to public safety.

The attack and defense scenarios represent the total scope or classes of actions that the AI-based system can execute on its own with little to no human interference. Whilst attack resilience implies the natural abilities of the system to regulate system-internally generated threats and ward off external attacks; defense mechanisms also cover internal and external scopes to protect against sustained failures.

3.4.2 Security information mechanisms or programs

Mechanisms or security mechanisms are special programs that align with the scope of AI-based SCADA operations to reveal more specific details about the attack and defense scopes of the observation. Denoted by M– this is the security mechanism used to define any aspect of the security scope. In principle, there may be more than one mechanism to effectively define an attack or defense scope. Therefore, a P_1 can be addressed by a list of Mechanisms (M_1, $M_2 \ldots M_\beta$), where β is the maximum number of security mechanisms supported within a scope. For the present observation, the following mechanisms were diagnosed:

M_1: Mechanisms Internal to the SCADA system within any defined scope

M_2: Mechanisms External to the SCADA system within any defined scope.

M_3: Human governance role within a defined scope; a critical mediator of attack and public safety.

These three mechanisms are fundamental to the observation matrix; whereas the first two mechanisms apply to both external and internal scopes, human governance is considered only from the attack perspective, as supported by the earlier diagnosis. This is based on the assertion that policy and governance are mainly to ensure the attack resilience of SCADA systems.

3.4.3 Security and general staff identification in SCADA security policy implementation

The next stage of the definitions is to specify the personnel, staff or users in charge of the security system, mainly regarding policy implementation. It is, however, considered that the AI system might as well act on its own, with little to no human interference. The staff or system is therefore denoted as 'S' - system or staff responsible for addressing a security mechanism 'M' within a defined scope 'P'. The responsible party can be categorized into at least two types:

a. **Security Team Members (Staff)** – this is labelled as S^{sec} - represents staff specialized in IT of the SCADA Control room management and client portal security. Three main levels of security personnel are maintained in this observation as informed by the diagnosis. The first two staff positions focus on the control room actors whilst the last position is on staff at the client side of the SCADA system:

S^{sec1}: Control room supervisor – full access control

S^{sec2}: Control room assistant – partial control

S^{sec3}: Client company infrastructure supervisor

b. **System –** System operating mode, labelled as S^{sys}, including internal and external system behaviour. Internal systems are grouped into AI and automated systems; whereas AI operates data and information, system automation helps the AI implement the most feasible human action in any instance. Nonetheless, external systems were unexplored as part of this observation and represented by a single actor, even though such systems may no doubt implement AI and automation alike:

S^{sys1}: Internal AI system integration

S^{sys2}: Internal Robot Process Automation (RPA) systems

S^{sys3}: External system

It must also be added that the staff and systems are not independent. In several cases, staff and systems need to work together in the same information security network to ensure safety.

3.4.4 Policy mechanism mapping to staff in security policy implementation

This section maps each policy mechanism onto the respective staff in charge of its implementation. For any policy implementation, multiple security systems and teams may be responsible for different aspects of the same mechanism; therefore, $S^{sec} = S^{sec1}, S^{sec2}, \ldots, S^{secmax}$, an indication of all security team members in the Control Room and the Client organization responsible for the security mechanisms. Likewise, more than one system may be in charge of operationalizing any security

mechanism: therefore, $S^{sys} = S^{sys1}, S^{sys2}, S^{sysmax}$, an indication of all security systems responsible for all security mechanisms.

On this note, it is important to add that all security team members (S^{sec}) and systems (S^{sys}) have an unlimited number of specific functional areas. Let each functional security area be represented by a, b, c, d…. z where z represents the last most important functional area necessary for the security mechanisms and performed by the system or the security team. Considering the three most critical functional areas based on the diagnosis, the following top priority areas are considered:

a = Security related to the management of the risk of attack

b = Physical and environmental security management

c = Access control management

To ensure public safety, it is imperative that all three functional areas of security information policies are addressed. The next section of the analysis combines the various components to arrive at the observation matrix.

3.4.5 Analytical model for information security policy implementation towards public safety

The definitions presented in the earlier sections are combined in this section to identify each row within the matrix, as applicable to any given functional area. Considering the two scopes necessary to define any public safety outcome, the three security mechanisms are handled either by the system or the security team. The state of public safety for any SCADA system is, therefore, a combination of specific functions addressing all security mechanisms required by every scope necessary for the achievement of public safety:

$$\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta_j}\langle P_i, M_j\rangle \rightarrow S^{\text{sec }|sys}_{(a,b,c\ldots z)\langle P_i,M_j\rangle} \quad (1)$$

Building on this model, the total amount of Scope-Mechanisms can be mapped onto appropriate staff or system roles. Three main attack sequences may be established; the first two sequences of internal and external security mechanisms are handled only by the system. Humans can mediate attacks but do not stand a chance as defense agents. All attack scope-mechanism combination is therefore presented as follows:

Internal Attack Resilience - $\langle P_1, M_1\rangle \rightarrow S^{sys}_{(a,b,c\ldots z)\langle P_1,M_1\rangle}$ (2)

External Attack Resilience - $\langle P_1, M_2\rangle \rightarrow S^{sys}_{(a,b,c\ldots z)\langle P_1,M_2\rangle}$ (3)

System Governance - $\langle P_1, M_3\rangle \rightarrow S^{sec}_{(a,b,c\ldots z)\langle P_1,M_3\rangle}$ (4)

All defense Scope-Mechanisms scenarios are as well presented below.

Internal System Defense - $\langle P_2, M_1\rangle \rightarrow S^{sys}_{(a,b,c\ldots z)\langle P_2,M_1\rangle}$ (5)

External System Defense - $\langle P_2, M_2\rangle \rightarrow S^{sys}_{(a,b,c\ldots z)\langle P_2,M_2\rangle}$ (6)

It must be added that human intervention only takes the form of attack mediation and does not play an active role in defense since human defense against AI can only be at least not until an attack has been recorded or suspicion registered. In addition, security personnel are only assigned to M3 to provide system control and monitoring. Given these five-underlying scope-mechanisms-staff/system combinations, the field observation was ready to be conducted to assess how the highlighted functional areas affect public safety.

3.5 Action taking (qualitative study observational analysis)

The observation was conducted on both the oil and gas and utility qualitative studies, and the results are presented in the form of the observation matrix. The action research methods and other definitions of terms used in the observation matrix are originally presented in [23]. The observation was conducted for two main qualitative studies, the findings of which are presented in this section. The observation of the oil and gas was conducted and presented first, followed by the observation of the utility organisation.

3.5.1 Oil and gas qualitative study observation

For each functional area, a positive security state is offered "Y" = (Yes), and a negative attack state "N" = (No). For $<P_1M_1>$, the observation results are presented in Table 2 below.

Table 2: Observation results – internal attack resilience for Case 1

$<P_1M_1>$	Attack-Internal Resilience		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys1}	Y	Y	Y
S^{sys2}	Y	Y	Y
S^{sysall}	Y	Y	Y

For $<P_1M_2>$, all external attack resilience of SCADA systems is measured within the scope of the three functional security areas, taking into consideration internal AI, automation, and external systems. The results consider the performance of key system areas without any human intervention, as observed for $<P_1M_1>$. A summary of this observation is presented in Table 3.

Table 3: Observation results – external attack resilience for Case 1

<P_1M_2>	Attack-External Resilience		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys1}	Y	Y	Y
S^{sys2}	Y	Y	Y
S^{sys3}	Y	Y	Y
S^{sysall}	Y	Y	Y

For <P_1M_3>, the role of humans is brought into perspective across the three functional areas to model system governance. The same functional areas of risk management, physical and environmental management, as well as access control are maintained (Table 4). All three definitions of humans/staff are employed in this model.

Table 4: Observation results – AI system governance by humans for Case 1

<P_1M_3>	System Governance by Humans		
Staff ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sec1}	Y	Y	Y
S^{sec2}	Y	N	N
S^{sec3}	Y	Y	Y
S^{secall}	Y	N	N

Given these findings, the overall attack scenario is presented by collating the three scenarios covering the three functional areas of public safety.

Table 5: Attach resilience and governance observation results for Case 1

	<P_1M_1>	<P_1M_2>	<P_1M_3>
a	Y	Y	Y
b	Y	Y	N
c	Y	Y	N

For the defense scope, two other combinations are required. The first of these is defense scope and internal mechanism combination <P_2M_1>. We can generate the defense-internal matrix using the top three functional areas, as presented in Table 6.

Table 6: Observation results - internal defense for Case 1

<P_2M_1>	Defense-Internal Systems		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys1}	Y	Y	Y
S^{sys2}	Y	Y	Y
S^{sysall}	Y	Y	Y

The external defense matrix is employed without any internal systems at work. As opposed to the attack resilience, only the external system component is useful in this case. The observation output is presented in Table 7.

Table 7: Observation results – external defense for Case 1

<P_2M_2>	Defense – External		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys3}	Y	Y	N

By combining the last two tables, the defense matrix is presented in Table 8.

Table 8: System defense results for Case 1

	<P_2M_1>,	<P_2M_2>,
A	Y	Y
B	Y	Y
C	Y	N

Given the attack, governance, and defense observations, the final matrix on public safety is given, as indicated below.

	Int	Ext	Gov	P_1	Int	Ext	P_2	P_{all}
a	Y	Y	Y	60%	Y	Y	40%	100%
b	Y	Y	N	40%	Y	Y	40%	80%
c	Y	Y	N	40%	Y	N	20%	60%

Pertaining to the security related to the management of the risk of attack (a), 100% public safety may be achieved within the qualitative study organisation. Pertaining to physical and environmental security management (b), public safety stands at 80%. The area of access control management (c) has the weakest form of safety, with lapses in the human elements and external defense networks; were public safety stands at 60%.

3.5.2 Utility qualitative study observation

For the utility qualitative study, a similar observation was conducted. For <P_1M_1>, the observation results are presented in Table 4.8. For <P_1M_2>, external attack resilience of SCADA systems in the utility company is as well presented (Table 9). For <P_1M_3>, the role of humans is modelled as well as presented in Table 4.10. An overall attack resilience and governance are presented in Table 11.

Table 9: Observation results – internal attack resilience for Case 2

<P_1M_1>	Attack-Internal Resilience		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys1}	Y	Y	Y

S^{sys2}	Y	Y	Y
S^{sysall}	Y	Y	Y

Table 10: Observation results – external attack resilience for Case 2

<P_1M_2>	Attack-External Resilience		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys1}	Y	Y	Y
S^{sys2}	Y	Y	Y
S^{sys3}	Y	Y	Y
S^{sysall}	Y	Y	Y

Table 11: Observation results – AI system governance by humans for Case 2

<P_1M_3>	System Governance by Humans		
Staff ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sec1}	Y	Y	Y
S^{sec2}	Y	Y	N
S^{sec3}	Y	Y	Y
S^{secall}	Y	Y	N

Table 12: Attack resilience and governance observation results for Case 2

	<P_1M_1>	<P_1M_2>	<P_1M_3>
a	Y	Y	Y
b	Y	Y	Y
c	Y	Y	N

For the defense matrix, internal<P_2M_1>, and external defense<P_2M_2>rows are presented in Table 13 and Table 14, respectively. A combined defense matrix is also presented in Table 15.

Table 13: Observation results - internal defense for Case 2

<P_2M_1>	Defense-Internal Systems		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys1}	Y	Y	Y
S^{sys2}	Y	Y	Y
S^{sysall}	Y	Y	Y

Table 14: Observation results – external defense for Case 2

<P_2M_2>	Defense – External		
System ID	Managing Risk (a)	Physical and Environment Management (b)	Access Control (c)
S^{sys3}	Y	Y	N

Table 15: System defense results for Case 2

	<P_2M_1>,	<P_2M_2>,
A	Y	Y
B	Y	Y
C	Y	N

Given the attack, governance, and defense matrix for the utility case study observations is indicated below.

$$
\begin{array}{c}
 \\
a \\
b \\
c
\end{array}
\begin{bmatrix}
\text{Int} & \text{Ext} & \text{Gov} \\
Y & Y & Y \\
Y & Y & Y \\
Y & Y & N
\end{bmatrix}
\begin{array}{c}
P_1 \\
60\% \\
60\% \\
40\%
\end{array}
\begin{bmatrix}
\text{Int} & \text{Ext} \\
Y & Y \\
Y & Y \\
Y & N
\end{bmatrix}
\begin{array}{cc}
P_2 & P_{all} \\
40\% & 100\% \\
40\% & 100\% \\
20\% & 60\%
\end{array}
$$

For the utility company, the security related to the management of the risk of attack (a) was scored 100% with regards to public safety. On physical and environmental security management (b), the company scored 100% on public safety from the observation. The last area of access control management (c) has the weakest form of public safety with 60% public safety.

3.6 Results evaluation and specific learning

Following the observation, the overall public safety performance of both the oil and gas and utility company was generally high. Security related to the management of the risk of attack was at an optimum level in both case observations. Physical and environmental security management was optimum for the utility qualitative study but 20% short for the oil and gas company. The last area of access control management had just above average score for both qualitative study observations.

The observation reveals that the strongest aspects of the system are those complete managed by the system; these include internal attack resilience, external attack residence, and internal system defense capabilities. These three areas were flawless within the SCADA system. Nonetheless, in the areas where human involvement was registered, the attack was at its weakest point. This outcome was observed in both the utility and oil and gas qualitative study companies. A key learning is that humans are the weakest point on the attack resilience of SCADA systems, and the main weak point is access control management. Access control is one of the key pathways into SCADA systems.

To gain access into SCADA networks, perpetrators often need physical or network access to the controls. These strategies often target the humans who operate user accounts within the network. By sending malicious emails and convincing the users to click on special links where their credentials are collected or using other physical theft

means, perpetrators are able to easily gain access through these channels. The governance of AI-based SCADA systems, therefore, remains a critical area that deserves the needed attention. The defense matrix is weakest at the point of external system defense. Defense systems external to the SCADA network lag in terms of their access control mechanisms. It is often easy to penetrate the access-control blocks put in place by the network providers, even though these external systems are resilient to risks and have good physical and environmental security management.

4. Conclusion

The purpose of this study was to understand the role of AI in SCADA systems in terms of its impact on public safety in the UAE. The study found that the threat-resilience of AI-SCADA systems is crucial for improving public safety. The findings showed that both internal and external threat-resilience play a vital role in ensuring public safety. Additionally, three main areas of security implementation were identified as being fundamental to achieving public safety: risk management, physical and environmental management, and user control. These areas are crucial in ensuring the attack resilience and defense preparedness of AI-SCADA systems and play a key role in maintaining public safety.

References

[1] Government.ae, 'UAE strategy for artificial intelligence.', 2017.

[2] E. Wilson, 'Artificial Intelligence and Human Security: AI Strategy Analysis', 2019.

[3] 2018 Ryan, P., 'The UAE will save billions thanks to artificial intelligence, says AI minister'.

[4] E. Azar and M. A. N. Haddad, 'Artificial Intelligence in the Gulf: Prospects and Challenges', 2019.

[5] 2016 Government of Dubai, 'AI and Robotics Award for good', 2016.

[6] J. Ahokas, 'Secure and Reliable Communications Solution for SCADA and PPDR Use', 2013.

[7] A. RULE and Y. G. WORKFLOW, 'TOGETHER AT LAST'.

[8] T. Macaulay and B. L. Singer, *Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press, 2011.

[9] U. P. D. Ani, H. He, and A. Tiwari, 'Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective', *J. Cyber Secur. Technol.*, vol. 1, no. 1, pp. 32–74, 2017.

[10] X. You, C. Zhang, X. Tan, S. Jin, and H. Wu, 'AI for 5G: Research directions and paradigms', *arXiv*, pp. 1–12, 2018, doi: 10.1360/n112018-00174.

[11] P. Dickens, *Capital and the Cosmos: War, Society and the Quest for Profit*. Springer Nature, 2023.

[12] A. Aloisi and V. De Stefano, 'Between risk mitigation and labour rights enforcement: assessing the transatlantic race to govern AI-driven decision-making through a comparative lens', *Eur. Labour Law J.*, 2023.

[13] C. Ganguli, S. K. Shandilya, M. Nehrey, and M. Havryliuk, 'Adaptive Artificial Bee Colony Algorithm for Nature-Inspired Cyber Defense', *Systems*, vol. 11, no. 1, p. 27, 2023.

[14] T. Mazhar *et al.*, 'Analysis of Challenges and Solutions of IoT in Smart Grids Using AI and Machine Learning Techniques: A Review', *Electronics*, vol. 12, no. 1, p. 242, 2023.

[15] P. Hazell, P. Novitzky, and S. van den Oord, 'Socio-technical system analysis of responsible data sharing in water systems as critical infrastructure', *Front. Big Data*, vol. 5, 2023.

[16] R. C. Swallow, 'Considering the cost of cyber warfare: advancing cyber warfare analytics to better assess tradeoffs in system destruction warfare', *J. Def. Model. Simul.*, vol. 20, no. 1, pp. 3–37, 2023.

[17] M. Halaweh, 'Artificial intelligence government (Gov. 3.0): The UAE leading model', *J. Artif. Intell. Res.*, vol. 62, pp. 269–272, 2018.

[18] F. Liu, Y. Liu, and Y. Shi, 'Three IQs of AI systems and their testing methods', *J. Eng.*, vol. 2020, no. 13, pp. 566–571, 2020.

[19] P. Shah *et al.*, 'Artificial intelligence and machine learning in clinical development: a translational perspective', *NPJ Digit. Med.*, vol. 2, no. 1, p. 69, 2019.

[20] A. Dafoe, 'AI governance: a research agenda', *Gov. AI Program, Futur. Humanit. Institute, Univ. Oxford Oxford, UK*, vol. 1442, p. 1443, 2018.

[21] K. Grace-Martin, 'Can Likert scale data ever be continuous', *Artic. Alley*, 2008.

[22] M. Jouini, L. B. A. Rabai, and A. Ben Aissa, 'Classification of security threats in information systems', *Procedia Comput. Sci.*, vol. 32, pp. 489–496, 2014.

[23] M. AlHashmi, G. Chhipi-Shrestha, K. M. Nahiduzzaman, K. Hewage, and R. Sadiq, 'Framework for Developing a Low-Carbon Energy Demand in Residential Buildings Using Community-Government Partnership: An Application in Saudi Arabia', *Energies*, vol. 14, no. 16, p. 4954, 2021.