Journal of Engineering and Technology

ISSN 2180-3811 eISSN 2289-814X https://journal.utem.edu.my/index.php/jet/index

ENHANCING PHYSICAL SECURITY PERFORMANCE IN THE OIL AND GAS INDUSTRIES THROUGH THE INTEGRATION OF FACIAL RECOGNITION TECHNOLOGY

S. Al Zaabi*[1] and R. Zamri[2]

[1] Institute of Technology Management and Entrepreneurship, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

[2] Faculty of Manufacturing Engineering, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia.

corresponding_ sss2111567@gmail.com

Article history:
Received Date: 23 June 2021
Revised Date: 26 November 2021
Accepted Date: 29 June 2022

Keywords:
Facial Recognition Technology, Oil And Gas Industry, Physical

Abstract— The physical security of critical facilities in the oil and gas industry has become a pressing concern due to scientific and technological progress and new mechanisms to bypass the physical security controls. The current study is dedicated to a critical examination of the performance of the physical security system in the Oil and Gas Industries and the potential of integrating facial recognition technology to improve its resilience towards physical security threats. The research was conducted within the integrative conceptual framework of the physical security culture that distinguishes between the technological, human, and organizational

Security Culture, Physical Security Performance, Physical Security Threats

physical security domains. The author surveyed 186 employees working in an oil and gas company in the UAE. The organization has an effective physical security system that does not display critical vulnerabilities. Based on the study's findings, the performance of this organization's physical security system is high across all three domains of physical security culture. Furthermore, most employees believe that the organization could benefit from integrating facial recognition technology as an additional defence layer against physical security threats to alleviate the negative impact of external factors on the company's physical security performance. Therefore, the study results could be valuable from the theoretical and practical perspectives by providing valuable insights into the projected performance of facial recognition technology.

I. Introduction

The rapid expansion of scientific and technological progress and increased tension in the international arena contribute to the growing topicality of physical security vulnerabilities in many organizations. As a result, firms in different corners of the globe are looking for new instruments to protect their assets from external and internal threats. However, despite these attempts, such factors as terrorism, vandalism, burglary, sabotage, and theft remain disturbing risks for many organizations. Therefore, topics related to physical security performance

are prevalent in contemporary research.

It is often suggested that physical security performance can be measured using technological, human, and organizational factors [1]. Accordingly, companies seeking to enhance the performance of their physical security systems seek improvements in specific physical security domains. In particular, the idea of reinforcing the technological domain with the help of facial recognition technology, which allows significantly increasing organizations' resilience towards physical security threats, is becoming increasingly popular [2]. Furthermore, the notion of integrating facial recognition technology with prevailing physical security controls appears attractive for organizations because it could potentially address those vulnerabilities that are overlooked by other physical security measures, such as a CCTV surveillance system or fingerprint sensor.

Vulnerabilities in physical security systems are alarming for companies operating in the oil and gas industry because their assets are especially likely to become targets of criminals attempting to steal critical assets or disrupt facilities' operations. In this situation, an investigation of physical security in the oil and gas industry is becoming more topical than ever, encouraging scientists to explore factors that could strengthen the existing physical security systems and develop new strategies for implementing effective and efficient solutions. The oil and gas industry of the UAE is a bright example of a sector whose physical security performance is currently a critical concern for many stakeholders. Organizations operating in this industry use many physical security controls, such as CCTV surveillance, security officers, protective barriers, locks, access control, perimeter intrusion detection, and other systems. At the same time, the available evidence provides a compelling reason to believe that many companies in this sector remain vulnerable to physical security threats. In particular, the

surveyed organization is an example of a critical oil and gas facility in the UAE that is partially exposed to physical security threats [3]. Considering the facility's vital importance to the UAE's economy, designing an effective security system that safeguards it from any external and internal threats becomes a matter of high priority. Such a strategy should be implemented by companies in the UAE oil and gas industry.

The purpose of this article is to conduct a critical investigation of the performance of the physical security system utilized in the Oil and Gas Industries operating in the UAE and explore whether its performance could be enhanced with the help of facial recognition technology. The article seeks to evaluate the physical security performance of one of the organizations in this sector and determine how physical security threats and external factors impact the facility's physical security. Furthermore, it will measure the influence of physical security domains on integrating facial recognition technology. The article also seeks to project the potential impact of facial recognition technology on the facility's physical security performance. The study relies on a quantitative research methodology and the method of survey. A regression analysis was run to measure a relationship between the three domains of physical security culture and the projected performance of physical security systems following the implementation of facial recognition technology.

II. Literature Review

A. Measurement of Physical Security Performance

Whereas it may seem that the measurement of security performance implies using specific quantitative parameters to assess a set of indicators, this task is complex and challenging. The literature does not offer a single model for measuring physical security performance. For example, the official website of [4], a well-known consulting agency, indicates that the organization offers customized services to its clients that offer unique physical security risk

assessment metrics based on a particular firm's specifics. Similarly, New Zealand's government's official website states that a company is supposed to design its system of physical security indicators [5]. It could be inferred from these two sources that there is currently no single physical security model that could be universally employed in any company to assess its physical security performance. Accordingly, each company should create its measurement approach.

Due to such controversy, the idea of using perceived physical security measures is becoming increasingly popular. For example, in a recent study by [6], they used the measure of perceived security as one of the key independent variables. [7] also utilized a similar approach, who argued that mobile wallets' perceived security was a reasonable and valid security measure. Even though these studies did not focus on physical security, their methodologies illustrate that perceived security measures are often used in those situations when the "objective" security measurement is problematic. In line with this recent security measurement trend, the current study will also utilize perceived physical security indicators to measure physical security performance.

B. Physical Security Performance in the Oil and Gas Industry

In the most general view, physical security refers to the system and process of protecting physical resources, restricted areas, and personnel within a company from any physical events and actions that may lead to damage or losses to an agency, institution, or enterprise. According to [8], the prioritization of physical security in the overall information security system is usually low. However, physical security is crucial for various facilities in the oil and gas industry seems evident. According to [9], physical security is an inalienable part of the systems engineering framework in the oil and gas sector and operations, information, network, communications, administrative, computer, personnel, and

emanation security. Furthermore, facilities in this industry face several physical security threats, such as unintentional operator errors that could damage the equipment or disrupt an entire organization's operations [10]. Therefore, the issue of their physical security becomes crucial.

As oil and gas facilities are often of critical importance for national economies, they use advanced physical security systems. Access to many facilities is restricted and controlled with various physical security controls that allow only authorized personnel to access them [11]. Simultaneously, the available evidence indicates that simple locks and security officers' presence might not be sufficient for maintaining a desirable level of physical security in the oil and gas industry. In order to safeguard critical assets from physical security threats, organizations operating in the industry use a plethora of controls, such as locks and keys, doors, gates and barriers, security officers, fingerprint technology, electronic access card control systems, perimeter intrusion detection, and CCTV surveillance systems.

Furthermore, they also have strict security procedures and company policies to minimize exposure to physical security threats. These physical security controls are supposed to ensure that oil and gas facilities adequately detect and deter physical security threats that the organization faces, ensuring a sufficient protection level across the technological, organizational, and human domains of a physical security culture. In addition, facilities' physical security systems should display high performance across all three physical security domains to safeguard assets from external and internal physical security threats. Therefore, understanding the specific domains of a physical security culture is critical for ensuring a sufficient level of oil and gas facilities' protection from physical security threats.

C. Physical Security Culture

The literature offers valuable insights into the phenomena of physical security culture. This concept may be described as a system of factors spanning the

technological, organizational, and human domains that protect an organization against external and internal threats [1]. Understanding a security culture as a set of values, principles, policies, and assets in predetermining a firm's resistance against physical security threats have been among the most common ways to conceptualize an organization's physical security for decades. Therefore, adopting a conceptual framework on physical security culture to discuss and analyze one of the organization's physical security performances in the UAE's oil and gas industry appears to be a rational option aligned with current security studies' trends. Furthermore, a physical security culture concept implies differentiating between three domains organizational, technological, and human.

The organizational domain

The organizational domain of physical security culture comprises tangible components of security in an organization. Tangible security components in an organization are the qualities that can be observed when moving around in an organization [1]. Company policies are vital components of the organizational environment that relate to basic rules that all the employees must follow to protect the organization's assets from internal and external physical security threats [12]. Security procedures are closely related to the company policies. Their influence on physical security performance is even more pronounced than company policies.

The technological domain

The technological domain of physical security culture consists of the organization's security technology, material, and equipment [1]. Most frequently, companies seek to improve the technological domain of physical security culture. Unfortunately, organizations spend resources on upgrading information security, leaving the physical security element of the company prone to weaknesses. Physical security threats have intensified in many companies since security emphasis tends to be elsewhere.

The human domain

The human domain of an organization consists of less tangible or non-observable security components. Physical security effectiveness as evaluated by employees is an example of a non-observable security component in an organization [1]. This area may also include the degree of security experts hired by an organization. In addition to the cutting-edge security technology utilized by many organizations in critical infrastructures, the security officers are highly trained experts.

Combining all the three domains of physical security culture and all the controls used in these domains is crucial for maintaining an adequate physical security performance.

D. Physical Security Control

Most secure locations in modern organizations use rigorous physical security control measures. The first line of defense in every industry or organization focuses on defending its perimeter [13]. Different techniques have been utilized to prevent unauthorized personnel's entry into the restricted zones and identify such instances on time. Most measures incorporated into a conventional perimeter intrusion detection system entail providing access points with sensing devices, such as door switches, glass break detectors, window screens, lace and panels, and interior sensors. Unfortunately, such systems have evident security vulnerabilities. Determined assailants may bypass defensive measures by breaking through a wall, entering via a ventilation system, or remaining within a building beyond closure. Therefore, a perimeter intrusion detection system shows minimal efficacy in identifying and preventing physical security threats.

If criminals penetrate through the first line of defense, their further advance is supposed to be deterred by various other mechanisms. Traditional physical security controls, such as locks and keys, doors, gates, and barriers, are physical security controls widely used to protect the assets and employees throughout the industry to deter and detect physical security

threats such as penetrators from entering critical facilities. Unfortunately, determined criminals can easily exploit these physical security controls' limitations and vulnerabilities [14]. For example, a penetrator could use a stolen key to access a facility or open a door through lock picking.

Electronic access control systems have been implemented in many organizations to address vulnerabilities of traditional controls and regulate employees' access into facilities through doors, gates, barriers, turnstiles, and other physical security controls. Various access cards, such as magnetic strips and HID cards, are used to deny and authorize personnel to secured zones [15]. Despite the seeming advantages of this measure, an access card could be stolen or lost and then used by unauthorized individuals to access restricted areas, resulting in the increased risk of potential losses caused by theft and other physical security threats. As a result, an electronic access control system might sometimes fail to deter physical security threats.

Fingerprint technology seems to be a more effective instrument than traditional locks and an electronic access control system since this biometric system regulates access based on individuals' fingerprints. Due to this benefit, fingerprint technology offers a higher level of protection [16]. Unfortunately, criminals have recently become more sophisticated, undermining fingerprint technology's effectiveness. For example, they use compromised templates to clone fingerprints and access restricted facilities, or determined criminals could cut off a thumb of a bank manager to access vaults utilizing this technology [16]. As a result, fingerprint technology alone cannot protect an organization from physical security threats.

A CCTV surveillance system is another example of a popular physical security control mechanism that is often integrated into the physical security systems of modern organizations. Many companies operate security control rooms, and security officers observe activities through CCTV

surveillance systems to monitor potential events that may negatively impact entities [17]. However, vulnerabilities of such systems include the risk of human errors and possible disruptions of CCTV cameras. In particular, cameras could be easily manipulated or vandalized by criminals in different ways, including using sprays of gum on the lenses [18]. Such a threat could be, to a large extent, prevented with the help of attentive, committed security officers, who represent the key elements of the human domain of a physical security culture. However, even skilled officers might fail to detect criminals in certain situations, such as during rush hours. Therefore, effective organizational policies and security procedures should be implemented to prevent such scenarios.

E. Facial Recognition Technology

The previous section of the literature review showed that all the existing physical security controls have critical vulnerabilities that determined criminals could exploit. In this situation, the idea of implementing new mechanisms to eliminate these vulnerabilities and introduce an additional layer of defense for an organization seems promising. Facial recognition technology is a novel type of technology that identifies a person based on a video frame or a digital image. In most cases, facial recognition applications compare digital images of people with pictures in the database to identify specific individuals [2]. As the market continues to grow, the UAE airports were equipped with facial recognition technology in 2008, increasing the security level and prevent questionable individuals from entering the country [19]. In addition, unlike other physical security controls, the system allows identifying and screening individuals from different angles without involving immigration officials at the airport [19]. This technology's advantages are so promising that the industries spend a significant amount of resources developing and integrating facial recognition applications.

Facial recognition applications could reduce the impact of internal and external physical security threats. In particular, the technology could provide

organizations with an opportunity to automatically grant or deny access by verifying the authorization through the comparison of the individuals' identity with the records of enrolled employees in the database, as opposed to manually verifying their identities with the help of ID cards [14].

One of the most evident benefits of facial recognition technology applications is preventing unauthorized access to restricted facilities. The scenarios of stolen access cards and cloned fingerprints do not apply to organizations that regulate access with the help of facial recognition technology, which provides superior physical security performance [20].

Another promising area of the technology's implementation is processing high personnel volumes during rush hours. The risks of providing unauthorized individuals with a right to access restricted facilities magnify during rush hours because security officers might not have enough time to examine the situation. Integrating facial recognition technology into the existing physical security controls to interrupt people's flow from one area to another could reduce the chances of admitting unauthorized individuals.

The third benefit of the technology is connected with its utilization during emergencies. A surveillance system integrated with facial recognition technology could quickly locate missing persons at the emergency assembly point [21]. Real-time tracking of these missing persons' exact locations could be pinpointed, which would allow the Incident Management Team to dispatch response teams within a short time to save their lives [8]. All the arguments above illustrate that implementing facial recognition technology could positively affect an organization's physical security performance.

F. Challenges of Facial Recognition Technology

Despite facial recognition technology being a novel type of technology that identifies a person based on a video frame or a digital image, still, there are specific challenges to implementing the technology. For example, [22] argued that

variations such as pose, facial expressions, and illumination significantly affect the facial recognition algorithm, and its overall performance is degraded. Simultaneously, the recent global pandemic of COVID-19 requiring individuals to use face masks and other face coverings to stay protected. Individuals can be authenticated using facial recognition technology even when wearing face masks.

If proven to be effective in addressing the challenge of partially masked faces, facial recognition technology will likely continue to expand rapidly to include various institutions and industries. Furthermore, recent data show that facial recognition applications' success rate in identifying persons' identities is around 95% for people wearing masks and 99.5% for people without them [23]. Accordingly, it seems justified to argue that even if developers do not improve the technology to identify people despite partially obscured faces, facial recognition instruments could still recognize the overwhelming majority of organizations' employees.

There is evidence that facial recognition technology can recognize partially obscured facial features. A recent innovation developed by [24] can match an individual's images even if the recognition technology can only see the person's back or side [24]. Even if part of the facial features is covered, this particular technology will allow spontaneous recognition. The rapid development of facial recognition technology will likely lead to increased accuracy in identifying individuals, even when their faces are fully covered.

In the past few years, the development and adoption of facial recognition, detection, and analysis technologies have seen considerable growth, which has led to the identification of critical biometric elements used within facial recognition technology [25]. In addition, many companies use facial recognition to make products more user-friendly for consumers to secure their devices, such as mobile phones and laptops, with an encryption tool [14]. Thus, it is sufficient to argue that such challenges hardly influence the industry's development, and the global biometrics technology market

will reach $59.31 billion by 2025 [26].

G. Integration of Facial Recognition Technology

The available evidence provides a compelling reason to believe that integrating facial recognition technology with the existing physical security systems in the oil and gas facilities could improve the effectiveness of technological, organizational, and human domains of physical security culture [1], [9]. Unfortunately, the existing literature does not provide important data on the applicability of facial recognition technology for enhancing the elements of subdomains across the domains of physical security culture in the oil and gas industry. Therefore, the study's findings could be considered a valuable contribution in the literature regarding the applicability of facial recognition technology to the existing security domains of oil and gas facilities to enhance the performance of physical security systems.

This study will examine the dependence of this integration process on the effectiveness of the organization's physical security culture's technological, organizational, and human domains. Furthermore, it is planned to examine the impact of these three domains on physical security performance while also investigating the physical security performance in light of external factors and physical security threats. Such a broad yet practical scope is novel for the literature. Therefore, it is expected that the study will be valuable both from the practical and the theoretical perspectives.

The study was conducted in line with an integrative conceptual framework of physical security culture. The model was initially constructed by [1] to describe and conceptualize the technological, organizational, and human domains of a physical security culture of an organization. The framework allows scholars and practitioners to analyze the physical security of a particular organization by scrutinizing its different domains and revealing a plethora of factors affecting physical security performance.

Furthermore, using a physical security culture model allows the author to investigate a physical security culture in detail and link it to physical security performance and the integration of facial recognition technology.

III. Research Methodology

Considering that the article seeks to examine the performance of physical security systems in the oil and gas industry, it seems rational to choose the research philosophy of critical realism for this study. As it is known, critical realism allows scholars to explore reality through the analysis of sensations of research phenomena that humans share while also thoroughly addressing and eliminating the biases that inevitably accompany such feelings. Using this philosophy, the author of this research managed to collect sufficient data from employees of one organization in the UAE to achieve the objectives of this study.

It was decided to choose an explanatory design rather than a descriptive or an exploratory one. This design is usually deployed exclusively to examine a causal relationship between variables, which applies to the current study. The article seeks not only to measure the physical security performance in the companies operating in the oil and gas industry but also to examine a relationship between weaknesses in the technological, human, and organizational domains of the organization's physical security culture and the anticipated performance of a facility's physical security system following the integration of facial recognition technology. In this situation, the choice of an explanatory research design seems natural.

The current study uses thirteen dependent variables, including the perceived effectiveness of security officers, traditional security controls, fingerprint technology, CCTV surveillance system, intrusion detection system, electronic access control system, security procedures, company policies, and the employees' attitudes towards the organization in detecting and deterring physical security threats. At the same time, the

facility's anticipated physical security performance following the integration of facial recognition technology are the only two dependent variables in the study.

A combination of inductive and deductive research approaches was used in this study within the cross-sectional time horizon. Simultaneously, the choice of a quantitative rather than a qualitative methodology is based on the author's intention to examine a causal relationship between variables, which is impossible in qualitative studies. Furthermore, quantitative research methods allow evaluating specific quantitative parameters of interest. Using the quantitative approach, the author collected credible data on the organization's physical security systems' critical vulnerabilities associated with the effectiveness of existing elements of the subdomains and vulnerabilities across the technological, human, and organizational domains.

An online survey method was used to collect data on the problem under investigation from employees currently working in this organization. A complete list of requirements for potential respondents includes the aging, experience, and awareness criteria. In particular, potential participants of the study had to be at least 18 years old and have overall work experience in the company of at least six months. Furthermore, they also had to claim to be aware of the specifics of facial recognition technology and the various physical security controls utilized by the organization. If the study engaged respondents with limited experience or those who were not aware of the nature of facial recognition technology, such individuals would not have shared informed opinions on the problem under investigation.

The author of the research has found and recruited respondents with the help of the probability sampling method. In addition, the researcher has contacted senior management at the organization, provided brief information about the research, and asked their permission to engage the company's employees in the survey. The survey was conducted using the

SurveyMonkey platform. All the respondents received links to an online questionnaire. Accordingly, their responses were automatically processed by the system. It was decided to choose an online survey method because of its simplicity and effectiveness in collecting essential data without allocating significant resources. The questionnaire comprised three major sections: first, a demographic section, second, a part dedicated to the physical security performance in the organization, and the third section is focusing on integrating facial recognition technology with other physical security controls.

The data were analyzed based on the variables' descriptive statistics. Furthermore, a regression analysis was conducted to measure a relationship between the perceived effectiveness of various physical security controls and the anticipated performance of the facility's physical security system following the integration of facial recognition technology. The Shapiro-Wilk test was run first to check the data for the assumption of normal distribution. After that, a multivariate regression analysis was run in SPSS to test research hypotheses.

IV. Results

A. Demographics

An analysis of respondents' answers to demographic questions reveals that the sample is diverse. For example, around 20% of the study's participants are younger than 26 years old; simultaneously, approximately 24% are older than 40. Such aging characteristics seem natural.

Table 1: Respondents' Age

Age group	N	%
18-25 years	38	20.43%
26-30 years	42	22.58%
31-35 years	31	16.67%
36-40 years	29	15.59%
41-45 years	17	9.14%
46-50 years	25	13.44%
51-60 years	3	1.61%
More than 60 years	1	0.54%
Total	**186**	**100.00%**

The organization has employed a fifth of the sample for more than five years. At the same time, inexperienced

employees who worked at the facility for around 6-12 months account for 18.82% of the sample. Therefore, the selection could be considered diverse in terms of respondents' age and work experience. Such diversity is crucial as it indicates that respondents are supposed to have informed opinions on physical security in the company.

The sample is diverse regarding respondents' age and work experience. However, it is relatively homogeneous regarding employees' gender. The majority of the survey's participants (81.72%) are males. Such a regularity seems natural due to the specifics of the UAE labor market.

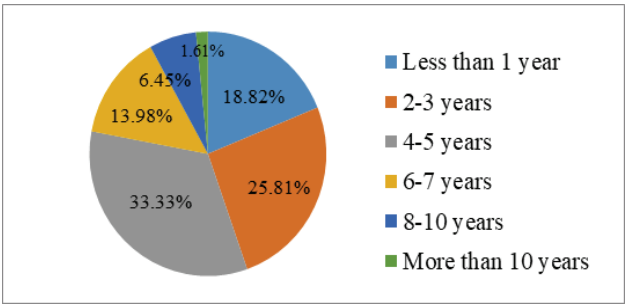

Figure 1: Respondents' Work Experience in the Industry

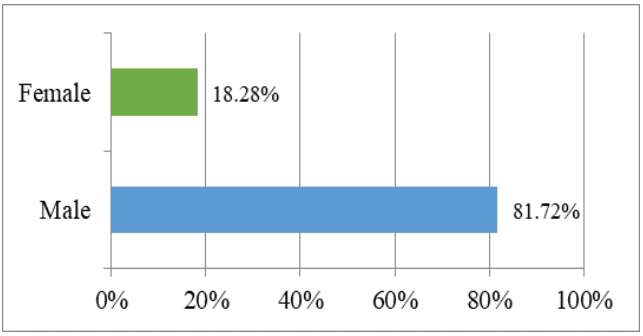

Figure 2: Respondents' Gender

B. Physical Security Systems at the Organization

Respondents consider the current physical security controls that are used in the surveyed organization as effective. The table below illustrates that all the physical security controls except traditional security controls have received relatively high average marks.

The survey results show that respondents are familiar with the security procedures used at the organization. 72.58% and 17.74% of respondents indicate that they are incredibly familiar and very familiar with these procedures, respectively. Such a high level of awareness is essential since respondents are likely to possess detailed knowledge of the existing physical security controls used by the organization and their vulnerabilities.

Table 2: Perceived Performance of Physical Security controls

Physical Security Controls	Mean Value
Security officers	7.35
Traditional security controls	6.24
Fingerprint technology	7.81
CCTV surveillance system	8.24
Intrusion detection system	8.11
Electronic access control system	9.03
Security procedures	8.34
Company policies	8.13

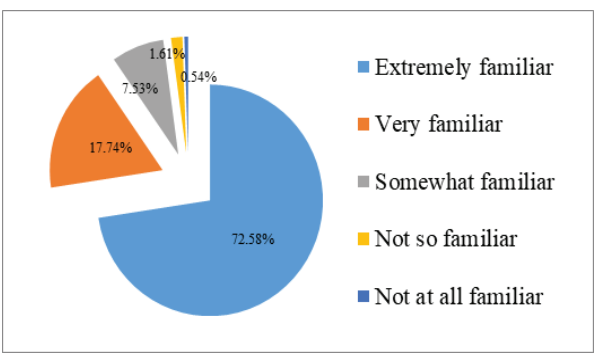

Figure 3: Respondents' Awareness of Security Procedures

The mean value of 8.24 illustrates that the overall performance of the physical security system at the organization is high. Furthermore, it has improved in the last three years. Even though most respondents consider these improvements as slight (59.14%), it is essential to emphasize that 72% of the study's participants agree that these positive changes took place. When discussing the pace of improvements across the three domains of physical security culture, it should be noted that the technological domain demonstrated the most significant improvement, which was recognized by 88% of the sample. On the other hand, 25.27% and 27.42% of the sample reject any progress in the human domain and remain neutral on this matter, respectively. Similar results were also reported regarding the organizational domain. 58% of the sample believe that the organizational domain displays signs of significant or slight improvements, whereas 19.35% believe that the domain had not been enhanced.

Interestingly, there is no agreement among respondents concerning a domain of a physical security culture that is especially vulnerable to physical security threats. 19.35%, 17.20%, and 18.82% of the sample believe that the technological, human, and organizational domains, respectively, are the most vulnerable. At the same time, 44.62% of them do not have a clear opinion on this matter. This finding illustrates that the organization's physical security system vulnerabilities encompass all three domains rather than originate from a single dimension.

Whereas it is not completely clear what exact areas of physical security culture are especially vulnerable to physical security threats, almost 70% of the sample believes that the organization should enhance the physical security system. The existing physical security system is relatively effective, as illustrated by the average 7.82 out of 10. At the same time, the significance of physical security threats and external factors affecting physical security

performance received high average marks by respondents (7.53 and 7.89, respectively). Therefore, the idea of implementing new technologies or policies to enhance physical security performance in the organization operating in the oil and gas industry seems promising.

Table 3: Recent Improvements in Performance of the Three Domains of a Physical Security Culture

	Significant Improvement		Slight Improvement		No Improvement		Neutral	
	N	%	N	%	N	%	N	%
The technological domain	36	19.35%	128	68.82%	5	2.69%	17	9.14%
The organizational domain	23	12.37%	85	45.70%	36	19.35%	42	22.58%
The human domain	14	7.53%	74	39.78%	47	25.27%	51	27.42%

Table 4: Respondents' Evaluations of Physical Security Performance and Its Resilience towards Physical Security Threats and External Factors

Indicators	Average Marks
Performance of the existing physical security system	7.82
Significance of physical security threats for the facility's physical security performance	7.53
Significance of external factors for the facility's physical security performance	7.89

C. The Implementation of Facial Recognition Technology

Results of the study illustrate a high level of respondents' awareness of facial recognition technology. For example, 82.26% of the sample believe that they are aware of this technology's specifics. In comparison, 15.59% of them have chosen a response "maybe yes" to a question about their awareness of facial recognition technology. These numbers show that the study's participants are supposed to possess enough knowledge for

sharing informed opinions on the problem under investigation.

Even though respondents believe to be aware of facial recognition technology's nature and distinctive features, their knowledge of this technology is theoretical. Around a third of the sample cannot identify specific features of facial recognition technology that make it fundamentally different from other physical security controls. Furthermore, 25.27% of them are unsure whether the technology could be effectively integrated with other physical security controls. At the same time, it is essential to point out that the facility's staff is prepared to implement the technology. Such an opinion is supported by 78% of respondents.

Table 5: Respondents' Awareness of the Specifics of Facial Recognition Technology

	N	%
Definitely yes	153	82.26%
Maybe yes	29	15.59%
Not at all	0	0.00%
Not sure	4	2.15%
Total	**186**	**100.00%**

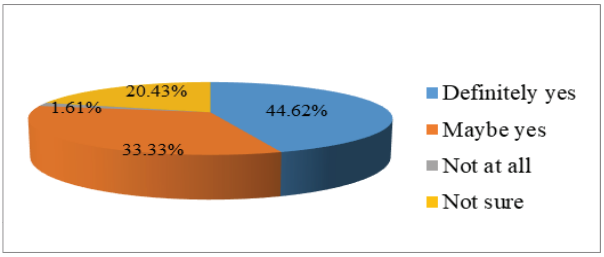

Figure 4: Staff's Preparedness for The Implementation of Facial Recognition Technology

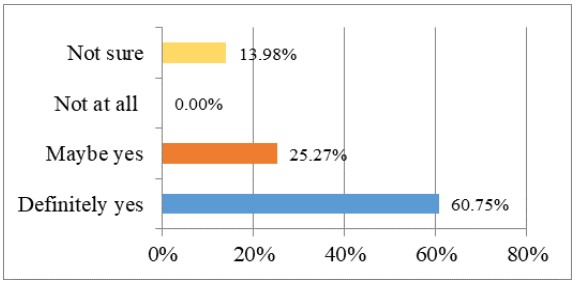

Figure 5: Respondents' Opinion on the Potential of Facial Recognition Technology to Improve the Facility's Physical Security Performance

When asked to reflect on the projected performance of physical security systems following the implementation of facial recognition technology, 60.75% and 25.27% of the study's participants believed that the technology could definitely or possibly enhance the performance of a physical security system, respectively.

Table 6: Respondents' Opinion on Whether the Facial Recognition Technology Could Improve the Facility's Physical Security Performance

	N	**%**
Definitely yes	113	60.75%
Maybe yes	47	25.27%
Not at all	0	0.00%
Not sure	26	13.98%
Total	**186**	**100.00%**

D. Statistical Tests

Results of the Shapiro-Wilk test indicate that the data for all the variables are normally distributed. Furthermore, the Sig. value for the dependent variable is higher than 0.05. Therefore, the instrument of a regression analysis could be utilized to measure a relationship between the independent variables and the dependent variable of the projected performance of physical security performance following the implementation of facial recognition technology.

All nine p-values in the table are below the 0.05 significance level, indicating a strong relationship between the variables. It seems that company policies and employees' attitudes are the least significant predictors of the projected performance of the physical security system following the implementation of facial recognition technology. Their p-value is relatively high (0.41 and 0.40, respectively). Nonetheless, they are lower than 0.05; therefore, their effect on the dependent variable could be essential.

Results of the regression analysis show a statistically significant relationship between all the eight independent variables and the dependent variable.

Table 7: Results of the Regression Analysis

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
	(Constant)	7567.341	1632.346		4.286	.000
1	Security procedures	.578	.075	.865	7.834	.029
2	Company policies	.687	.035	.731	6.523	.041
3	Traditional physical security controls	.623	.071	.822	7.239	.003
4	Fingerprint technology	.586	0.45	.756	7.834	.000
5	Electronic access control system	.672	0.54	.823	7.293	.000
6	Perimeter intrusion detection system	.694	0.24	.841	7.993	.000
7	CCTV surveillance system	.723	0.45	.873	7.025	.000
8	Security officers	.813	0.68	.871	7.423	.000
9	Employees' attitudes	.743	0.46	.885	7.001	.040

V. Discussion

The study's findings illustrate that facial recognition technology could significantly improve the physical security performance of organizations operating in the oil and gas industry. In respondents' opinion, this technology can address weaknesses and vulnerabilities of the existing physical security controls. A view that facial recognition technology has impressive features that are not inherent to other security mechanisms conforms to the literature review's findings [14], [20]. At the same time, it is essential to emphasize that the employees' awareness of facial recognition technology is rather theoretical. They know the most important specifics of this technology but barely understand how this technology could be utilized in practice. It might seem that such a regularity might constitute a disturbing problem for the surveyed organization, but it might be reasonable to disagree with such an impression. The

staff's detailed knowledge of the specifics of facial recognition technology is not necessary for its effective implementation because this knowledge could be later enhanced with the help of relevant training. Simultaneously, most respondents believe that the organization is prepared to integrate the technology with other physical security controls. This readiness to embrace illustrates that the organization is unlikely to face substantial challenges related to integrating facial recognition technology in physical security culture's human and organizational domains.

The study did not find a specific area of physical security culture's domains that could significantly benefit from integrating facial recognition technology. It was shown in the research that the current physical security system that the organization utilizes is effective across all three domains. The existing vulnerabilities are slight and hardly compromise the organization's physical security performance. In this situation, facial recognition technology could become an additional defense layer that would reinforce other physical security controls and help the facility become more resilient to physical security threats. It was demonstrated in the study that both external factors and physical security threats have a substantial impact on physical security performance. Therefore, the idea of using facial recognition technology to create an additional layer of protection seems topical.

VI. Limitations, Conclusion, and Future Work

Contrary to the initial expectations, it was found that all three domains of a physical security culture demonstrate similar performance levels. Thus, recent improvements in the technological domain seem more radical than those in the organizational and human ones. However, the current physical security culture of the organization does not have evident vulnerabilities in any of the three security domains. In this situation, it seems justified

to assume that facial recognition technology could positively impact the entire physical security system by enhancing all three physical security culture's domains. Such an assumption was confirmed in the study with the help of the regression analysis. In general, the research findings indicate that facial recognition technology is necessary for the organization. Furthermore, the staff is already prepared for embracing it, which could significantly simplify and facilitate the integration process.

Two recommendations for further research could be formulated based on this study's findings. First, scholars should consider exploring three physical security culture's domains of the organization in detail to determine their specific weaknesses and vulnerabilities. The study did not discover any evident vulnerabilities across these domains; nonetheless, the sole fact that both the external factors and physical security threats were found to have a significant effect on physical security performance is indicative of the presence of such vulnerabilities. Understanding these vulnerabilities could help create a customized strategy for integrating facial recognition technology with the existing physical security controls. Second, scientists recommend investigating how the technology could be integrated with other physical security controls by examining possible overlapping areas. The discoveries of these areas could help the organization prepare for potential challenges likely to be experienced during the integration process.

The research has two significant limitations. First, the study focused exclusively on data collected from employees. Accordingly, respondents' biases could have made a particular impact on the survey's findings. The author tried to analyze the data thoroughly to identify and eliminate biases; nonetheless, it is still possible that these biases had influenced the study's findings. Second, the research approaches the concept of physical security broadly. Therefore, employees' specific

responses provided general information about physical security performance without clarifying the company's resilience towards particular threats. Further research is required to provide more details about how facial recognition technology could help organizations operating in the oil and gas industry address specific physical security threats and how the technology could be used during emergencies. Despite these limitations, the findings of this study provide a compelling reason to believe it could be valuable in theoretical and practical perspectives.

VII. Acknowledgement

The authors declare that they have no conflict of interest. Due to the sensitivity of this study, the participants did not agree for their data to be shared publicly, so supporting raw data is not available.

VIII. References

[1] K. Van Nunen, M. Sas, G. Reniers, G. Vierendeels, K. Ponnet, and W. Hardyns, "An integrative conceptual framework for physical security culture in organisations," *Journal of Integrated Security Science*, vol. 2, no. 1, 2018.

[2] W. Wójcik, K. Gromaszek, and M. Junisbekov, "Face Recognition: Issues, Methods and Alternative Applications," in Face Recognition, S. Ramakrishnan, Ed. Rijeka: IntechOpen, 2016. doi: 10.5772/62950.

[3] W. Barnes, P. Goydan, and M. Berns, Protecting Oil Infrastructure in an Era of New and Emerging Threats. BCG Global, 2019. [Online]. Available: https://www.bcg.com/publications/2019/protecting-oil-infrastructure-in-era-of-new-and-emerging-threats

[4] RSM, Physical Security Assessment. RSMUS, 2021. [Online]. Available: https://rsmus.com/what-we-do/services/risk-advisory/cybersecurity-data-privacy/cybersecurity-compliance-governance/cyber-risk-assessment-services/physical-security-assessment.html

[5] New Zealand Government, About the PSR. New Zealand Government: PSR, 2021. [Online]. Available: https://www.protectivesecurity.govt.nz/about-the-psr/overview

[6] V. L. Johnson, R. W. Woolridge, W. Wang, and J. R. Bell, "The impact of perceived privacy, accuracy and security on the adoption of mobile self-checkout systems," *Journal of Innovation Economics & Management*, vol. 31, no. 1, pp. 221–247, 2020.

[7] P. Sunny and A. George, "Determinants of Behavioral Intention to Use Mobile Wallets - A Conceptual Model," 2018.

[8] D. Hutter, Physical Security and Why It Is Important. SANS Institute Reading Room, 2016.

[9] S. and Yasseri, "A Systems Engineering Approach to Physical Security of Oil & Gas Installations," *International Journal of Coastal and Offshore Engineering*, vol. 3, no. 3, 2019.

[10] L. Cordner, Offshore oil and gas safety and security in the Asia Pacific: The need for regional approaches to managing risks. S. Rajaratnam School of International Studies, 2013. [Online]. Available: https://www.rsis.edu.sg/wp-content/uploads/2014/07/Monograph2613.pdf

[11] W. Sizemore, Addressing Common Vulnerabilities and Security Gaps in the Oil and Gas Industry. Security Intelligence, 2017. [Online]. Available: https://securityintelligence.com/addressing-common-vulnerabilities-and-security-gaps-in-the-oil-and-gas-industry/

[12] F. H. Alqahtani, "Developing an Information Security Policy: A Case Study Approach," *Procedia Computer Science*, vol. 124, pp. 691–697, 2017.

[13] T. A. Ricks, B. E. Ricks, and J. Dingle, Physical Security and Safety: A Field Guide for the Practitioner, 1st ed. CRC Press, 2014.

[14] M. Hassaballah and S. Aly, "Face recognition: challenges, achievements and future directions," *IET Computer Vision*, vol. 9, no. 4, pp. 614–626, 2015, doi: https://doi.org/10.1049/iet-cvi.2014.0084.

[15] J. Perdikaris, Physical security and environmental protection, 1st ed. CRC Press, 2014. [Online]. Available: https://doi.org/10.1201/b16861

[16] C. Schwarzl and E. Weippl, "A Systematic Empirical Analysis of Forging Fingerprints to Fool Biometric Systems," *Int. J. Secur. Softw. Eng.*, vol. 2, no. 1, pp. 40–83, 2011, doi: 10.4018/jsse.2011010103.

[17] M. P. J. Ashby, "The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis," *European Journal on Criminal Policy and Research*, vol. 23, no. 3, pp. 441–459, 2017, doi: 10.1007/s10610-017-9341-6.

[18] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations," *6th International Workshop on Trustworthy*

Embedded Devices, New York, NY, USA, 2016, pp. 45–54. doi: 10.1145/2995289.2995290.

[19] A. Al-Khouri, "Biometrics Technology and the New Economy: A Review of the Field and the Case of the United Arab Emirates," *International Journal of Innovation in the Digital Economy*, vol. 3, pp. 1–28, 2012, doi: 10.4018/jide.2012100101.

[20] M. Rouse, Physical Security. Search Security., 2016. [Online]. Available: https://searchsecurity.techtarget.com/definition/physical-security

[21] A. Albattat and A. P. Mat Som, "Biometric Technologies in Emergency Management: The Case of Hotels," *International Journal of Tourism & Hospitality Reviews*, vol. 1, pp. 44–50, 2014, doi: 10.18510/ijthr.2014.115.

[22] K. Singh, M. Zaveri, and M. M. Raghuwanshi, "Illumination and Pose Invariant Face Recognition: A Technical Review," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 2, 2010.

[23] M. Pollard, Even mask-wearers can be ID'd, China facial recognition firm says. Reuters, 2020. [Online]. Available: https://www.reuters.com/article/us-health-coronavirus-facial-recognition-idUSKBN20W0WL

[24] NEC Corporation, NEC technology recognizes people based on partial images. NEC Corporation, 2019. [Online]. Available: https://www.nec.com/en/press/201902/global_20190208_01.html

[25] S. Ramakrishnan, Face Recognition - Semisupervised Classification, Subspace Projection and Evaluation Methods. InTech, 2016. [Online]. Available: https://doi.org/10.5772/61471

[26] S. Shepard, Biometric Technology Market to Grow to $59.31 Billion by 2025. Security Today, 2019. [Online]. Available: https://securitytoday.com/articles/2019/04/22/biometric-technology-market-to-grow-to-59.31-billion-by-2025.aspx