**Slide 1 Title:**  
Good Morning/Afternoon panel members and fellow students today I am presenting our collaborative paper on ‘Adversarial Attacks on Battery Energy Storage Systems Using Physics-Based Models in PyBaMM’.

**Slide 2 Motivation:**

In 2025 DHS warned of escalating threats to US critical infrastructure and earlier this year Australian signal directorate put out a vulnerability assessment of Russian military cyber actors targeting global critical infrastructure. What do both articles have in common? They both list Battery Energy Storage Systems or BESS as critical infrastructure under risk of attack.

This is why motivation for this research stems from the increasing risk of cyber-attacks on energy systems. BESS are a key part critical infrastructure, but their vulnerabilities to adversarial attacks haven’t been fully explored. Using the physics-based model PyBaMM, we can accurately simulate the internal behaviour of batteries under attack Allowing for a better understanding how adversarial attacks impact key battery metrics aiming to improve the robustness of these models.

**Slide 3 Importance:**  
BESS are at the forefront for modern energy infrastructure. They play a critical role in supporting renewable energy integration, maintaining grid stability, and powering electric vehicles. Adversarial attacks on BESS can manipulate key battery metrics like SoC and SoH potentially leading to system failures, safety risks, and even faster battery degradation.

We examine how the attacks directly affect the parameters they are targeting, such as disrupting current flow or altering voltage behavior. This research aims to provide valuable insights into how adversarial manipulations can compromise the performance, safety, and long-term resilience of BESS.

The research offers a unique approach by combining the physics-based model PyBaMM with machine learning models. This combination allows us to explore adversarial attacks in a more comprehensive way. By integrating these two models, we can address both the physical vulnerabilities that come from the battery’s electrochemical processes and the cyber vulnerabilities present in the machine learning models.

This approach not only increases the accuracy of predictions for battery metrics such as SoC and SoH under adversarial conditions but also enhances the system's overall resilience. This is particularly crucial for real-world applications where ensuring reliable and secure battery operation is critical.

**Slide 4 Current Gaps:**

Existing literature on BESS primarily focuses on improving performance under normal operating conditions. However, there's a significant gap when it comes to understanding how these systems respond to adversarial attacks.

Most current models don't account for the nonlinear dynamics that arise during such attacks, leaving a critical vulnerability in performance under attack conditions.

Additionally, while machine learning models are used for battery management, there is limited exploration into how adversarial attacks on these models, combined with physical vulnerabilities, could lead to increased system failures.

There's a lack of available models capable of simulating these kinds of attacks. Physics-based models like PyBaMM accurately represent battery behaviour but their application to adversarial scenarios remains underexplored.

In addition to the lack of models, there is also a shortage of suitable datasets for machine learning applications. Many existing datasets are either designed for clean data applications or are proprietary and unlabelled, making it difficult to simulate real-world adversarial attack scenarios. This lack of adversarial data limits the ability to train and test models under conditions that more accurately reflect how BESS would respond to cyber-physical threats.

**Slide 5 Objectives:**

The goal of our research is to expose and analyze vulnerabilities in BESS by simulating adversarial attacks. Specifically, we focus on attacks targeting critical parameters such as current, voltage, temperature, and SEI resistance. By leveraging the Doyle-Fuller-Newman (DFN) model within the PyBaMM framework, we can simulate these adversarial scenarios with high accuracy and observe how they affect key battery metrics.

This semester, I’ve collaborated with Alaa Selim with the goal of producing a research paper

Our aim is to submit this paper to the journals Advances in Electrical Engineering, Electronics and Energy or journal of energy storage. We believe submitting to this journal will validate the novelty of our work and offer a new underutilized approach to BESS systems.

**Slide 6 DFN Model:**  
The Doyle-Fuller-Newman (DFN) model is a well-established electrochemical model that provides a detailed simulation of lithium-ion battery behavior. It simulates interactions between the solid and electrolyte phases, accounting for lithium diffusion and potential distribution across the battery. By representing both the solid-phase lithium-ion concentration and the electrolyte phase, the DFN model captures key dynamics that are crucial for understanding battery performance.

We use the DFN model because it offers a physics-based, detailed view of battery processes, which is essential for simulating adversarial attacks. Unlike simpler models, it can accurately reflect the non-linear behaviors that occur under attack conditions, such as unexpected changes in voltage, temperature, and resistance. This makes it ideal for our research, where precision and realism are key.

The DFN model governs important metrics such as SoC and SoH which are the same metrics that adversarial attacks aim to compromise, making the DFN model indispensable for accurately assessing the impact of such attacks.

By integrating the DFN model with PyBaMM, we can simulate realistic perturbations in parameters like current, voltage, temperature, and SEI resistance. This allows us to study how adversarial manipulations affect not only the metrics we observe but also the underlying electrochemical processes within the battery.

**Slide 7 Key Equations:**

These equations are central to the DFN model, which we use to simulate the battery's electrochemical processes.

The first equation governs the diffusion of lithium ions within the solid particles of the electrode. When attacks manipulate the current, they induce non-uniform diffusion of lithium ions, leading to inaccurate predictions of SoC.

The second equation focuses on lithium-ion transport in the electrolyte. A temperature attack could disrupt this transport, which is crucial for the accurate estimation of SoH.

The solid-phase potential equation describes how current flows through the electrode. attacks that manipulate current inputs can lead to miscalculations of the battery’s electrochemical state, affecting both performance and safety.

The electrolyte-phase potential is highly sensitive to temperature changes. A temperature spike can significantly alter the electrolyte's potential, causing voltage deviations that compromise system stability.

Finally, the Butler-Volmer kinetics equation governs the reaction rates at the electrode-electrolyte interface. attacks can disrupt these reaction kinetics, which in turn degrades the battery's performance and accelerates wear over time.

**Slide 8 Simulating Adversarial Attacks Overview:**

We introduced several types of adversarial attacks targeting different battery parameters. These attacks are not applied abruptly but are introduced gradually to mimic a more realistic scenario, where adversarial attacks would slowly build up over time.

To simulate these adversarial attacks, we use time-dependent equations for each attack.

For current we modify the current using the equation [REFER TO EQUATION]

where gamma ensures that the attack is gradually applied during the defined time window, avoiding abrupt changes that may be easily detected.

For temperature manipulation, we a temperature spike during the attack period [REFER TO EQUATION] where Delta T represents the change in temperature, affecting the battery's chemical reactions and possibly causing thermal runaway or degradation.

The SEI resistance attack increases the internal resistance of the battery over time [REFER TO EQUATION] This increase in resistance leads to greater voltage drops and reduced energy efficiency, impacting both SoH and the overall battery performance.

SoC is determined by integrating the current over time, reflecting the amount of charge remaining in the battery.

Similarly, SoH which represents the overall condition and capacity retention of the battery, is influenced by the battery's voltage and internal resistance.

Each of the parameters are explained.

**Slide 10/11/12 Methodology:**

The battery system is modelled using PyBaMM for the DFN model.

The battery parameters are defined, including the key inputs, followed by setting the electrochemical properties, which govern diffusion, concentration, and potentials.

The governing equations of the DFN model are then set.

Once the model is established, the initial conditions are set, and we also run baseline calculations to get the initial values for SoC and SoH. After that, calibration and validation are performed to ensure that our model behaves as expected

Next, we introduce adversarial perturbations. These involve attacks on different parameters of the battery system. Each type of attack is modelled individually, and then can be combine them to simulate complex, real-world attack scenarios.

Next is the simulation phase, where we run the battery's response to these adversarial conditions using PyBaMM. During this phase, key metrics are monitored and recorded.

Lastly, we analyse the results, focusing on the battery's system stability and long-term impact of these attacks. The results help us assess how well the system holds up against these attacks and allows us to uncover critical vulnerabilities and propose more robust defences against adversarial attacks.

**Slide 12 Simulation Settings:**  
We assumed a nominal discharge current of 2A. The initial SoC was set at 80%, which is a commonly observed value in battery applications. We maintained a constant temperature of 298.15Kduring the normal operation phase.

Additionally, the baseline SEI resistance is set at 1 × 10⁻³ Ω·m², which is a typical value observed in lithium-ion batteries and electrolyte concentration, we assumed a uniform distribution across the battery.

The adversarial attack window was defined between 100 and 200 seconds in which intensity of the attacks increased smoothly, reached a peak, and then gradually decreased, to mimic realistic attack scenarios and assess their impact on battery performance.

**Slide 13 Data Input and Attack Parameters:**

For current perturbation, we started with an initial amplitude of 0.005A and gradually increased it by 0.02A per second during the attack window.

For voltage attacks, we introduced a deviation of 0.01V from the baseline voltage, simulating errors in the voltage readings.

The temperature manipulation involved spiking the temperature up to 308K during the attack, which reflects a typical thermal degradation scenario.

For the SEI resistance attack, we gradually increased the resistivity within the window, causing a spike that directly impacts internal resistance, leading to voltage drops and degraded performance.

Our optimization goal was to maximise the deviation in the terminal voltage, as it serves as a key indicator of battery health and performance. To achieve this, we used the L-BFGS-B algorithm initially but switched to the solver, *pybamm.CasadiSolver()*, efficiently handles the dynamics of the system

This allowed us to control the amplitude and rate of the attack, ensuring that they remained within safe operational boundaries while still having a significant impact on the battery metrics.

**Slide 14/15 Results:**

we observe the impact of different adversarial attacks on the battery system’s behavior. Additionally, the small attack window, in combination with realistic system noise, adds complexity to the analysis, making the results more representative of real-world conditions.

the current behavior under a combined noise attack is shown Initially, the current remains steady at around 3 A under normal conditions. However, during the small attack window, we see rapid fluctuations in the current, reaching a peak of nearly 6 A. this attack causes instability however the current returns to its nominal value once the attack ends. the attack affects the current only within the attack window, yet these spikes still pose a threat due to the stress they introduce into the system which is reflecting in degradation of the voltage

The temperature behavior subject the same combined attack under normal conditions, the temperature remains stable at approximately 298 K. When the attack is introduced, there are noticeable spikes in temperature, reaching around 301 K. Although the system shows signs of recovery, returning to its base temperature after each spike, these disturbances during the attack induce wear on the battery system in the long term.

The voltage figure shows a small deviation in voltage during the attack phase, particularly around the 200-second mark where the attack begins. This slight dip in voltage, followed by a decline, shows that the battery is attempting to recover after the attack but continues to lose voltage slowly over time. highlights the cumulative degradation the battery undergoes as the attack progresses for a single attack window

**Slide 14/15 Results:**

For multiple attack windows temperature, The temperature exceeds 300 K several times as noise is injected. The continuous and repeated spikes lead to thermal stress on the battery, which can shorten its lifespan.

The current behavior over multiple attack window has focused on the repeated current spikes. Each attack window introduces distinct spikes in the current, peaking at around 4 A multiple times during the simulation. This behavior illustrates how repeated current fluctuations could lead to inefficiencies or damage over time, as the battery is subjected to continual stress during each attack window.

The second figure provides a clearer depiction of the impact of multiple attack windows. The voltage curve shows distinct dips corresponding to each attack window, with the most significant collapse occurring between the 400- and 600-second range. During this period, the voltage drops sharply and fails to stabilize, leading to a complete collapse towards the end of the simulation.

The presence of multiple attack windows is a key reason for the larger deviation in voltage seen in the results. Each subsequent attack window adds stress to the system, compounding the voltage collapse and further destabilizing the battery.

**Slide 15 Critique Analysis:**

The results clearly show that adversarial attacks have a severe impact on the stability of BESS, particularly in voltage collapse scenarios. Sensor-based attacks make models highly vulnerable to voltage collapse, which we can see in the results where the adversarial attacks drastically reduce the terminal voltage.

The consequences of these attacks are not limited to voltage alone. Both SoC and SoH metrics are impacted, which in turn affects the battery’s health and efficiency, and this has direct implications for grid-level decision-making. The combined attacks, where multiple sensors like current, temperature, and SEI resistance are attacked simultaneously, demonstrate a significant deviation in the voltage curve. The voltage curve undergoes a sharp decline, particularly under extended attack windows, indicating a faster degradation of the system.

Moreover, the spike in the attack timing plays a crucial role in attack readiness. By targeting specific periods with increased spikes, the adversarial influence becomes even more severe, amplifying the destabilization of the battery. These prolonged and spiked attacks lead to quicker deterioration of battery performance and escalate the risk of grid instability.

**Slide 16 Future Research: Slide 16 Future Research:**

Future research will focus on three main areas

The first thing that can be conducted is the development real-time detection mechanisms for adversarial attacks. The goal is to create algorithms capable of detecting and flagging abnormal battery behaviour as soon as an attack begins. These detection mechanisms will be integrated directly into BMS, allowing for rapid response and mitigation of potential risks.

The first thing that can be conducted is the development real-time detection mechanisms for adversarial attacks. The goal is to create algorithms capable of detecting and flagging abnormal battery behaviour as soon as an attack begins. These detection mechanisms will be integrated directly into BMS, allowing for rapid response and mitigation of potential risks.

Second, is the expansion to different battery chemistries. While this research focuses on lithium-ion batteries, which are widely used, other chemistries such as solid-state batteries and flow batteries are gaining attention for future applications. Exploring how adversarial attacks impact these types of batteries will provide a broader understanding of the vulnerabilities across different energy storage technologies. Second, is the expansion to different battery chemistries. While this research focuses on lithium-ion batteries, which are widely used, other chemistries such as solid-state batteries and flow batteries are gaining attention for future applications. Exploring how adversarial attacks impact these types of batteries will provide a broader understanding of the vulnerabilities across different energy storage technologies.

Lastly, enhancement of the robustness of the models to better withstand complex, coordinated attacks. By improving model resilience, we can help ensure that future battery systems are better protected against sophisticated cyber-physical threats.

Future research will focus on three main areas

Lastly, enhancement of the robustness of the models to better withstand complex, coordinated attacks. By improving model resilience, we can help ensure that future battery systems are better protected against sophisticated cyber

Lastly, enhancement of the robustness of the models to better withstand complex, coordinated attacks. By improving model resilience, we can help ensure that future battery systems are better protected against sophisticated cyber-physical threats.

Lastly, enhancement of the robustness of the models to better withstand complex, coordinated attacks. By improving model resilience, we can help ensure that future battery systems are better protected against sophisticated cyber-physical threats.

The first thing that can be conducted is the development real-time detection mechanisms for adversarial attacks. The goal is to create algorithms capable of detecting and flagging abnormal battery behaviour as soon as an attack begins. These detection mechanisms will be integrated directly into BMS, allowing for rapid response and mitigation of potential risks.

Second, is the expansion to different battery chemistries. While this research focuses on lithium-ion batteries, which are widely used, other chemistries such as solid-state batteries and flow batteries are gaining attention for future applications. Exploring how adversarial attacks impact these types of batteries will provide a broader understanding of the vulnerabilities across different energy storage technologies.

Lastly, enhancement of the robustness of the models to better withstand complex, coordinated attacks. By improving model resilience, we can help ensure that future battery systems are better protected against sophisticated cyber-physical threats.

Slide 20 Conclusions:  
This research demonstrates that adversarial attacks on BESS can severely disrupt key battery metrics such as SoC and SoH. These attacks can not only degrade battery life but also destabilise the entire system, leading to potential failures.

The results highlight the urgent need for improved defences in these systems.