LA-UR-20-23318
Approved for public release; distribution is unlimited.

Title: Encryption of Signal Pulses to Replace Tamper-indicating Conduit

Author(s): Newell, Matthew R.

Intended for: proposal

Issued: 2020-05-01

Encryption of Signal Pulses to Replace Tamper-indicating Conduit

LA-UR-????

WBS:

24.1.3.5 Data Management

Project Type:

New Project Topic: Other, 5, New Ideas for Data Management

Scoping Study: No

SP-1: No

Action Sheet: No

Start Year: FY21

Key Performers

*Matt Newell, LANL, Keith Morgan, LANL, David C. Jones, LANL

Lab	Lab Program Manager	Principal Investigator	PI's Email	PI's Phone
LANL	Holly Trellue	Matt Newell	mnewell@lanl.gov	505.667.1327

PROPOSED STATEMENT OF WORK

Abstract

In order 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 electronic techniques, we propose the development of a signal pulse signing and encryption in-line device. In measurement applications in which the data acquisition electronics is separate from the enclosed, sealed detector, tamper-indicating techniques are required to protect raw TTL pulse streams between the detector and the data acquisition module, i.e UMSR. The goal of this proposed project is to design a rad-tolerant transmitter that would mount inside the sealed detector system and a receiver in the sealed electronics cabinet with the data acquisition instrument. This transmitter/receiver pair would digitally sign and encrypt the pulse stream data at the detector then transmit the data to the sealed cabinet where the receiver would decrypt the data and reproduce the original pulse stream. Existing tamper indicating techniques, such as LiveWire's spread

spectrum time domain reflectometry rely on detecting physical changes to the wiring system and can be blind to fast coupling of micro-second wide pulses. Digital signing and encryption techniques such as the Sandia Laboratories Enhanced Data Authentication System (EDAS) are capable of encrypting communications data, i.e. RS-232, but are not capable reproducing a critical time correlated data streams. Recent NA-241 Safeguards Technology supported developments have reduced the need for special conduit to transmit data via Ethernet by incorporating the IAEA RAINSTORM data encryption and authentication protocol, a tamper indicator is still required to protect raw pulse data from detectors to the acquisition electronics. Encrypting pulse data is especially complicated for radiation detection instruments due to the time correlation data analysis that is performed on this data stream. Any corruption in the timing information will produce errors in measurement values.

Mission Relevance

IAEA detectors connect to data acquisition instruments with standard coaxial cables. These cables can be tampered with if not protected. The Agency installs special expensive conduit to ensure tampering with the cables is easily determined. The proposed development would be used to sign and encrypt pulse data streams at the detector and thereby eliminating the need for special conduit.

This work directly addresses one of the IAEA Top priority R&D needs, T.1.R.9, as described in the IAEA Department of Safeguards Research and Development Plan, STR 385. The IAEA describes the development and implementation plan for this work in STR-386 section SGTS-002 Expected Outcome 4: the replacement of tamper indicating conduit would greatly decrease the cost and complexity of UMS systems.

Scope of Work

1. Overview

In order 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, we propose the development of a signal pulse digital signing and encryption in-line device. This device 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 or JSR.

The head end takes asynchronous pulse data in from up to 32 channels, signs and encrypts the data using an industry-standard public key encryption algorithm. The resulting encrypted data word is sent down the unsecured cable connecting the head and tail ends of this device. The tail end takes the encrypted data word and decrypts it, checking that the data and checksum are properly formatted. Any attempt to inject spoofed data will fail the decryption step and that data packet will be dropped. An alarm notification line signaling the receipt of improperly formatted data packets will be available.

The unencrypted synchronous data can be directly output on a digital bus for instruments that can accept synchronized digital event records, e.g. List mode instruments. The tail end can synthesize a pseudo-asynchronous pulse stream based on the contents of the unencrypted data and send this out for instruments that are expecting to see raw pulse data, e.g. the UMSR. In this way, this signal verification device is transparent to the remainder of the system. This device could easily be used in any detector installation in which a pulse-generating detector is physically separated from its data acquisition system by an unsecured cable.

2. **Description of project trajectory events, including overview of tasks, milestones, deliverables, and decision points**

Task #1. Develop the Appropriate Encryption Approach and Implement in Firmware

Selecting the appropriate signing and encryption technique as well as the optimum data block size and key size will be the first task in the project. Close attention will need to be paid to the required data rates, 100ns between sets of pulses in list mode modules, and the integrity of the timing between pulses to ensure multiplicity information is not corrupted. The developed approach will be documented in a design specification document. The completion of the design specification document will be an important milestone and deliverable.

The firmware developed at LANL will be used as the wrapper around commercially available encryption intellectual property firmware cores. LANL will purchase the base encryption core and then design the firmware wrapper such that the resulting system delivers the required performance. Firmware test benches and simulation results will be an important milestone and deliverable.

Task #2. Design Circuit Board

The head electronics will be located near the detector assembly and therefore may receive a high dose rate. Use of radiation tolerant FPGAs will be considered. The IAEA UNAP design uses radiation tolerant devices and this project will consider using the same devices. The new circuit board design including the possible use of radiation tolerant devices will be documented in a drawing package. The complete drawing package will be an important milestone and deliverable.

Task #3. Assemble and Test

The highly skilled NEN-1 electronics team, including NASA certified soldering, will assemble the circuit. The circuit will then be tested on the bench as well as in an NEN-1 neutron counting system. Comparisons between the encrypted/decrypted data measurement results and results without the encryption/decryption will be performed.

Task #4. Documentation

Documentation will include drawing packages that will completely define the new board, test results and a User's Manual.

Pertinent references

1. Rocchi S. et al.; "Use of Specialized Security Techniques to Enhance the Authenticity of Serveillance Data", IAEA Symposium on International Safeguards 2014: IAEA-S22-04, 2014
2. Thomas, Maikael A., Hymel, Ross W., Baldwin, George, Smejkal, Andreas, and Linnebach, Ralf. Field trial of the enhanced data authentication system (EDAS). United States: N. p., Web.

3. Newell M. R., "Safeguards Technology Factsheet Unattended Dual Current Monitor (UDCM), LA-UR-16-22490, March 2016.

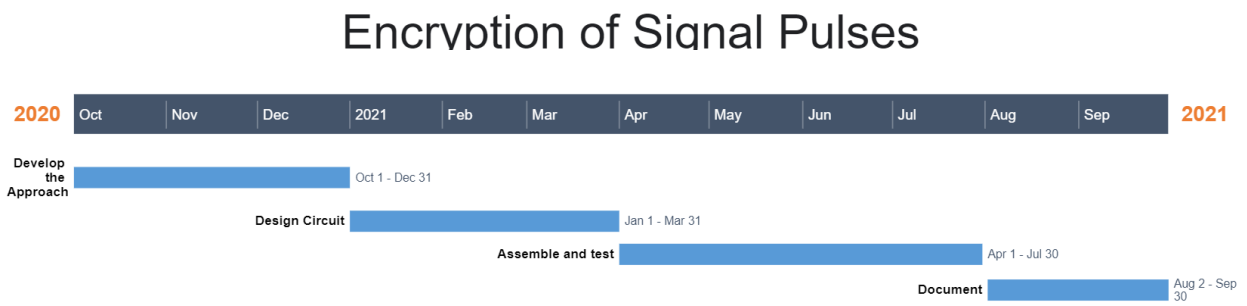
Associated Work

Project Title	Funding Agency	Major accomplishments and safeguards relevance	Years funded
N/A			

Technology Readiness Level

Start TRL	End TRL	Component(s)	Notes
2	5	**Pulse Encryption Circuit**	At the conclusion of this project we will have a prototype device that is tested in a relevant environment

Gantt Chart (FY21)



Joule Metric

The final product from this work will be a prototype system that can be used to encrypt and decrypt a raw pulse stream to allow for secure data transmission of time correlated pulse data. The prototypes will be transferred to the IAEA for testing and recommendations.

Task Summary

Task No.	Event Type	Event Title	Responsible Lab	Event Date	Actual Date
1	Milestone	Develop approach and firmware	LANL	12/31/2020	
	Deliverable	Firmware to test			
	Publication	Design specification document			
2	Milestone	Design circuit board	LANL	3/31/2021	
	Deliverable	Board design			
	Publication	Schematics			
3	Milestone	Assemble and test	LANL	7/30/2021	
	Deliverable	Prototype tested			
	Publication	Test results			
4	Milestone	Fully documented design	LANL	9/30/2021	
	Deliverable	Drawings, test results, and user manual			
	Publication	User manual, Final report			

Quarterly Reports will be due on January 10, April 10, July 10, and October 10.

HQ reviewed and R&R'd project interim reports, annual reports, final reports, are to be uploaded (with marking HQ only) and conference presentations and publications (wide distribution) to the Safeguards Knowledge-management Repository (SKR), https://skr.nsis.anl.gov/skr/.

Closeout reports are due 60 days after the end of the project.

Funding by Task

Task	LAB1 Estimated Carryover Funds ($K)	LAB1 New Funding Requested ($K)	LAB2 Estimated Carryover Funds ($K)	LAB2 New Funding Requested ($K)	Total Funding Needed ($K)	Total New Funding Requested ($K)
1. **Encryption of signal pulses instrument.**	$0	$330	$0	$0	$330 Carryover + new funding	$330 Just new funding
TOTAL		$330			$330	$330

Helium-3 Allocation

No Helium-3 will be needed

Project Risks and Mitigation Plan

Risk	Level [H/M/L]	Mitigation
There is a medium risk in this work due to digitizing this type of high integrity pulse timing data. Corruption of the timing cannot be tolerated by the analysis instruments.	M	Our expertise in designing pulse stream analysis instruments and our experience analyzing correlated pulse stream data puts us in a very good position to identify problems with the encryption and to determine appropriate design changes.

Anticipated Future Needs and Activities

Year	New Funding ($K)	Anticipated Future Tasks
2022	$170	Commercialization of this instrument upon successful completion of this FY21 task and if the IAEA would like to see the instrument commercialized. The final outcome will be a commercial product that the IAEA can use in place of tamper indicated conduit.

Data Management Plan

All project data including schematics, software, test documents and manuals will be stored on the LANL backed up server. Regular reports will be sent to SGTech to highlight progress on the project. At the conclusion of the project all documents will be reviewed and released through the LANL document control process.

Conferences and Workshops

NONE

Human Capital Development Funding

Name	New or Continuing	Position	University / Degree Program	Mentor	Cost	Duration of appointment
Jerry LI	New	Undergraduate Intern	UCLA/ Electrical Engineering	Matt Newell	$17k	Jun15-Sep15

Justification

Employment on this project will continue to advance the students safeguards career. The student has been part of our organization for three summers now, including high school co-op, and has gained valuable experience. Losing this young talented individual to other organizations due to lack of funding would be detrimental to our organizations continued safeguards expertise and ultimately negatively affect our ability to support SGTech electronics programs. So for both the career development of the student and the knowledge management for our organization, Human Capital Development funding is critical.

100% of Jerry's time is planned to support this project.