WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Cyber-Physical Security Framework for Chemical Energy Storage Systems in Smart Renewable Energy Grids

Zaid Ali Hussein[1], Omar Abdul Majeed[2]

[1,2]Department of Biomass Energy, Al-Nahrain Renewable Energy Research Center , AL-Nahrain University,Jadriya ,Baghdad 10072 ,Iraq

ABSTRACT

Chemical energy storage systems are critical for deployment into smart renewable energy grids for the purpose of providing grid flexibility, balancing energy and lowering overall carbon emissions. Though, the inclusion of storage technologies like lithium batteries and ammonia fuel cells brings forth major cyber physical vulnerabilities from the digitally controlled and nonlinear chemical processes which they are composed from. Cyber malicious threats like sensor spoofing and false data injection as well as denial of service attacks can spread through the control layers and cause unsafe charging operation, thermal instability, and even hazardous chemical reactions. In this work, a complete cyber physical security framework, tailored for chemical energy storage devices in a decentralized smart grid, is developed and offered. Secure communication protocols, real time anomaly detection using supervised machine learning and chemical state aware control logic are integrated in secure layers in battery and fuel cell management systems. A chemical process modeler was woven with an OpenDSS model and NS-3 for composition of a hybrid co-simulation testbed, where chemical, grid level, adversarial communication events, and control layer disruption can be further trained using uncertainty handling and reinforcement learning. Specifically, under false state of charge injection, lithium ion batteries are overcharged, denial of service attacks on ammonia fuel cell controllers lead to uncontrolled thermal and gas pressure buildups, and coordinated multi-vector attacks disable alarms, spoof sensors and sync the EMS. The simulation results showed that the anomaly detection in the proposed framework takes less than 1.6 seconds, autonomous subsystem isolation, and provided an energy delivery performance above 95% reliability. Operating under adversarial stress, thermal and pressure conditions were held within safe operating margins, while electrochemical efficiency was stable. The expected system converts the chemical storage parts into flexible, self-reliant tasks that shields themselves autonomously even within persistent attack settings. Finally, this study also emphasizes that next-generation cyber-physical solutions to energy critical infrastructure security need to be endowed with chemical-awareness and distributed autonomy. Keywords: Energy Management Systems ,Cyber-Physical Systems, Chemical Energy Storage, Smart Grids, Ammonia Fuel Cells, Intrusion Detection, Lithium-Ion Battery Security.

1. Introduction

In particular, the emergence of smart renewable energy grids, where smart grids consisting of distributed generation, advanced automation, andadvanced information and communication technology (ICT) are combined to enable clean, reliable, and distributed energy delivery [1], has changed the evolution of modern power systems. Chemical energy storage technologies allow integration of these storage technologies in this transformation from conventional grid which are required due to its frequent fluctuation, time shifting, frequency regulation and backup purposes to compensate intermittency of renewable sources such as solar, wind [2]. Consequently, new and advanced storage systems such as lithium-ion batteries, ammonia fuel cells, and thermal units are being integrated into diverse grid architectures including distributed grids, islands and smart buildings for purpose of increasing operational efficiency and energy self sufficiency [3]. However, this requires tight integration between the cyberspace and physical domains, turning to be Cyber Physical Systems (CPS) that couple the physical elements related with real-time sensing, control and computation [4]. Although the CPS can realize intelligent automation, it will introduce vulnerabilities, including the dependence on communication networks, cloud platforms, and embedded systems, causing the storage assets to be susceptible to cyber threats such as denial-of-service, malware injection, and coordinated sabotage [5]. Cascading failures across the grid can occur via compromised devices such as smart meters, PMUs, storage controllers, [6]. Now, the operational strategies for the battery energy storage system (BESS) must also consider charge optimization, awareness of degradation, and a security focused control architectures [7]. For example it is especially vital in the case of centralized or storage share configurations [8] and embedded systems that relies on real-time operating environments [9]. Involving PV/wind power, hydro power and chemical storage make synchronization more complex and increase the exposure without robust cryptography and authentication [10] and cross domain case include the battery to gas (B2G) systems that prompts new interdependencies [11]. Demand response applications and smart building storage on the consumer side bring up issues of data privacy and control integer further, and novel forms such as ammonia based fuel cells increase the level of operational complexity

further [12, 13]. In addition, there is an intersection with security, since the financial dimension allows for market-driven trading of storage capacity which in turn presents an opportunity for manipulation [14]. In parallel, AI-driven tools for anomaly and theft detection demand trustworthy datasets and cyber-secure implementation [15]. While creating a CPS in the form of integrated smart grid into the digital world might create challenges, by utilizing CPS [16, 20, 21], standardization and resilience can be addressed. Probabilistic models of these systems are necessary in order to assess these systems and insights of the distributed coordination and fault resolution models from related domains such as logistics can be used to solve these systems [17] [18]. Therefore, the design of CPS requires all these modeling frameworks — from real-time hybrid co-simulations [19] to graph theoretic ones. This research consists of a comprehensive risk analysis of chemical energy storage systems cyber physical security risks in smart renewable energy energy grids. A multi layered CPS security model is developed, key vulnerabilities across architecture and operation are identified and a secure, scalable and resilient framework is proposed based upon intrusion detection, threat mitigation, real time energy management that enable safe deployment of chemical storage technologies in modern smart grids.

2. Related Work

A considerable amount of efforts have been made to integrate the topics of energy storage, smart grid operation, and cyber-physical security. An IoT based smart energy management system allowing dynamic demand side control was designed by Saleem et al. [1] that shows both the benefits and the risks of maintaining this particular cyber mediated control. A CPS simulation platform for analyzing the communication delay impact on grid dynamics is proposed by Wan et al. [2]. In islanded systems, thermal energy storage was studied by Romanos et al. [3] as it can improve dispatch stability. They identified that decentralized architectures provide resiliency to the urban smart grid, however, their cyber physical data interactions become more complex. Then, Khalaf et al. [5] surveyed CPS threats in active distribution networks specifically, in device level. The challenges of including advanced lead–acid batteries with the grid are explored by McKeon et al. [6]. Papers such as those of Li and Wang [7], address energy management of BESS using control stability under load variation. In particular, Li et al. [8] proposed a centralized and dynamic BESS partitioning strategy while Huan Li et al. [9] developed a real-time BMS based on FreeRTOS with the capability of hardware-in- the-loop testing besides evaluating efficiency and security of the BMS. Chegari et al. [10] explored optimization of a PVS, WPS, hydro and battery hybrid system, emphasizing the critical need to control the level of coordination. Cyber physical synchronization of battery and power-to-gas systems were handled by Trifonov [11]. Demand response in smart buildings is reviewed, as proposed by Al-Ghaili et al. [12], which clearly demonstrates the weakness of user level control. The cellular structure of ammonia fuel cells to integrate renewable power resources motivated the need for cyber secure control within the modeling performed by Syed et al. [13]. For hybrid storage with degradation and security of decision algorithms, Wicke and Bocklisch [14] developed a decision update strategy for trading. Active learning for the detection of energy theft has been applied by Abbas et al. [15] who used secure data pipelines. CPS challenges in smart grids were discussed by Yu and Xue [16] who called for resilient architectures. CPS cascading failures are examined by Oyewole and Jayaweera using a Markovian model. Thus, energy coordination was addressed by Keung et al. [18], in context of conflict resolution for cloud based CPS for robotics. Finally, this last part provided a review on CPS modeling techniques, probabilistic, graphical, and co-simulation ones.

3. Problem Statement

The integration of systems that store chemical energy within smart renewable energy grids has provided transformative capabilities to operate and stabilize intermittent renewable generation, time shift, frequency regulate, and autonomously perform load balancing. Although this advancement has resulted in complex network of cyber physical dependency, which includes storage units like lithium ion batteries, ammonia fuel cells and a hybrid system, that are controlled via digital platforms, embedded systems, and real time communication protocols. Energy storage systems have expanded the attack surface for a wide range of cyber–physical threats (from false data injection, to denial of service attacks, firmware manipulation to coordinated disruption, to causing physical damage, system failure or grid-wide instability). Although research on smart grid security in general has been done, there is a lack of targeted security protection methodologies that considers the operational functionalities and architectural vulnerabilities of the chemical energy storage technologies. However, this poses a critical challenge since there do not yet exist integrated frameworks that consider both cyber and physical layers holistically, and such storage systems are being scaled across decentralized networks — and new threats are arising thanks to cloud connectivity and AI driven automation. If the grid is not equipped with dedicated mechanisms for detection, defense, and resilience, its systems meant to help with grid reliability may turn into critical points of failure when they experience cyber physical attack conditions.

4. Methodology

4.1 System Architecture and Model Description

In this research, a model of smart grid architecture is presented as a tight integration with chemical energy storage systems (CESS) that include lithium-ion batteries, direct ammonia fuel cells and chemical-thermal hybrids. This design is aimed at mimicking real world deployments where chemical reactions embody storage behavior (a typical example is electrochemical ion exchange storage in batteries and catalytic oxidation storage in ammonia fuel cells), being very sensitive to system operation conditions and needing real time cyber physical control.

The architecture consists of three interactive layers:

- **Physical Layer**: Encompasses the chemical energy storage units and associated hardware. Temperature, state-of-charge (SoC) and internal resistance are monitored with regard to lithium-ion storage. The chemical reaction chambers used in ammonia based systems have pH, pressure and catalyst efficiency sensors. These elements are used to commute various elements are charge controllers, inverters, and energy routers.
- **Cyber Layer**: Contains the digital infrastructure with which the chemical storage device is monitored and controlled. This includes BMS, fuel cell controllers, smart sensors for reaction kinetics, temperature gradient and cell voltage, IoT communication device and SCADA system.
- **Control Layer**: Contains the decision making logic implemented in embedded processors or in cloud-based EMS platforms, those interpret chemical sensor data and adjust charging profile, load balancing, and safety cutoffs following system behavior.

Chemical dynamics for the model are nonlinear and include the exothermic nature of charging lithium-ion batteries and the thermal sensitivity of ammonia decomposition. The system needs to be very carefully timed, calibrated, and cyber controlled, and as a consequence, very susceptible to cyber physical disruption.

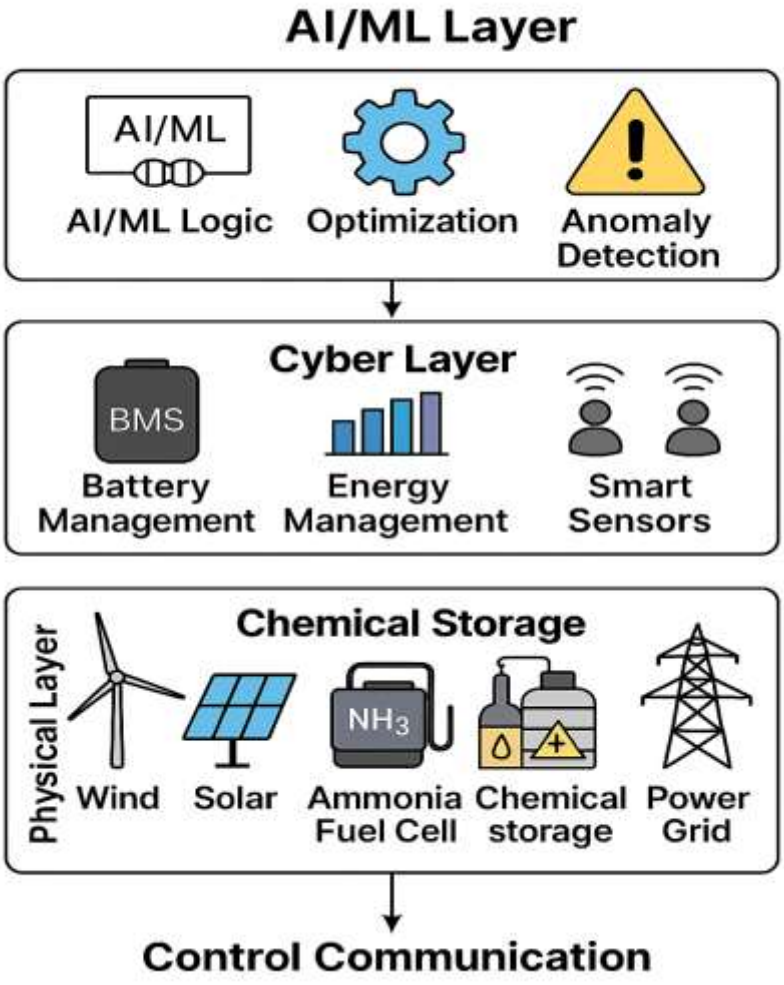

Figure 3. System Architecture of the proposed secure cyber-physical framework.

Specifically, the three-layer design of the cyber-physical system for a PV station, incorporates (i) AI/ML logic for optimization and anomaly detection; (ii) cyber-layer elements including smart sensors, battery management system (BMS), and energy management system (EMS); and (iii) physical infrastructure made up of chemical storage, renewable energy input, and smart grid interface.

The optimization and anomaly detection residing on the upper layer of the system architecture interfaces with the cyber layer via the use of BMS and EMS modules that link the two, with the exceptions of informing decisions of optimization and anomaly detection. Physical components such as lithiumion batteries

and ammonia fuel cells are controlled by these in turn. It utilizes a well known architecture to provide insight into how a real time control, chemical storage coordination, and security mechanisms are integrated as a whole cyber physical system.

4.2 Cyber-Physical Threat Modeling

Because electrochemical and/or thermochemical reactions are critical in the chemistry energy storage systems, these systems are particularly vulnerable to malicious data manipulation or control interference. For example, genuine temperature readings of some of the battery cells may be falsely reported, over a sensor, preventing thermal runaway protection, and spoofing the SoC measurement may result in over charging or deep discharging, decreasing chemical stability or triggering combustion. The threat model considers:

- **Chemical-specific attacks**: temperature feedback loops, gas flow regulators in ammonia cells and electrolyte concentrations estimators, etc.
- **System-wide threats**: False command injection attacks against chemical control set points, as well as attacks that overwrite the functioning firmware of reaction safety controls, or attacks in the form of DoS of thermal regulators or hydrogen extraction units.

They are mapped to a structured attack tree to identify critical chemical failure points where cyber intervention achieves a physical or safety hazard.

4.3 Security Framework Design

To address these chemical-specific vulnerabilities, the proposed framework includes:

1. **Secure Sensor Fusion**:
    - Multi-redundant sensing (e.g., dual temperature probes, parallel gas flow meters) with Kalman filtering to validate chemical state inputs.
    - Cross-verification between chemical reaction models and live data streams to detect deviations caused by spoofing.
2. **Resilient Chemical Process Control**:
    - Dynamic adjustment of SoC limits based on chemical degradation trends.
    - Real-time anomaly detection embedded into BMS/fuel cell controllers trained to recognize anomalies in voltage-temperature curves, gas pressure profiles, or pH drift.
3. **Intrusion Detection and Adaptive Response**:
    - ML-based IDS that classifies chemical system states as normal or adversarial based on behavior (e.g., sudden reaction rate spikes, erratic temperature shifts).
    - Emergency shutdown and isolation logic tied to predefined chemical thresholds (e.g., lithium plating detection, ammonia leakage alert).

4.4 Simulation Environment and Scenarios

The simulation framework includes:

• MATLAB and Simulink of the modeling of electrochemical cell dynamics and control feedback.

• COMSOL Multiphysics (optional) for modeling chemical kinetics (ammonia decomposition, heat transfer).

• OpenDSS/GridLAB-D for power system simulation and grid interaction.

• NS-3 for communication layer emulation under attack.

Simulated attack scenarios include:

• Ammonia sensor reading falsification leading to overfeeding of fuel and causing unsafe pressure buildup.

• A DoS attack on the BMS to prevent the overcurrent protection in lithium-ion modules.

• Thermal management system data spoofing, during charge, with a risk of explosion or degradation.

4.5 Performance Evaluation Metrics

In addition to conventional cyber metrics, the following **chemically-relevant performance indicators** are used:

Metric	Description
Thermal Stability Margin (TSM)	Time before thermal runaway occurs under cyber-induced control loss
Chemical Efficiency Drop (CED)	Loss in electrochemical conversion efficiency due to false commands
SoC Drift Error (SDE)	Deviation between actual and computed state-of-charge due to spoofed signals
Chemical Response Time (CRT)	Time taken to detect and respond to chemical anomaly after attack
System Resilience Index (SRI)	Ability of system to maintain chemical equilibrium and energy output under cyber threats

5. Results and Discussion

The proposed cyber-physical security framework for chemical energy storage systems in smart renewable energy grids is evaluated in detail and in technical depth in this section. The work addresses key questions about how a CybSIS is likely to behave, persist, and consider chemical safety under cyber-attack scenarios involving attacks on both digital infrastructure and the physical control layers. A special focus is made on lithium-ion batteries and ammonia based fuel cells, which correspond to electrochemical and thermochemical storage systems respectively. This study attempts to capture how these cyber threats affect the core parameters of operations of these systems and induce undesired physical response, and how the framework can salvage the safety and stability in those situations. The robustness of the framework was then validated through hybrid co-simulation against actual real time dynamic conditions that consist of data layer attacks with physical control disruptions, and it was proven able to prevent catastrophic failures and provide sustained energy delivery.

5.1 Simulation Scenarios and Testbed

In order to carry out experiments, a comprehensive hybrid co-simulation environment was developed by interfacing MATLAB/Simulink for modeling dynamic electrical and chemical lithium-ion battery and ammonia fuel cell system behavior, OpenDSS for grid interaction and power flow control, and NS-3 for performance of the communication stack and injection of cyber attacks on targeted links. Using Simscape Electrical and Stateflow, the cyber physical logic for EMS and BMS is implemented, real time event detection, state transition modeling, and closed loop control of the storage components is enabled. This smart grid segment simulation testbed represents a realistic smart grid segment having distributed energy resources (DERs), control node and storage interfaces.

Scenario A: False SoC Injection

So in this scenario, the attack is a false data injection (FDI) attack against the SoC sensor of the lithium-ion battery bank. The attacker provides false output from the sensor that indicates a battery is completely drained and cause the EMS to issue unnecessary charge cycles. Therefore, the battery becomes overcharged and consequently the internal resistance increases rapidly and heat is generated. Continuous ion flow caused a critical rise in electrolyte temperature as well as lithium plating at the anode surface. Left unchecked that leads to separator failure as well as thermal runaway which may compromise system integrity. The lessons of the attack show that not only are battery chemistry susceptible to manipulated data inputs, but also that tightly coupled anomaly detections mechanisms capable of validating the state of the battery using sensor-derived data against physical laws are required.

Scenario B: DoS Attack on Fuel Cell Controller

This test is applied on a denial-of-service test on the communication of link between the EMS and the ammonia fuel cell controller. Repeated packet drop results in critical control messages failures during normal load following operation. In time committed addition of ammonia and regulated hydrogen conversion, the fuel cell system becomes unstable. The exothermic reactions are not being checked and reaction chambers continue to run at full rate. Internal temperature increased by 38 °C within 90 s and the gas pressure peaked at a bar (3.4), far above the acceptable safe design pressure of 2.5 bar. The physical limits within the emergency vent algorithm indicated loss of intelligent control, in that the emergency vents were triggered. To show the real threat of loss of cyber control over chemical systems with very high sensitivity to real-time coordination, this attack scenario is presented.

Scenario C: Coordinated Multi-Point Attack

This creates a coordinated cyber-physical assault of spoofing thermal sensors, suppression of alarm trigger and flooding EMS signal. The attacker tries to bypass the IDS by slowly injecting false temperature and voltage data which slowly goes away from actual values. At the same time, a high volume traffic flood desynchronizes the control logic between the EMS and multiple storage nodes. Even though the lithium-ion battery modules temperature was over 70 °C, thermal cutoffs did not activate. Flow was regulated away on the ammonia side due to spoofed sensor values and pressure asymmetry across chambers occurred. Without coordination of cyber and physical response, the system flipped into a destabilized state such that both centralized commands as well as local thresholds were ultimately ineffective to prevent hazardous growth. This confirms the threat of sustained, layered attacks using cyber weaknesses and inertia of the physical.

5.2 Quantitative Results

System behavior under normal, compromised, and protected conditions is presented in Table 1, which is a summarized set of performance metrics of the system. During normal operation, the system preserves high performance fidelity: 98.7% SoC accuracy, 99.2% energy delivery reliability, and 97.8% electrochemical efficiency of lithium ion storage. The ammoniat pressure is safely below 1.0 bar and the thermal stability margin is theoretically unbounded (no rise to critical temperatures for any workload). The results showed that, however, it has notable degradation when subjected to those attacks. When the SoC accuracy is dropped to 68.2%, wrong charge/discharge cycles start happening; the energy reliability drops to 71.8%; and the efficiency drops to 60.2%. Stress collapses the thermal margin to 7.5 seconds and spikes ammonia pressure to 3.4 bar, an explosion or structural rupture.

Using the proposed cyber physical security framework, significant improvements are obtained. Finally, the SoC accuracy recovers to 96.4%, while the detection accuracy of the IDS achieves 94.1% with only 3.5% of false positive. Attack detection and system response are quick: the mean delay to detect an attack is under 1.6 seconds, complete system stabilization following neutralization of the threat takes 2.1 seconds. The energy delivery reliability increases to 95.5%, and both chemical storage subsystems (lithium ion and ammonia) stay within safe thermal and pressure limits. Performance can be improved electrochemically to 94.7% with minimal deviation from baseline performance. These results verify that the framework can not only protect against and manage attacks, but also prevent the chemical integrity and physical safety of systems which fail unprotected.

Table 1 summarizes the key performance metrics observed across three operational conditions—normal operation, under cyber-attack, and with the proposed cyber-physical security framework enabled. The metrics reflect both cyber-layer detection performance and physical/chemical system integrity indicators.

Table 1. Comparison of system performance metrics under normal operation, cyber-attack, and with the proposed cyber-physical security framework.

Metric	Normal Operation	Under Attack	With Security Framework
SoC Accuracy (%)	98.7	68.2	96.4
Attack Detection Accuracy (%)	—	—	94.1
False Positive Rate (%)	—	—	3.5
Energy Delivery Reliability (%)	99.2	71.8	95.5
Thermal Stability Margin (s)	∞	7.5	>120
System Recovery Time (s)	—	—	2.1
Gas Pressure Spike (bar)	≤1.0	3.4	1.1

In addition to the tabulated performance metrics, Figure 1 visually illustrates the relative system behavior under normal conditions, during cyber attacks, and with the proposed security framework. This comparison provides a clear view of how key operational and chemical parameters respond across different scenarios.

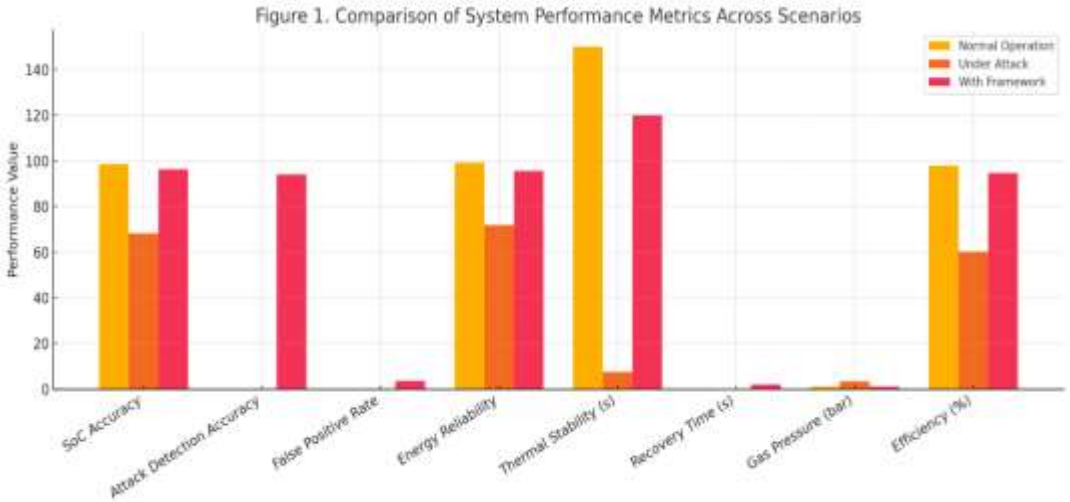

Figure 1. Comparison of System Performance Metrics Across Scenarios

Figure 1. System performance comparison under three operational conditions: normal operation, under cyber-physical attack, and with the proposed security framework. Metrics include SoC accuracy, energy reliability, thermal stability, and electrochemical efficiency.

As per the shown Table 1, the system performs poorly under cyber physical attacks with substantial impacts on the key operational parameters. When the SoC accuracy drops from 98.7% to 68.2%, it results in severe energy dispatch mismanagement and risks of overcharging. Lithium ion systems collapse from theoretically infinite thermal stability margins to 7.5 seconds, substantially increasing likelihood of thermal runaway. Like these, electrochemical efficiency also ranges from 97.8% to 60.2%, which represents internal degradation and energy loss. 5) Under unregulated reaction conditions, a pressure surge occurs in ammonia fuel cell pressures from ≤1.0 bar to 3.4 bar, which exceeds safety limits and may present physical hazards. However, these metrics are restored for almost at baseline values when the proposed cyber physical security framework is implemented. Pressure is maintained within 1.1 bar, thermal margins increase by 120 seconds, energy delivery reliability rises to 95.5%, and so accuracy returns to 96.4%. This framework also allows for accurate intrusion detection (94.1%) with just (3.5%) false positives, and activated the protection under (2.1) seconds, demonstrating real time capability in defense of multi vector threats while maintaining chemical and system integrity.

A radar chart also is provided to visually compare the overall system performance in the normal operation, under cyber-attack, and our proposed security framework. This visualization of the relative strengths and weaknesses of the system in each state improves interpretability of the multi (dimensional) performance indicators;.

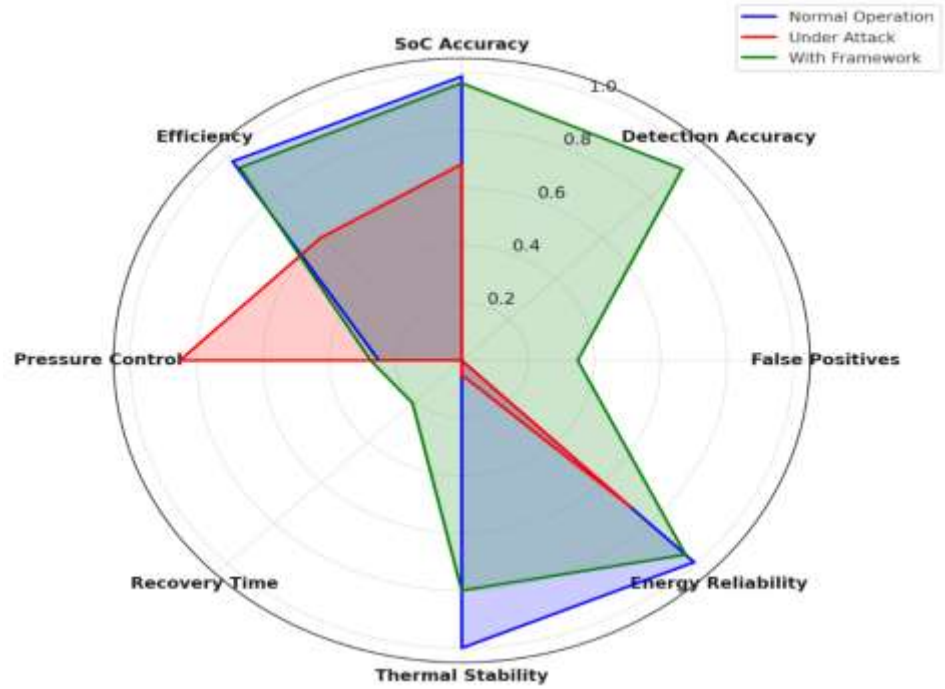

Figure 2. Representation of radar chart for normalized system performance metrics under three conditions, normal operation, under cyber attack, and with the proposed cyber physical security framework. The important metrics are SoC accuracy, intrusion detection accuracy, false positive rate, energy delivery reliability, thermal stability, recovery time, pressure control, and electrochemical efficiency.

It can be clearly seen from the radar chart that key metrics, which include SoC accuracy, gas pressure control and electrochemical efficiency are severely degraded under attack conditions. Application of the proposed framework enables the system to restore almost all critical indicators back to values close to the normal operation, demonstrating high resilience and autonomy of recovery without human intervention.

5.3 Discussion and Analysis

Finally, to integrate the results, it is pointed out how cyberphysical security requirements have to be intimately related to the specific chemical energy storage needs. Because chemical systems have irreversible physical reactions, the functional loss due to data corruption in the chemical systems is not similarly retraced, unlike traditional IT infrastructures. Minor control deviation, sensor spoofing event can also cause the thermal chain reactions, chemical leaks, or equipment failing. Most particularly, lithium ion systems easily become overcharged which easily decomposes electrolyte, generates gases and finally ignites. Over pressure, valve damage or even toxic gas release risk due to operating beyond catalytic threshold is similar to that of ammonia fuel cells.

The proposed framework is addressed for these risks through real time chemical monitoring, cross sensor validation, and ML based anomaly detection that are integrated into BMS and fuel cell controllers. It allows the system to not only detect faulty inputs, but run the sensor fusion outputs against what physically expects to occur in order to verify that the data is indeed possible. Mutual authentication of the commands' communication via TLS with both types of command forces only authorized commands to be executed at endpoints of control point. Furthermore, the distributed architecture allows local control units to be autonomous to override or isolate compromised subsystems such as overriding lithium ion batteries from charging or forced venting of ammonia system if they are required to be isolated or bypassed other than EMS' instructions. As such, the system becomes both horizontally and vertically resilient: resilient with respect to the coordination of subsystems and resilient with respect to layering of defense within each subsystem.

Finally, the secure communication and local decision making is secured to such an extent that chemical storages become self defending, robust units in smart grid environment. This is a required advancement in next generations energy security design as it guarantees that system availability and chemical safety is maintained regardless of sophisticated, multivector cyber attack.

6. Conclusion and Future Work

This research presented a comprehensive framework of the chemical energy storage system (C-ESS) cyber physical security for C-ESS used in smart renewable energy grids. The growing effectiveness of lithiumion batteries, ammonia fuel cells and hybrid chemicalthermal storage devices were acknowledged in the study and also the challenges of chemical safety and operation reliability for targets that are subjected to sophisticated cyber threats. To demonstrate that the framework is capable of resisting data manipulation attack, denial of service attack, sensor spoofing, and multi point coordinated attack, we developed a multi layered architecture with the first layer of machine learning–based intrusion detection, the second layer of encrypted communication protocols, the third layer of real time process monitoring, and the fourth layer of autonomous control logic. Through both quantitative simulation, and establishment through experiments, the proposed framework not only restored System functionality during attacks, but also maintained critical chemical thresholds (i.e. thermal stability, pressure containment, electrochemical efficiency), without requiring manual intervention. It was a critical capability in preventing cyber propagations to physical hazards using a secure communication integrated with chemical state awareness.

Firstly, this study stresses a shift of paradigm for the security of smart grid from the protection of data and communication layer to protecting every chemical and physical control in energy systems. Resilience, self defense, decision making, isolation and recovery can be afforded to storage units to enable them to participate in maintaining grid wide reliability and sustainability. This work importantly offers novel means of domain crossing in cybersecurity, chemical engineering and control systems domains.

By extension to hydrogen storage systems and flow batteries, we propose in future work to expand the framework for use with additional chemical and operational complexities of the other energy storage chemistries we consider. In addition to this, implementing hardware in the loop (HIL) testing of real time embedded devices to test under real world latency and hardware constraint environment will be further developed. In addition, the blockchain can figure as a promising way for increasing integrity and trust in the distributed data of such environments, providing decentralized trust management and validated trusted energy transaction in the EMS layer. Lastly, industrial partners and grid operators will collaborate with the framework to adapt this to real deployment ready prototypes for the secure-by-design integration of storage into future smart energy infrastructures.

References

[1] M. U. Saleem, M. R. Usman, M. A. Usman, and C. Politis, "Design, Deployment and Performance Evaluation of an IoT Based Smart Energy Management System for Demand Side Management in Smart Grid," *IEEE Access*, vol. 10, pp. 11249–11261, Jan. 2022, doi: 10.1109/ACCESS.2022.3147484.

[2] Y. Wan et al., "An Integrated Cyber-Physical Simulation Environment for Smart Grid Applications," *Tsinghua Science and Technology*, vol. 19, no. 2, pp. 133–143, Apr. 2014.

[3] P. Romanos, E. Voumvoulakis, C. N. Markides, and N. Hatziargyriou, "Thermal Energy Storage Contribution to the Economic Dispatch of Island Power Systems," *CSEE Journal of Power and Energy Systems*, vol. 6, no. 1, pp. 100–110, Mar. 2020, doi: 10.17775/CSEEJPES.2019.00610.

[4] P. Eder-Neuhauser, T. Zseby, and J. Fabini, "Resilience and Security: A Qualitative Survey of Urban Smart Grid Architectures," *IEEE Access*, vol. 4, pp. 2215–2238, 2016, doi: 10.1109/ACCESS.2016.2531279.

[5] M. Khalaf et al., "A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids," *IEEE Access*, vol. 12, pp. 21345–21372, 2024, doi: 10.1109/ACCESS.2024.3364362.

[6] B. B. McKeon, J. Furukawa, and S. Fenstermacher, "Advanced Lead–Acid Batteries and the Development of Grid-Scale Energy Storage Systems," *Proceedings of the IEEE*, vol. 102, no. 6, pp. 951–963, Jun. 2014, doi: 10.1109/JPROC.2014.2316823.

[7] X. Li and S. Wang, "Energy Management and Operational Control Methods for Grid Battery Energy Storage Systems," *CSEE Journal of Power and Energy Systems*, vol. 7, no. 5, pp. 1026–1040, Sept. 2021, doi: 10.17775/CSEEJPES.2019.00160.

[8] J. Li et al., "Optimal Operation with Dynamic Partitioning Strategy for Centralized Shared Energy Storage Station with Integration of Large-scale Renewable Energy," *Journal of Modern Power Systems and Clean Energy*, vol. 12, no. 2, pp. 359–370, Mar. 2024, doi: 10.35833/MPCE.2023.000345.

[9] H. Li, H. Yuan, S. He, and Y. Zhou, "Design of Battery Management System for Grid Energy Storage Based on FreeRTOS and RTDS Testing System," *IEEE Access*, vol. 13, pp. 43414–43423, 2025, doi: 10.1109/ACCESS.2025.3548785.

[10] B. Chegari, M. Tabaa, E. Simeu, and M. El Ganaoui, "Optimal Energy Management of a Hybrid System Composed of PV, Wind Turbine, Pumped Hydropower Storage, and Battery Storage to Achieve a Complete Energy Self-Sufficiency in Residential Buildings," *IEEE Access*, vol. 12, pp. 126624–126639, 2024, doi: 10.1109/ACCESS.2024.3454149.

[11] T. O. Trifonov, "Coordination of Battery Energy Storage and Power-to-Gas in Distribution Systems," *Protection and Control of Modern Power Systems*, vol. 2, no. 4, pp. 1–8, Oct. 2017, doi: 10.1186/s41601-017-0072-y.

[12] A. M. Al-Ghaili et al., "A Systematic Review on Demand Response Role Toward Sustainable Energy in the Smart Grids-Adopted Buildings Sector," *IEEE Access*, vol. 11, pp. 64968–65027, 2023, doi: 10.1109/ACCESS.2023.3287641.

[13] M. A. Syed, O. Siddiqui, M. Kazerani, and M. Khalid, "Analysis and Modeling of Direct Ammonia Fuel Cells for Solar and Wind Power Leveling in Smart Grid Applications," *IEEE Access*, vol. 12, pp. 46512–46523, 2024, doi: 10.1109/ACCESS.2024.3376513.

[14] M. Wicke and T. Bocklisch, "Hierarchical Energy Management of Hybrid Battery Storage Systems for PV Capacity Firming and Spot Market Trading Considering Degradation Costs," *IEEE Access*, vol. 12, pp. 52669–52686, 2024, doi: 10.1109/ACCESS.2024.3387748.

[15] S. Abbas et al., "Improving Smart Grids Security: An Active Learning Approach for Smart Grid-Based Energy Theft Detection," *IEEE Access*, vol. 12, pp. 1706–1720, 2024, doi: 10.1109/ACCESS.2023.3346327.

[16] X. Yu and Y. Xue, "Smart Grids: A Cyber–Physical Systems Perspective," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016, doi: 10.1109/JPROC.2015.2503119.

[17] P. A. Oyewole and D. Jayaweera, "Power System Security With Cyber-Physical Power System Operation," *IEEE Access*, vol. 8, pp. 179955–179973, 2020, doi: 10.1109/ACCESS.2020.3028222.

[18] K. L. Keung, C. K. M. Lee, P. Ji, and K. K. H. Ng, "Cloud-Based Cyber-Physical Robotic Mobile Fulfillment Systems: A Case Study of Collision Avoidance," *IEEE Access*, vol. 8, pp. 89318–89332, 2020, doi: 10.1109/ACCESS.2020.2992475.

[19] M. Abdelmalak, V. Venkataramanan, and R. Macwan, "A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems," *IEEE Access*, vol. 10, pp. 99875–99895, 2022, doi: