Contract No:

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-08SR22470 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Data Splitter for Joint Use with Oversight Agencies

[1] Nicholas DeRoller, [2] Richard Poland, [3] Jeff Chapman
[1] *Nicholas.DeRoller@srnl.doe.gov, Savannah River National Laboratory, 730-A, Aiken, SC, 29808 USA*
[2] *Savannah River National Laboratory, Aiken, SC, USA*
[3] *Oak Ridge National Laboratory, Oak Ridge, TN, USA*

Abstract

To establish and verify declarations of nuclear materials, frequently neutron coincidence counting is performed by both the host country and the IAEA to determine the amount of fissionable isotopes. Due to the cost, size and weight of the neutron detection system of neutron coincident counters, the practical practice of jointly using the neutron detector system located at the facility has been adopted. The IAEA has a policy for allowing an authorized joint use of equipment by the facility operators and the IAEA inspectors. The shift register component and controlling computer systems however are not currently shared. Frequently, the facility operator and the IAEA make measurements concurrently where the signals from the joint use neutron detector system are split to each party's separate and independent shift register and data collection electronics To ensure that neutron pulse streams cannot be maliciously manipulated through the signal splitting connection Savannah River National Laboratory (SRNL), in cooperation with Oak Ridge National Laboratory (ORNL), has developed a Coincidence Counter Signal Splitter (C2S2) that will allow each party to have confidence that the other party is not manipulating the detector system signal to misrepresent the material being measured. While simple in principle, the device employs several design methodologies to make the split output tamper resistant, ensuring that the IAEA receives the same pulse stream that the host country receives. Additionally, the signal is amplified and terminated to allow possible long cable runs and avoid signal reflections which may create erroneous signals. The device also contains a switched power supply that allows the device to be resistant to interruptions which may "cancel" pulses as well as provide a much wider tolerance to input power voltages. Because this device exceeds intended specifications for duplicating a 200 kHz pulse stream from a coincidence counter, it may be used for more than just its intended purpose and serves as a first toward a set of joint use industrial hardware being produced. In this paper we will discuss the importance of joint use measurements, as well as explore the functionality and usefulness of the developed device with regard to splitting other sensor/detector type signals and in unattended and remote monitoring scenarios.

Introduction

Many instances of measurements being made with duplicate sets of equipment exist in international safeguards. The major reason for this practice is the necessity to have confidence in the measurement; that external influences have not altered the measurement to misrepresent the nuclear material being measured. Among these instances there are times when using shared equipment would either simplify deployment of safeguards systems or increase inspector efficiency. The key to jointly using equipment is to incorporate mechanisms that ensure equipment has not been tampered with or can be manipulated to present errant results which lead wrong safeguards conclusions.

Policy Paper 20 – "Joint Use"
This paper outlines the joint use of safeguards equipment between the IAEA and facility operator and ensures that this joint use does not weaken the IAEA's safeguards system or their right to make independent measurements and observations.

In performing safeguards activities the IAEA may be requested by the operator to share the safeguards equipment or the IAEA may request use of equipment owned by the operator. Sharing of this equipment is broadly consistent with paragraph 31 of INFCIRC/153 that encourages the IAEA to "make full use of the State's system of accounting and control" and to avoid "duplication of the State's accounting and control activities".

Joint use of the equipment may provide safeguards data that may be more easily obtained by the IAEA using operator provided equipment, rather than data that would be obtained by independently owned equipment. Because resources are being shared the operators and the IAEA will find that the costs associated with acquiring, maintaining, and operating said equipment will be less. Also, the operators may find that the IAEA safeguards are less burdensome if the installed equipment is also used for safeguards measurements. This reduction in potentially unnecessary redundancy may also reduce inspector and technician exposure.

As a general rule, the data attained by the IAEA should not be made available to the operator. Though (especially in our case) some level of sharing is unavoidable and also may be requested by the operator. What data is to be shared must be specified in detail in the Joint Use Agreement.

Other than neutron coincident counting measurements, other safeguards measurements could benefit from joint use equipment; facility process monitoring and control sensors and loadcells. Several concepts developed in this paper for signal isolation and power management could be integrated into the signal splitting equipment for other sensors.

Signal Splitting Case
A neutron coincidence counter is used to establish and verify the amount of fissionable isotopes of nuclear material. A shift register is used to tabulate the neutron pulses from a neutron detector system surrounding the nuclear material. Signal cables from the detector system connect to a shift register. Current IAEA safeguards policy establishes that when the operator takes a measurement using the operator's shift register, a separate measurement must also be made using the IAEA's shift register. In this procedure, after the operator makes their measurement the coaxial signal carrying cables must be physically detached from the operator's shift register and re-attached to the IAEA's shift register.

While the equipment to make the measurement is technically "joint use" because the operator and the IAEA are sharing the neutron detection system, current measurement practice does not align with the recommendations in paragraph 31 of INFCIRC/153 which states that duplication of the operator's accounting and control activities should be avoided. This also does little to make the measurement practice less burdensome. Additionally this measurement procedure requires great bit of trust that the operator will in fact run a duplicate measurement on the same bit of material, or run the duplicate measurement at all.

This procedure also places a good bit of unnecessary wear on the signal cables leaving the operator's hot cell through repeated connection and disconnection. These actions place wear on any non-oxidizing plating that the terminals may have which could change the receiving terminal's matched impedance and reduce the signal quality. Also, while the exact cable type used is unknown to the developer, a worst-case scenario for an "all cases solved" solution must be assumed. If a simple single-stranded center conductor type coaxial cable (such as an RG58 type) is used, because copper is a work-hardened metal, the center conductor may become brittle after prolonged constant adjustment. Unless the center conductor is multi-stranded, movement of these types of wires must be kept to a minimum. Given these usage scenarios, it is understandable that handling of the conductors leaving a hot-cell should be kept to a minimum. Current policy in use at does not take into mind these considerations.

Solution

In hopes of better aligning with the aforementioned IAEA policies by removing unnecessary redundancy and making compliance with safeguards agreements less burdensome to the operator, Savannah River National Laboratory in cooperation with Oak Ridge National Laboratory has developed a solution to this real problem. Our Coincidence Counter Signal Splitter (C2S2) is an example of a potential advancement of the joint-use policy to ensure that safeguards compliance is more streamlined for the operator and the IAEA. With this device, the TTL signal that leaves the hot cell High Activity – Active Well Coincidence Counter (HA-AWCC) is run to a powered splitter, which may be mounted in a convenient location outside the cell, and splits this signal to both the operator's and the IAEA's separate shift-register hardware. This device still relies on the same level of trust given to the operators in the previous procedure. As noted, the advancement provided is the increased ease of compliance by reduction of redundancy in the compliance procedure.

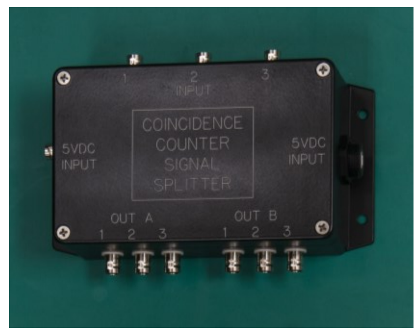

Figure 1 – The Coincidence Counter Signal Splitter (C2S2) in its aluminum enclosure.

Hardware

The C2S2 is built to take in a noisy, possibly low or underpowered signal, and reproduce the signal as a clean $5V_{DC}$ TTL signal with enough power to run longer coaxial cable distances. The circuit is replicated three times, one for each channel leaving the coincidence counter. The external BNC connectors are wired internally to the board using smaller coaxial wires to reduce radiated and accepted noise. Also, the board is routed to ensure that parasitic capacitances and inductances are kept to a minimum as the circuit is designed to have a fast rising and falling signal edge (measured at ~700ps). This transition speed may be tailored for any future design needs.

After the signal is fed to the circuit it is run through transient voltage protection (Fig.2). This is in place to protect the device from accidental mishandling and possible attack. After the protection circuit the signal is split and run through two separate optical isolators. The signal is then fed through paralleled amplifiers to give the device greater current sourcing capacity. This allows for longer than normal cable runs to overcome the parasitic capacitance inherent in coaxial cables. Finally, the output is run through a signal protection circuit like the one at the device inputs to again protect against operator error or attack.

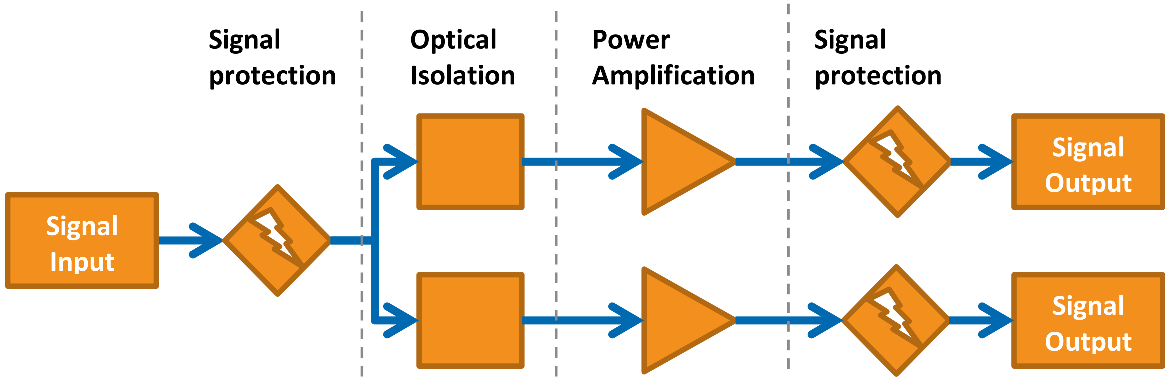

Figure 2 – Signal splitter block diagram.

The device is powered by either (or both) of the $5V_{DC}$ inputs located on opposite sides of the device. One connector is a BNC to allow connection of a possible 5V output from a coincidence counter; the other is an USB type-B connector to allow connection to a computer or commonly available USB phone charger found in the consumer market today. The design goal is to make the device as easy to use, place, and power as possible for the operator to encourage its use. The device also contains a power-conditioning circuit to help guard against operator error through improper connection, power sourcing problems, or power source manipulation. This device may be connected to a voltage source outputting between $2.5V_{DC}$ to $24V_{DC}$ and will continuously output a $5V_{DC}$ signal, even when the supply voltage is transient. For ease of use and operator convenience, both power inputs are automatically switched and may be connected simultaneously if the operator so desires.

Why not use a simple BNC T-Splitter?

One might ask this obvious question. It is recognized that while the measurement device (coincidence counter) itself is shared between the operator and IAEA, the IAEA would still like a separate isolated signal for use with its own analysis equipment (shift register). A BNC splitter gives the operator direct access to the signal that is fed to the IAEA's shift register. Because the standard BNC splitter is not a diode device, even if the splitter and IAEA shift register were contained in a tamper-evident box, specially designed pulse cancelling/creating circuits may be created and attached to the operator cable to 'trick' the IAEA analysis device into seeing a less/more active material than accounted for. The output signal isolation ensures that any pulse altering circuitry is contained to its respective output, rendering the activity pointless. In addition to the BNC splitter as an attack vector, introduction of this component can help create a transmission circuit conducive to signal reflections. These reflections, which may arise from possible unequal cable lengths and a now mismatched signal impedance path has shown during our experimental testing to increase the number of pulses measured at the shift register, creating spurious signal content.

Security

The main security component of the device is split signal isolation. However a few more electrical security measures have also been included. First, the power condition circuit has a reserve bank capable of supplying operating power during possible power line manipulation. During this type of attack an operator might attempt to switch the power to the device in synchronization with the arriving pulse train to simulate a less active material. While the power bank is not large enough to supply power during a brownout or power loss event, it is capable of supplying energy during a pulse cancellation event, as tested by our lab.

The signal protection components shown in Figure 2 prevent out-of-bounds transitions at the inputs and outputs. To test the circuit operation a signal splitter was placed at the input of the C2S2 and run to a pulse cancellation circuit. This cancellation circuit was designed to provide a ground or -5VDC pulse in synchronization with the incoming pulse train. The aim of this device was to be able to either cancel pulses at the opposite output or pull the entire circuit power bus low enough to cancel the pulse through an indirect power line attack. Given this test scenario we were also unable to make counts 'disappear' from the pulse train output to the IAEA.

Unattended and Remote Monitoring

If the source signal can be split securely, the signal cable protected adequately, and there are assurances of signal integrity at the measurement location, it is conceivable that process sensors, load cells, and radiation detectors used by the host facility could be jointly used for unattended and remote monitoring systems. It may be necessary to implement video surveillance in these situations. Sensors with the intelligence to digitally sign the data at the source and living within a tamper indicating enclosure (TIE) is an important consideration for joint use equipment where two independent data streams can be supplied.

Current Policy

Policy Paper 16 – "Remote monitoring for safeguarding nuclear facilities"

In policy paper 16, the IAEA states that remote monitoring techniques may be used with unattended monitoring and measurement systems to electronically transmit data collected by these systems to headquarters or the regional office of the IAEA for review.

The IAEA may improve the efficiency of their safeguards by replacing certain inspection activities with unattended monitoring and measurement systems with data collection review and evaluation at a remote location [ref PP 16]. By reducing the need for inspector presence during the data collection, remote monitoring may also decrease radiation exposure of inspectors and personnel while reducing the burden on the facility. Containment and surveillance techniques, verification availability, and employed transmission technology are considered along with costs of implementing a new remote monitoring protocol before the IAEA consults the operator about the need for change in technology.

Article 14(a) of the Model Protocol provides a legal basis for application of remote monitoring if the state has accepted the Protocol Additional to Safeguards Agreements. This stipulates that the State "…shall permit and protect free communications by the Agency for official purposes between Agency inspectors in the State and Agency Headquarters and/or Regional Offices, including attended and unattended transmission of information generated by Agency containment and/or surveillance or measurement devices".

Policy Paper 16 enumerates three levels of data transmission for RM systems; Equipment state-of-Health, Summary Data, and Detailed Data. The device detailed in this paper addresses the transmission of detailed) data from an individual device, namely a pulse train from a neutron coincidence counter housed in the operator's hot cell, which may be used in deriving safeguards conclusions. This data should be evaluated and compared with the operator's accounting and operating data when deriving these conclusions.

IAEA remote monitoring systems "may utilize any communications means which have been agreed between the IAEA and the State". The communications means will be based on reliability, installation, and transmission cost. Measures shall be taken to ensure authenticity of the transmitted data and encryption should be applied during transmission as agreed with the state.

Future Direction

At the given stage of development there are some obvious attack vectors when using this device. Namely the line from the coincidence counter to the C2S2 is completely unprotected, as is the line from the splitter to the IAEA's shift register. However, this is considered a demonstration device and serves as a positive step towards making safeguards policy easier to comply with for the cooperative host country. Should the agency choose to implement the C2S2 they may request additional protection features, such as TIE and cable protection, which SRNL and ORNL will work together to implement.

References & Acknowledgements

IAEA Policy Paper 16 – Remote Monitoring for Safeguarding Nuclear Facilities

IAEA Policy Paper 20 – Joint Use of Safeguards Equipment between the IAEA and an External Party

Project Sponsor

NNSA's Office of International Nuclear Safeguards' International Safeguards Engagement Program (INSEP)