Food-for-Thought Paper: Equipment Authentication for Nuclear Dismantlement Monitoring

Working Group 3: Technical Challenges and Solutions
November 2017

Introduction

Equipment authentication and certification needs of the host and monitor are interdependent and balancing these needs is a challenge for a nuclear disarmament monitoring regime. Both will be discussed briefly next, although this paper will focus on equipment authentication.

First, equipment authentication is a process by which a monitoring party to a treaty or agreement obtains confidence that the information reported by the monitoring equipment accurately reflects the true state of a monitored item. With monitor-supplied equipment, this is in general less of a concern initially because the monitor has control over the acquisition process and can complete necessary testing to ensure proper functionality of the equipment. If the monitoring equipment is supplied by the host, then initial authentication of the equipment becomes a more significant monitor concern. In either case, once the equipment is introduced into a regime, then authentication remains an important concern of the monitor because the equipment may be inspected and/or operated by the host, and may be stored in locations under host control. In addition to ensuring initial functionality of the equipment, authentication also allows the monitoring party to maintain confidence that the monitoring equipment has not been altered, removed, or replaced, and functions throughout the regime such that it provides accurate and reproducible results at all times.[1]

Second, equipment certification is the process by which the host party to a treaty or agreement assures itself that a monitoring system meets safety and security requirements and will not divulge classified or proliferative information to a monitoring party.[2] As is the case with monitor authentication of monitor-supplied equipment, certification by the host of host-supplied equipment may be much easier than certification of monitor-supplied equipment. To maintain equipment certification throughout the regime the host will want

[1] Department of Energy, NNSA, Office of Nonproliferation and Arms Control and AWE for the UK Ministry of Defence, *Joint US-UK Report on Technical Cooperation for Arms Control*, (Washington, DC: Department of Energy, 2015).

[2] Department of Energy, *Joint US-UK Report on Technical Cooperation for Arms Control*.

confidence that the monitoring equipment has not been altered, removed, or replaced, and continues to function throughout the regime as expected. In short, certification is primarily a concern of the host, while authentication is primarily a concern of the monitor.

A determination to use either monitor-supplied equipment or host-supplied equipment will be regime dependent. There may be different reasons for choosing one option over the other, which would depend on the specifics of the regime. This paper provides an overview of equipment authentication objectives, techniques, and challenges for nuclear dismantlement monitoring applications and focuses on equipment authentication of host-supplied equipment. Although not the focus of this paper, monitor-supplied equipment could reverse roles and challenges, and the ability to gain confidence in the supplied equipment. In this case, however, many of the same discussion points contained in this paper would continue to apply, although they may apply from a perspective of reversed roles.

Authentication Principles

Objectives

Authentication techniques aim to provide assurance that systems function as designed, are assembled as designed, exhibit only expected functionality, and contain no hidden controls. These authentication techniques are used to assure the integrity of data collected by the monitoring equipment while respecting the host's need to protect proliferative or other sensitive information, and are essential in ensuring that data gathered during verification processes can be trusted. Although equipment authentication is conducted principally for the benefit of the monitoring party to gain assurance that the equipment is functioning as expected and is providing accurate information while conducting verification activities, the host party also has equities in the process that must be respected. The monitoring party's objectives in the equipment authentication process are:

- To ensure that verification equipment design does not contain features that could be exploited to subvert the processes in which the equipment is to be used (i.e., to ensure that the equipment design possesses only expected functionality and does not have hidden features);
- To ensure that the equipment used matches the exact design specified in the agreed treaty verification protocol (i.e., to ensure that the equipment has been assembled as designed);
- To ensure that the environment in which the equipment is used matches that specified in the treaty verification protocol (i.e., to mitigate external influences that may influence the equipment functions);
- To ensure that the procedures under which the equipment is used—including any procedures governing its manufacture, storage, and entry/egress from the facility where verification takes place—do not allow for the verification process to be

subverted, and that those procedures are followed (i.e., to ensure that the equipment functions as designed throughout its lifecycle); and

- To ensure that the interplay of the authentication processes and approaches used with the equipment does not allow the verification process to be subverted (i.e., to ensure that the equipment functions as designed under use case scenarios).

The host party's principal focus is equipment certification and the need to be assured that sensitive information is protected while conducting verification activities, and while conducting any equipment authentication activities. This might include information that relates to Treaty Accountable Items but that is not released or subject to verification under the agreed treaty verification protocol, but might also include information about facilities, processes, environments, and other items that are neither accountable nor releasable under the verification protocol. In contrast to the monitor's objectives, the host's objective for equipment authentication is to be assured that the information collected supports host compliance with the treaty or agreement.

Finally, it is important to note that both parties, if acting in good faith, have the shared objective of ensuring that verification equipment produces accurate and reproducible results. This contributes to confidence-building between the two parties, and helps third parties build confidence in the process.

Confidence in Authentication

In practice, there will likely be tension between the monitor's objective of obtaining the highest level of confidence in host-supplied monitoring equipment, and the host's objective of maintaining equipment certification. Complete satisfaction of the monitoring party in equipment authentication processes may only come with a level of information release and intrusiveness that the host party is not willing to tolerate. This has two implications: first, equipment authentication techniques and processes may therefore themselves be subject to negotiation, and agreements between monitoring and host parties will therefore specify the techniques and approaches to be used for each piece of verification equipment throughout its lifecycle (potentially extending all the way from pre-concept to disposal); and second, that complete confidence by each party in the equipment authentication process may not be achievable. The majority of the rest of this paper deals with the former point, while this section briefly discusses the latter.

Given that total confidence in equipment authentication may not be achievable by either party, each must decide how much it needs in order to meet its objectives. This will need to be balanced against the costs incurred (which may be high if the most exhaustive technical authentication options are pursued) and other resource constraints, including time and availability of personnel. It would therefore be helpful for each party to develop a way to understand the contribution of any given approach to confidence in equipment authentication, in isolation and in combination with other techniques, in order that the balance between confidence that may be achieved and the resources required to achieve it can best be accomplished. Any such method might also help the parties understand how

best to reach a mutually acceptable negotiated outcome for equipment authentication processes.

There are various approaches to gain confidence in equipment authentication to balance host and monitor needs. One might involve defining a broad set of evaluation criteria for equipment authentication, perhaps with an associated scoring methodology; another might look at confidence in authentication from a probabilistic perspective. There is no accepted method for addressing this problem as yet, although some steps have been taken: efforts to apply international standards (e.g., Information Technology security standards) have been explored by Kouzes et al. to establish assurance levels for authentication procedures.[3] Other analytical approaches to decision support under uncertainty (e.g., Beaumont et al. examine Bayesian Belief Networks[4] and Game Theory[5] in the context of arms control verification more broadly) may also be helpful in quantifying and analyzing confidence in authentication activities.

Ultimately, the application of any such process will require a cost-benefit analysis in which each party determines whether or not it wants to pursue a given approach. As part of that, each party will also need to determine target and minimum acceptable levels of confidence from equipment authentication in each circumstance. Precisely how these confidence levels are expressed will depend on the method by which they are determined.

Verification Equipment and Lifecycle Authentication

During the life of a treaty, various constraints and requirements may be placed on equipment authentication activities. There is no certainty that these constraints and requirements will remain constant in all places at all times. Similarly, equipment authentication is not carried out at a single point in the lifetime of verification equipment: it is instead a set of complementary processes and technical measures carried across the lifecycle of the equipment, designed to achieve the objectives laid out above.

Concept and Design

Equipment used in verification activities may be commercially available, custom-designed with commercially available components (in whole or in part), or custom-designed with

[3] R. T. Kouzes, R. Hansen, and W. K. Pitts, *Introduction to Methods Demonstrations for Authentication* (Richland, WA: Pacific Northwest National Laboratory, 2002).

[4] P. Beaumont et al., "Confidence Analysis for Nuclear Arms Control: SMT Abstractions of Bayesian Belief Networks," in *20th European Symposium on Research in Computer Security, September 21–25, 2015, Proceedings, Part I* (Vienna, Austria, 2015).

[5] P. Beaumont et al., "Confidence Analysis for Nuclear Arms Control: SMT Abstractions of Game Theoretic Models," in *Proceedings of the 57th Annual Meeting of the Institute of Nuclear Materials Management* (Atlanta, GA, 2016).

entirely bespoke components. Early lifecycle decisions on verification equipment drive much of the subsequent approach to equipment authentication:

- Commercial-off-the-shelf (COTS) systems can deliver good technical performance with a low associated purchase cost. They may, however, require modification in order to be fit for purpose, and may have functionality that—while useful in their intended application—is extraneous and unhelpful in a treaty monitoring context. Software in these systems is likely to be relatively complex, and is unlikely to have been designed to be robust to subversion. COTS systems are unlikely to have been designed with authentication in mind.
- Using custom-designed equipment with COTS components allows monitor and host to have a greater level of understanding of the design intent and final implementation of the verification system, allows for the possibility of joint design, and makes full design disclosure easier. Security features tailored to monitoring applications can also be incorporated;[6] design for authentication is possible, including in any software; and use of COTS components helps to keep costs relatively low.
- Using custom-designed equipment built with entirely bespoke components retains all the benefits of a custom-designed system down to the component level. Such a system could allow the greatest possible level of design understanding by the host and monitoring party, if there is full-design disclosure between both parties. Implementation of a jointly designed process could address host and monitor requirements for the equipment during the design process. Depending on complexity of the component-level, custom-designed equipment in question, design and manufacture costs could be very high.

Incorporating equipment authentication concepts and measures during the design process of verification equipment has been recommended by various researchers,[7] which suggests that the entirely COTS option may only be suitable in less sensitive areas of verification activity. The main disadvantage of this "design-for-authentication" approach is the considerable extra associated up-front expense. However, if made available to both parties, the resulting comprehensive documentation of system hardware and software will facilitate easier authentication of the equipment throughout its entire lifecycle; and, if done sufficiently well, it would help to avoid potentially costly modifications in future.

Early consideration also needs to be given as to whether the overall authentication approach should rely on authentication by association, or by authentication applied to the specific equipment that is used during verification, or by a combination of the two. Authentication

[6] K. Seager et al., *Trusted Radiation Identification System* (Sandia National Laboratories, 2001).

[7] D. W. MacArthur and J. K. Wolford, Jr., "Information Barriers and Authentication," in *42nd Annual INMM Meeting* (Indian Wells, CA, 2001); B. D. Geelhood et al., *Design Guidelines for Authenticable Systems, PNNL-13386* (Richland, WA: Pacific Northwest National Laboratory, 2001); and K. Allen, "UKNI Project Context and Concepts," January 13, 2016, available at http://ukni.info/mdocs-posts/ib-project-context-and-concepts/.

by association relies on the availability of a (ideally large) pool of identical items of verification equipment, from which the monitor selects a subset for use in verification processes and a separate subset for authentication activities. This allows for the fullest range of monitor equipment authentication capabilities to be deployed against the second subset of equipment. In contrast, if authentication activities are to be applied to the specific equipment used during verification, either the monitor could be allowed to conduct only non-destructive testing prior to using the equipment during verification, or the host could have the option of releasing the equipment following its use (the decision would depend upon the monitoring agreement or treaty between parties). It is worth noting that it may well be that the host would be unwilling to allow equipment to leave certain sensitive facilities—perhaps for reasons of information security.

Manufacture and Supply Chain Issues

Depending on the design concept for the verification equipment in question, treaty partners could consider lifetime buys of systems or components—or, if the components are entirely bespoke, sufficient production capacity—to allow a large enough pool of verification equipment for authentication by association while guarding against obsolescence. Each party will need to assure itself that the procurement route chosen does not introduce any risks to the authentication process that it does not understand or that it is not willing to tolerate. If COTS components or systems are involved, then this could potentially involve some discussions with third parties, if the relevant manufacturing facilities are not based in territories under the control of the monitoring or host parties. If entirely bespoke components are used, then joint production becomes a possibility—although the precise details of how this might work have not been well developed to date.

Equipment development and fabrication should consider joint or private authentication processes for monitoring, design, functional testing (destructive and non-destructive), and operational procedures. If bespoke components are used, this process could extend down to the component level. After the equipment has been fabricated and assembled—and any mid-assembly authentication processes conducted—chain of custody (CoC) measures may be applied to assure treaty partners that unauthorized access to authenticated items has not occurred.[8] These CoC measures can be used throughout the treaty lifetime to maintain confidence or to identify events requiring investigation (refer to Inspection Procedures and Chain of Custody below for additional discussion on CoC measures).

Deployment and Use in Verification Activities

As monitoring equipment and systems move to the installation phase for the regime, additional authentication measures may need to be performed. This could be performed when receiving the equipment at a joint-custody monitored storage area as well as when

[8] Nuclear Threat Initiative, "Chain of Custody, Tags, Seals & Tamper-Indicating Enclosures," September 16, 2015, available at http://www.nti.org/analysis/articles/tags-seals/; and J. M. Benz, J. E. Tanner, and L. L. Duckworth, "Templating as a Chain of Custody Tool for Arms Control," in *35th ESARDA Annual Meeting - ESARDA Symposium, May 28–30, 2013* (Bruges, Belgium, 2013).

installing equipment in the facility where verification activities are to be conducted. Acceptance testing of equipment to be used in the facility should include inspection of any CoC measures (e.g., tamper indicating devices or surveillance video and verification of unique identifiers on the system and system components) applied post-manufacture. Acceptance testing will likely be limited to non-destructive functional testing of hardware and software that is intended to establish authenticity of the equipment and the functions it is designed to perform. Physical oversight and presence of host and monitor personnel should be evaluated prior to equipment deployment and use for the development of authentication procedures.

For equipment that requires a persistent presence in a host facility—a portal monitor, for example, or a tamper-indicating seal—the monitoring party may well have limited access to it once it is installed. Continuous monitoring party presence at the facility for the duration of the treaty is unlikely, and certainly cannot be guaranteed. CoC measures (discussed in Inspection Procedures and Chain of Custody below) may therefore be required to ensure that monitors are able to detect any attempt to subvert the equipment while monitors are not present. This may include remote monitoring, although hosts may not be willing to allow the unmediated transmission of signals from sensitive facilities that would be necessary for this to be implemented. On-site inspections by the monitoring party can be used to authenticate CoC measures on the monitoring systems. If authentication activities are to be conducted in host- or jointly controlled facilities, then the provenance of any technical equipment used to conduct authentication activities also needs to be considered—a monitoring party may not trust the results of authentication conducted using host-provided laboratory equipment. These issues also apply to items held in a host-controlled storage area, rather than a joint-custody storage area.

If authentication activities are to take place at monitor-controlled facilities, CoC measures may be required to assure both parties that the designated equipment has been received without modifications. Authentication activities will need to be considered for all functional testing (destructive and non-destructive) of the system (refer to Hardware Authentication below), operational procedures, maintenance and repair procedures, and storage of authentication items (such as equipment, CoC tools, and trusted references). For authentication procedures involving destructive functional testing, equipment would be taken out of the monitoring regime. Procedures developed for the authentication measures would need to consider the presence of host or inspector personnel to observe authentication processes and operation by host or inspector personnel either under joint or private processes.

Authentication Techniques and Processes

Some recommendations for authentication techniques and processes for treaty verification equipment are suggested here, based upon past implementation and operational

experiences[9] and emerging and evolving needs for future nuclear arms control initiatives.[10] They are meant to provide a starting point for researchers considering how best to tackle this complex problem, but are neither prescriptive nor complete. As monitoring requirements evolve, policy directives change, and advancements in new technologies systems are realized, new approaches will continue to need to be developed and applied to authentication measurement systems and processes.[11]

Design Information Verification

Design information on verification equipment can be used to confirm that the system should be able to perform the expected function and that the design does not contain any additional functionality or covert features.[12] This can be facilitated by a fully transparent design,[13] and should be done with reference to the complete hardware and software design documentation on an actual system. Although complete design documentation would ideally guarantee that all functionality can be clearly defined and understood, even limited design documentation analysis might help to provide some confidence; alternatively, joint system development allows mutual understanding and ownership of design intent from the concept and design phase onwards.

When design information is limited, then verification of the equipment is more difficult. This might be the case for COTS systems in particular. Functional testing may assist the authentication process, but functional testing is not a substitute for complete hardware and software design information. In the case of limited design information, treaty partners would have to come to agreement on the equipment authentication process and may be willing to allow the use of verification equipment where design information has not been fully shared or is not available.

Hardware Authentication

---

[9] Department of Energy, *Joint US-UK Report on Technical Cooperation for Arms Control*; R. Kouzes et al., *Authencation Procedures—the Procedures and Integration Working Group, PNNL-13550* (Richland, WA: Pacific Northwest National Laboratory, 2001); and D. K. Haucket al., *Defining the Questions: A Research Agenda for Nontraditional Authentication in Arms Control, LA-UR-10-03785* (Los Alamos, NM: Los Alamos National Laboratory, 2010).

[10] R. T. Kouzes, R. Hansen, and W. K. Pitts, *Introduction to Methods Demonstrations for Authentication*; and J. Yan and A. Glaser, "Nuclear Warhead Verification: A Review of Attribute and Template Systems," *Science & Global Security* 23 (2015): 157–70.

[11] J. Doyle, *Scenarios for Exercising Technical Approaches to Verified Nuclear Weapons Reductions, LA-UR-10-02687*, (Los Alamos, NM: Los Alamos National Laboratory, 2010); and A. Pregenzer, "Advancing the Goals of NPT Article VI," *The Nonproliferation Review* 15 (2008): 529–38.

[12] Department of Energy, *Joint US-UK Report on Technical Cooperation for Arms Control*; B. D. Geelhood et al., *Design Guidelines for Authenticable Systems, PNNL-13386*; and J. Whichello et al., *Authentication of Systems Used for IAEA Safequards* (Vienna, Austria: International Atomic Energy Agency).

[13] K. Allen, "UKNI Project Context and Concepts."

Hardware authentication procedures will likely differ based on where the testing will be conducted (i.e., in a host facility or in a monitor facility). Testing at a monitor facility could include destructive and non-destructive testing, and could use a wide range of capabilities to the extent that the monitor feels is proportionate to the confidence sought.[14] In contrast, functional testing at the host facility will be somewhat limited in scope as the equipment clearly cannot be subject to destructive analysis. Non-destructive techniques that could be used include:

- **Trusted references**, including unclassified calibration and reference sources, could be incorporated in the functional testing of measurement systems to authenticate the system under a range of testing conditions.[15]
- **Electronic signal measurements** of the hardware, perhaps at agreed nodes in any system electronics, could be performed to look for extra functionality or potential vulnerabilities that could influence the true system output.
- **Physical inspection** of the hardware using visual inspection.
- **Image comparison techniques**, for example against a trusted system's components or against historic measurements of the same system. Some common imaging systems include digital cameras,[16] x-ray instruments,[17] and scanning electron microscopes.

These techniques will involve a range of intrusiveness—depending on such factors as the degree of dismantling required of the system—and will therefore likely depend also upon accessibility of constituent parts of the system. This will also impose restrictions on where specific techniques can and cannot be conducted within a treaty regime. Any equipment used for authentication activities must also itself be trusted, and may itself need to be subject to authentication procedures.

Software Authentication

If software is present then it will be a critical element that requires special attention, as it will contain a large part of the functionality and decision-making logic of a system. Software authentication processes therefore need to verify high-level code intent (that the claimed functionality of the code implements the intended functionality of the system), code

[14] R. T. Kouzes, R. Hansen, and W. K. Pitts, *Introduction to Methods Demonstrations for Authentication*; R. Kouzes et al., *Authencation Procedures—the Procedures and Integration Working Group, PNNL-13550*; and G. K. White, "Trends in Hardware Authentication, LLNL-CONF-674264," in *INMM Annual Meeting* (Palm Springs, CA, 2015).

[15] R. T. Kouzes, R. Hansen, and W. K. Pitts, *Introduction to Methods Demonstrations for Authentication*.

[16] G. E. Weeks et al., "Analog Video Authentication and Seal Verification Equipment Development," in *ANS/INMM 9th International Conference* (Savannah, GA, 2012).

[17] E. I. Esch, D. J. Desimone, and R. E. Lakis, *Preliminary Report for Using X-Rays as Verification and Authentication Tools, LA-US-16-22320* (Los Alamos, NM: Los Alamos National Laboratory, 2016).

correctness (that the code itself implements the claimed functionality), and—ideally—the validity of the translation of this high-level code down to machine code. Functional testing may also contribute to overall authentication by verifying the performance and operation of the monitoring system.[18]

Automated analysis of the source code (including separate and combined analysis) should be performed using static and dynamic analysis. Manual inspection and code review is recommended—although this may be impractical to do exhaustively in many cases. Developments in the use of formal methods in software verification may also provide a route to additional confidence in software authentication, although these are as yet at the proof-of-concept stage.[19] Finally, as with hardware authentication, ancillary equipment and software may itself be subject to authentication, depending on where it is used.

Inspection Procedures and Chain of Custody

Inspection procedures for the authentication techniques are created to maintain confidence in the inspection regime, including any equipment that is used within it. Although equipment used in such regimes should have features engineered into its design that prohibits the disclosure of proliferative or sensitive information, procedural controls (by means of inspection procedures) may also serve to protect sensitive or proliferative information from unintended disclosure or to provide a deterrent to host modifications of equipment (by means of random selection procedures)[20] especially in conjunction with CoC measures.[21]

These procedures may include private and joint examinations of the entire system and hardware and software components; examinations may cover some of the techniques discussed in the sections above. Due to host safety and security concerns, it is likely that private examinations by a monitoring party can only be performed off-site—considerable restriction may be placed on the extent of inspection procedures conducted on-site. Examination of CoC measures, however, may well be conducted jointly, and are important for verifying the physical integrity of equipment and maintaining continuity of knowledge on a system and components.[22] Equipment (such as tags and seals) and procedures (such as installation and inspection of the equipment) can be combined to provide a complex CoC

---

[18] R. T. Kouzes, R. Hansen, and W. K. Pitts, *Introduction to Methods Demonstrations for Authentication*; B. D. Geelhood et al., *Design Guidelines for Authenticable Systems, PNNL-13386*; and J. K. Wolford et al., "Software Authentication, UCRL-JC-144254," in *42nd Institute of Nuclear Materials Management Annual Meeting* (Indian Wells, CA , 2001).

[19] N. Evans, "Software Development and Authentication for Arms Control Information Barriers," in *Proceedings FM 2015: Formal Methods—20th International Symposium, June 24–26, 2015* (Oslo, Norway, 2015).

[20] R. Kouzes et al., *Authencation Procedures—the Procedures and Integration Working Group, PNNL-13550*; and D. MacArthur et al., *Random Selection as a Confidence Building Tool, LA-UR-03607* (Los Alamos, NM: Los Alamos National Laboratory, 2010).

[21] Nuclear Threat Initiative, "Chain of Custody, Tags, Seals & Tamper-Indicating Enclosures."

[22] J. Whichello et al., *Authentication of Systems Used for IAEA Safequards*; and G. E. Weeks et al., "Analog Video Authentication and Seal Verification Equipment Development."

regime that controls access to the verification equipment, not just to treaty-accountable items.

Some examples of CoC measures include:

- **Containment technologies**, such as tags and seals, can be used to demarcate items of interest within the treaty; and in the case of seals, may also provide indication of attempted access to the item or area being contained.[23]
- **Unique identifiers**, which ensure that no swapping of components of the system has occurred.
- **Cameras** can be used to image tags, seals, or unique identifiers. By comparing the current image against a previous or library image, the integrity or tampering of a tag or seal may be detected. If necessary and permitted, the resulting data could be authenticated using cryptographic methods.[24]
- **Surveillance systems** (camera or video) can monitor the system and activities performed on the system, and may use similar analysis technologies and authentication methods to still images.[25]
- **Tamper-indicating devices or enclosures** provide an additional controlled boundary to items of verification or authentication equipment.[26]

Summary and Authentication Challenges

Authentication techniques and processes for nuclear monitoring regimes are crucial to ensuring that conclusions from data collected during these regimes are accurate and genuine. Factors affecting equipment authentication techniques to establish validity and confidence include:

- **Design information** of each system (including hardware and software),
- **Functional and operational testing** of each system's hardware and software,
- **Inspection procedures** to meet treaty obligations and perform authentication of the systems, and
- **CoC measures** implemented throughout the lifecycle of authentication activities.

---

[23] Nuclear Threat Initiative, "Chain of Custody, Tags, Seals & Tamper-Indicating Enclosures."

[24] G. E. Weeks et al., "Analog Video Authentication and Seal Verification Equipment Development."

[25] G. E. Weeks et al., "Analog Video Authentication and Seal Verification Equipment Development"; and R. T. Kouzes and J. L. Fuller, "Authentication of Monitoring Systems for Non-proliferation and Arms Control," in *IAEA Symposium* (Vienna, Austria, 2001).

[26] Nuclear Threat Initiative, "Chain of Custody, Tags, Seals & Tamper-Indicating Enclosures."

The authentication of monitoring equipment is challenged by advancements in technology. Potential benefit from additional quality of measurement data may increase, but it is likely that the increase in complexity of software and hardware likely to be used in monitoring devices will introduce further challenges. One example of such a challenge is new security concerns for data collection and information protection. To meet these challenges, development of authentication methods to support technology concepts with higher levels of complexity and functionality are needed, again highlighting the value of incorporating authentication measures during the design process.

Development of the highest achievable authentication level for the monitoring regime requires a compromise be made between costs, intrusiveness to host operations, and confidence levels assured for the host and monitor. The implementation of a combination of authentication techniques, procedures, and measures provides a robust set of authentication assurances: to prevent single-point failures, to provide multi-layered defense measures, and to increase the probability of detecting tamper events and vulnerability exploitations. As political and security environments change, equipment authentication techniques will continue to evolve and will need to address and provide solutions that anticipate future requirements.

International Partnership for Nuclear Disarmament Verification

The International Partnership for Nuclear Disarmament Verification (IPNDV), is an ongoing initiative that includes more than 25 countries with and without nuclear weapons. Together, the Partners are identifying challenges associated with nuclear disarmament verification, and developing potential procedures and technologies to address those challenges.. Learn more at www.ipndv.org.

About Working Group 3: Technical Challenges and Solutions

Throughout Phase I, the IPNDV Technical Challenges and Solutions Working Group has investigated effective technologies, methods, and procedures that can be used for the specific technical challenges in the dismantlement process, such as identifying a nuclear device, maintaining chain of custody, and protecting proliferation sensitive material. This group is co-chaired by Sweden and the United States.