Securing Marine Renewable Energy Systems : Understanding Cyber-Physical Threats and Evaluating Consequences via Hardware-in-the-Loop

Sasha Fung, Carter Nichols, Yufei Tang, James VanZwieten
Florida Atlantic University

Hardware-in-the-loop simulation efficiently demonstrates the impact of cyber-physical attacks on an marine current turbine island microgrid

OVERVIEW

This paper addresses the cybersecurity challenges of marine renewable energy systems, focusing on Marine Current Turbines (MCTs). It explores cyber-physical threats, including tampering with industrial control systems and falsifying sensor data, using a man-in-the-middle attack model and hardware-in-the-loop (HIL) simulation to demonstrate real-time impacts on energy production and grid stability.

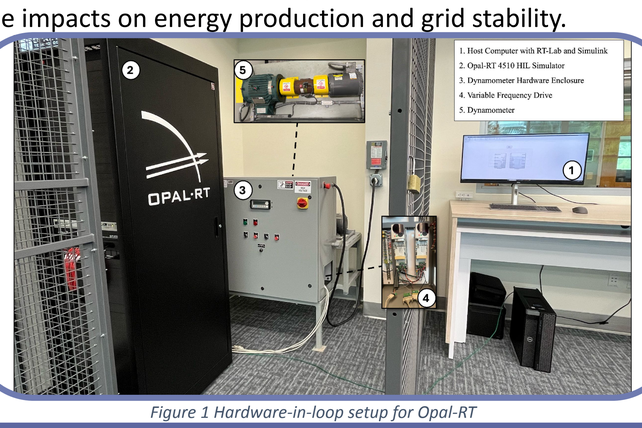

Figure 1 Hardware-in-loop setup for Opal-RT

SIMULATION MODEL

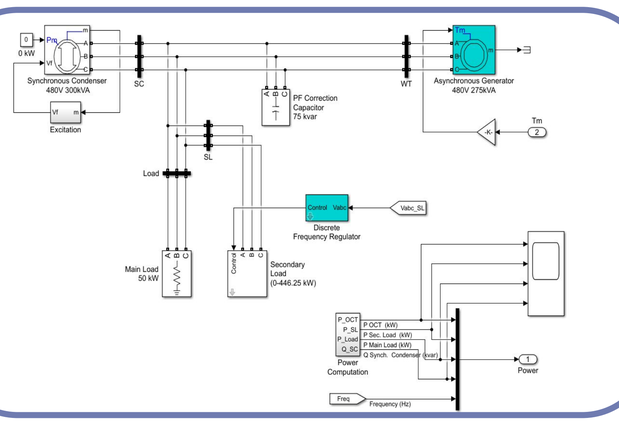

Figure 2 RT-Lab Simulink master subsystem

ATTACK TYPES

MAN IN THE MIDDLE

MITM attacks intercept and alter communication without needing administrative access, making intrusion easier. MITM attack is used to manipulate control parameter signals going into a PID controller which manipulates the blade pitch of the turbine

FALSE DATA INJECTION

The FDI attack is executed by injecting an attack vector *a* into the measurement vector *z*, creating a compromised measurement *z'* as follows:

$$z' = z + a$$

RESULTS

Case 1: Oscillating Blade Pitch

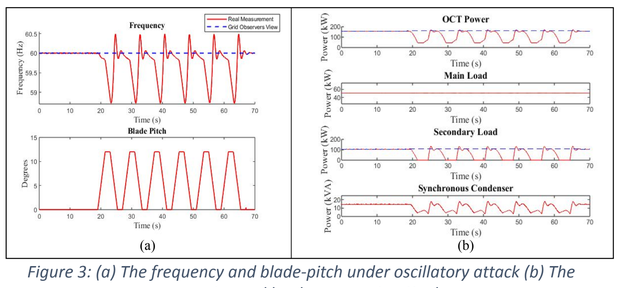

Figure 3: (a) The frequency and blade-pitch under oscillatory attack (b) The generator and load response to attack

The power quality is affected during this attack (right), seen by the Total Harmonic Distortion (THD). Prior to the attack, the THD on the output current of the generator is -93.46dB (0.002%). During the attack, a 15x increase to -70.27dB (0.03%) is observed.

In 3a (left), oscillations in blade pitch can be observed starting at 19s. The frequency oscillates with the blade pitch, as does the MCT (3b). This can cause damage to the rotor and create instability in the grid. The grid observations are shown as normal, signifying a stealth attack.

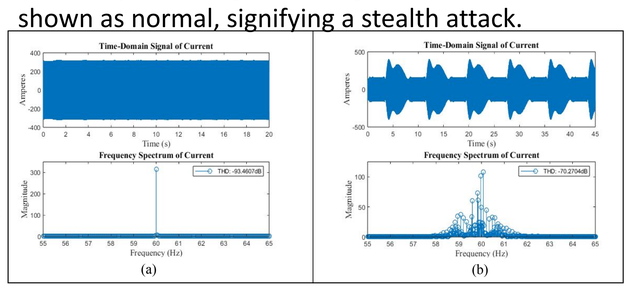

Figure 4: (a) Total Harmonic distortion without attack; (b) Total harmonic distortion with attack

Case 2 : Decreasing Blade Pitch

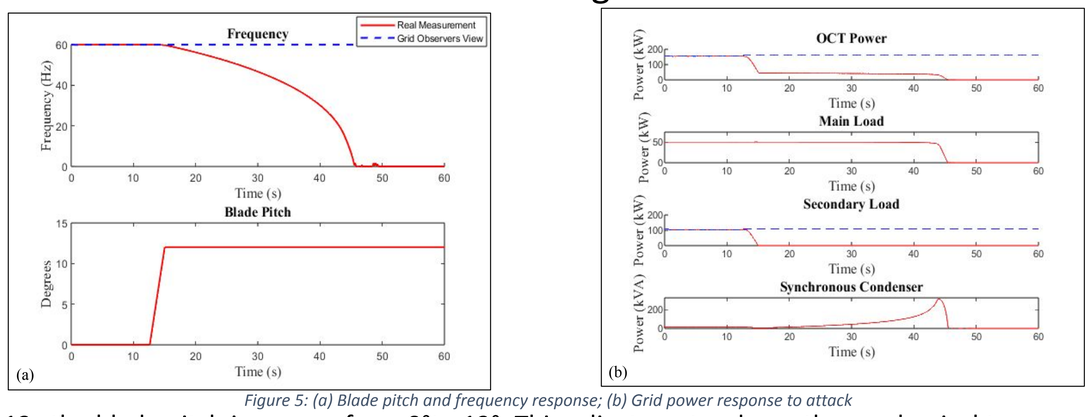

Figure 5: (a) Blade pitch and frequency response; (b) Grid power response to attack

At 12s the blade pitch increases from 0°to 12°. This adjustment reduces the mechanical torque on the rotor, resulting in insufficient power generation. Following the attack, the MCT power, (5b), decreased from 160 kW to about 48kW and then gradually reduces, until ultimately crashing.

ATTACK SCENARIO

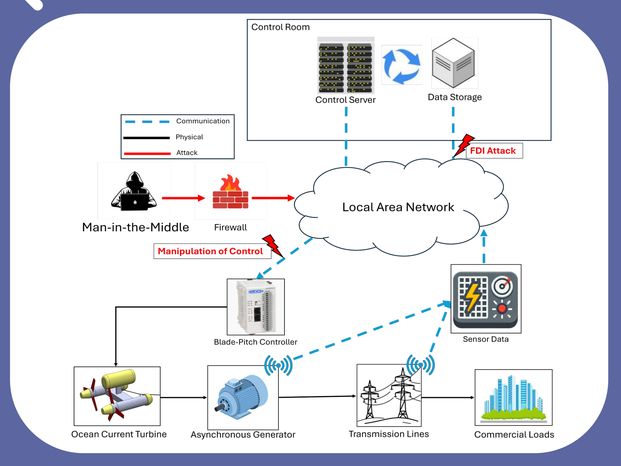

Figure 3 MITM Attack Scenario Flow Chart

CONCLUSION

This study demonstrated the impact of cyber-physical attacks on a microgrid connected to an marine current turbine using hardware-in-the-loop simulation with Simulink. Coordinated attacks on the blade pitch controller and false data injection attacks were shown to cause instability and potential failures in energy management systems. The HIL platform proved to be efficient and reliable, allowing realistic and repeatable testing without the risks and costs of in situ testing. These experiments highlighted the need for enhanced security measures in marine energy systems. Future work will focus on developing data-driven attack detection and fault-tolerant controllers to improve resilience

CONTACT

sfung2017@fau.edu