

Kennesaw State University

DigitalCommons@Kennesaw State University

Symposium of Student Scholars

A Low-Cost, low-power, SCADA Testbed Solution for Secure Remote Monitoring

Connor Berger

Follow this and additional works at: <https://digitalcommons.kennesaw.edu/undergradsymposiumksu>



Part of the [Electrical and Electronics Commons](#), [Other Electrical and Computer Engineering Commons](#), and the [Technology and Innovation Commons](#)

Berger, Connor, "A Low-Cost, low-power, SCADA Testbed Solution for Secure Remote Monitoring" (2022). *Symposium of Student Scholars*. 130.

<https://digitalcommons.kennesaw.edu/undergradsymposiumksu/Fall2022/presentations/130>

This Poster is brought to you for free and open access by the Office of Undergraduate Research at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Symposium of Student Scholars by an authorized administrator of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

A Low-Cost, low-power, SCADA Testbed Solution for Secure Remote Monitoring

Authors: Connor D. Berger*, Soin Traore – Co-author

Advisors: Dr. Maria Valero, Dr. Liang Zhao

Introduction: Similar to software application systems adopted by companies and businesses for product logging, payroll, human resources, Supervisory Control and Data Acquisition (SCADA) systems control the distributed processes with multiple components located on different machines that communicate and coordinate actions in order to appear as a single coherent system. SCADA systems severely lack the appropriate security and hack prevention measures. We propose a low cost, low power SCADA testbed solution for secure remote monitoring. The goal of this research is to implement and test the testbed's security by emulating attack vectors on both hardware components and communication channels to probe the system for weaknesses.

Materials and Methods: SCADA systems are comprised of 4 components. The Field Instrumentation Devices (FID) which consist of sensors and actuators connected to distributed processes [2 Voltage, 1 current sensor]. The Remote Terminal Unit (RTU) usually microcontrollers receiving and sending the remotely gathered data [ESP32Thing Microcontroller]. The Master Terminal Unit (MTU) where acquired data is processed and displayed [Thingier.io IoT Platform]. Finally, the Communication Channel (COM Channel) providing connection between the RTUs and MTUs [D-Link Wi-Fi Router]. We have connected our testbed to a small Solar Panel 10W 12V. We intend to remotely monitor the system, while attempting to break through security measures set in place i.e. (User and device authentication, network connection to cloud server).

Conclusions: We have set up the testbed per methods detailed in [1]. Development of low-cost, low-power SCADA testbed solution to demonstrate secure and remote monitoring of a small PV system. Moving forward, penetration tests will be performed to enhance the security of these systems. We hope our findings inspire others in the future to further develop SCADA security for hardware and software applications. Besides, our work promotes awareness and overall knowledge level of SCADA systems.