AN INTERNET-BASED REMOTE COMMAND AND TELEMETRY SYSTEM FOR A MICROWAVE PROPAGATION STUDY

Mario Colapelle, Brian Zamore, Brian Kopp
Electrical Engineering Department
University of North Florida
Jacksonville, Florida, 32224
Brian.kopp@unf.edu

Randy Pierce
Intelligent Transportation Systems Office
Florida Department of Transportation
Tallahassee, Florida, 32301
Randy.Pierce@dot.state.fl.us

ABSTRACT

A research project investigating microwave radio frequency propagation in a 500 mile link across the Gulf of Mexico requires a remote-control process to command microcontroller-based devices including power control modules and antenna feedhorn positioners, and to telemeter system parameters back to the operators. The solution that was developed is a simple, webserver-based user-interface that can be accessed both locally and remotely via the internet. To interface the webservers with the microcontroller-based devices, a polling protocol, based on MODBUS, was developed that provides an efficient command and telemetry link over a serial RS-485 interface.

KEY WORDS

Command, telemetry, MODBUS, webserver, internet.

INTRODUCTION

This paper discusses the remote command and telemetry process under development at the University of North Florida (UNF), in support of a joint-research project with the Intelligent Transportation Systems (ITS) office of the Florida Department of Transportation (FDOT). The background section discusses the purpose and design of the research project and the need for remote command and telemetry. The design of the test stands is presented next and then the Telemetry and Command (T&C) requirements are discussed. There are multiple devices that can

be commanded and have their status telemetered. These are reviewed in the T&C section of the paper. A brief discussion on off-the-shelf protocols that were reviewed and considered for use in the project is presented next. This is followed by a discussion of the serial protocol that was ultimately developed by UNF and used in the project. The paper concludes with a discussion on the status of the project.

BACKGROUND

The University of North Florida and the ITS office of the FDOT are conducting a study to investigate the feasibility of using the atmospheric evaporative duct at sea-level to create a communications link across the Gulf of Mexico between Key West and Destin, Florida, a distance of 500 miles. It is hoped a reliable enough link can be established to offer some data network redundancy to the single points of failure that the FDOT's statewide ITS network has along the Florida Keys and Florida panhandle. The first phase of this project is underway and involves a propagation study at 5 and 10 Giga-Hertz (GHz) to assess the suitability of the evaporative duct over a long period of time.

To implement the propagation study, a transmitter is being constructed for deployment at Naval Air Station (NAS), Key West and a receiver is being constructed for deployment at Henderson Beach State Park in Destin Florida. The transmitter will be capable of transmitting Continuous Wave (CW) signals and modulated signals for the study. Software Defined Radios (SDR) will be used to transmit and receive the test signals. Microwave component up-conversion and down-conversion will permit propagation studies at 5 and 10 GHz. Large prime focus 2.4 meter dish antennas mounted at a height of approximately 30 feet will launch and capture the microwave signals into and out of the evaporative duct, at an elevation angle near zero degrees and an azimuth that matches Key West with Destin.

The propagation tests will be conducted over a long duration period of at least 6 months to evaluate seasonal and environmental effects on propagation. Remote operation of the transmitter and receiver will be necessary to support the testing in a cost effective manner. Students in the UNF Advanced Telecommunications Research Program (ATRP) will conduct the propagation tests from the ATRP lab at UNF in Jacksonville, Florida. Internet connectivity at the ATRP lab will be used to remotely operate the transmitter and receiver test stands. The test stands are being constructed on communications trailers provided by the FDOT and will use cellular modems for internet connectivity. Both test stands must be similar in design to reduce design risk and cost. Mains power is anticipated to be available at the NAS Key West transmitter site but will not be available at the Destin receiver site, at Henderson Beach State Park in Destin. Due to the power limitations at Destin, and the need to use similar designs, the overall design used by both test stands will therefore be power efficient.

TEST STAND DESIGN

In combination, the two test stands form a complete communications link. The transmitter test stand uses an SDR radio that is controlled by a mini Personal Computer (PC). The mini PC is

remotely controlled through the internet using a commercial remote, computer-control, software package. A cellular modem/router provides the internet connection. The mini PC has a dual-port Network Interface Card (NIC) to interface directly with the SDR and also connect to the internet via Ethernet. Mathworks Simulink simulates the transmitter source and receiver sink on the mini PCs and controls the interfaces with the SDRs.

The SDRs use a first Intermediate Frequency (IF) of 270 Mega-Hertz (MHz). A second IF of 1020 MHz is used in between the first IF and the two selectable RF frequencies of either 5840 MHz or 10250 MHz. The SDRs and the IF and RF oscillators are all disciplined with a 10 MHz reference provided by a Global Positioning Satellite (GPS) receiver on each test stand. The SDR and mini PC equipment are housed in an insulated enclosure on the FDOT provided trailers. The second IF and RF microwave equipment are housed in a tower mounted enclosure behind the antennas to keep the RF cable runs short. The large antennas are mounted on combination azimuth and elevation rotors, controlled via an Ethernet connected controller housed with the mini PC and SDR at the bottom of the towers. Figure 1 contains a high level schematic of the communications architecture on the transmitter test stand. The receiver test stand communications architecture is nearly identical to the transmitter test stand, with the exception that there is no transmit power meter in the up-tower components.

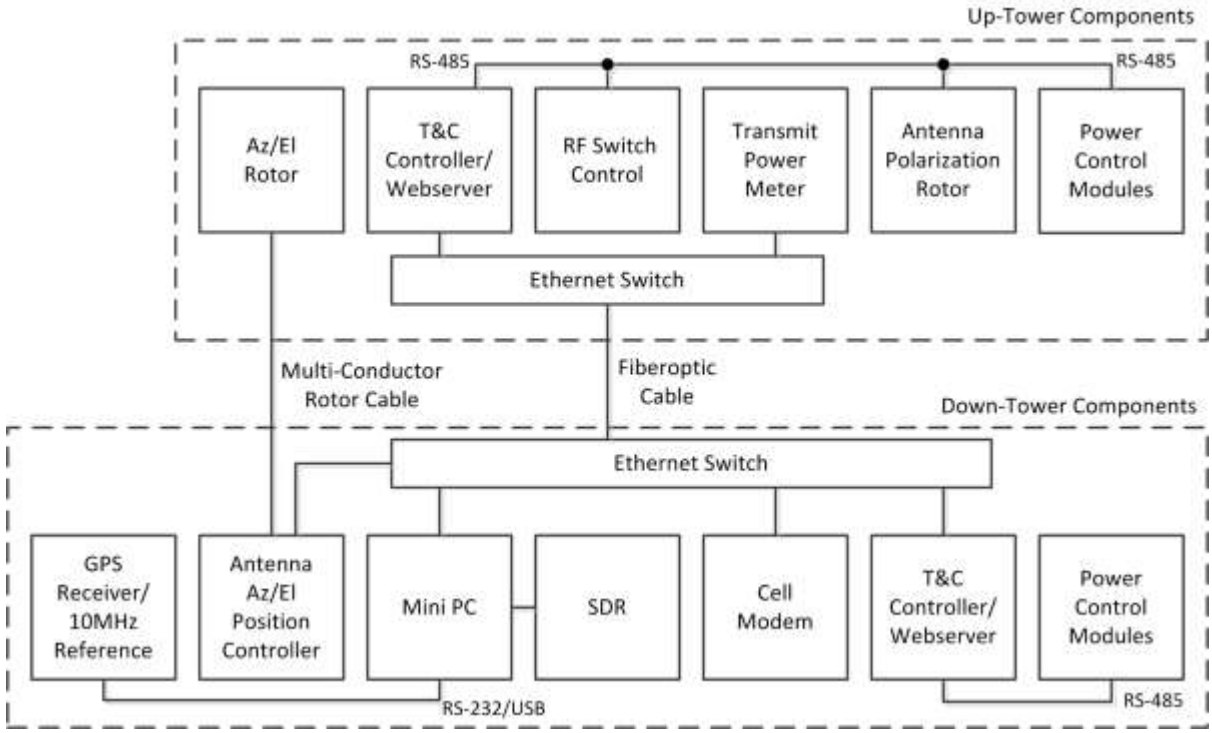

Figure 1. Transmitter test stand communications architecture.

The feedhorns on the prime focus antennas have dual linearly polarized feeds, one matched to 5840 MHz and the other to 10250 MHz. Polarization rotation by the evaporative duct is one parameter that will be studied in this project. Rotating the linear transmit and receive feedhorns will facilitate this investigation. The feeds will be mounted on a UNF designed polarization rotor

assembly that uses a stepper motor. A motor control interface is being designed to connect the T&C controller to the polarization rotor assembly.

TELEMETRY AND COMMAND REQUIREMENTS

The use of the internet and the Ethernet Local Area Network (LAN) on the test stands will provide remote access from the ATRP lab at UNF to the mini PCs on the test stands. Most of the remaining devices on the test stands will be controlled via the LAN from the mini PC during tests. The mini PC will use vendor software to interface with the antenna azimuth and elevation position controller and the Transmit Power Meter via the LAN. To monitor and command many of the other devices on the test stand that do not have built in Ethernet capability a T&C controller is being developed.

The T&C controller serves two purposes. It interfaces with the user via Ethernet and it interfaces with the devices. To connect the T&C controllers to the users via Ethernet, webservers were chosen. This choice permits the user to interface with the T&C controllers from the mini PC (via remote PC access) or through the internet directly from the ATRP lab. A maintainer can also attach a laptop to the test stand LAN and have access to the T&C controllers. On the device side, the T&C controllers have several duties to perform. They must control power management by commanding power supplies to turn on and turn off and they must also telemeter bus voltages. The T&C controllers must also be able to command the RF switches on the test stands that route IF and RF signals between various microwave components. The most challenging task for the T&C controllers is the control of the polarization rotor by commanding it to move to a specific position. When queried, the current position of the rotor must be reported as well.

Each test stand has several dozen devices requiring T&C control. All of the devices are physically close to one another with only relatively short cable runs between them. No wireless connectivity is necessary. The data rate requirements of the T&C control operations are low because none of the devices have high speed telemetry or command needs. In addition, erroneous commands cannot cause damage or create an unrecoverable condition. The environment does contain RF energy of multiple watts so there is concern for Radio Frequency Interference (RFI) on the test stands. There is no perceived threat that dictates a strong need for communications security on the test stands.

OFF-THE-SHELF PROTOCOLS

The T&C controller requirements suggest a simple wired protocol will suffice for interfacing with the various devices on the test stand that do not already have an Ethernet interface. Several industrial and military protocols were initially reviewed. Ultimately, a custom protocol that closely models one of the reviewed protocols was developed.

From the industrial market two protocols that are typically used for process control and monitoring were reviewed: MODBUS RTU [1] and CANbus [2]. Other industrial protocols including Foundation Fieldbus H1 [3], Profibus DP [4], and Distributed Network Protocol 3

(DNP3) [5], are known to the authors but were judged to not offer anything significant to the relatively low protocol demands of this project beyond what MODBUS or CANbus offer.

MODBUS, is a query and response (master and slave) protocol that can be implemented in hardware using Ethernet, a high speed tokens scheme, or asynchronous serial communications. This protocol is mature and is very popular for simple network connections between host computers and Remote Terminal Units (RTUs) or industrial process devices. Its asynchronous serial communication version, known as MODBUS RTU, makes it a good candidate for low-speed, low-overhead, byte-oriented, communication schemes. The MODBUS protocol has been in use since the late 1970's.

MODBUS, like many protocols, uses addresses to identify which device is to respond to a query. However, the industrial CANbus protocol does not use any addresses. This pier to pier protocol uses message identifiers to indicate what type of device sent the message, not which specific device the message came from or is going to. A simple but very effective bus priority-arbitration scheme ensures that data collisions are resolved. This permits CANbus devices to communicate whenever they have something to say. CANbus is mature and used extensively in the automotive industry, where many modern cars have multiple CANbuses onboard. In the past 30 years CANbus has also spawned related protocols including Allen Bradley's DeviceNet, in the process control industry, and the National Marine Electronic's Association (NMEA) 2000 protocol in the marine industry.

One military protocol, the Military Standard 1553 protocol was considered. Like MODBUS it is a query and response protocol where a bus controller communicates with multiple remote terminals. The protocol operates at 1 Mega-bit-per-second (Mbps) and uses a dual-redundant bus architecture. Signaling of data uses Manchester coding which assists in synchronization. The Military Standard 1553 protocol is popular in military avionics because of its reliability. It is a mature protocol and has been used on many military avionics systems as well as the space shuttle.

UNF T&C CONTROL PROTOCOL

After reviewing the available off-the-shelf protocols it was decided to develop a custom protocol for this project that is very similar to the asynchronous MODBUS RTU protocol. The CANbus protocol could have been adapted for use but since the nature of the T&C controller function in this project is that of a query and response transaction from specific addressed devices, it was decided to use a more simple conforming protocol. The chosen physical layer is RS-485, which is supported by MODBUS RTU. The twisted-pair cabling and differential signaling of RS-485 will help mitigate any RFI and also any motor noise from the antenna azimuth, elevation, and feedhorn polarity rotors. The data link layer will consist of asynchronous byte oriented data transfers, which also conforms with MODBUS RTU. This will facilitate the use of simple hardware interfaces available in microcontroller peripherals. In this particular case, the mode chosen for asynchronous byte transmissions is to send 1 start bit, 8 data bits, an odd parity bit and one stop bit. The data frame formats for MODBUS RTU and for the UNF T&C control protocol are shown in Figure 2.

The UNF T&C control protocol introduces several minor changes to the data frame structure. The start and stop flags consist of 4 full bit times of silence, instead of a minimum of 3.5 bit times. This will simplify the timer computation requirements slightly in a typical microcontroller program. In addition, the Cyclic Redundancy Check (CRC) error detection field is optional in the UNF T&C control protocol. The reason for this requires a discussion on the general topic of T&C control error checking.

As mentioned above, the UNF T&C control protocol has been developed for a specific project that will control simple devices that are not operating on a time critical scale. An error in transmission of a command cannot cause an unrecoverable condition. If an erroneous command is executed it can be easily detected by direct means via the telemetry data in a status check command response, or indirectly by monitoring the other systems on the test stand, such as the RF power meter, mini PC, or SDR. Similarly, a suspected erroneous response can be easily checked with a repeated command query. Never the less, there are mandatory error checking processes built into the protocol. The first one has already been mentioned. Odd parity is required on all byte transmissions in the UNF T&C protocol. The use of parity is well known, easy to implement in hardware, and can detect any single bit errors in a byte (as well as any 3, 5, and 7 bit error patterns in the byte). A higher layer error checking process that is also mandatory involves the handling of the data frame. Delays between bytes, or reception of an incorrect number of data bytes for a particular function code, will trigger an error in the software reception process and this will be reported to the user as a failed (unexecuted) transaction. If the error occurs in the reception process of a field device, the response to the query will include an error code that indicates a communications failure.

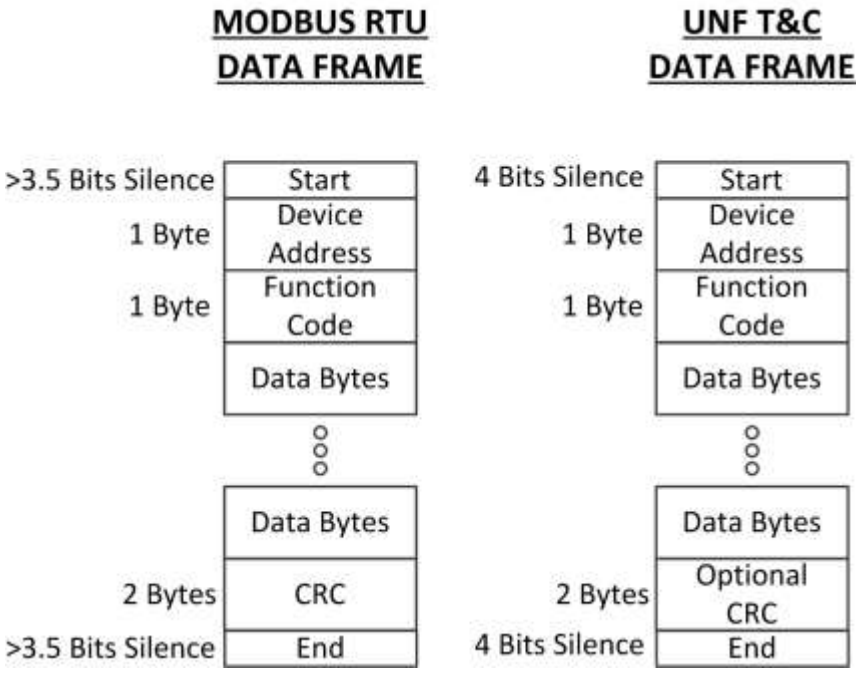

Figure 2. Comparison of MODBUS RTU data frame and UNF T&C data frame.

Given the use of the mandatory error checking processes built into the UNF T&C control protocol, coupled with the less demanding needs of the project in general, it was decided to make the use of the CRC error checking optional. The option to use the CRC is invoked through the function code. The MODBUS RTU function code is an 8-bit byte but there are only 128 recognized function codes. The Most Significant Bit (MSB) of the MODBUS RTU function code is used by field units to indicate an error either during command reception or command execution. However, it is unused on the outbound command query function code. In the UNF T&C data frame we set this bit in the command data frame to indicate that a transaction (query and response) does NOT use the optional CRC error checking. This effectively creates a second set of 128 possible identical function codes that are executed without a CRC check.

Through this point the UNF T&C control protocol has maintained compatibility with the MODBUS RTU protocol. Nothing in the UNF T&C control protocol would prevent a MODBUS RTU compatible field device from being added to a UNF project using the UNF T&C control protocol (with CRC enabled). The function code assignments and error handling processes in the MODBUS RTU protocol include public codes used universally, as well as vendor specific codes. Most of the public function codes in MODBUS are very flexible to facilitate use by various types of field devices. For instance, the MODBUS public function code to enable multiple field device discrete outputs is function code 15, known by the arcane name: “Force Multiple Coils” [1, pg. 29]. The data field in the command query of this function code contains as few as 6 bytes and as many as 251 bytes, permitting control of as few as 1 discrete output and as many as 1968 discrete outputs. Rather than adapt these public function codes for use on this relatively simple project, UNF chose to take advantage of the user defined function code assignments available in the MODBUS protocol. Figure 3 shows the MODBUS function code assignment space. Note that there are 17 addresses available for user defined function codes.

By employing these user defined function codes the UNF T&C protocol can maintain compatibility with MODBUS RTU for some future projects that are as yet undefined. Several user defined function codes have already been developed for the field units being used in the current project. They are shown in Table 1. More function codes will be developed as needed for the project.

PROJECT STATUS

The field device that will be used in this project to control either power modules or RF switches, has been developed. The combined device is referred to as a Power Control Module (PCM). Two PCMs are shown below in Figure 4. They use a PIC18F2580 microcontroller and support five discrete outputs. Three discrete outputs control the delivery of DC power to three power outputs via independent high-side load switches. The two remaining discrete outputs can be used to command two non-latching relays or a single latching relay, using the Pulse Output function code. The DC power bus used to supply the power outputs is monitored by the microcontroller and reported when queried with the Read ADC Value function code. The T&C controller and webserver is being developed on an Arduino platform with an Ethernet shield and an RS-485 shield to support the webserver and the T&C control interface, respectively. The T&C controller and webserver hardware is also shown in Figure 4. The polar rotor controller is still under

development. The test stands and the entire command and telemetry system are expected to be operational by the fall of 2017.

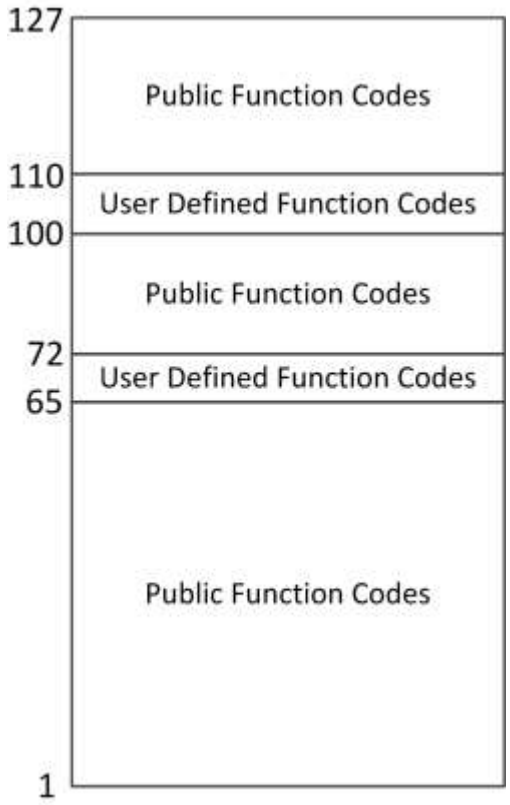

Figure 3. MODBUS Function code assignment space [1, pg. 10].

Table 1. UNF T&C control protocol user defined function codes.

Function Code	Function Code Without CRC	Name	Description
65	193	Do Outputs	Set and clear 1 – 16 discrete outputs
66	194	Get Outputs	Query status of 1 – 16 discrete outputs
67	195	Pulse Output	Apply pulse output to 1 of 16 discrete outputs (Used for latching relays. Pulse duration set by device)
68	196	Read ADC Value	Query for report of monitored bus voltage
100	228	Broadcast output clear	Clear all discrete outputs on all output devices
105	233	Rotor Position Set	Set the rotor position to a specific angle (0-360 deg.)
106	234	Read Rotor Position	Read the current rotor position

CONCLUSIONS

The development of a simple T&C control protocol has leveraged an available off-the-shelf industrial protocol to help develop a command and telemetry system for a joint UNF and FDOT research project in a cost effective and timely manner. By also using low-cost and easy-to-learn solutions for the T&C controller and webserver, students at the UNF ATRP lab have been able to participate in this research project as well. After this project is completed it is hoped other UNF research projects will be able to take advantage of the lessons learned and deploy the new UNF T&C control protocol.

REFERENCES

[1] The MODBUS Organization, "MODBUS Protocol Specification", V1.1b3, Available www.modbus.org/specs.php

[2] Robert Bosch GmbH , "CAN Specification", V 2.0, 1991, Stuggart, Available http://www.bosch-semiconductors.de/media/ubk_semiconductors/pdf_1/canliteratur/can2spec.pdf

[3] M. C. Carolan, "Foundation Fieldbus: Fieldbus Basics", Brisbane, 2011, Available www.fieldbus.org/images/stories/international/asiapacific/singapore/presentations/2011-04%20Vietnam/1_ff_basics_with_additional_points.pdf

[4] Profibus and Profinet International, "Profibus System Description", 2016, Available www.profibus.com/nc/download/downloads/ profibus-technology-and-application-system-description/download/21420/

[5] DNP User Group, "DNP3 Primer", Revision A, 2005, www.dnp.org/AboutUs/DNP3%20Primer %20Rev%20A.pdf

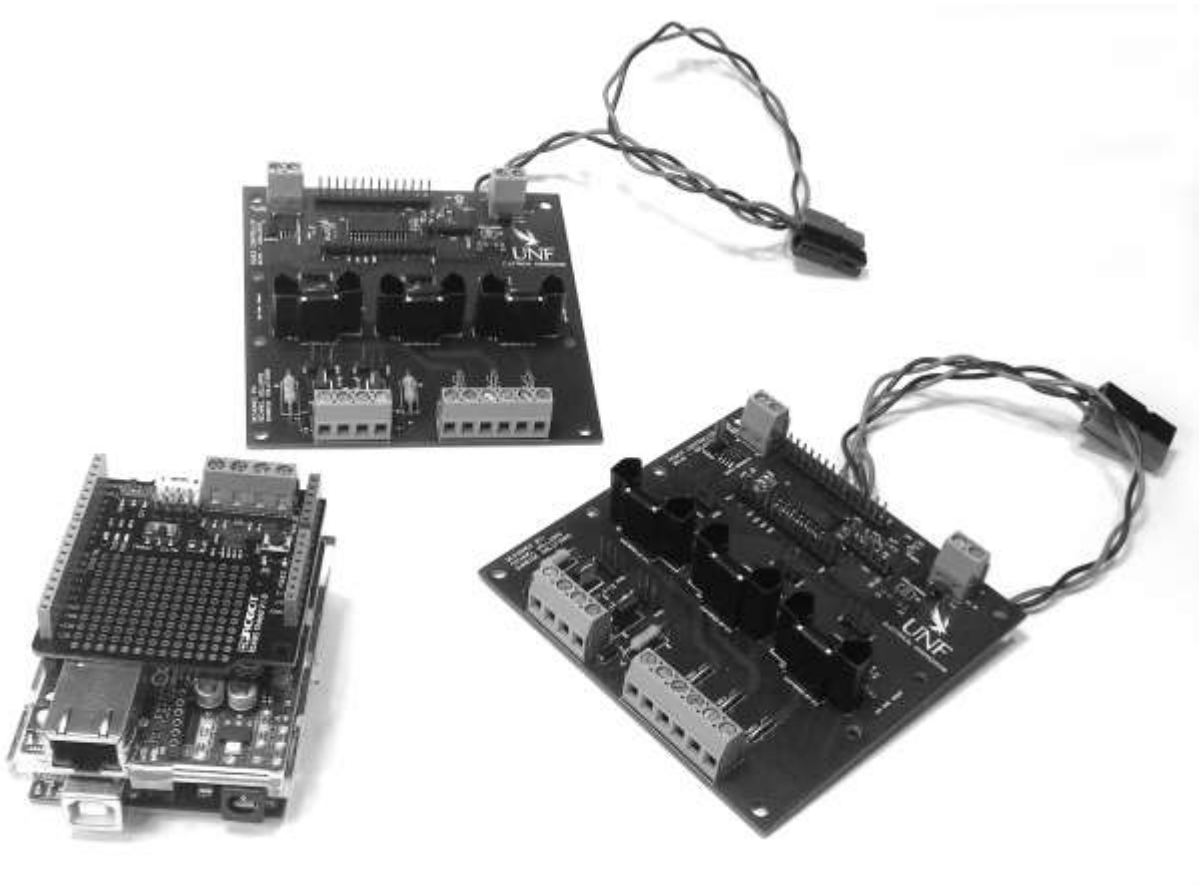

Figure 4. UNF T&C control hardware for the propagation project.

The opinions, findings and conclusions expressed in this publication are those of the author(s) and not necessarily those of the Florida Department of Transportation or the U.S. Department of Transportation.