SANDIA REPORT
SAND2017-12727
Unlimited Release
September 2017

Minimally Intrusive Verification of Deep Nuclear Warhead Reductions: A Fresh Look at the Buddy-Tag Concept

Sharon DeLand,[1] Alexander Glaser,[2] Jay K. Brotz,[1] Heidi Smartt,[1] Andrew Kim,[2] Dan Steingart,[2] and Benjamin Reimold[2]

Prepared by
[1]Sandia National Laboratories, Albuquerque, NM, USA
[2]Princeton University, Princeton, NJ, USA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

SAND2017-12727
September, 2017
Unlimited Release

Minimally Intrusive Verification of Deep Nuclear Warhead Reductions: A Fresh Look at the Buddy-Tag Concept

Sharon DeLand, Alexander Glaser, Jay K. Brotz, Heidi Smartt, Andrew Kim, Dan Steingart, and Benjamin Reimold
Sandia National Laboratories, Albuquerque, NM, USA
Princeton University, Princeton, NJ, USA

Abstract

Future nuclear arms-control agreements may place numerical limits on the total number of warheads in the nuclear arsenals of states. Verifying these limits may require inspectors to account for individual warheads, both deployed and non-deployed. This task could be accomplished with unique identifiers, but standard tagging techniques may be unacceptable in this case due to host concerns about safety and intrusiveness. To resolve this dilemma, we revisit the so-called "Buddy Tag" concept first proposed by Sandia National Laboratories in the early 1990s. The conceptual innovation in the Buddy Tag was to by separate the tag from the treaty limited item itself. Verification of the pairings between tags and limited items would take place during a short-notice inspection, where the host would be required to produce one buddy tag for each item. Sensors on the Buddy Tag would show that it had not been moved to the inspected site after the inspection was declared (e.g., within the last 24–48 hours). If the inspector counted more (or fewer) treaty limited items than Buddy Tags at the inspected site, a treaty violation could be asserted. Using a number of single-site inspections, an inspecting party can hold the host at risk for discovery of violating the treaty at an enterprise level by possessing more treaty limited items than the treaty allows. In this project, we developed a buddy-tag prototype for demonstration and evaluation purposes. This paper summarizes the performance requirements for an advanced Buddy Tag, the proposed conduct of operations, the design choices and functionalities of the different subsystems, and initial testing results. The report also summarizes peer review feedback obtained throughout the project.

ACKNOWLEDGMENTS

This work is generously supported by the U.S. Department of State's Bureau of Arms Control, Verification and Compliance (AVC) and the U.S. Department of Energy's Consortium for Verification Technology under Award DE-NA 0002534. Alexander Glaser wishes to thank Jim Fuller and Keith Tolk who first mentioned the concept of the Buddy Tag, making this collaboration possible. The authors also wish to thank Stan Fraley, Sabina Jordan, Ross Hymel, and Keith Tolk for feedback on throughout this project. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

TABLE OF CONTENTS

1. INTRODUCTION

Future arms control initiatives may place limits on the total number of nuclear warheads possessed by states party to such an agreement or, more specifically, may place limits on non-deployed warheads and/or nonstrategic weapons. Note for example, that the US Senate Resolution of Ratification for the New START Treaty required the Obama Administration to engage Russia on limits on non-strategic weapons before seeking further reduction in strategic weapons. Furthermore, General James Mattis, former Commander of U.S. Central Command and current U.S. Secretary of Defense, raised the question in a U.S. Senate Armed Services Committee hearing in January 2015 [1]: "Could we re-energize the arms control effort by only counting warheads vice launchers?"

When a treaty-limited declared inventory is numerous and widely dispersed, it is impractical to verify limits are being observed by counting all of the items in the inventory—to be effective, the counting process has to occur essentially simultaneously across the entire enterprise.

Tagging treaty-limited weapons with identifiers can, under the right circumstances, provide an effective approach for verifying numerical limits. In an exemplar tagging-based verification approach, the number of tags created is equal to the numerical limit in the treaty. Each tag is affixed to (or associated with) a unique treaty-limited item, typically during an initialization phase. During an on-site inspection, inspectors observe the treaty-limited items, authenticate the tags and verify their integrity. This protocol provides confidence that the observed treaty-limited items are part of the allowed stockpile. The observation of any untagged item is evidence of a treaty violation. The use of tagging thus transforms a numerical limit into a ban on untagged items [2,3].

Direct tagging of warheads or associated storage gear may be difficult to implement in practice, however, because the host may have safety, performance, or other concerns, and inspections could be highly intrusive. Development of concepts to support verifying limits on non-deployed and nonstrategic warheads therefore faces important challenges. On the one hand, the capability to verify numerical limits on weapons in these categories could be useful in both bilateral and multilateral contexts. On the other hand, the locations and movements of warheads and weapons in these categories may be considered sensitive information, and robust verification measures to ensure the authenticity and integrity of a declared treaty limited item could put such information at risk.

To address this dilemma, research staff at Sandia National Laboratories and Princeton Universities, supported by the State Department Verification Fund program, revisited the "Buddy Tag" concept first proposed by Sandia National Laboratories in the early 1990s [4]. The key conceptual innovation of the Buddy Tag is that it could be possible to use the tagging concept to verify numerical limits without actually attaching the tag to the limited item or even uniquely associating a specific tag with a specific item. The tag then functions as something like a passport. These innovations offer the potential to limit operational impacts between inspections, manage safety and security concerns and verify numerical limits without revealing patterns in movements between facilities.

Given the challenges that tagging warheads could entail, the Sandia and Princeton team proposed exploring the applicability of the Buddy Tag concept to verifying numerical limits on warheads. The two questions to be addressed were how the Buddy Tag concept could be applied to relatively small treaty limited items such as warheads and what improvements in size and performance might be expected with modern hardware and software techniques. Sandia focused on developing the concept of operations, defining high-level concept of requirements, developing a simple enclosure, and conducting peer reviews of the concept. Princeton focused on designing and developing the evaluation platform, including the motion detection subsystem at the core of the Buddy Tag concept. This report describes key results of this joint effort, including a concept of operations, a description of the evaluation platform Buddy Tag prototype, and results of peer reviews conducted during the project. Note that Princeton is providing a separate report on the motion detection algorithm.

2. PRIOR WORK

Fetter and Garwin [3] discuss the use of tagging to verify numerical limits in arms control treaties, including a concept for limits on troop deployments in geographical areas, tanks, mobile ICBMS, and cruise missiles. They identify nine general characteristics of an effective tagging system. Such a system:

1. Must make it impossible to copy the tag without detection
2. Must be impossible to spoof
3. Must make it impossible to move the tag from one limited item to another without detection
4. Must not aid the monitoring party in locating weapons in real time
5. Should only reveal information required for verification (e.g., no sensitive data about the data or deployment patterns)
6. Must be reliable and operate with a low false alarm rate
7. Should not impair or impede normal functioning or operations
8. Should be reliable in the full range of environments in which the limited weapons will be stored or deployed
9. Should not be excessively costly. Fetter and Garwin suggested that a tagging system cost on the order of a few percent of the cost of the limited systems might be reasonable.

The Buddy Tag concept seeks to relax the third requirement in this list.

Fetter and Garwin also discuss the pros and cons of tagging systems. One important application is the use of tagging in conjunction with, and as a supplement to, on-site inspection. As noted in the introduction, on-site inspection of individual sites does not provide conclusive information about the total number of weapons a monitored party may have unless all sites are inspected at the same time. With the addition of tags, the observation of a single limited weapon without a tag is a strong indication of a violation. Fetter and Garwin also suggest that monitored destruction of the tags could alleviate the need for detailed monitoring of weapon destruction processes.

There are several challenges for using tagging systems. The first is that tags cannot directly detect hidden stockpiles of weapons. However, the use of tags to identify and distinguish items that are part of the declared stockpile makes it difficult to mix in excess weapons into the allowed stockpile without detection. The risk of detecting excess weapons in declared, inspected facilities could drive a party that wishes to cheat to create a parallel system for deployment, storage, maintenance, and production, increasing costs and the potential for detection through other means. This particular example highlights the relationship of a tagging system to a broader regime. A tagging system is not a sufficient verification system by itself, but must operate within a larger regime.

A second challenge for tagging systems is when the limited item is not easily distinguishable from legitimate items that may appear in the civilian enterprise. Fetter and Garwin note for example, that tanks are readily identifiable and have no application in the civilian enterprise. However, if tags were used to limit troop levels and deployments, there might be questions about how to handle a civilian found with an automatic weapon – he or she could be a police officer but could also be a soldier out of uniform. In the same way, an application of tags to monitoring non-deployed warheads may have to address this challenge as some warheads are stored in containers.

A third challenge for tagging systems is when a tag cannot be directly applied to the limited weapon itself. Mobile ICBMs are typically placed into canisters; tags would likely need to be applied to the canisters instead of the missiles themselves. This type of application raises the risks of shell games that allow excess weapons to be moved in and out of declared facilities without detection. Fetter and Garwin note the need for other measures such as seals to ensure that dummy weapons or empty containers are not being used to hide the existence of excess weapons.

The Buddy Tag concept proposed in the 1990s built on the fundamental understanding of tagging systems but proposed that tags could still effectively contribute to verifying numerical limits even if the tag was not attached to the limited weapon and even if it was not uniquely associated with a specific weapon. The concept works as follows: [4]

Each party was issued a specified number of Buddy Tags, one for each treaty limited item. The treaty partner was expected to keep the Buddy Tag "near" the treaty limited item so that the tag could be produced when requested. Verification relied on short notice inspections. Once an inspection was declared for a site, neither treaty limited items nor Buddy Tags could enter or leave the site. Portal-perimeter monitoring or other reconnaissance measures would be used to confirm that treaty limited items had not left the site. Sensors on the Buddy Tag would show that it had not been moved to the inspected site after the inspection was declared (e.g., within the last 24–48 hours). The ability to produce a Buddy Tag for each treaty limited item declared and observed in an inspection provided confidence that treaty limited items found at the site are part of the population of items allowed within the limits of the treaty.

The use of random, short-notice inspections across the declared enterprise gave a finite probability of detecting excess (undeclared items) that may be kept within the declared infrastructure.

Application of this concept to potential future limits on warheads offers some important differences. First, the original Buddy Tag concept was developed with missiles in mind as the treaty limited item. The concept included inspecting any facility on site large enough to contain a missile. On-site intrusiveness was limited because of the size of the missiles. Applying this concept to smaller treaty limited items such as a warhead increases the intrusiveness as more facilities are capable of holding a warhead than a missile. Second, the ability to monitor the site perimeter during the period between when the inspection is announced and when it is conducted is essential. Smaller treaty limited items (compared to missiles) can make such monitoring more challenging and/or more intrusive. The current project did not consider how to accomplish monitoring the site.

Figure 1 shows examples of the Buddy Tag concepts from the 1990s and from this project.

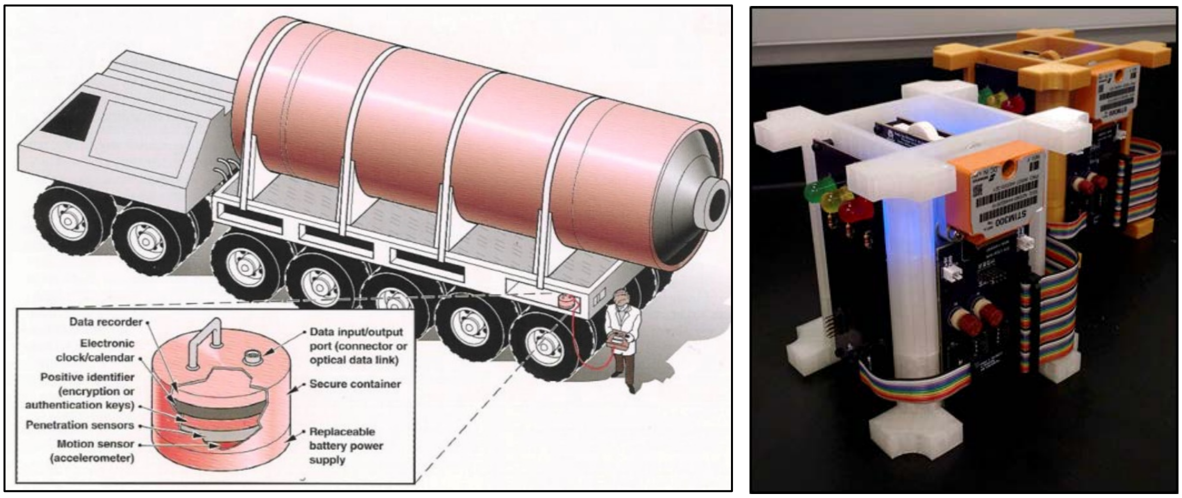

Figure 1: Buddy Tag Concepts. On the left is an artist's conception of the original Buddy Tag for confirming limits on numbers of treaty limited missiles. Shown on the right is the 2017 buddy-tag package (discussed further below) during field-testing. Image credit, original concept (left): James Fuller [5].

3. CONCEPT OF OPERATION

In order to define a concept of operations, we assume that a treaty is being negotiated between two parties to place limits on non-deployed nuclear warheads. We assume that treaty partners wish to verify these limits while reducing risks that operational patterns can be discerned as a result of the monitoring regime. In a tagging regime using Buddy Tags, a party would declare a certain number of treaty limited items and receive exactly one tag for each of these items from the monitoring party. The basic idea is that, during a short-notice on-site inspection later on, the inspected party must be able to present one Buddy Tag for every declared treaty limited item encountered at the site. Per the 1990s design, the Buddy Tag will contain a motion sensing system that can determine if the tag has been moved a significant distance in between the time the inspection is called and the time the inspection is completed.

With respect to safety and security considerations, the project team assumed that the Buddy Tags were battery-powered and did not use any type of remote communications. The team originally posited that the Buddy Tags would operate continuously albeit potentially in a low power mode. Operated in this mode, the Buddy Tags would require some sort of way to "forget" older data not relevant to the inspection. One reviewer (Jordan) suggested an alternative approach in which the Buddy Tags are not powered up until placed for inspection. This approach significantly reduces the power burden and reduces the data collected to the specific time period of interest. This approach is incorporated into the CONOPS Discussion section below. The project team did not make any other implementation-related assumptions.

The concept of operations considers four phases of operations: (1) Start Up or Initialization, (2) Enterprise Operations Between Inspections, (3) Conduct of On-Site Inspections and (4)

Destruction of Buddy Tags. Iterations of the concept of operations have been discussed in [6] and [7].

Start up or Initialization

Each party gives the other a set of Buddy Tags equal to the declared number of items that party has. At the beginning of the treaty, the declared number of items could exceed the eventual limit under the treaty. The monitored party is responsible for distributing the Buddy Tags within its enterprise so that there is one Buddy Tag for each treaty-limited item at each site.

Enterprise operations between inspections

The monitored party's nuclear weapons infrastructure is expected to be able to operate as "normally" as possible in between inspections. Non-deployed warheads may move between sites as needed to support deployment, storage, maintenance, and surveillance/testing activities. Warheads may also be moved to support dismantlement; this project did not explicitly consider monitored dismantlement.

The monitored party is required to keep Buddy Tags associated with treaty-limited items "near" the associated item. This could be a centralized repository for each site or separate storage areas in or near each individual storage facility on a site. If a treaty limited item is moved between sites, a Buddy Tag goes with it.

Conduct of short-notice inspections

The primary verification measure is based on short notice on-site inspections. The objective of such inspections is to gain confidence that there is an authentic Buddy Tag for each Treaty Limited Item present, that Buddy Tags have not been brought on site to make up for a shortfall and that treaty limited items have not been removed to cover up the presence of excess weapons.

Once the inspection is called, the designated site goes into a stand down—that is, traffic in and out of the site is either halted or severely constrained. In addition, some operations may need to be halted, including potentially the movement of treaty limited items. The purpose of the stand down is to aid verification that treaty limited items have not been taken off site prior to the arrival of the inspectors. Given the relatively small size of warheads, it is possible that most operations would need to halted. Effective monitoring, either through national technical means or through cooperative portal/perimeter monitoring is required to ensure that treaty limited items are not removed from the site. Options for this complementary monitoring were beyond the scope of the project; the team notes that such monitoring is a requisite for any tagging based scheme, not just Buddy Tags.

Note that it is possible that treaty limited items would be in transit between sites when the inspection is called. The verification regime would have to specify how this situation might be addressed. One option might be to allow these items to be brought on site and segregated in some way until they are inspected. Associated Buddy Tags would show movement for these items and could introduce uncertainty about compliance. A more complete analysis is needed to understand how likely this situation is and how much uncertainty would be introduced.

Assuming the Buddy Tags powered off between inspections, the host must power them up once the inspection request is received. Depending on how the Buddy Tags are stored between inspections, the host may move them to a display configuration before turning them on. Note that there must be a time limit between the time the inspection is called and the time by which Buddy Tags must be turned on. The parameters affecting this time limit are how quickly the Buddy Tags could be turned on and how far a Buddy Tag could be moved in that time. The time must be sufficiently small that Buddy Tags could not be moved on site from a different location.

Figure 2 illustrates the basic procedure of a notional Buddy Tag based inspection. After inspectors arrive on site, they count and inspect the Buddy Tags presented for each treaty limited item to confirm their authenticity and to verify that the tags have not been moved within the agreed upon time. Inspectors then visually confirm the number of treaty limited items without directly accessing them.

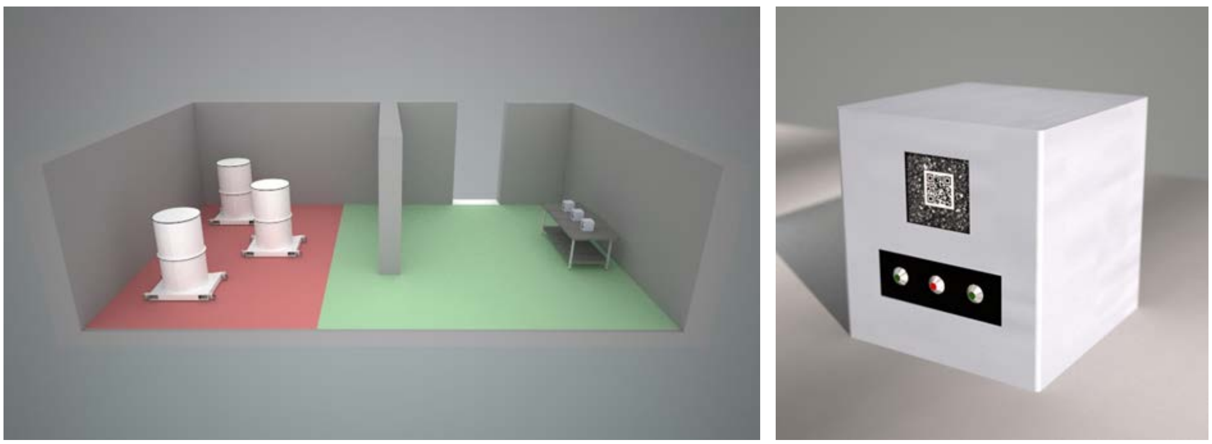

Figure 2: Scenes from a notional Buddy Tag inspection. During an onsite inspection, inspectors would access the Buddy Tags in the non-sensitive area (green) to inspect them. Inspectors would then request to visually confirmation of treaty-limited items (stored in the red area). Shown on the right is a close-up of a Buddy Tag with a unique identifier (shown in the image as a Reflective Particle Tag [7]) and LED indicators in a tamper-indicating enclosure. Image credit: Tamara Patton.

The way in which the monitoring party develops confidence that there is an authentic Buddy Tag for each treaty limited item varies somewhat depending on how and where the Buddy Tags are stored with respect to the treaty limited items as well as the features of the Buddy Tag. In essence, a relationship between each Buddy Tag and the treaty limited items must be established. Consider the following options:

- All Buddy Tags are stored at a central location on a site and the monitoring party inspects both the Buddy Tags and all (declared) treaty limited items. In this case, the inspector counts, authenticates, and reads each Buddy Tag in the central repository. Authenticating a Buddy Tag requires establishing its authenticity, perhaps through a unique identifier, and assessing it has not been tampered with through various tamper-indicating devices. Methods for reading the Buddy Tag for detected motion could vary; the project team assumed a simple red/green light type of interface. Assuming none of the Buddy Tags indicated they had been moved, inspectors would then visually observe each declared treaty limited item at the site and verify that the number observed matches the declaration.
- Buddy Tags are distributed throughout a site in close proximity to the associated treaty limited items. In this case, the monitoring party would provide a declaration of treaty limited items and locations. Inspectors could choose a subset of locations to visit,

authenticating the Buddy Tags as described above, counting them, and making sure that the number of Buddy Tags matches the number of treaty limited items in that area.

- In either case, it would be beneficial to allow the inspection to access other areas large enough to contain a warhead even if no warheads are declared to be in those areas. The value of this step is to create a finite probability that any excess warheads that were simply hidden rather than removed from the site will be detected.

It is possible that an inspector may come across containers that look like warhead containers but are empty. The inspection protocol would allow the inspectors to verify any item resembling a treaty limited item but declared not to be one. This could be as simple as verifying that a container is empty or it could utilize a measurement. In New START, something similar is done with a neutron absence measurement.

Another potential concern is the presence of items that are not governed by the treaty (e.g., components resulting from dismantlement may be stored on the same site as warheads). The verification regime needs to address whether these items are segregated and what measures could be taken to ensure treaty limited items are not being hidden in such areas.

Destruction of Buddy Tags associated stockpile reductions
In the event of stockpile reduction (verified separately) Buddy Tags must be jointly destroyed or returned to monitoring party. Some form of joint storage of destroyed Buddy Tags may be necessary.

Discussion
When implemented effectively, the Buddy Tag approach makes it difficult for an inspected party to store undeclared treaty limited items at a declared site. The party would be forced to hold such items at undeclared sites, which may be difficult to conceal from national technical means over time, especially when it is assumed that adequate security and a parallel support infrastructure would have to be maintained.

Figure 3 illustrates two important scenarios that are effectively addressed with the Buddy Tag concept. Both scenarios assume that a future treaty places numerical limits on treaty limited items, i.e., on the number of warheads that each party possesses. States obtain the number of tags that correspond to the number of items declared in their baseline declarations. In Scenario 1, non-compliance is detected because not enough Buddy Tags are present at the storage site and cannot be moved there in time. In Scenario 2, the state is compliant, but treaty limited items are observed by an inspector in an unexpected location; since these items are accompanied by an identical number of Buddy Tags, however, the inspector accepts them as part of the declared inventory.

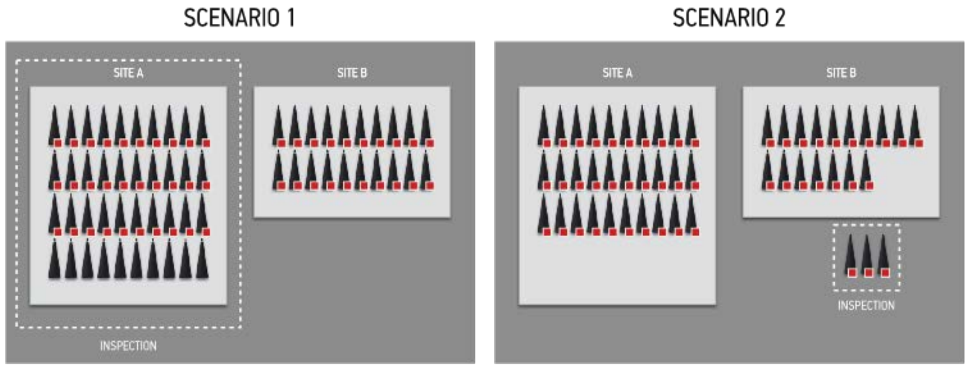

Figure 3: Two scenarios that are addressed with the Buddy Tag concept. In Scenario 1, a state stores treaty limited items at two storage sites (A and B), but declares fewer than actually exist; if the inspector randomly selects Site A for an inspection, non-compliance will be evident as not enough Buddy Tags are present at that site (and tags can't be moved there without detection). In Scenario 2, the state is compliant with the treaty, but the inspector observes treaty limited items in an unexpected location; since these items are accompanied by an identical number of Buddy Tags, however, the inspector accepts them as part of the declared inventory.

In the fairly basic version of the Buddy Tag concept outlined above, there is no connection or association between the tag and the treaty limited item. This allows the host to use any tag to represent any treaty limited item. This feature could allow the treaty partner to protect operational details (movements of specific items between specific sites) and was considered as an option in the original Buddy Tag concept.

One critique that has repeatedly emerged with respect to the Buddy Tag concept is that it does not account for the possibility that a monitored party might replace authentic treaty limited items with a mockups, concealing the true items elsewhere. This concern potentially can be mitigated in different ways. First, such items would no longer be "tagged" as part of the legitimate stockpile. As noted in the Prior Work section, the use of tags deters mixing legitimate and excess stockpiles; such diverted items might need to be managed in a parallel structure. If the verification regime allowed for inspections of suspect facilities and untagged items were discovered anywhere they would be a clear indicator of a violation. Another option would be to consider seals to ensure containers are not opened outside of an inspector's presence. This option could be intrusive if impacts to monitored party operations are considered. Finally, it could be possible to couple the Buddy Tag with additional technical measures to confirm the presence of a warhead on a random sampling basis. While this would counter some of the benefits of the Buddy Tag concept, it may provide sufficient confidence.

A second critique is whether the Buddy Tag offers any advantages over a simple declarations-based regime. The authors argue that there are two benefits. The first is that the Buddy Tag regime offers independent evidence that observed items are part of the legitimate stockpile. An inspection-based regime can confirm that observations are consistent with a declaration at a given site but offer no direct evidence about the relationship of these observations to the size of the larger stockpile. Tagging regimes are specifically designed to address this problem. The second benefit is more conditional. The Buddy Tag approach could offer up a mechanism to verify limitations in the absence of a declaration. Suppose treaty partners did not wish to share the distribution of their treaty limited weapons. Buddy Tags could be used to assure the monitoring party that observed weapons are part of the legitimate stockpile without detailed declarations. Monitoring parties may require wide access to declared sites to raise confidence in this approach.

With respect to the CONOPS described above, there are a number of variations that are similar that could be explored. One additional idea emerged that merits highlighting here. This is the possibility of using Buddy Tags in a regime in which the parties agree on a limit but do not declare how many items they actually have. Inspections of declared enterprises could help provide confidence that limits are being observed while severely limiting information about operations and deployments.

Finally, the procedures for authentication and certification of Buddy Tags (how the monitoring party and monitored party establish and maintain trust that the Buddy Tags operate within safety and security requirements, respond accurately and appropriately to activity in the environment, and do not record information beyond that required by the treaty) in this regime are an important consideration but were not in scope for this project. Such procedures depend in part on the details of the implementation.

4. HIGH LEVEL REQUIREMENTS

Based on the concept of operations outlined above, we outlined four high-level requirements and six design goals. The intention with respect to both requirements and design goals is to specify the performance objective to be met without specifying implementation options. The requirements and design goals are summarized in the Tables 1 and 2 below.

5. IMPLEMENTATION APPROACH

Prototyping Platform

Over the course of the project, the Buddy Tag implementation evolved from a prototype to an evaluation platform that allowed iterative development of Buddy Tag components and supported software development and testing . The evaluation platform, and the motion detection algorithms will be described in more detail separately. For completeness, this report provides a brief summary of both. Development of the prototype has been discussed in [6] and [7].

The evaluation platform uses a modular design, with each tag-subsystem contained on its own printed circuit board and mounted on one side of a 3D-printed support structure (Figure 4). This allows for quick design changes and swapping of components to compare performance. Computing power is provided by a Raspberry Pi 3, and motion detection is enabled by the Sensonor STIM300, an advanced inertial measurement unit (IMU) based on micro-machined electro-mechanical system (MEMS) technology [8] Power to the Raspberry Pi and the STIM are supplied by six 18650 lithium-ion battery cells with a total capacity of about 20,000 mAh, giving the system a battery life of more than 24 hours.

Table 1: High Level Requirements for the Buddy Tag

Req. No.	Requirement	Verification Method
1	The Buddy Tag shall indicate to the inspector that it is authentic.	Analyze the authentication mechanism for possibility of false positives; analyze the system for ability to bypass authentication mechanism
2	If the Buddy Tag has been tampered at any point following initialization, it shall indicate to the inspector that it has been tampered. Otherwise, it shall indicate to the inspector that it has not been tampered. It is assumed that each Buddy Tag is used only once following initialization.	Look for indication of not being tampered; tamper the tag in various ways and look for indication of tamper
3	If the Buddy Tag has moved (translated) more than one meter from its original location during the short notice inspection period, it shall indicate this motion to the inspector.	Translate the tag more than one meter in various ways and look for indication of movement
4	If the Buddy Tag has moved (translated) less than .75 meter from its original location during the short notice inspection period, it shall indicate to the inspector that it has not moved.	Look for indication of not moving under quiescent as well as vibrational and translation less than .75 meter conditions

Table 2: Design Goals for the Buddy Tag

Goal No.	Goal (in order of priority)	Evaluation Method
1	Minimize time to verify the authenticity, tamper state, and motion state of the Buddy Tag	Measure time to perform each verification
2	Design for a ten year lifetime	Analyze design for power consumption over ten years
3	Minimize opportunities for tampering	Analyze design and prototype for opportunities for tampering
4	Maximize reliability	Analyze design and prototype for reliability concerns
5	Maximize robustness to handling	Analyze design and prototype for robustness to handling
6	Maximize robustness to environment	Analyze design and prototype for robustness to a variety of environments

The tag's current status is indicated to the inspector (or the developer) by three LEDs: Yellow indicates that the tag has not detected a displacement since activation but hasn't reached a pre-defined minimum uptime of, say, 24 or 48 hours yet; green indicates that the tag has not detected any illicit displacements in a time period exceeding the minimum up-time; red indicates a violation. This instantaneous feedback functionality also aids in the development and fine-tuning of the algorithm parameters.

Figure 4: Buddy Tag Modules. The module with the inertial measurement unit (left) forwards the incoming data to the GPIO pins of the Raspberry Pi 3 located on a separate module (middle), where a dedicated algorithm processes the data in real-time. Result are displayed via the output module (right).[7]

The Buddy Tag has a number of separate subsystems, most of them linked to a central microcontroller. These include standard systems such as a real-time clock, data storage, battery management, and the LED display. The tag also requires robust tamper-indicating capabilities and some of them may also be connected to the microcontroller. As a default unique identifier for confirmation of a tag's authenticity, we envision the Reflective Particle Tag (RPT), which has been under development at Sandia National Laboratories since the 1990s as a robust, low-cost, hard-to-counterfeit passive tagging system for treaty verification and international safeguards applications [9]. The RPT could be read out with a non-contact handheld tag reader if disturbance of the Buddy Tag is undesired [10]. The central (and most unique) subsystem, however, is the motion-detection subsystem, which is discussed briefly below and described more fully in a separate report.

Motion-detection Subsystem

As recognized in the original work on the Buddy Tag [4], the critical and most unique element of the Buddy Tag is the motion-detection subsystem. The Buddy Tag has to reliably distinguish stealthy motion from all relevant types of environmental noise in a variety of locations throughout the warhead lifecycle. The ambient vibrational noise may vary significantly from location to location, while false-alarm rates must remain extremely low under all circumstances. These requirements inform the choice of hardware and algorithm for the motion-detection subsystem*. After considering a range of options [6] the Princeton team selected the STIM300. The STIM is an inertial measurement unit consisting of three high-stability accelerometers, three high-accuracy gyroscopes, and three inclinometers. The unit uses a 5 V power supply and a 32-bit RISC ARM microcontroller and communicates via a standard RS422 interface [8]. In contrast to other

* Already, by the late 1970s, Sandia National Laboratories had developed an "incredibly sensitive motion sensor," which was considered at the time for a similar application in the context of a possible SALT 2 verification [5].

packages with similar performance, the STIM300 is ITAR-free, i.e., it is not subject to export controls, which facilitates research, development, and testing of Buddy Tag prototypes. The sensitivity of the STIM is about 2 μg for the least significant bit (LSB).

For development and testing, data is recorded for a fixed period of interest (e.g., 30 seconds, during which the system can be exposed to shocks and movements) and analyzed at a later point. For deployment of the Buddy Tag, data processing would have to take place in real time. In both cases, algorithms are only allowed to "look back in time" to decide if a violation has occurred. The Princeton team has so far explored two approaches for analyzing the data: an integration method to directly estimate the tag's displacement and a heuristic approach based on the autocovariance of the data. These approaches are described more fully in [7] and will be reported on separately by the Princeton team.

6. ENCLOSURE CONSIDERATION

A tamper indicating enclosure is needed to ensure the integrity of the Buddy Tag's operation and accurate indication of its status. Robust tamper-indicating measures ensure that the host has not tampered with the motion detection subsystem to hide undeclared movement or introduced counterfeit Buddy Tags to hide excess treaty limited items. One of the primary design considerations in developing the enclosure is to minimize penetrations as much as possible, recognizing that most enclosures will have to have some penetration and opening. Best practice would be to locate these openings physically far from security critical components.

As part of the project, Sandia designed a tamper-indicating enclosure that could be used to demonstrate and discuss desirable features. The enclosure consists of a two-part metal box (base and lid) with welded aluminum sections. Creating an enclosure without welded sections would have cost significantly more. The team considered a one-piece design (perhaps fabricated through 3D printing) but determined that two pieces were required to allow access to the current Buddy Tag components, allowing its continued use as an evaluation platform and demonstration device. Holes were fabricated in the lid and base for application of tamper-indicating devices (seals). A seal such as the Cobra Seal could be used on these hasps. The enclosure is shown in Figure 5.

With the selection of metal as the material for the enclosure, eddy current scanning can be used to detect any anomalous penetrations. A small window inset into the metal allows viewing of the tag LEDs – this window can be tempered glass or plastic. An adversary would need to open the enclosure in order to replace a damaged piece of glass or plastic. The window was minimized to reduce available surface area that may be prone to attack.

The need to change or charge batteries can also affect enclosure design. Since the current enclosure uses a two-part design, batteries can be changed or charged as needed. As noted above, a more robust design would minimize penetrations, or locate penetrations away from security critical components. For instance, a port for recharging could be designed into the TIE, but located such that security critical components would be difficult to access for illicit purposes.

Enclosure designs must also consider dissipation of heat generated by electronics. While the selection of a metal enclosure what primarily based on its tamper-indicating properties, the metal also acts as a heat sink.

(a) *(b)* *(c)*

Figure 5: Buddy Tag Enclosure. (a) Side view showing the opening for the window and openings for the hasp seal. (b) Top view showing the Buddy Tag placed within the enclosure. (c) Side view showing the top in place on the enclosure.

7. TECHNICAL REVIEWS

Sandia conducted technical reviews with three knowledgeable subject matter experts: Sabina Jordan (lead engineer for the original Buddy Tag concept), Ross Hymel (an embedded systems engineer knowledgeable in development of unattended tags and sensors for arms control and safeguards) and Keith Tolk (an expert in development of arms control technologies, tamper-indicating devices, and information security measures). Key points from these reviews are summarized below:

- The availability and effectiveness of additional monitoring to assure that limited items do not leave a site once an inspection has been called is very important for the effectiveness of the Buddy Tag concept.

- Reconsider the statement of the motion-sensing requirement. The original concept framed the requirement in terms of an acceleration.
- If an IMU is used as the motion sensor, examine all six axes of acceleration (3 angular and 3 linear). Otherwise, the host could move an object a little bit, rotate it, move it a bit more in the same direction and effectively zero out the total movement.
- Could a GPS be used rather than an IMU? Fully integrated GPU receivers can be had for less than $20 these days, and they are relatively low in power (50mA @ 3.3V is typical). One would have to relax the 0.75m requirements though, as most have accuracy (CEP) of around 2.5m. However, because the GPS provides a measure of absolute position, as long as the sensor hasn't been moved more than perhaps 10 or so meters, there would be inherent assurance that it hasn't been brought on site from a separate location (that would be many kilometers away).
- One option for power management is to allow the monitored party to turn the Buddy Tag on when the inspection is called. This prevents collection of data between inspections and reduces power requirements. There would need to be some sort of time limit for powering on all of the Buddy Tags.
- The effectiveness of the Buddy Tag is completely dependent on the tamper-indicating measures employed and on the unique identifier (e.g., RPT). Any final design will need to ensure these measures are robust and have been subjected to vulnerability assessments.
- The concept of operations should be clear that the declaration will associate specific Buddy Tags with specific items or specific storage areas (e.g., magazines) during the inspection. This step is needed to allow the inspection results to be extrapolated to the larger population. The Sandia team notes that this comment applies if the monitoring party only inspects a subset of the treaty limited items.
- While the specifics of site preparations and shutdown in preparation are beyond the scope of this project, one option that may be worth exploring is implementing the shutdown and monitoring at the magazine level.
- Other tamper-indicating enclosures have included designs that place the batteries outside the enclosure, allowing for easier replacement while protecting security-critical components. This could be considered in a future tamper indicating enclosure design.
- The current enclosure uses aluminum. Stainless steel could be a good option. The welds used in the current enclosure were a cost saving measure and are not optimal. One option for reducing the need for welds is to spin the stainless steel in a cylindrical container. The Sandia team notes that an eddy current problem could be used on the welds to establish a unique identifier.
- The use of a window to observe the LEDs makes sense. Windows have been used in other containment and surveillance equipment (e.g., cameras) that have undergone multiple vulnerability assessments.
- The on-board processing capability (e.g., the Raspberry Pi) could be used to monitor its tamper status and state of health and signal when these are compromised.
- The motion detection and assessment problem (distinguishing intentional movement) has been and continues to be a difficult problem worthy of further research.

8. NEXT STEPS

There are a number of activities that could meaningfully extend the work of the current Buddy Tag collaboration. In approximate chronological order, the recommended next steps are:

1. Requirements validation with stakeholders
2. Modeling and simulation of concept
3. Technical improvements
    a. Long life power source
    b. Wireless power charging
    c. Active tamper detection
    d. Improved passive tamper resistance and indication
    e. Improved motion detection subsystem
    f. Reduced cost
4. Requirements verification
5. Exercise
6. Vulnerability analysis

Requirements validation with stakeholders: The requirements that the team developed were drawn from the original Buddy Tag effort in the early 1990s as well as the team's concept of operations for the tags. It would be a good idea to validate both the concept of operations and the requirements with relevant stakeholders, including government experts in treaty negotiations and treaty operations. Some requirements – for example, the motion requirements – were somewhat arbitrary and could be refined. There had been a question about whether the tag should indicate that it has moved at all (beyond small movement induced by normal vibration) or the tag should indicate that it has moved a large enough distance (within the short notice period) to be moved from one site to another. In the end, without analyzing the actual enterprises within which this might be deployed, we required that the tag indicate if it had been translated one meter (and not indicate if it had been translated less than .75 meter), as an arbitrary target for development. Validating these requirements with stakeholders could yield a requirement for the motion subsystem that is not arbitrary.

Modeling and simulation of concept: The concept of operations for the Buddy Tag is very simple to explain but difficult to understand on an enterprise scale. Modeling the concept and simulating the confidence gained while varying the size of the enterprise, the time of the short notice inspection period, and the motion detection parameters of the tag could yield some insight as to whether the concept has flaws. It could also help the negotiators of a treaty using Buddy Tags to determine how many inspections would be necessary each year in order to have sufficient confidence in a warhead limitation.

Technical improvements: The design of the current Buddy Tag, while a modernization of early efforts, could be improved in several ways. If the concept of operations requires a tag that is always on (i.e., it does not need to be switched on at the beginning of the short notice period prior to an inspection), the tag will need to be designed to have more stored power, to use less power, or both. Alternatively, the tag could be designed to be recharged (or even continuously charged in some kind of dock). This charging could be designed to be wireless, using something like resonant inductive charging, so that no enclosure penetrations are needed, or the enclosure could have embedded photovoltaic cells to harvest energy from the environment. The enclosure could include tamper planes that are actively monitored such that a sensed tamper event would render the tag permanently and visibly compromised. Other active tamper sensors could include extreme temperature swings or visible light inside the enclosure. The passive tamper indication and tamper resistance of the enclosure could also be improved. Improvements could be made to the motion detection of the Buddy Tag, to decrease both false positives (indicating motion when the tag is not moved) and false negatives (indicating no motion when the tag is moved), though more testing is needed to understand the current performance of the Buddy Tag. Supervised machine learning could be evaluated as a better way to distinguish between a tag motion in violation of the treaty concept from tag motion that is not in violation. Finally, the design of the Buddy Tag could be made less expensive. The unit currently has an IMU with a price of several thousand dollars and an equally expensive custom aluminum enclosure. In order to deploy several thousand Buddy Tags in a treaty regime, it is likely that the price will need to be lower.

Requirements verification: After a design is completed, the Buddy Tag prototype should be tested for compliance with each requirement. Each requirement has a verification method listed in the High-Level Requirements section. These verification methods could be developed further in some cases (such as the goals, especially for environmental testing) to assess the performance of the tag and lead to design improvements.

Exercise: Several Buddy Tags could be built and put through a live play exercise with a hypothetical treaty and a hypothetical nuclear enterprise. This would have the benefit of validating the concept of operations and the technical design of the tag as well as allowing a more in-depth peer review by arms control experts.

Vulnerability analysis: After the Buddy Tag has been verified through testing and design improvements have been made, a vulnerability analysis should be performed to understand the most likely pathways to a successful tamper. The results could help to inform more design improvements.

9. CONCLUSION

There are currently no established methods for an inspecting party to independently confirm a numerical limit on treaty limited items if the items themselves are highly sensitive in nature. In the case of nuclear warheads in particular, affixing unique identifiers directly to these items may be considered unacceptable by the host, and inspections may also reveal sensitive operational information. The Buddy Tag concept offers a radical solution to this dilemma by separating the treaty limited item from its tag. We examined the opportunities that this technology would offer and the challenges it would face for the verification of next-generation nuclear arms control treaties.

On the conceptual level, we find that the Buddy Tag concept does indeed enable more flexible and much less intrusive verification approaches. Moreover, the concept offers the possibility for gradual enhancements as parties to a treaty become more comfortable with the verification provisions. Preliminary results also indicate that the performance of the Buddy Tag could benefit enormously from a number of technological advances that have been made since the concept was first considered 25 years ago.

Finally, and perhaps equally importantly, the Buddy Tag offers a platform to demonstrate a wide range of relevant technologies without involving sensitive nuclear information. In particular, the Buddy Tag concept can be used to develop and benchmark the performance of unique identifier technologies, tamper indicating enclosures, secure electronics, secure software, and advanced algorithms for motion detection. Research in this area would not involve sensitive information of any kind and may therefore also offer opportunities for international collaboration. Since the Buddy Tag concept offers particularly simple and non-intrusive implementations, it might be appealing to a number of weapon states and could facilitate early consideration of a verification regime that tracks treaty limited items. Taken together, the Buddy Tag concept may therefore help chart a path toward multilateral nuclear arms-control agreements.

10. ENDNOTES

[1] General James N. Mattis, USMC (Ret.), Testimony, Senate Armed Services Committee, Global Challenges and U.S. National Security Strategy, January 27, 2015.

[2] Thomas Garwin, Tagging Systems for Arms Control Verification, AAC-TR-10401/80, Analytical Assessment Corporation, Marina del Rey, CA, sponsored by the Office of Technology Assessment, Washington, DC, February 1980.

[3] Steve Fetter and Thomas Garwin, "Using Tags to Monitor Numerical Limits in Arms Control Agreements," Chapter 3 in Barry M. Blechman (ed.), Technology and the Limitation of International Conflict, Washington, DC, 1989, pp. 33–54.

[4] Sabina E. Jordan, Buddy Tag's Motion Sensing and Analysis Subsystem, Sandia National Laboratory, Albuquerque, New Mexico, 1991.

[5] Jim Fuller, "US START TID Development Program: The Quest for Extreme Security Unique Identifiers (1986–1992)," April 2006, www.inmm.org.

[6] Sharon DeLand, Alexander Glaser, Jay K. Brotz, Andrew Kim, Dan Steingart, and Ben Reimold, "Minimally Intrusive Verification of Deep Nuclear Warhead Reductions: A Fresh Look at the Buddy-Tag Concept," 57th Annual INMM Meeting, Atlanta, Georgia, July 2016.

[7] Benjamin Reimold, Jay K. Brotz, Sharon DeLand, Alexander Glaser, Michael Hepler, Andrew Kim Thomas Schaffner, Heidi Smartt, and Dan Steingart, Development and Demonstration of a Buddy Tag Prototype, 58th INMM Annual Meeting, Indian Wells, CA, July 2017

[8] Detailed data sheet and user manual for the STIM300are available at www.sensonor.com/gyro-products/inertial-measurement-units/stim300.aspx.

[9] Keith Tolk, "Reflective Particle Technology for Identification of Critical Components," 33rd Annual INMM Meeting, Orlando, Florida, July 1992.

[10] Heidi A. Smartt et al., "Status of Non-contact Handheld Imager for Reflective Particle Tags," 55th Annual INMM Meeting, Atlanta, GA, July 2014.

11. DISTRIBUTION

1 Mr. Dan Wurmser
US Department of State

(electronic copy)

1 Dr. Alex Glaser
Princeton University

(electronic copy)

1	MS0159	Sharon DeLand	Org. 0159 (electronic copy)
1	MS1371	Dianna Blair	Org. 6830 (electronic copy)
1	MS1371	Tina Hernandez	Org. 6832 (electronic copy)
1	MS1371	Amir Mohagheghi	Org. 6833 (electronic copy)
1	MS1373	Mary Clare Stoddard	Org. 6831 (electronic copy)
1	MS1373	Jay Brotz	Org. 6831 (electronic copy)
1	MS1373	Heidi Smartt	Org. 6833 (electronic copy)
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories