Adopting AI and IoT Technologies in the Renewable Energy Sector for the Operational Technology Environment

This is a research paper produced by the Fellows taking part in the UK-Gulf Women in Cybersecurity Fellowship 2023-24. The paper reports on how critical sectors are having to embrace new technologies, but also need to invest in new training, awareness and security measures to ensure physical infrastructure in protected from digital threats.

The Fellowship is funded by the UK's Foreign, Commonwealth and Development Office and delivered by Plexal and Protection Group International

Read more about the Fellowship here:

www.plexal.com/our-work/ukgulfwic

The members of the Research Syndicate Group who produced this paper are:

- *Dr. Hanan Waheed Alhindi, Assistant Professor, King Saud University*
- *Moudi Yousef Al Rashdan Mariam, SOC Division Manager Defence, Saudi Electric Company*
- *Rawiya Rashid Khalid Al-Barwani, CISO at the Ministry of Energy and Minerals, Sultanate of Oman*
- *Khadeejah Abdullah, Network Specialist at Public Institution for Social Security, Kuwait*
- *Mariam Ali Ibrahim, Information Security Governance Section Manager at Digital Dubai.*

The Fellows were supported by their mentors:

- *Heba AlSawan, Head of Infrastructure, IT and Security Operations, PIFSS*
- *Dr. Hoda Al Khuzaimi, Assistant Professor, NYU*

Introduction

We proudly present our collaborative endeavour: a comprehensive research paper on the appetite for using artificial intelligence (AI) and Internet of Things (IoT) technologies in the renewable energy sector, specifically in the operational technology (OT) environment, and the impact on cyber risks. This report looks at the Gulf Cooperation Council (GCC) region.

The authors hail from various countries within the GCC and possess diverse backgrounds in cybersecurity industry, IT academia.

The findings have been informed by reviewing over 50 relevant research papers and interviewing C-level executives in the energy and cybersecurity sectors.

This paper and its recommendations aim to serve as a guide for stakeholders, policymakers and practitioners, while stimulating discussion about the opportunities and threats within OT environments.

It is a testament to the collective strength, expertise and dedication of women in cybersecurity within the GCC region. It is our sincere hope that our efforts will contribute meaningfully to the advancement of improved cybersecurity practices and pave the way for a safer and more resilient digital ecosystem.

We extend our heartfelt gratitude to all those who generously contributed their time and insights.

Literature review

In the literature review, four papers are highlighted as examples of how emerging technologies are being used in the OT environment in the renewable energy sector.

Smart building automation systems

The papers delve into the evolving landscape of smart building automation systems (BAS), emphasising the IoT devices with OT. This integration creates cybersecurity concerns, as it broadens the attack surface and introduces new vulnerabilities.

There is the potential for disruption in BAS operations through simple attacks on common network protocols. There has been BAS-specific malware development that persists within the BAS network using both

OT and IoT devices. This research provides valuable insights into the vulnerabilities and potential attack strategies within modern smart buildings, highlighting an urgent need for more robust security measures in building automation systems.[1]

The paper 6TiSCH Centralized Scheduling: When SDN Meet IoT [2] discusses the convergence of OT and IT in the context of IoT, focusing on deterministic networking and its implementation in low-power wireless sensor networks (WSNs) through 6TiSCH and DetNet efforts. It explores the integration of Software Defined Networking (SDN) in IoT, addressing the challenges in managing large-scale IoT networks and their complex routing topologies.

It highlights the evolution of SDN and its application in IoT, particularly in industrial WSNs, to achieve deterministic and reliable networking. It emphasises the importance of centralised network control, scheduling, and the need for new routing and resource allocation schemes to support the growing IoT infrastructure.

The research contributes to an understanding of the synergy between SDN and IoT in creating efficient, scalable, and reliable IoT networks.

IoT and IIoT

The paper Industrial Internet of Things (IIoT) Forensics: The Forgotten Concept in the Race Towards Industry 4.0 [3] presents a comprehensive study on the convergence of OT and Information IT within the context of IIoT. It emphasises the urgent need for digital forensic methodologies, standards, and processes in IIoT environments.

The research highlights the absence of focused forensic approaches in the rapidly evolving IIoT landscape, which is increasingly vulnerable due to the integration of various technologies and the proliferation of IoT devices. The paper argues for the development of IIoT-specific forensic frameworks to address these challenges, aiming to enhance security and incident response in smart manufacturing and automated processes, a critical aspect often overlooked in the pursuit of Industry 4.0.

The paper The FORA Fog Computing Platform for Industrial IoT [4] presents an in-depth exploration of the integration of fog computing within the Industrial Internet of Things (IIoT). It emphasises the necessity for a robust and efficient computing framework to handle the complex demands of IIoT systems. The research proposes a comprehensive Fog Computing Platform (FCP), which is designed to address the unique challenges of IIoT such as real-time data processing, resource management and security concerns. This platform aims to enhance the

performance and scalability of IIoT systems by using advanced computing and networking technologies, paving the way for more effective and efficient industrial automation and data management. The study provides a detailed framework and methodology for implementing fog computing in industrial settings, highlighting its potential to revolutionize IIoT applications.

Interviews

Interviews were conducted with six participants across the Gulf Cooperation Council (GCC) from different parts of the OT sector to gather insights from participants, explore complex phenomena, and find potential solutions.

Interview questions covered areas such as demographics, OT governance, AI/IoT technology, renewable energy, workforce capabilities, challenges, solutions and technology implementation.

#	Interviewee	Country	Sector	Position/job title
1	Eng.Nasser Aldossari	Saudi Arabia	OT/Utility company	Cyber Security Consultant in OT/Utility
2	Dr.Hoda Alkhzaimi	United Arab of Emirates	Education	UAE Researcher in advanced technology
3	Eng. Yahya Khoja	Saudi Arabia	Saudi Ministry of Energy	General Manager of AI in Saudi Ministry of Energy
4	Eng. Asim Tourjami	Saudi Arabia	Saudi Electricity Company	Renewable Energy Director in Saudi Electricity Company.
5	Eng.Yousif Albalwi	Saudi Arabia	NEOM	Cyber Security Director in NEOM
6	Eng. Mohammad Al-Safi	Kuwait	Kuwait Oil Company	Team Leader Information Security

Organisational size and structure

The organisations interviewed had OT departments that varied in size, with employee numbers ranging from approximately 500 to over 10,000. In cybersecurity, about 100 employees – constituting 20% of the total workforce – underscore a strong emphasis on security.

The annual budget for OT is reported at $5m, with an additional 15% of the overall budget dedicated to IoT/AI solutions, reflecting a commitment to technological innovation.

The renewable energy sector operates without a specified budget but focuses on training and awareness, with a substantial 40% of the overall budget allocated to renewable initiatives. Collectively, these figures depict an organisation deeply invested in both technology and sustainability, allocating dedicated resources towards cybersecurity and renewable energy to align with its strategic goals and enhance operational efficiency.

Themes and key findings

OT governance

Each company has a unique approach to aligning strategy and vision with OT governance. This diversity reflects the varied priorities and contexts of different organisations. Company 1 and 2 prioritise a risk awareness and compliance-driven approach, especially for large scale operations like ARAMCO. Company 3 integrates cybersecurity measures into its strategy to safeguard critical infrastructure and promote innovation within a secure framework. This approach reflects its proactive stance towards cybersecurity.

Company 1 emphasises addressing the shortage of cybersecurity experts through automation and AI augmentation, while company 2 takes a more moderate approach. Meanwhile, company 4 prioritises innovation and emerging technology investments, showcasing varied strategic priorities.

All companies stress the importance of robust risk management practices, cybersecurity measures and compliance with laws and regulations. This underscores the shared commitment to mitigating risks effectively and maintaining regulatory compliance. The interviews also acknowledge the challenges faced by companies when integrating AI/IoT systems, such as device incompatibilities and cybersecurity issues.

However, the proposed strategies like standardising data, testing and collaboration with system vendors demonstrates proactive measures to address these challenges.

Company 1's insights into utilisation of renewable energy reflect a commitment to sustainability and regulatory compliance. This aligns with broader environmental goals and initiatives like KSA 20230 Vision for sustainability.

AI/IoT Technology

Adopting AI and IoT in the OT environment is crucial for several reasons, including:

- *enhancing operational efficiency*
- *improving safety and compliance*
- *reducing cost*
- *data-driven decision-making*
- *enhancing customer experience*
- *scalability, flexibility, and sustainability*

The companies interviewed embrace the adoption of new technologies and innovations in the OT environments at different levels. Some of them embrace the adoption of new technologies at a moderate level while others embrace the adoption at an increasingly high level. For example, the Kuwait Oil Company is open to adopting new technologies as part of its digital transformation programme. Companies are increasingly embracing digital technologies to enhance operational efficiency, productivity, and decision-making in OT.

Digital technologies are converging with traditional industrial processes to enhance efficiency, productivity, and decision-making in various industrial sectors, while the Ministry of Energy in Saudi Arabia has an aim of using AI to strengthen its leadership in the energy sector.

Not all organisations have fully integrated AI into their OT environment. In the Oil and Gas sector businesses are considering the criticality of their operations while some sectors such as NEOM in Saudi Arabia have integrated AI/IoT technology into their OT environment as this is a part of a broader trend known as the Industrial Internet of Things (IIoT).

There are several factors that contribute to the adoption of new digital technologies in the OT environment: digital transformation initiatives, IoT integration, robotics and automation, augmented reality and virtual Reality, and data analytics and visualisation

Assessing how new technology will integrate with existing infrastructure

AI/IoT can support the cybersecurity of an organisation by providing several critical solutions such as:

- *proactive threat detection*
- *real-time monitoring*
- *automated response capabilities*
- *threat detection and analytics*
- *network security*
- *safety shutdown system*
- *isolated system and endpoint protection*

This does require significant investment but using these technologies can also help an organisation realise it's strategic goals. For example:

- *Optimising energy production*
- *Enhancing predictive maintenance*
- *Improving operational efficiency*

It is complex and challenging to integrate any solutions from outside the company because several needs should be considered, including legacy systems, cost and different network connections. Companies must perform a risk assessment for new technology implementations to identify information security risks.

There are several challenges that companies can face in using AI/IoT with OT in the renewable energy sector, including:

- *finding suitable data*
- *cleaning, processing and customising data*
- *storage capacity,*
- *processing power*
- *interoperability issues*
- *safe connections to IoT devices*
- *data security concerns*
- *the need for specialised skills and training*

Spotlight on Neom

Eng.Yousif Albalwi, Cyber Security Director at NEOM, an urban area being built by Saudi Arabia in Tabuk, shared several challenges that should be considered when using AI/IoT with OT systems in the renewable energy sectors:

1) Integrating AI and IoT technologies with existing OT systems, legacy infrastructure, and diverse equipment from different vendors can be

challenging. Ensuring seamless interoperability is crucial for effective data exchange and system operation.

2) The renewable energy sector, like any other critical infrastructure, is a target for cyber threats. Ensuring the security of AI and IoT devices, data and communication channels is paramount to prevent unauthorised access, data breaches and disruptions to energy production.

3) Handling sensitive data generated by AI and IoT devices raises concerns about data privacy. Compliance with data protection regulations and industry-specific standards is crucial, and navigating these requirements adds complexity to implementation.

4) AI applications in renewable energy often requires real-time data processing for efficient decision-making. Achieving low-latency communication between IoT devices and AI systems is critical to respond promptly to dynamic environmental conditions.

5) Collaborating between IT and OT teams, as well as involving experts from diverse fields like data science, electrical engineering, and cybersecurity, is essential. Bridging the gap between these disciplines is critical for successful implementation.

6) Finding and retaining skilled professionals with expertise in AI, IoT, and renewable energy technologies can be a challenge. The skills gap may hinder the effective deployment and maintenance of these advanced systems.

Neom's objective is to "judiciously evaluate available technologies and implement necessary measures to bolster organisational cybersecurity without unnecessary complexity", according to Albalwi.

Neom's overarching aim is to enhance operational efficiency by automating tasks, optimising resource utilisation and minimising downtime. Through predictive maintenance strategies powered by AI, it aims to forecast equipment failures and minimise downtime while optimising maintenance costs.

Real-time monitoring and control facilitated by IoT sensors enable Neom to analyse data promptly, ensuring informed decision-making to optimise operations. Ultimately, its goal is to harness AI to derive meaningful insights from IoT-generated data, empowering decision-makers with accurate information for improved decision-making processes.

Renewable energy

Renewable energy in the Gulf region is gaining momentum due to several factors, including abundant sunlight, vast open spaces and growing concerns about climate change. Companies are aligned with their country's vision for sustainability as well as to local regulations.

Utilising emerging technologies in the renewable energy sector holds immense promise for addressing the challenges of climate change, energy security, and economic sustainability. Here's a summary on the potential benefits of leveraging these technologies:

1. *Efficiency: Emerging technologies such as advanced photovoltaics, wind turbine designs, energy storage solutions and smart grid systems are continuously improving the efficiency and reliability of renewable energy sources. These innovations help to drive down costs, making renewable energy more competitive with fossil fuels.*
2. *Enhanced integration and flexibility: Technologies like AI, IoT and blockchain are facilitating the integration of renewable energy into existing energy systems. They enable better forecasting, management and optimisation of renewable energy resources, enhancing grid stability and flexibility.*
3. *Empowering decentralisation: Distributed energy resources (DERs) and microgrid technologies empower communities, businesses, and individuals to generate, store and manage their own renewable energy locally. This decentralisation of energy systems increases resilience, reduces transmission losses and fosters energy independence.*
4. *Unlocking new opportunities: Emerging technologies open up new opportunities for renewable energy deployment in previously untapped areas. For example, floating solar panels can be deployed on reservoirs and offshore wind farms can harness powerful ocean winds. Additionally, innovations in materials science and bioenergy technologies offer novel pathways for sustainable energy production.*
5. *Addressing global challenges: By harnessing the power of emerging technologies in the renewable energy sector, we can address pressing global challenges such as climate change, air pollution, and energy poverty. These technologies offer scalable, affordable and environmentally friendly solutions that can be deployed worldwide, driving the transition towards a more sustainable energy future*

Key renewable energy sources in the Gulf region

The sources are summarised below:

1. *Solar energy: The Gulf region receives some of the highest solar irradiance levels in the world, making it ideal for solar power generation. Countries like Saudi Arabia, the United Arab Emirates (UAE), Oman and Qatar have launched ambitious solar energy projects including large-scale solar farms and rooftop solar installations.*
2. *Wind energy: While solar energy dominates discussions about renewables in the Gulf, wind energy also has potential, particularly in coastal areas. Countries like Bahrain, Oman and the UAE are exploring wind power projects, with offshore wind farms being considered due to the region's long coastlines.*
3. *Geothermal energy: Although not as widely discussed as solar and wind, the Gulf region does have some potential for geothermal energy due to its geological features. However, the exploitation of geothermal energy is still in its infancy in the region.*
4. *Biomass energy: Derived from organic materials, it has limited potential in the arid Gulf region. However, waste-to-energy projects, such as converting agricultural waste or municipal solid waste into energy, are being explored in some Gulf countries.*
5. *Hydropower: The Gulf region has limited opportunities for traditional hydropower due to its arid climate and lack of significant rivers. However, some countries are exploring small-scale hydropower projects, particularly in mountainous areas.*
6. *Nuclear energy: While not strictly renewable, nuclear power is often considered within the broader energy transition discourse. The UAE is leading in this aspect with its Barakah Nuclear Power Plant, which aims to diversify its energy mix and reduce reliance on fossil fuels.*

Several GCC countries have set ambitious renewable energy targets and commitments. These targets are often part of broader national strategies to diversify energy sources, enhance energy security and reduce dependence on fossil fuels. Therefore, different projects were established focusing on generating energy from solar and wind resources.
The challenges faced when adopting renewable energy technologies can be summarised into seven main challenges.

These challenges are:

1. *Intermittency and variability: Many renewable energy sources such as solar and wind are intermittent and variable. The availability of sunlight and wind is not constant, leading to fluctuations in energy production. This poses challenges for maintaining a stable and reliable power supply. There is a need for protecting power supply during low solar input periods, such as cloudy weather. Moreover, there is a prevailing perception that renewable energy is unreliable due to its dependence on natural conditions.*
2. *Energy storage efficiency: The need for effective energy storage solutions is critical to address the intermittency of renewable energy sources. Developing cost-effective and efficient energy storage technologies, such as batteries, is a significant challenge.*
3. *Grid integration: Integrating renewable energy into existing power grids can be challenging. The grid infrastructure may need upgrades to handle decentralised and fluctuating power generation, and grid management systems must adapt to the variability of renewable sources.*
4. *Technological development and cost: While the cost of renewable technologies has decreased over the years, initial installation costs can still be high. High capital cost of batteries being a significant hurdle as well. Continued research and development are needed to make renewable energy technologies more affordable and efficient.*
5. *Specialised skills and workforce development. Expertise in areas such as engineering, data analytics and cybersecurity is needed. Ensuring an adequate talent pool and investing in workforce development are essential for successful implementation.*
6. *Regulatory Hurdles: Regulatory frameworks still require enhancement to better support sustainability initiatives. However, it was found that cybersecurity concerns have not been addressed by the interviewees.*

There are a number of successful projects utilising renewable resources can be found in the GCC. These include:

Solar Power: • Shams 1 (UAE): Shams 1 is a concentrated solar power (CSP) plant located in Abu Dhabi, United Arab Emirates. It has a capacity of 100 megawatts and uses parabolic trough technology to generate electricity.

Wind Power: DumatAl Jandal (Saudi Arabia): Dumat Al Jandal is a significant wind farm project in Saudi Arabia with a capacity of 400

megawatts. It represents Saudi Arabia's commitment to diversifying its energy mix.

*Apart from solar and wind**,** Saudi Arabia also exploits waste energy, concentrated solar power, geothermal power and biomass energy as part of KSA diverse renewable energy portfolio.*

Hydropower Wadi Dayqah Dam (Oman): While not a traditional hydropower project, the Wadi Dayqah Dam in Oman contributes to water storage and can be associated with certain hydropower-related benefits, such as regulating water flow.

Cyber threats and the need for training

Organisations might face a lot of risk after applying AI/IoT and they can mitigate the risks effectively by instituting multi-layered security protocols, conducting routine audits and prioritising cybersecurity training for our workforce.

Recognising that cybersecurity encompasses more than just technology, interviewees emphasised the importance of people and processes. Through a comprehensive framework encompassing governance, documentation, training, and ongoing awareness initiatives for both IT and non-technical staff, coupled with the implementation of necessary technologies, continuous monitoring, and regular audits, cybersecurity threats can be minimised proactively.

Interviewees spoke about the need for a holistic blend of technical solutions, best practices and organisational initiatives to ensure a robust cybersecurity posture.

There is also a need to comply with regulation before applying IoT/AI to the renewable energy solutions, such as:

- *National Institute of Standards and Technology (NIST)*
- *International Electrotechnical Commission (IEC)*
- *ISO/IEC 27001 for information security management systems.*
- *Saudi National and Regional Regulations: NCA, NDMO”*

Workforce capabilities

As they adopt new technology, OT organisations across the GCC face workforce, skills and training challenges – in particular when it comes to maintaining a secure cybersecurity posture.

Aramco in Saudi Arabia addresses this by implementing a continuous training programme for every employee and enhancing retention through share-based partnerships.

Similarly, the UAE has a focus on developing and retaining cybersecurity skills through comprehensive training programmes and certifications.

As companies across the GCC, like Neom in Saudi Arabia, strive to integrate AI and IoT within existing OT systems, they encounter significant hurdles such as interoperability issues, integration complexities and the relentless pace of technological change which necessitates constant employee training and adaptation. Neom particularly emphasises certifications, continuous education, and offering career paths to foster a continuous learning culture and ensure its workforce is up to date with the latest technological and industry trends.

Moreover, the pervasive threat of cyber attacks on increasingly interconnected systems calls for a robust focus on cybersecurity skills, as evidenced by the efforts of Kuwait Oil Company. It has dedicated an Information Security team to safeguard company assets through comprehensive cybersecurity training, governance and resilience practices. Additionally, regulatory compliance complicates the operational landscape, requiring that employees not only remain technologically adept but also legally vigilant. This is a challenge that companies like the Ministry of Energy in Saudi Arabia addresses through strategic skill-building initiatives that emphasise hands-on learning.

Such strategies ensure that employees are well-equipped to navigate the demanding environments of OT and IoT. The collective efforts of these organisations showcase their commitment to enhancing workforce capabilities, highlighting the importance of continuous training, professional development opportunities, and a supportive work environment to maintain industry competitiveness and operational excellence in the face of evolving technological landscapes.

Conclusion and analysis of strengths, opportunities and weaknesses

Countries visions, government initiatives, favourable policies, and partnerships with international renewable energy companies are driving the adoption of renewable energy in the Gulf region.

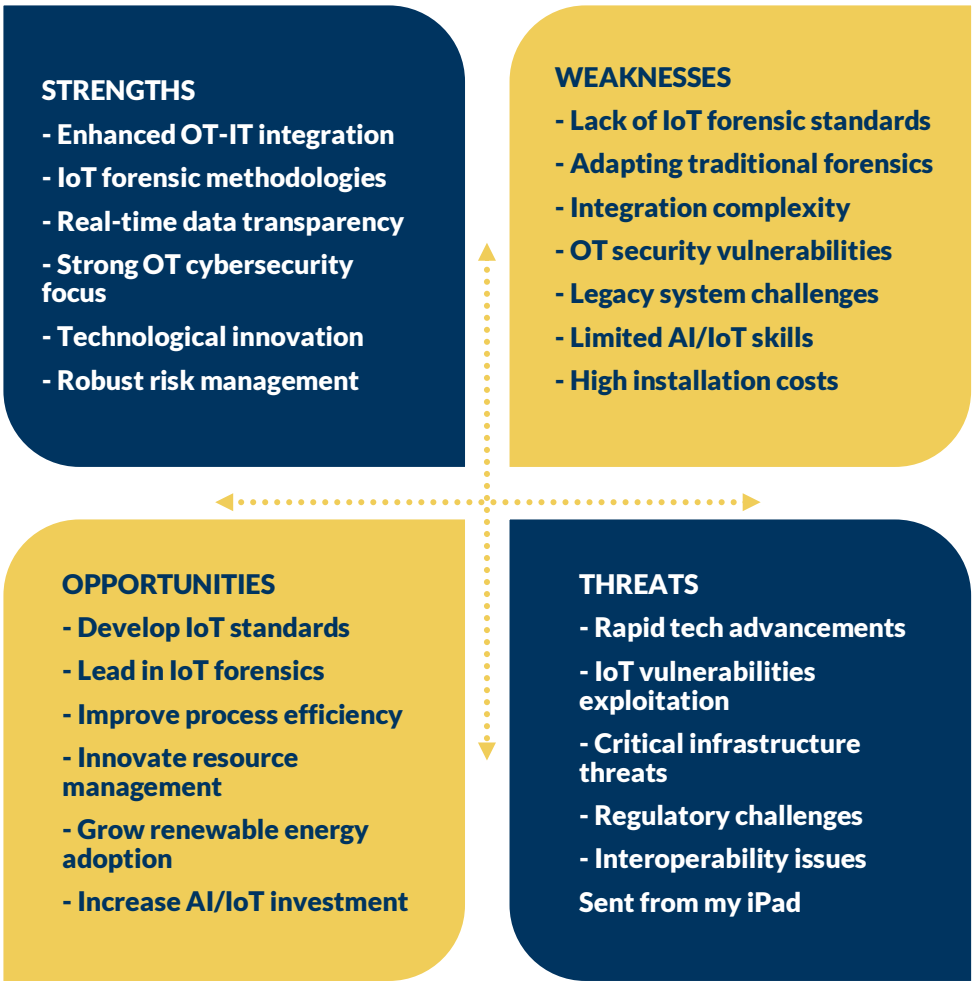
These efforts not only aim to meet domestic energy demand but also position Gulf countries as leaders in sustainable energy production and reduce their carbon footprint.

The integration of emerging technologies is essential for unlocking the full potential of renewable energy sources, accelerating the transition towards a low-carbon economy, and ensuring a more sustainable and resilient energy future for generations to come. However, concerns of renewable energy sources being intermittent, variable and costly are still being a significant hurdle. The increasing digitisation and connectivity of renewable energy systems introduce new cybersecurity risks, such as hacking, data breaches, and system vulnerabilities. Safeguarding against these threats requires robust and resilient cybersecurity measures and protocols.

Nevertheless, government initiatives in the GCC are continuing to drive the adoption. Additionally, countries have embedded cybersecurity into their renewable energy strategies to safeguard the critical infrastructure and promote innovation within a secure framework. This approach reflects a proactive stance towards cybersecurity.

Continued research, investment, and collaboration are crucial to harnessing the transformative power of these technologies and develop technologies that are secure by design.

Given the findings of the interviews and an analysis of the current landscape, a summary of the opportunities and threats is below.



Recommendations

The GCC region is actively promoting renewable energy as part of their diversification strategies to reduce dependence on fossil fuels. And there is a growing appetite for adopting AI and IoT technologies in the GCC renewable energy sector within the OT environment. Below are recommendations:

1. ***Cybersecurity protection**: Implement cybersecurity measures to protect IoT devices and AI systems from cyber threats through:*

    a. *Network security: Ensuring that the communication networks are secure from unauthorised access. This involves implementing firewalls, intrusion detection systems, and intrusion prevention systems.*
    b. *Secure protocols: Using secure communication protocols such as HTTPS, TLS, and SSH to protect data transmission between devices and systems.*

c. *Secure remote access: Identification and inventory of all remote access points and restricting remote connectivity through multi-factor authentication, privileged access limitation, micro-segmentation and encryption to protect remote connections.*
d. *Patch management: Regularly updating and patching software and firmware to address known vulnerabilities and protect against exploitation by cyber attackers.*

2. *Data privacy protection: Implement measures such as data anonymisation, user consent mechanisms, encrypting sensitive data and secure data storage to protect privacy.*
3. *Continuous monitoring and activated incident response: implement continuous monitoring of IoT and AI systems to detect and respond to security incidents in real time. This includes redundancy in critical systems, backup power sources, and disaster recovery plans to minimise downtime and maintain operational continuity.*
4. *Regulatory compliance: Stay informed about evolving regulations and standards related to IoT and AI in the renewable energy sector.*
5. *Employee training and awareness: provide comprehensive training and awareness programs for employees involved in managing and operating IoT and AI systems.*
6. *Physical security: securing physical access to the critical infrastructures to prevent unauthorised tampering or sabotage.*

By implementing these recommendations in the renewable energy sector can effectively mitigate the risks associated with enabling IoT and AI, ensuring the security, privacy, and reliability of their digital infrastructure.

References

[1] Santos, D., Dagrada, M., & Costante, E. (2020). leveraging operational technology and the internet of things to attack smart buildings. Journal of Computer Virology and Hacking Techniques, 17(1), 1-20. https://doi.org/10.1007/s11416-020-00358-8

[2] Thubert, P., Palattella, M., & Engel, T. (2015). 6tisch centralized scheduling: when sdn meet iot.. https://doi.org/10.1109/cscn.2015.7390418

[3] Kebande, V. (2022). industrial internet of things (iiot) forensics: the forgotten concept in the race towards industry 4.0. Forensic Science International Reports, 5, 100257. https://doi.org/10.1016/j.fsir.2022.100257

[4] Pop, P. (2021). the fora fog computing platform for industrial iot.. https://doi.org/10.5281/zenodo.5856300