This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government

SAND2020-6102C

Proceedings of the INMM 61st Annual Meeting
July 12-16, 2020, Baltimore, MD, USA

A Modular Approach to Trusted System Design for Arms Control Treaty Verification

J. K. Polack[1], E. Brubaker[1], M. C. Hamel[2], R. R. Helguero[2], D. L. Maierhafer[2], P. Marleau[1], E. A. Padilla[2], T. M. Weber[2]
[1]Sandia National Laboratories, Livermore, CA, USA
[2]Sandia National Laboratories, Albuquerque, NM, USA

ABSTRACT

Radiation detection systems for verification of warhead limitation treaties face a unique challenge not present in other mission areas. The challenge stems from involvement of multiple parties, who may have very little trust in one another, and the fact that all parties need to maintain high confidence in the results obtained from a measurement system that is also designed to protect against the release of one party's sensitive information. Design of trusted systems for warhead confirmation has been an area of research at Sandia National Laboratories for 20 years and has led to the development of systems such as TRIS and TRADS. Traditionally, past design efforts focused on mitigating trust concerns at the system level while, at the same time, frequently using commercial embedded computers or off-the-shelf microprocessors to control the system and process the acquired data. Giving a processor this level of access presents its own concerns because all parties must be confident that the processor is only performing the agreed upon tasks. As a potential solution to this problem, we are exploring a modular radiation detector architecture for arms control treaty verification applications. We believe that there are many potential benefits to using a modular approach for trusted system development. Breaking down a system into simple building blocks with defined functionality enables functionality testing on a modular level, which may reduce the overall authentication and certification burden for a complex system. Additionally, a modular architecture can mitigate the risk of using an off-the-shelf processor by limiting the access of the processor and facilitating strategic bottlenecking of the data stream. Furthermore, a modular design can help establish multilateral trust in a measurement system by providing a framework of module requirements and interface specifications that can facilitate collaborative design with international treaty partners. We have started exploring this concept by developing a notional architecture that will accommodate several systems with differing capabilities that may be relevant to future warhead confirmation measurement agreements. This paper will further discuss our ongoing efforts towards the development a of a modular architecture and the perceived benefits of a such a design.

INTRODUCTION

Arms control treaty verification and monitoring regimes require trusted technologies that can deliver the required information without leaking sensitive information. Stakeholders seek to find long-term solutions to the technical challenges of verifying compliance with nuclear reduction agreements. Development of trusted technologies is an arduous and costly process and traditionally results in a technology that meets one specific need. However, given that the treaties these technologies will support have yet to be negotiated, designing a device for a specific purpose runs the risk of having a tool that does not meet the negotiated verification needs or is not accepted by all parties of the treaty. Furthermore, in a warhead dismantlement confirmation regime, it is possible that multiple measurement modalities will be required. This will, in turn,

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. Approved for unlimited release. SAND2020-6102 C

require multiple systems, each with their own authentication and certification procedures, which increases the complexity and cost of the regime as well as the room for human error.

To create a solution for this potential issue we are working to develop and demonstrate a modular radiation detection architecture for use in arms control treaty verification (ACTV) applications that will facilitate rapid development of trusted systems to help meet the needs of future treaties. The architecture will define broad functional requirements, interface specifications, allowable inputs and outputs, and recommended high-level inspection and testing procedures for a series of modules. Furthermore, the architecture will be designed such that conforming modules can be developed to reproduce the functionality of an array of different radiation measurement and analysis capabilities.

Our goal is to deliver specifications for a modular and inspectable architecture that allows for implementation of a variety of current state-of-the art detection systems, while also making it possible to implement new detectors and/or processing algorithms without needing to redesign a system from the ground up. Development of such an architecture will provide a toolkit for rapid development of trusted systems that can meet the currently unknown needs of future treaties. As work progresses, we will demonstrate the benefits of this architecture by developing prototypes of functional hardware that conforms to this architecture, as well as suggested procedures for inspecting the hardware from an authentication and certification perspective. We hope that the modular architecture and example hardware can be used in the future to facilitate discussion on a process where international partners can collaboratively design monitoring and verification equipment that conforms to a jointly agreed upon architecture.

MOTIVATION

Radiation detection systems employed for verification of warhead limitation treaties face a unique challenge that is not present in other mission areas. The challenge stems from involvement of multiple parties, who may have very little trust in one another, and the fact that all parties need to maintain high confidence in the results obtained from a measurement system that is also designed to protect against the release of one party’s sensitive information. Although there have been several decades of work related to implementing technology within treaties, only one radiation detector has been used within a nuclear weapons limitation treaty, the Radiation Detection Equipment (RDE) [1]. Sandia National Laboratories (SNL) developed and maintains this simple neutron detector that is currently used in the New START treaty to confirm the absence of a nuclear weapon. In this treaty, the RDE is used to verify that an object declared to be non-nuclear is so by confirming that the measured neutron count rate does not exceed an agreed upon threshold.

Future agreements may require the confirmation of warhead presence which will increase the complexity of the measurement and will also significantly increase the sensitivity of the information being measured. A system that is designed for warhead confirmation measurements will be in the presence of warheads and is likely to process sensitive data to arrive at a non-sensitive answer. The sensitive data needs to be protected from the monitoring party. The monitoring party will need to trust the data stream to know that the measurement is correct and complete. Furthermore, the equipment will need to pass the safety and security requirements of the host party/facility. As such, systems used in in treaty monitoring scenarios must be authenticated and certified by all involved parties, where authentication and certification is defined by the International Partnership for Nuclear Disarmament and Verification (IPNDV) as follows [2]:

Authentication – A mechanism by which a verification entity obtains confidence that the information reported by monitoring equipment accurately reflects the true state of an item that is subject to verification, and that the monitoring equipment has not been altered, removed or replaced, and functions such that it provides accurate and reproducible results at all times.

Certification – A mechanism by which an inspected State assures itself that an inspection or monitoring system meets safety and security requirements and will not disclose sensitive information (including proliferation-sensitive information) to an inspector

As no prior treaties have allowed for positive warhead confirmation measurements[i], there is no operational precedent for the type of measurements to be made or the best methods to protect sensitive data. Nonetheless the United States needs to be prepared for this possibility and as such, there have been several efforts over the past several decades that have focused on the design of trusted systems for warhead confirmation. At SNL these efforts have included the Trusted Radioisotope Identification System (TRIS) [3], the Trusted Radiation Attribute Demonstration System (TRADS) [4], and CONFIDANTE (CONfirmation using a Fast-neutron Imaging Detector with Anti-image Null-positive Time Encoding) [5]. Other notable efforts include Third Generation Attribute Measurement System (3G-AMS) [6] developed by Oak Ridge National Laboratory and the UK Norway Initiative Information Barrier (UKNIB) [7].

As part of these efforts, several demonstrations and exercises involving radiation measurement equipment have taken place, notably the Fissile Material Transparency Technology Demonstration (FMTTD) and Trilateral Initiative which took place in the 1999-2000 timeframe and included Russian involvement, and several cooperative exercises with the United Kingdom Atomic Weapons Establishment. Results of these past initiatives have included some of the following conclusions:

- Trust is difficult to establish in complex systems, especially microprocessor-based systems with large amounts of embedded software. Authentication becomes even more difficult when proprietary intellectual property prohibits open sharing of embedded code.
- Flexibility and modularity are necessary as allowed measurements and equipment may change during the course of treaty negotiations. The timelines of treaty negotiations do not allow for a full cycle of engineering development to provide a specialized system, therefore existing solutions must be rapidly reconfigurable to adapt to changes in negotiating positions. This is especially true given the range of potential treaty partners, verification needs, and inspection techniques that may need to be addressed in a hypothetical treaty.
- Commercial radiation detection equipment has evolved over time to incorporate many of the same communication and interface technologies present in consumer electronics, making authentication of such hardware more difficult. 20 years ago, commercial detection equipment with limited functionality might have been acceptable for sensitive measurements; at the present time, integration of smartphone interfaces and wireless data transfer with most commercial off-the-shelf (COTS) systems make this possibility seem remote.

These observations highlight the need for a modular radiation detector architecture custom designed to facilitate the functional as well as the authentication and certification needs of future ACTV activities.

Fortunately, radiation measurements are well suited to modular signal processing hardware, with many detector systems being constructed from the same basic building blocks: the detector itself, preamplifier and shaping amplifier stages, histogramming, and analog to digital conversion as necessary to facilitate further application-specific signal processing. For many decades, commercial radiation detection equipment has been produced to provide these building blocks using standard formats, such as NIM (Nuclear Instrumentation Modules), that enable rapid configuration of measurement systems in the laboratory.

Advancement of modern radiation detection electronics (e.g. digitizers with on-board digital pulse processing), has made it even easier to develop a general-purpose flexible radiation detection system. However, with increased flexibility, comes a great deal of complexity. Many of the commercially available products available for such tasks include a variety of proprietary hardware and software, often loaded onto a high-performance field programmable gate array (FPGA). From a data security standpoint, this complexity at best makes it challenging for an end-user to know exactly what is happening inside the system and at worst opens many possibilities for a nefarious actor to corrupt a data stream by hiding unwanted functionality within the complex system structure.

Because commercial hardware was not designed to facilitate authentication or certification, complex COTS solutions can be difficult to build into multilateral arms control treaties. However, prior efforts have demonstrated that it is possible to develop custom modules can be built into a trusted system. This philosophy has been explored, in part, through the development of the trusted processor used with TRIS [3] and TRADS [4]. TRIS and TRADS were both built in the year 2000 timeframe to explore different verification techniques. TRIS is a radiation template matching system using a low-resolution scintillation detector, while TRADS is an attribute measurement system using a high-resolution semiconductor detector. Both systems utilized a trusted processor designed by Sandia which separated sensitive signal processing (analysis of the collected radiation spectrum) from non-sensitive processing (messages to and from a user) using a physical information barrier. Even though the measurements were different, the same trusted processor could be used as an information barrier, leading to design cost savings and shared authentication procedures.

Also, the recently completed Portal Monitor for Authentication and Certification (PMAC) project [8], sponsored by the National Nuclear Security Administration Office of Nuclear Verification, fabricated separate modules for power, detection, and alarm processing, which can be built into a custom sized portal monitor for different types of monitoring needs. Each module is a separate tamper indicating enclosure (TIE) and the simple 2-layer circuit boards used within the modules were designed to facilitate visual and X-ray inspection.

ARCHITECTURE DESIGN PRINCIPLES

In our initial assessment of prior trusted system development endeavors, we identified two shortcomings that we hope to address with our modular architecture concept. The first is that all prior work has focused on the development of systems meant to perform a specific measurement, which makes their utility dependent on the treaty language allowing for that specific measurement. The second is that past design efforts have traditionally focused on mitigating trust concerns at the system level while, at the same time, frequently using commercial embedded computers or off-the-shelf microprocessors to control the system and process the acquired data. Giving a processor this level of access presents its own concerns because all parties must be confident that the processor is only performing the agreed upon tasks and not secretly manipulating the system or data to the benefit of one treaty party.

To help address these shortfalls, we have established three main design principles that guide our design decisions:

1. Modules will be self-contained – all necessary controls will be on the module and each module can maintain its functionality without communication from other modules (aside from data from the prior module)
2. Modules will have simple functionality with well-defined inputs and outputs
3. Data and signals will only flow in one direction through the chain of modules

These design principals provide several technical advantages that we believe can facilitate inspection and reduce the overall authentication and certification burden of fielding a complex system:

- Restricted functionality of individual modules motivates simple topology and design, and also aids in the ability to effectively test the functionality of a module. Each party should be able to verify that the module produces the expected output for a given input.
- With the availability of conforming function modules, more complex measurement system architectures can be built up without increasing or changing the authentication and certification concerns. Each module can be authenticated independently such that the whole system can be trusted once assembled. Additionally, if a warhead confirmation regime requires data from multiple measurements, a modular design will facilitate re-use of already trusted modules for additional measurements, reducing additional authentication and certification needs.
- One-way data flow inhibits the ability of "downstream" modules, which may be able to aggregate sensitive information, to control "upstream" modules and enable "hidden switches" that alter their functionality. This mitigates the risk of using a COTS processor that may not be fully trusted by all parties.

Additionally, the development of a modular architecture has several potential benefits that can facilitate multi-lateral trust:

- Providing a framework of module requirements and interface specifications can facilitate collaborative design with international treaty partners. This would allow partners to agree on the overall design architecture and develop their own modules that conform with the specified architecture.
- Furthermore, the modular design should enable the possibility of interfacing modules provided by different parties. For example, if each party provides every other module, then everyone can be assured that they control both the input and output of the other party's modules. If the functionality of those modules has been verified, then confidence is reinforced in the system's integrity.

A NOTIONAL ARCHITECTURE

Using the design principles defined above, we have established a notional architecture that will allow us to explore the feasibility and efficacy of an inspectable modular architecture for ACTV needs. To begin, we are focusing on four systems with differing capabilities that may be relevant to future warhead confirmation measurement agreements: TRIS (designed for gamma spectrum template matching) [3], TRADS (designed for plutonium mass attribute measurements) [4], CONFIDANTE (designed for direct object comparison with neutron imaging) [5], and MC-15[ii] (designed for neutron multiplicity analysis) [9]. Our assessment of these systems revealed that all four systems can be broken into approximately six modular blocks that share similar functionality across systems. A key commonality is that all four systems eventually operate on a histogram with TRIS and TRADS analyzing gamma energy spectra and CONFIDANTE and MC15 assessing multiplicity histograms.

Based off this initial assessment, we believe we can design an architecture that will allow us to replicate the functionality of our four target systems as well as other systems not considered that operate on histogrammed data. A high-level description of this architecture is depicted in Figure 1. In general, this architecture consists of six different module categories, which are outlined in blue:

1. Power Supply
2. Detector
3. Signal Conditioning and Pulse Shaping Electronics
4. Histogram Builder
5. Processor
6. Output

Also shown is a Time Gate Counter module. This module falls into the general category of Signal Conditioning and Pulse Shaping but is highlighted specifically because of the function it performs. The histogram builder is effectively a multichannel analyzer (MCA), but with a properly designed Time Gate Counter, an MCA can also be used to create multiplicity histograms, which are commonly used for neutron analysis.

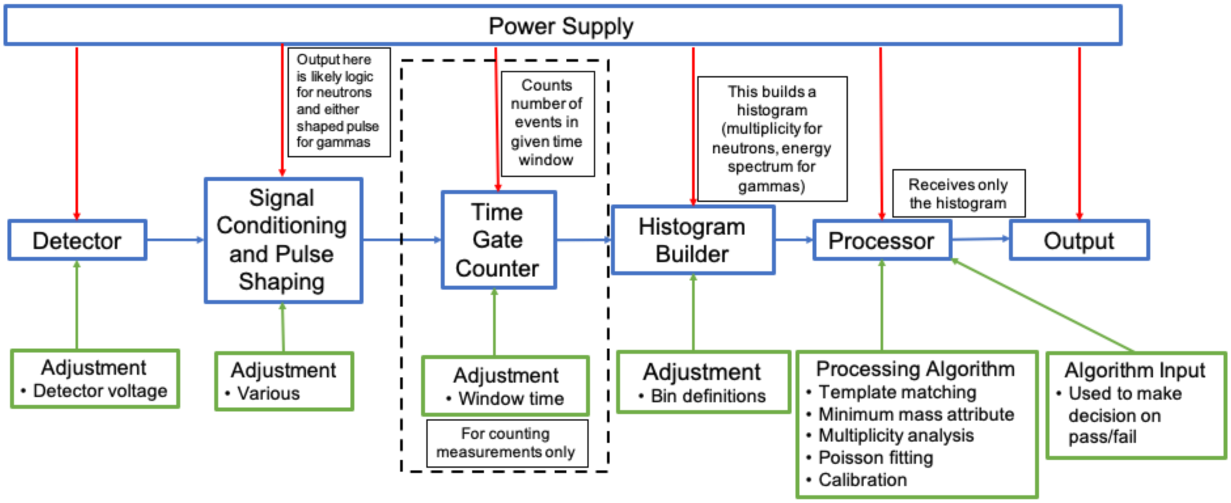
Power Supply
Output here is likely logic for neutrons and either shaped pulse for gammas
Counts number of events in given time window
This builds a histogram (multiplicity for neutrons, energy spectrum for gammas)
Receives only the histogram
Detector
Signal Conditioning and Pulse Shaping
Time Gate Counter
Histogram Builder
Processor
Output
Adjustment
• Detector voltage
Adjustment
• Various
Adjustment
• Window time
For counting measurements only
Adjustment
• Bin definitions
Processing Algorithm
• Template matching
• Minimum mass attribute
• Multiplicity analysis
• Poisson fitting
• Calibration
Algorithm Input
• Used to make decision on pass/fail

Figure 1. A notional modular architecture implementing self-contained module functionality and one-way data flow. Blue boxes denote modules, and green boxes denote possible inputs into the modules. The six module categories are Power Supply, Detector, Signal Conditioning and Pulse Shaping, Histogram Builder, Processor, and Output. The Time Gate Counter is a specific rendition of the Signal Conditioning and Pulse Shaping Module category. All inputs and data flow in the direction of the arrows.

In Figure 1 the green boxes give examples of possible inputs into each module category. In general, each module category provides a basic functionality, which limits the input required for the module to operate. The exception is the Signal Conditioning and Pulse Shaping category, which in practice would likely consist of several modules, each with a specified purpose (e.g. upper and lower level discriminators, integrators, etc.). Inputs to the Processor module include the Processor Algorithm as well as an Algorithm Input, which would be the information required for the algorithm to compare the data to in order to make a determination on whether or not the measurement passed or failed (e.g. a template, attribute threshold, etc.). Examples of the processing algorithms required are based on the four systems we evaluated. While not shown in Figure 1, it is likely that a processor module will also need to have one or more inputs related to encryption and/or data signing. Further details on how each of these four systems fit into this notional architecture can be found in Table 1.

Table 1. Properties of our four target systems broken into the five module categories (excluding the power supply) of our notional architecture.

System	Active Detector Volume	Signal Collection, Conditioning, and Pulse Processing	Histogram Builder	Processor (Analysis Required)	Output Display
TRIS[iii]	Collimated 2"x2" NaI scintillator coupled to a 2" PMT	Shaping preamplifier	Multichannel Analyzer	Chi-squared-based comparison to reference histogram	Confirmation message on user interface
TRADS	High-purity Germanium crtystal	Shaping preamplifier	Multichannel Analyzer	Minimum mass estimate and Pu-600 algorithm	Confirmation message on user interface
CONFIDANTE	1"x1" Stilbene scintillator coupled to a 2" PMT	Pulse shape discrimination and count accumulator for each rotation position	Multiplicity histogram	Chi-square or likelihood estimator comparison to Poisson	Likely a simple confirmation message, but could include the decision metric (actively under development)
MC-15	15 He-3 tubes embedded in a HDPE matrix	Preamplifier, discriminator, and count accumulator for each time window	Multiplicity histogram	Feynman multiplicity analysis	Multiplication and Pu-240 equivalent mass on user display[iv]

The module categories presented in Figure 1 should come as no surprise to those familiar with radiation detection. It is for precisely this reason that development of a modular architecture makes sense. What is unique about this design (when compared to modern radiation detection systems and electronics) is that the processor module is unable to control any of the signal processing until the data has been histogrammed. If the number of bins in the histogram is limited and the bin definitions are strategically chosen, the amount of information contained in the data available to the processor is also limited. Similar to one-way data flow, which prevents the processor from manipulating the functionality of upstream modules, this strategic data reduction further mitigates the risk of using a COTS processor in a trusted system and is a key feature of our proposed architecture.

ONGOING EFFORTS

To date, we have developed a notional architecture that will allow us to replicate the functionality of several radiation detection systems, each with varying functionality that may be relevant to future treaties, through a series of inspectable modules. This modular architecture has many perceived benefits, including increased inspectability, mitigation of unintended data loss, and increased multi-party trust. However, the efficacy of this architecture needs to be tested in order to confirm the value of these benefits.

Our ongoing efforts are focused on the design, prototyping, and testing of the more unique modules in our architecture which are well suited for generalizability. These modules include the Histogram Builder, the Processor, and the Output. We will also pursue the design and testing of the Time Gate Counter, which is a specific realization of the Signal Conditioning and Pulse Shaping module category, that will allow us to expand the capability of the Histogram Builder beyond that of a standard MCA.

Our goal for the Histogram builder module will be to convert analog pulses directly to a histogrammed data set, ideally without the need to digitize the exact value of interest itself (e.g. the pulse height). The number of output channels will be limited to reduce the information available to the processor. We envision a series of adjustable voltage/energy bin boundaries that do not need to be uniformly spaced. Bin edges would be defined by hardware inputs on the module (e.g. dip switches, or value display potentiometers), which would be feasible due to the limited number of channels. By itself, this module is effectively a multichannel analyzer (MCA) that will be designed to promote inspectability. Within our architecture, this module will be a pivotal point in enabling a variety of detection techniques while also minimizing the information available to the processor.

One major question that needs to be answered to enable this proposed design is the determination of the minimum number of channels that is required and how to the optimize variably sized bins for our target use cases. This will entail assessing the algorithms used by TRIS, TRADS, CONFIDANTE, and MC15. Although TRIS only uses 16 channels for analysis, these channels are down-sampled from a 1024-channel MCA. TRADS makes use of a 4096-channel MCA, but typically analyzes a portion of the available energy spectrum. We will need to determine not only the reduced number of channels we would like to use, but also the ideal binning structure to be implemented. A related challenge is determining how to best calibrate an MCA with limited channel count and variably sized bins.

The Time Gate Counter is anticipated to be the most straightforward of the modules we plan to demonstrate. The goal will be to convert the timed logic pulses typically output by counting electronics (e.g. electronics in a multiplicity counter) to a signal that meets the input specifications of our Histogram Builder. Development of this module will allow us to extend the functionality of our Histogram Builder module beyond that of an MCA.

The Processor module is anticipated to be the most complex module we plan to demonstrate. The Processor module will need to be designed to accept the histogrammed data generated by the Histogram Builder and process it using the relevant analysis code. This might include template matching algorithms, attribute algorithms, or calibration algorithms. There will be several challenges in designing an inspectable Processor module designed to perform an array of analysis techniques. Best practices dictate that extraneous functionality should be limited. As such, we will explore options for minimizing the information persistently stored in the module. One design option might be to load programs from external memory devices at run time. We will also need to determine a suitable processor that balances functionality and inspectability. Finally, we will need to assess additional inputs and outputs required to perform our target analysis routines. Depending on the design, this might include ports for processing code, templates and/or thresholds, and keys for encrypting and signing data.

The Output module will attach to the Processor module and will display the result of the analysis. The goal of the output module will be to act as a control valve between the processor and observers. The module will be designed to accept and display only agreed upon information. Consideration will be given on how to balance the amount of information displayed vs. authentication and certification concerns. For example, an output that only displays pass or fail provides the minimum amount of information, and therefore the amount of sensitive information a compromised output could pass is limited. However, additional information, such as the confidence level of a result or diagnostic failure modes, is also useful and should be considered within the architecture.

As we design example modules, we will consider not only the functionality that is necessary to perform a radiation measurement but will also consider ease of inspectability. We will limit extraneous functionality. Input and output testing will be developed generally at the module description level but will be tailored to our custom modules as necessary. The goal will be to minimize module-specific procedures (i.e. different realizations of the same module category should be inspected in similar way) and we will make an effort to define testing procedures that utilize common laboratory devices (e.g. function generators, oscilloscopes, multimeters, etc.) The modules we prototype will be tested individually and as part of a complete detection system, which will in-turn allow us to refine our architecture, iterating on initial functional, authentication, and certification requirements based on lessons learned in the design and testing process.

CONCLUSIONS

The treaty verification community continues to pursue ideas for higher confidence measurements that will confirm warheads while not revealing sensitive information and can be trusted by multiple treaty parties. Pursuing a detector design architecture is a novel approach of incorporating the critical design features required by treaties while simultaneously increasing the flexibility of the system and facilitating authentication and certification of both the detection system and data stream. A modular architecture is ideal for rapidly assembling, authenticating, and certifying a variety of radiation detection systems for ACTV applications and could reduce costs when compared to the use of one or many purpose-built systems.

If successful, our efforts will lead to the development of an architecture that allows for implementation of a variety of current state-of-the art detection systems, while also making it possible to implement new detectors and/or processing algorithms without needing to redesign a system from the ground up. Furthermore, we anticipate that a similar architecture could be used in additional ACTV activities that are not directly related to warhead confirmation or even radiation detection. Processing of histogrammed data or events aggregated over time windows is common and development of trusted hardware to perform these functions could also benefit activities applications including portal monitoring, video processing, active seals, or others.

To date, we have developed a notional modular architecture, that we believe will help meet the needs of ACTV community. The prototyping and demonstration of modules that conform to the proposed architecture will allow us to better understand where improvements can be made. As development and testing of modules progresses, we will continue to revise the architecture based on lessons learned. Our end goal is to provide suggested requirements and specifications for an inspectable modular radiation detection architecture in addition to several examples of modules designed and tested within that architecture. We believe both the architecture and the example hardware will be valuable for facilitating collaborative discussion amongst international communities in preparation for future ACTV activities.

[i] While the RDE was also used in the Intermediate-Range Nuclear Forces Treaty to make measurements on warheads, the purpose of these measurements was to confirm the number of warheads contained in a launch canister (one on the allowed SS-25 missile versus three on the banned SS-20 missile), rather than to confirm that the measured item was indeed a warhead [1].

[ii] MC-15 is the only of these four systems not designed for ACTV applications. Rather, the MC-15 is an emergency response tool with numerous analysis capabilities. For our purposes, we are only concerned with replicating the most basic multiplicity analysis functionality of the MC-15.

[iii] These specifications specifically correspond to those of Next-Generation TRIS (NG-TRIS) [10] .

[iv] This information is available on the MC-15 but would likely not be the information displayed in an ACTV application. Nonetheless, it demonstrates the information available by a single multiplicity histogram (assuming reasonable gate times).

REFERENCES

[1] R. I. Ewing and K. W. Marlow, "A fast-neutron detector used in verifcation for the INF Treaty," *Nuclear Instruments and Methods in Physics Research A,* vol. 299, pp. 559-561, 1990.

[2] International Partnership for Nuclear Disarmament Verification, "A Framework Document with Terms and Definitions, Principles, and Good Practices," November 2017. [Online]. Available: http://ipndv.org/wp-content/uploads/2017/11/WG1-Deliverable-One-Final.pdf.

[3] K. D. Seager, R. L. Lucero and T. W. Laub, "Trusted Radiation Identification System," in *Proceedings of the INMM 42nd Annual Meeting,*, Indian Wells, 2001.

[4] D. J. Mitchell and K. M. Tolk, "Trusted Radiation Attribute Demonstration System," in *Proceedings of the Institute of Nuclear Materials Management 41st Annual Meeting*, New Orleans, 2000.

[5] P. Marleau, R. Krentz-Wee and P. Schuster, "Proof of concept demonstration of CONFIDANTE (CONfirmation usinga Fast-neutron Imaging Detector with Anti-image Null-positive Time Encoding)," in *Proceedings of the INMM 59th Annual Meeting*, Baltimore, 2018.

[6] D. Archer, "3rd Generation AMS Overview," in *Joint U.S-U.K. EIVR-58 Authentication Workshop*, 2014.

[7] D. Keir, D. M. Chambers, S. Høibråten, S. Backe, S. Allen and H. E. Torkildsen, "K-Norway Initiative: Research into Information Barriers to Allow Warhead Attribute Verification Without Release of Sensitive or Proliferative Information," in *Poceedings of the INMM 51st Annual Meeting*, Baltimore, 2010.

[8] A. Swift, T. Weber, M. Valdez, K. McIntosh and J. Benz, "Findings from the Portal Monitor for Authentication and Certification (PMAC) Project," in *Proceedings of the INMM 60th Annual Meeting*, Palm Desert, 2019.

[9] C. E. Moss, M. A. Nelson, R. B. Rothrock and E. B. Sorensen, "MC-15 Users Manual," Los Alamos National Laboratory, 2018.

[10] P. B. Merkle, T. M. Weber, J. D. Strother, J. Etzkin, A. J. Flynn, J. C. Bartberger, W. C. Amai and L. F. Anderson, "Next Generation Trusted Radiation Identification System," in *Poceedings of the INMM 51st Annual Meeting*, Baltimore, 2010.