Title: Safeguards Technology Development Program FY2021 Mid-Year Report
Encryption of Signal Pulses

Author(s): Newell, Matthew R.
Morgan, Keith S.

Intended for: Report

Issued: 2021-03-31

LAUR-????

Safeguards Technology Development Program
FY2021 Mid-Year Report
Encryption of Signal Pulses

March 25, 2021

WBS # – Project Title: 24.1.3.5 - Encryption of Signal Pulses to Replace Tamper-indicating Conduit

HQ Team Lead and PM: Arden Dougan and Barbara Hoffheins

Summary Statement of Work:

Develop a signal pulse digital signing and encryption in-line device to verify signal integrity and point of origin for TTL pulse data used in IAEA systems, and to avoid the need for expensive tamper-indicating conduit or techniques. This device will be called Transparent Remote Encryption of Correlated Signals (TRECS). TRECS consists of two parts, a head end which is located in or near the detector assembly and a tail end that is located with the data acquisition electronics, i.e. MiniGrand, UMSR, UDL1 or JSR.

Report Title: Mid-year report on the Transparent Remote Encryption of Correlated Signals (TRECS) project.

Names of Authors and Affiliations:

Matthew Newell, LANL
Keith Morgan, LANL

Major Highlights:

Highlights for the first half of this project include a very good conference call with the IAEA to clarify the Agency's needs and the expected functionality of the TRECS system. We also developed a couple of conceptual approaches both using Ethernet and coaxial cable data transmission. One approach uses Ethernet communications to exchange session keys while a coaxial cable transmits the encrypted pulse stream. The second approach, which early experiments show is promising, mutually authenticates the peer and encrypts the pulse stream over Ethernet performing the data transmission over a single Ethernet cable.

Safeguards Technology Development Program
FY2021 Mid-Year Report

March 25, 2021

.

Progress:

Task 1 – Develop the Appropriate Encryption Approach and Implement in Firmware

For the Transparent Remote Encryption of Correlated Signals (TRECS) project we have analyzed two high-level concepts for transmitting encrypted and authenticated pulses between two endpoints.

The first concept uses an out-of-band Ethernet cable plus coaxial cable. A block diagram is shown in Figure 1. In each endpoint is a System-on-Chip (SoC) containing an ARM microcontroller plus Field-Programmable Gate Array (FPGA), nominally the Xilinx Zynq 7020 SoC. In this concept the Ethernet connection is used by the endpoints to mutually authenticate and exchange ephemeral session keys. The ephemeral keys are passed to the FPGA. The FPGA uses the keys to encrypt the incoming pulse stream. The encrypted pulses are sent to the peer via a coaxial cable. At the receiving end the pulses are decrypted using the same session key and then serialized as TTL outputs. These outputs feed into, for example, shift register electronics.

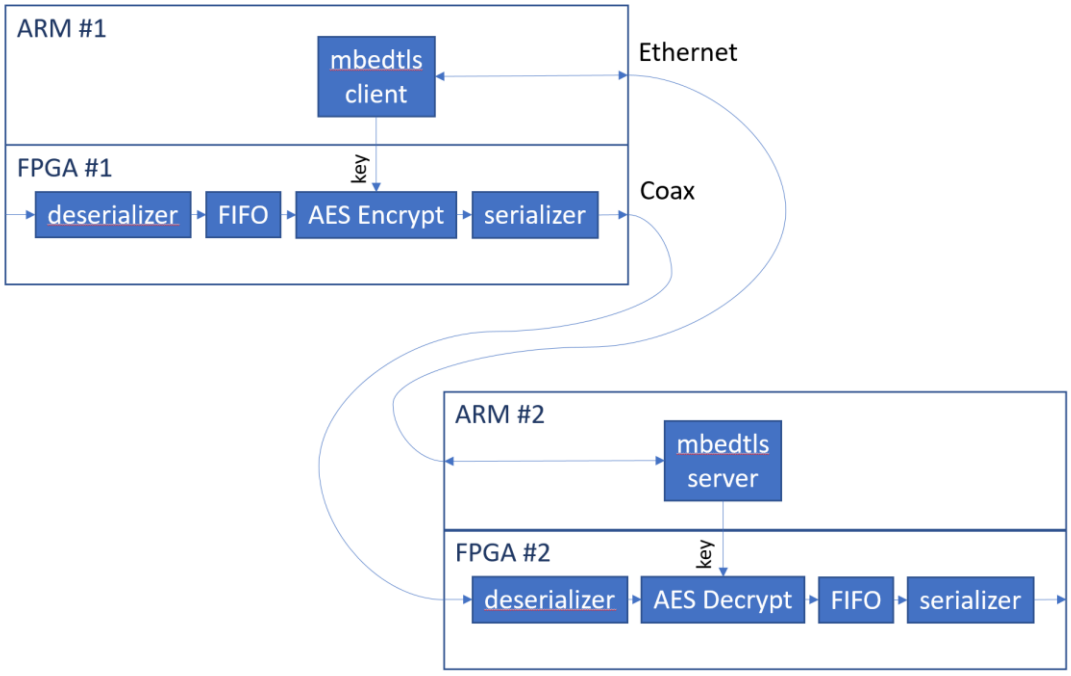

Figure 1. Ethernet plus coaxial cable data transmission approach.

The second concept uses only an Ethernet cable between the two endpoints. A block diagram is shown in Figure 2. Again, in each endpoint is a System-on-Chip (SoC) containing an ARM microcontroller plus FPGA. In this concept the incoming pulse stream is passed to the microcontroller. The microcontroller uses the Transport Layer Security (TLS) protocol to mutually authenticate the peer and encrypt the pulse stream over Ethernet. At the receiving end the pulses are decrypted in the microcontroller and passed back to the FPGA where they are re-serialized into TTL outputs. Again, these outputs feed into, for example, shift register electronics.

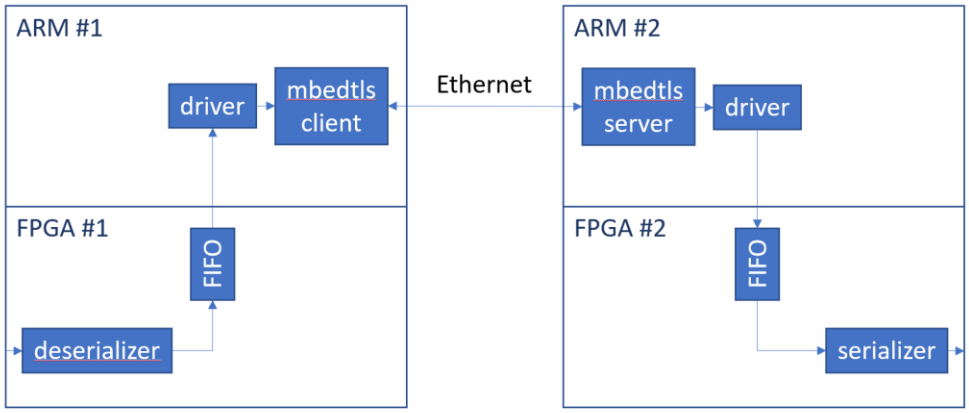

Figure 2. Ethernet only data transmission approach.

The advantage of the first concept is that timing is easily guaranteed by keeping the critical path in the FPGA. The disadvantage is that it requires an additional out-of-band Ethernet connection. The advantage of the second concept is that communication happens via a single Ethernet cable. The disadvantage is that the data pass through the ARM microcontroller and a TCP/IP stack which can introduce timing jitter. However, our experiments to date show that the relatively high bandwidth of Gigabit Ethernet (GbE) as compared to a 100 nanosecond pulse train is sufficient to smooth out any jitter introduced by the microcontroller and/or the TCP/IP stack.

For the second concept we have identified a commercial Ethernet over Coax adapter from Veracity that would allow TRECS to be used in legacy installations at existing facilities (see Figures 3 and 4).

Safeguards Technology Development Program
FY2021 Mid-Year Report
March 25, 2021

Figure 3. Commercial Ethernet over coaxial cable adapter. (source https://www.veracityglobal.com/media/59081/highwire_vhw-hw200-150.png)

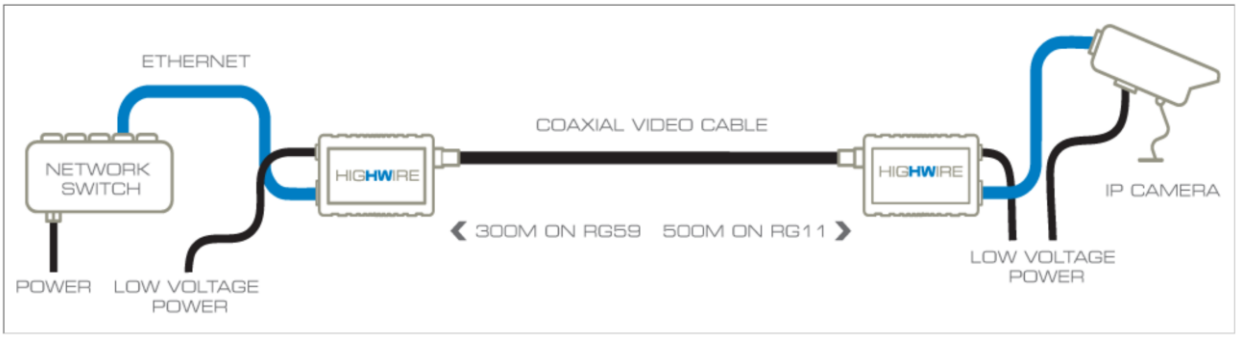

Figure 4. Example Use Case of the Veracity Highwire Ethernet Over Coax Adapter (source https://www.veracityglobal.com/media/64900/highwire-diagram-small.png)

Task 2 – Design Circuit Board

No progress yet on this task.

Task 3 – Assemble and Test

No progress yet on this task.

Task 4 – Documentation

The Design Specification Document is in progress.

Task 5 – Administration – Deliverable quarterly, annual/final, and closeout reports, midyear update

The first quarterly report and the mid-year report are complete.

Safeguards Technology Development Program
FY2021 Mid-Year Report

March 25, 2021

Publications: N/A

References: N/A