SANDIA REPORT
SAND2017-XXXX
Unlimited Release
Printed October 2017

Developing Reliable Safeguards Seals for Transportation Casks to be Applied, Verified, and Removed by State Operators

Robert J. Finch, Heidi A. Smartt, Risa Haddal

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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: http://www.ntis.gov/search

SAND2017-11187
Printed October 2017
Unlimited Release

Developing Reliable Safeguards Seals for Transportation Casks to be Applied, Verified, and Removed by State Operators

Robert J. Finch, Heidi A. Smartt, Risa Haddal
International Safeguards and Engagements
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS1371

Abstract

Once a geological repository has begun operations, the encapsulation and disposal of spent fuel will be performed as a continuous, industrial-scale series of processes, during which time safeguards seals will be applied to transportation casks before shipment from an encapsulation plant, and then verified and removed following receipt at the repository. These operations will occur approximately daily during several decades of Sweden's repository operation; however, requiring safeguards inspectors to perform the application, verification, and removal of every seal would be an onerous burden on International Atomic Energy Agency's (IAEA's) resources. Current IAEA practice includes allowing operators to either apply seals or remove them, but not both, so the daily task of either applying or verifying and removing would still require continuous presence of IAEA inspectors at one site at least. Of special importance is the inability to re-verify cask or canisters from which seals have been removed and the canisters emplaced underground. Successfully designing seals that can be applied, verified and removed by an operator with IAEA approval could impact more than repository shipments, but other applications as well, potentially reducing inspector burdens for a wide range of such duties.

ACKNOWLEDGMENTS

The authors thank Bruce Moran, Lars Hildingsson, and Camilla Andersson for helpful comments and discussions. This work was supported by the Office of International Nuclear Safeguards Concepts and Approaches Subprogram under NNSA's Defense Nuclear Nonproliferation Office of Nuclear Nonproliferation and Control.

Sandia National Laboratories is a multi-mission 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-NA-0003525.

TABLE OF CONTENTS

FIGURES

TABLES

ABBREVIATIONS & ACRONYMS

ADSL	Asymmetric digital subscriber line
AES	Advanced Encryption Standard
ALIS	All-in-one surveillance camera
AP	Additional protocol
BWR	Boiling water reactor
C/S	Containment and surveillance
CASTOR	CAsk for Storage and Transport Of Radioactive material
CoK	Continuity of knowledge
COTS	Commercial off the shelf
CSA	Comprehensive safeguards agreement
DMOS	Digital multi-camera optical surveillance system
DSA	Digital Signature Algorithm
DSL	Digital Subscriber Line
EOSS	Electronic optical sealing system
ESI	EOSS interface tool
EURATOM	European Atomic Energy Community
FBOS	Fiber optic general purpose seal (*cf.* COBRA seal)
HLW	High-level waste
IAEA	International Atomic Energy Agency
IBE	Identity-based encryption
INFCIRC	Information circular (IAEA)
IPSec	Internet protocol security
IS	Integrated safeguards
ISDN	Integrated services digital network
ISVS	Integrated safeguards verification system
JRC	Joint Research Center
LAN	Local area network
LMCV	Laser mapping system for containment verification
LWR	Light water reactor
MEMS	Microelectromechanical system
MGR	Mined geological repository
MOSS	Multi-camera optical surveillance system
MUND	Mobile unit neutron detector
NDA	Nondestructive assay
NGSS	Next generation surveillance system
NIST	National Institute of Standards and Technology
NM	Nuclear material
NMA	Nuclear material accountancy
NPP	Nuclear power plant
PDV	Partial-defect verification
PSTN	Public switched telephone network
PWR	Pressurized water reactor

RDT	Remote data transmission
RF	Radio-frequency
RMDC	Remote Monitoring Data Centre (IAEA)
RM-DMZ	Remote monitoring – demilitarized zone
RMS	Remote monitoring system
RMSA	Remotely Monitored Sealing Array
RSAC	Regional system of accounting for and control of nuclear material
RSI	Remote safeguards inspection
SDIS	Server-based digital-image surveillance
SG-LAN	Safeguards Local Area Network (IAEA)
SLA	State-level approach
SLC	State-level concept
SNF	Spent nuclear fuel (also “used nuclear fuel”)
SoH	State of health
SQL	Structured query language
SSAC	State system of accounting for and control of nuclear material
SSM	Swedish Radiation Safety Authority
TID	Tamper-indicating device
TIE	Tamper-indicating enclosure
TRFS	Two-way radiofrequency seal
UFCF	Unirradiated Fuels Conditioning Facility (Dounreay facility, UK)
UMS	Unattended monitoring system
UPS	Uninterrupted power supply
USSB	Ultrasonic sealing bolt
UOSB	Ultrasonic optical sealing bolt
UWB	Ultra-wide band (radio frequency range)
VA	Vulnerability assessment (or analysis)
VACOSS	Variable coding seal system (also VACOSS-S)
VCOS	VACOSS-S electronic seal
VLAN	Virtual local area network
VMOS	VACOSS-S/MOSS system
VPN	Virtual private network

1. INTRODUCTION

The disposal of spent nuclear fuel in geological repositories presents an entirely new challenge for international nuclear safeguards. Whereas conventional safeguards approaches for other stages of the nuclear fuel cycle rely on nuclear material accountancy (NMA) supplemented by containment and surveillance (C/S), this conventional approach cannot be strictly applied to the disposal process. This is because, unlike conventional safeguards approaches by which NMA can be re-verified if supplementary C/S measures fail, re-verifying NMA of spent fuel that has been permanently encapsulated in disposal canisters is not realistic, and becomes impossible once disposal canisters have been emplaced in a geological repository.

For this reason, following the final NMA determination on spent fuel destined for permanent disposal, one critical objective is to maintain continuity of knowledge (CoK) on the verified fuel assemblies by using highly reliable, redundant C/S measures – from the point of the final NMA measurement through encapsulation, transportation and disposal. Indeed, IAEA policy requires that, after a disposal canister has been permanently closed, dual C/S measures[1] be applied to maintain CoK on the disposal canister and its contents, and that CoK continue to be maintained during transport of the disposal canisters to the geological repository (IAEA 2010a, p.5). The transportation link, such as from an encapsulation plant to the repository, represents one of the more challenging stages of the disposal process when it comes to maintaining CoK on encapsulated fuel assemblies, which will rely on C/S measures to a degree unprecedented in other stages of the nuclear fuel cycle (Baldwin, Haddal and Finch 2016, Mongiello, Finch and Baldwin 2013).

Once a geological repository has begun operations, the encapsulation and disposal of spent fuel will be performed as a continuous, industrial-scale series of processes (Mongiello, Finch and Baldwin 2013). Dual C/S measures will be applied to maintain CoK on spent fuel in disposal canisters during shipment from an encapsulation plant to a geological repository (IAEA 2010a, p.5) and could include one or more sealing systems for disposal canisters or transportation casks plus complementary surveillance or monitoring, such as video surveillance cameras or radiation monitors. Collectively, such C/S measures have the potential to add considerable burdens to an inspectorate's resources by requiring frequent verifications of sealing systems, as well as analyses of data from surveillance and monitoring equipment.

One potential component of dual C/S during transport would be effective containment by a transportation cask to include a seal that can assure each cask's containment integrity during transport. This may require a specially designed sealing system (or systems), as no current sealing system can assure containment integrity of a transportation cask during transport. If applied, seals on transportation casks would be verified after casks arrive at the repository The casks will be opened after removing the seals, and the disposal canisters containing spent fuel assemblies will be extracted and emplaced underground. These operations will occur approximately daily in the Swedish program during several decades of repository operation (Hildingsson and Andersson 2014).

Current IAEA practice may permit an operator to either apply or remove safeguards seals, but not both; an inspector must be involved with one or the other operation (Moran 2017). However, requiring

[1] Dual C/S requires two C/S devices that are functionally independent and are not subject to a common tampering or failure mode (IAEA, 2001).

safeguards inspectors to perform daily the tasks of applying and/or removing seals on every spent fuel transportation cask during routine repository operations will be an onerous burden on International Atomic Energy Agency's (IAEA's) resources. If seals on spent fuel transportation casks could be applied, verified *and* removed by an operator with IAEA approval, this could significantly reduce that burden.

Finland and Sweden are within a decade or so of beginning to operate their geological repositories (Finnish operations are scheduled to begin in 2023). The Swedish Radiation Safety Authority (SSM) in particular has expressed its desire for operator-applied and operator-removed safeguards seals to be available when that country's repository operations begin (Hildingsson and Andersson 2014). Successfully designing seals that can be applied, verified and removed by an operator could impact more than repository shipments, but other applications as well, potentially reducing inspector burdens for a wide range of such duties.

This study identifies criteria that might permit an operator to apply, verify, and remove safeguards seals on spent fuel transportation casks, including technical requirements such as assurance features, remote verification, data transmission and authentication, as well as procedural measures. Successful deployment of such a seal would enable operator management of safeguards seals on spent fuel transportation casks without compromising safeguards requirements for maintaining CoK on the cask contents: spent fuel.

2. IAEA EQUIPMENT, POLICIES AND PRACTICES

2.1. Seals and Sealing Systems

A seal is a tamper-indicating device (TID) used to detect unauthorized access to materials, documents, data signals, equipment, and other items within secured enclosures (containment). A sealing system includes (1) the seal itself, (2) a way to apply the seal (e.g., metal wire, optic cable) and (3) the containment[2] enclosing nuclear material (NM), safeguards equipment, or other protected items (IAEA 2011, p.69). All three components must be examined in order to verify that a sealing system has not been tampered with. Seals also uniquely identify secured containers to which they are attached, and are authenticated by confirming that identity. Several seals and sealing systems are used by the IAEA, and the choice of seal depends in part on the application (Table 1). IAEA-authorized sealing systems are assessed for vulnerabilities by an independent entity to identify and mitigate potential weaknesses (IAEA 2011).

[2] The IAEA defines containment as "structural features … used to establish the physical integrity of … items …" and to maintain CoK on items (IAEA 2001, p.66).

Table 1 IAEA Sealing Systems with Potential Applications to Transportation Casks*

Code	Equipment Name	Description & Application
FBOS	Fibre optic general purpose seal	*In situ* verifiable fibre optic seal
USSB & UOSB	Ultrasonic sealing bolt & Ultrasonic optical sealing bolt	USSB is a general-purpose bolt seal primarily used under water to seal lids on containers with spent fuel assemblies. UOSB is used to seal bolts on spent fuel dry-storage casks with EOSS or similar optical sealing system
VCOS	VACOSS-S electronic seal (variable coding sealing system)	Reusable seal consisting of a fibre optic loop and electronic seal. Laser-light pulses monitor the loop, and every opening and closing of the seal is recorded and stored in the seal. A palmtop computer reads the seal. VCOS is legacy equipment being replced by the electronic optical sealing system, EOSS.
EOSS	Electronic optical sealing system	Reusable seal consisting of a fibre-optic loop and an electronic seal. Laser pulses monitor the loop, and every opening and closing of the seal is recorded and stored in the seal. A dedicated reader is used to verify the seal. EOSS replaces VCOS
RMSA	Remotely monitored sealing array	Reusable seal consisting of a fibre-optic loop and an electronic seal. Communicates wirelessly to a data translator.
VMOS	VACOSS-S/MOSS system	Unattended sealing system that records closing or opening of VACOSS electronic seals by using a specially adapted multi-camera optical surveillance system (MOSS)

* Modified after Table 8 in (IAEA 2011, p. 71).

A seal is verified when it is inspected and either shows evidence of tampering or not.[3] However, verifying that a seal shows no signs of tampering is not sufficient assurance that a sealing *system* has not been tampered with or defeated. Maintaining CoK on items or materials under seal requires that the containment's integrity has also been maintained. If a sealing system shows evidence of tampering, the IAEA refers to this as an *anomaly* (IAEA 2001) and CoK on the contents of the containment has been

[3] This is known as an "attributes test" and results in a "yes" (no tampering) or a "no" (possible tampering) (IAEA 2001, p.83).

lost. The indication of an anomaly by C/S measures does not by itself indicate that material has been removed;[4] however, resolving C/S anomalies requires that the NM under seal be re-verified to re-establish CoK. But re-verifying spent fuel inside a welded canister would require delaying disposal so that a suitable determination can be made, which could require the canister be cut open, an operation that would need to be performed at an appropriate facility (e.g., the encapsulation plant), thus entailing additional transportation with further delay – and appropriate *additional* C/S measures be applied. Such a scenario is to be avoided if at all possible.

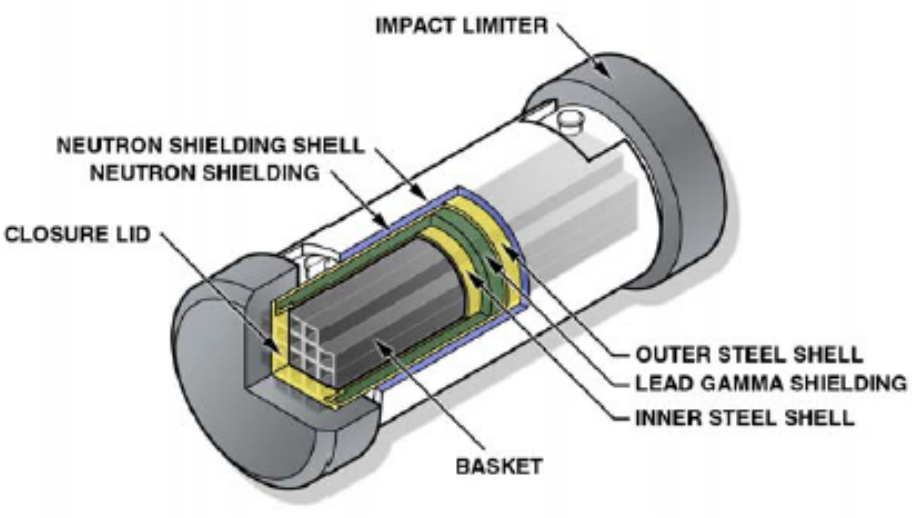

Figure 1. Generic Transportation cask for shipping spent fuel by rail (Source: USNRC).

In the context of transportation casks for spent nuclear fuel (Figure 1), suitable containment could be provided by a transportation cask *if* that cask's integrity could be verified. If so, the verified integrity of such a sealing system, cask plus seal, could assure that CoK has been maintained on the disposal canisters (and therefore on the fuel assemblies inside) during transport. Although seals are available that might be used to seal bolts on lids of transportation casks (e.g., the ultrasonic optical sealing bolt (UOSB); Table 1; Figure 2), simply sealing a transportation cask's lid may not be sufficient to assure a cask's integrity if the cask could be opened without removing the lid; e.g., by cutting through the bottom of the cask without disturbing the seal.[5]

[4] For example, seals may be broken accidentally or removed in an emergency without accessing or diverting NM.

[5] A common practice for verifying containment integrity is to visually inspect a container for anomalous features and possibly feeling the surface. This is qualitative and time consuming, and neither effective nor efficient.

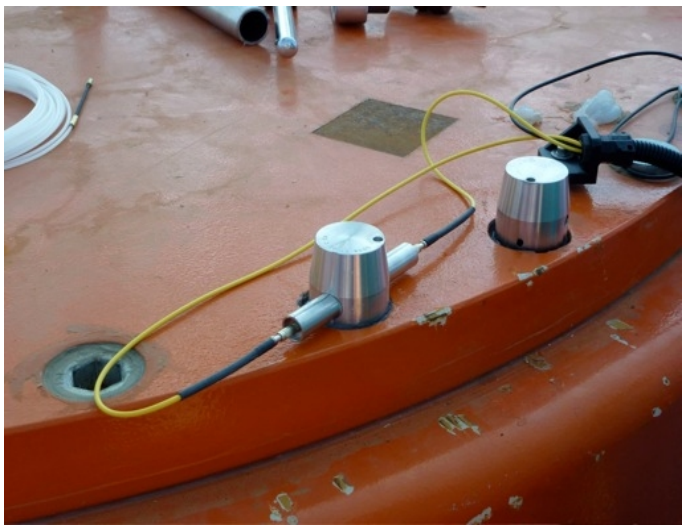

Figure 2. Ultrasonic Optical Sealing Bolt (left); installed on CASTOR storage cask with EOSS (right)

2.1.1. Prototype: Electronic ranging seal for unattended sealing of spent fuel transportation casks[6]

The IAEA is well aware of challenges presented by frequent transportation of spent fuel and has encouraged the development of seals that can be applied confidently without an IAEA presence. The EU's Joint Research Center (JRC) reports a recently invented system for automatically sealing a container lid to a container body without the need for an inspector to assure its proper application. The system comprises three anchors fixed to the cask body, three tags fixed to the cask lid, and a master unit fixed to the cask body (Figure 3). Each tag and anchor will have an ultra-wideband (UWB) module that transmits and receives time-of-flight data; they will also have a crypto module to store a private key and digitally sign data packages (see Section 4.2.4.1). The tags and anchors will have tamper-detection switches and a protective circuit mesh to deter drilling, and a temperature sensor to detect extremes that could negatively impact the seal's operation. An onboard voltage-monitoring circuit ensures proper power supply.

The three anchors are attached to the cask body by an inspector, equally spaced around the circumference of the cask on a plane parallel to the lid and separated by 120°. Anchors and tags exchange messages and, by using digitally signed time-of-flight information, each of the three anchors interrogates the three tags to determine the distance to each tag. The three anchors provide this distance information to the master over a wired communication channel. The master collects the authenticated information and, through a triangulation algorithm, determines the position of each tag.

Once an inspector has installed the proposed sealing system on a cask and lid, the system is transparent to an operator. An operator can then fill the cask and close its lid, automatically engaging the proposed sealing system; the operator does need to perform any special operation to install or activate the system.

---

[6] Source: https://ec.europa.eu/jrc/en/patent/2964-electronic-ranging-seal-unattended-sealing-spent-fuel-transportcasks-0

Although the status of this sealing system is not known, we are unaware of any such system currently in use. And while this system can ensure correct application of the correct seal in the absence of an inspector, it cannot ensure containment integrity as described, only that a lid has not been tampered with or removed. Verifying cask integrity after shipment would still require an inspector. Thus, this type of sealing system (alone) would be unlikely to suffice for both application and removal by an operator.

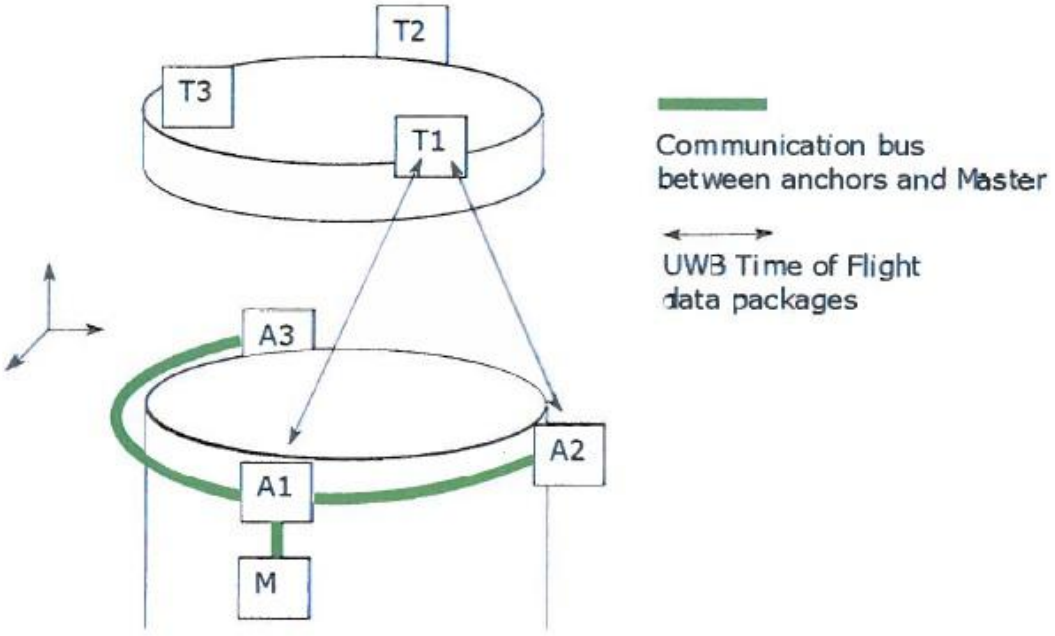

Figure 3 Proposed sealing system for sealing a container lid to a container body. The system comprises the anchors (A1, A2, A3) fixed to the cask body, three tags (T1, T2, T3) fixed to the cask lid, and a master unit (M) fixed to the cask body.[7]

2.2. IAEA Policy

Because spent-fuel assemblies inside a disposal canister cannot be re–verified after the canister has been emplaced underground in a repository, IAEA policy stipulates that sufficient redundancy, diversity and robustness be incorporated into the safeguards system, and that adequate maintenance measures be applied to avoid system failure and ensure CoK (IAEA 2003). As stipulated for spent fuel in long-term storage, spent fuel that has been encapsulated inside containers for shipment are deemed "difficult-to-access" and are subject to dual C/S[see footnote 1] after the safeguards verification measurement (IAEA 2005, SMC 9, p.7). Similarly, after a disposal canister has been permanently closed (usually welded shut), dual C/S measures should be applied to maintain CoK on the disposal canister, including during transport of the disposal canister to a geological repository (IAEA, 2010a). A highly reliable, redundant C/S system should be applied to minimize the possibility of C/S failure and any need to reopen a permanently closed

[7] Figure source: https://ec.europa.eu/jrc/en/patent/2964-electronic-ranging-seal-unattended-sealing-spent-fuel-transportcasks-0.

disposal canister. If CoK is lost during transport or storage, reverification would need to be performed in accordance with measures to be determined and approved by the IAEA (IAEA 2010b, p.12).

With regard to applying, verifying and removing seals, IAEA policy has been that the IAEA must be involved in either the application or the removal of a seal. In the case where an operator applies a seal, IAEA's removal of that seal verifies that an operator had applied the correct seal correctly. This addresses concerns that an operator could apply a seal incorrectly such that a container could be opened without breaking the seal. Alternatively, an operator could apply an incorrect seal (a dummy seal) that is not connected to IAEA's recording system. The dummy seal could be closed when the IAEA seal is closed and then reopened in a similar fashion such that the IAEA seal is undisturbed. These concerns are largely eliminated when IAEA installs a seal, as this assures that the correct seal is applied correctly. In addition, IAEA verification of a seal at the receiving end[8] permits the IAEA to observe the container and ensure its integrity – that a cask has not been opened during transit at a location on the container other than where the seal is attached, such as removing the bottom of a cask (Moran 2017). In other words, IAEA can verify, not only the seal, but the integrity of the entire sealing system.

In order to allow an operator to remove safeguards seals, the IAEA must assume that (if a trained IAEA inspector had applied the seal at the shipping end and the operator uses an approved verification measure at the receiving end) the container could not have been opened undetected: that the sealing system (not just the seal) has not been defeated without detection. If that is not the case, then the IAEA would be unlikely to approve an operator removing a seal. This is especially crucial for the case of removing and verifying a seal on a transportation cask, as there will be no opportunity, once the disposal canister has been emplaced, to re-verify the canister (and its contents) if CoK is lost. Thus, a seal on a transportation cask that could be removed by an operator would need to ensure that the cask's integrity (as containment) is verifiable, not just that a sealed lid has not been removed. To date, no seal for a transportation cask can provide that level of containment assurance.

2.2.1. Integrated Safeguards

In 2001, the IAEA started developing and implementing the "State level approach" (SLA) for implementing safeguards in States for which the IAEA had drawn the *broader conclusion*; i.e., that there is no diversion of NM and no undeclared NM or activities in the State. For such a State, the IAEA may implement Integrated Safeguards (IS), which refers to the optimum combination of all safeguards measures available to the IAEA under a State's comprehensive safeguards agreement (CSA) and additional protocol (AP) (IAEA 2015). Integrated safeguards can be used to achieve maximum effectiveness and efficiency in meeting the IAEA's safeguards obligations within available resources (IAEA 2001). Under IS, certain measures, such as inspections, may be applied at reduced levels compared with *traditional safeguards* measures that are applied in States without the broader conclusion (Drobysz and Sitt 2011).

All States with active repository programs have both a CSA and an AP in force, and the IAEA has reached the broader conclusion for all but one of those States[9]; these include Australia, Austria, Belgium,

[8] Receipt at the repository in the case of transportation casks with disposal canisters.

[9] As of 2013, the IAEA had not drawn the broader conclusion for Switzerland and did not implement IS there (IAEA

Canada, Chinese Taipei (Taiwan), Finland, Germany, Japan, South Korea (ROK), and Sweden (IAEA 2014a). The IAEA developed model IS approaches for encapsulation plants (IAEA 2010a) and geological repositories (IAEA 2010b); however, those guidance documents leave largely unanswered differences between traditional safeguards and IS for many specific measures (including C/S), procedures, inspections, or accountancy. In fact, the IS approach is not based on a fixed set of criteria; rather the IAEA will modify the IS approach for a State's geological repository over time, taking into account any developments (1) at the repository, (2) in safeguards concepts and technologies, and (3) in nuclear activities by the State (IAEA 2010b).

Some aspects of the model IS approach for a geological repository include (IAEA 2010b):

- The timeliness verification goal for spent fuel (irradiated direct-use NM) under IS is one year (an increase from three months under traditional safeguards)
- Item counting and verification of spent fuel not under successful C/S should be performed with low detection probability for gross defects
- IAEA safeguards measures, including dual C/S arrangements, should use unattended monitoring with remote data transmission (RDT) and use remote transmission of safeguards equipment state of health (SoH) and, when applicable, safeguards data
- Random inspections will be conducted in unannounced or short-notice mode to verify receipts of filled disposal canisters and declarations, to detect tampering with safeguards equipment and containment, and to validate verifications of approved C/S and monitoring measures in unattended mode with remote monitoring capability
- If seals are a part of the C/S system, a capability should be provided to verify and remove the IAEA seal from disposal canisters or transportation casks

The primary focus of this report addresses the last bullet; however, also of note are the second and third bullets that mention RDT and unattended remote monitoring. As will be discussed further in examples described in Section 2.3 below, RDT and remote monitoring have been crucial for successfully implementing operator-applied seals. The use of RDT and unattended remote monitoring also support the implementation of IS by enabling remote safeguards inspections, described briefly in the following section.

2.2.1.1. Remote Monitoring and Remote Safeguards Inspections

Remote safeguards inspections (RSIs) are one of the more important measures to help achieve the goals of IS for more efficient and effective use of IAEA resources through the use of unattended data-collection systems. The RSI safeguards approach is based on inspection activities that reduce the physical presence of IAEA inspectors in the field (1) by using remote transmission of authenticated data from IAEA equipment systems, (2) with the cooperation of the operator/SSAC/RSAC[10] and (3) monitoring process parameters and operator-owned measurement systems and remotely transmitting these process data to IAEA Headquarters or a Regional Office for safeguards evaluation.

2014a); however Switzerland does have a CSA and AP in force (IAEA 2015b).

[10] State and/or Regional authorities for the System of Accounting for and Control of NM (SSAC and/or RSAC)

The RSI approach does not eliminate the need for on-site inspections; however, it helps reduce the frequency of routine on-site inspections compared with traditional safeguards and helps to shift IAEA inspector resources from routine activities to non-routine activities (Araujo, Charlier, et al. 2010, Drobysz and Sitt 2011), and RSIs are complemented by unannounced inspections. A crucial condition for IAEA's use of RSI is a functioning infrastructure that allows secure RDT and remote access to remote-monitoring systems for maintenance and possible modification. Verification and monitoring data generated during RSI must satisfy IAEA requirements for authenticity, completeness and correctness (see Section 4.2.4.1). Data authenticity is a pre-requisite to ensure a valid interpretation of collected data. Completeness, meaning no data gaps, provides assurance that all items/materials are monitored. Correctness is necessary for data qualification and for quantifying verified and monitored items/materials (Araujo, Charlier, et al. 2010).

IAEA has been expanding its remote monitoring capabilities and increasing its use of unattended monitoring systems (UMS) that can operate in remote-monitoring mode, and in monitoring operators performing IAEA functions, including the application or removal of electronic seals (Araujo, Charlier, et al. 2010). Data acquired from UMSs are transmitted via secure remote-transmission technologies to agency headquarters for analysis (IAEA in Vienna or regional offices). Such data help support safeguards conclusions and can provide instructions for follow-up action, if necessary. RSIs can be especially useful where access to NM is difficult or impossible, as is the case for spent fuel assemblies inside a disposal canister or emplaced in a repository.

Fully implementing RSI requires a negotiated agreement between IAEA and the SSAC/RSAC that defines operational conditions of the specific RSI approach to be implemented. This includes a technical agreement with an operator to implement RSI measures while addressing security concerns of an operator and the SRAC/RSAC regarding RDT of data beyond obligatory NMA declarations (Araujo, Charlier, et al. 2010).

Security concerns of operators and State authorities can limit the use of RDT and RSI for some facilities. Nevertheless, the IAEA advocates continued research and development of equipment that can further enhance the efficiency and effectiveness of safeguards activities through increased use and effectiveness of RSI (Araujo, Charlier, et al. 2010). In the context of this report, the RSI approach seems likely to be instrumental in developing and approving seals that can be applied to, verified and removed from transportation casks by State operators in the absence of an inspector.

2.3. IAEA Practices and Examples

Seals that must be applied or removed by an inspector can demand considerable time and effort of both inspectorate and operator. This will be especially true for the approximately daily process of shipping, receiving and emplacing disposal canisters in a repository, as is foreseen for the Swedish program (Hildingsson and Andersson 2014). Allowing an operator to attach or remove electronic seals without an inspector present saves time and resources, and the IAEA has already approved a limited number of such activities in coordination with State agencies, operators, and regional inspectorates. An operator typically performs these activities under surveillance, which is recorded by specifically adapted equipment, with data transmitted to the inspectorate. Without an inspector present during a sealing procedure, an operator needs confirmation that the correct seal has been applied correctly, or has been verified and removed correctly. This avoids operator liability for improperly applied or removed seals, and provides assurance to the IAEA that the procedure has been executed properly.

2.3.1. German example: Spent Fuel Storage

The recent shift away from nuclear power in Germany's energy policy presented a new challenge for Germany's safeguards on spent nuclear fuel. The accelerated shut down and defueling of several nuclear power plants (NPP) substantially increased workload for NPP operators and for the two inspectorates, EURATOM and IAEA, primarily because of the dramatically increased number of annual storage-cask loadings. The challenge was addressed by allowing the NPP operator to seal storage casks in the absence of EURATOM and IAEA inspectors (Jussofie, van Bevern, et al. 2014). A special approach that adequately considered operators' requirements was developed by EURATOM and the IAEA in cooperation with the German Support Program (Jussofie, Graf and Filbert 2010).

Most spent fuel from German LWRs is stored in CASTOR multipurpose transportation-and-storage casks (Figure 4). Each cask is loaded and sealed at the NPP before transfer to a dry-storage facility. Fuel assemblies are loaded under water and must be dried before closing and sealing each cask, a process that can take anywhere from 10 to 100 hours.[11]. Multiple casks may be loaded consecutively during a single loading campaign.

In order to avoid inspectors having to remain on site or on call throughout the uncertain drying process, the IAEA and EURATOM proposed an approach to delegate to the operator the task of applying seals when inspectors are not present (Araujo, et al., 2014). The identity of the seals, and the sealing procedure itself, is recorded by video surveillance and is subsequently verified by an inspector after a sealed cask has been transferred to a spent fuel storage facility. This results in minimum delay for safeguards-related cask-handling procedures and also reduces the number of inspections necessary for checking the correctness of sealing systems, which can be accomplished during random inspections. The containment seal applied by an operator is verified by both inspectorates after the arrival of casks at the interim dry storage facility. Through these procedures, CoK is maintained on the seals as well as the NM under seal.

[11] Residual moisture must meet specific safety criteria, and the time needed to achieve those criteria will vary and is not predictable.

Figure 4. CASTOR® geo cask for storage and transportation (source: GNS[12]).

Once enclosed in the CASTOR cask the spent fuel assemblies are said to be "difficult-to assess items" (IAEA 2005, Annex 14), requiring dual C/S[see footnote 1]. In the German case, two independent sealing systems are used along with video surveillance. The two sealing systems – EOSS and the COBRA seal – are both attached to the protection plate on the cask (Figure 4, also see Figure 2). The operator applies both seals to each cask under continuous camera surveillance. The arrangement requires training for the operator on the sealing procedure and specially adapted IAEA/Euratom equipment (Figure 5). As an operator cannot assume liability for an improperly applied seal, EURATOM oversaw development of an EOSS Enhanced Seal Interface (ESI) to facilitate the sealing operation and to assure proper installation (Figure 5 and Figure 6). The ESI (Figure 6) guides the operator through the sealing procedure step by step by using self-explanatory menu navigation and displays each seal's data. In case of an incorrectly connected EOSS fiber-optic cable, the navigation will not proceed (Jussofie, van Bevern, et al. 2014).

[12] GNS Gesellschaft für Nuklear-Service mbH (http://www.gns.de/language=en/29778/castor-geo)

After closing seal, ESI provides confirmation that the procedure is complete; the confirmation can then be printed as a permanent record. The ESI is connected to both the EOSS seal and a surveillance camera throughout the procedure. The surveillance camera (an ALIS, All-in-One Surveillance camera, or, increasingly, the NGSS, Next Generation Surveillance System[13]) also serves as a backup for EOSS seal data.

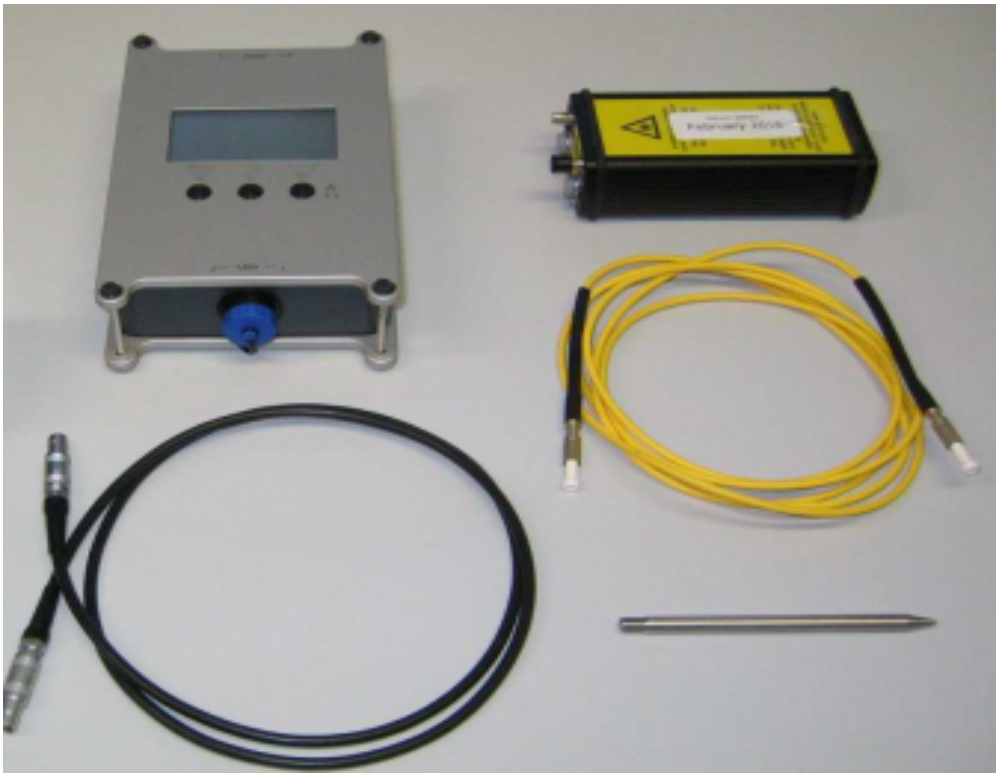

Figure 5. Equipment used by an operator when applying EOSS seal: ESI (top left); EOSS seal (top right); Interface-to seal/camera cable (lower left); fiber-optic cable for EOSS (middle right); Fiber-optic guiding needle (bottom right). Source: (Jussofie, van Bevern, et al. 2014).

[13] IAEA and Euratom are replacing ALIS cameras with the newer NGSS.

Figure 6. EOSS interface tool (ESI). Source: Unterweser Nuclear Power Plant.

The use of electronic seals allows seals data to be transmitted to EURATOM along with video surveillance data. This use of RDT allows the inspectorate to remotely maintain CoK on casks and seals. The use of RDT must meet German security requirements for sensitive data; that is, RDT cannot impact plant operations, transmit operating data, nor monitor personnel and storage operations. This was accomplished by installing a communication line that is isolated from the German operator's data network, and video-surveillance data are transmitted with a 24-hour delay. Although all data from seals and video cameras are transmitted to EURATOM, only select (and agreed upon) data are transmitted from EURATOM to IAEA once per week. Equipment and system SoH are also transmitted to the inspectorate during the period between inspection notification and an on-site inspection.

Efficiency gains under IS largely depend on the condition that no re-verification of the nuclear inventory will be required. Basic conditions for operator-managed cask sealing that must be satisfied from an operator's perspective are summarized below.

- Preserve CoK with camera surveillance
    - Surveillance camera is linked to the EOSS/ESI system
- No, or only minor, reverification measures will be required
- The risk for loss of CoK and reverification due to faulty cask sealing is low but not zero. [14]
- Operator is trained in the sealing procedure by EURATOM.
- Operator receives instruction manuals for both sealing procedures (EOSS and COBRA)
- IAEA acceptance of the sealing procedure and underlying technology[15]

[14] Reverification could be required if both EOSS and the COBRA seals are not intact when verified at the storage facility. However, if only one of the two seals is still intact and can be verified successfully in the storage facility, reverification is not mandatory. This criterion resembles the IAEA's "Acceptable Single C/S" for Dual C/S, according to which no re-measurement is required when one C/S system is Conclusive positive and one C/S system is Inconclusive (IAEA 2005, Annex 3).

- EURATOM assurance that an inspector will be on site within 24 hours if sealing is faulty
- Assurance that a second ESI and spare seals are available on site.

Figure 7 helps summarize gains of using the IS approach with operator-applied seals compared to the traditional safeguards approach (Brotz, et al. 2016).

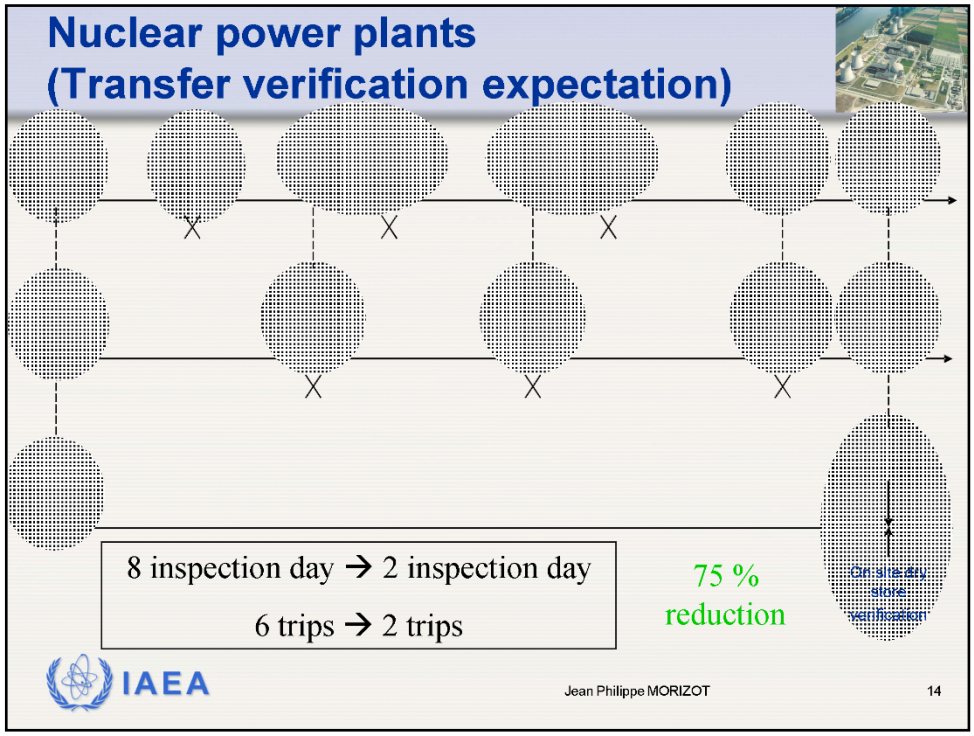

Figure 7. Comparison of different approaches for transfer verification.[16]

The top line in Figure 7 represents effort required when using a traditional safeguards approach for verifying and loading spent fuel assemblies into transportation-and-storage casks, followed by an inspector applying the safeguards seals. To prepare for each loading campaign, a 'pre-campaign' inspection is performed to install and test equipment such as surveillance cameras to monitor casks and loading activities. The pre-campaign applies to both safeguards approaches, traditional and IS.

Loading verification in Figure 7 refers to a partial-defect verification (PDV) determination that is performed on spent fuel being loaded into storage casks. Under traditional safeguards, this PDV was performed by an inspector for each cask during a cask-loading campaign. From the time of the PDV determination until the cask was loaded, closed and sealed, CoK was maintained through video surveillance. With the introduction of IS, loading verification by an on-site inspector was eliminated (Xs under top line in Figure 7).

---

[15] This requirement is met by including the operator cask-sealing procedure as an appendix to the IAEA-Euratom Partnership Approach Under Integrated Safeguards for Spent Fuel Storage Facilities (IAEA 2013).

[16] Source for Figure 7 (Brotz, et al. 2016, Figure 3).

Additional efficiency was gained by allowing the operator to apply safeguard seals without an inspector present, eliminating this activity by an on-site inspector (Xs under middle line in Figure 7). Instead, the operator attaches the COBRA and EOSS seals under surveillance and in accordance with procedure. As illustrated on the bottom line in Figure 7, the combined implementation of IS with operator-applied seals reduces the need for an on-site inspector from completion of the pre-campaign until a post-campaign inspection, which can be performed after the casks have been moved to the dry-storage facility. Thus, the inspection burden is reduced from eight inspection days and six trips to two inspection days and two trips (Figure 7).

The combination of ESI and EOSS is the only currently available technology that can provide assurance to German NPP operators of successful EOSS attachment as well as documentary evidence, as required by the operator. This allowed German NPP operators to agree to apply safeguards containment measures in the absence of an inspector.

The IAEA acknowledges that this approach allows for substantial gains in efficiency during SF cask-loading campaigns, because it requires only limited inspector presence to verify SF assemblies and cask sealing (Araujo, et al. 2014). Operators also profit from this approach through a reduced number of inspections. However, the IAEA does not consider this to be a generally applicable approach for every NPP. Implementing this approach would be evaluated on a case-by-case basis after accounting for a NPP's operational status, the number of dry-storage casks involved, and an NPP operator's readiness to provide the required information and to appropriately apply containment measures.

Using this example as a model for a similar approach to an operator applying seals to, and removing them from transportation casks carrying disposal canisters for emplacement in a geological repository, is limited. In the German example given here, operators only apply seals to dual-purpose transportation-and-storage casks. Once shipped, seals and casks remain accessible to inspectors for verification purposes during inspections at the dry storage facility. This will not be the case for disposal canisters after an operator has removed a seal and emplaced a disposal canister underground.

2.3.2. UK example: Nuclear Material Transfer[17]

As part of its effort to declassify a number of nuclear facilities, the United Kingdom (UK) has been transferring un-irradiated NM from Dounreay to Sellafield. Nuclear Material at Dounreay is in storage under seal or C/S and inspected monthly by EURATOM. Once released by inspectors, NM goes to the Unirradiated Fuels Conditioning Facility (UFCF) for sorting and characterization and is then placed into cans for shipment.[18] The cans are measured[19] and loaded into shipment containers under surveillance.

[17] This section draws substantially from (Persson, Synetos, et al. 2014a)

[18] The operator at Dounreay is allowed to detach seals on NM storage locations provided that all NM to which access is obtained is taken directly to the UFCF.

[19] EURATOM branches directly to the UFCF's Nondestructive Assay (NDA) system to obtain an independent evaluation of measurement data for safeguards purposes, maintaining the CoK thereafter to avoid unnecessary verification activities.

Once full, the operator seals the shipping container with an EOSS seal under surveillance. The shipping containers thus sealed are stored temporarily in a separate area for shipment to Sellafield.

During the next interim inspection at Dounreay, inspectors replace the operator-installed EOSS seals with EURATOM metal seals, and containers are shipped to Sellafield under metal seal. The metal seals are detached by inspectors at the receiving end (Sellafield facility).

Containers of NM under seal arriving at Sellafield will have been verified at the Dounreay site and (re)sealed there by EURATOM inspectors. A security door leading to an unloading and storage area at the Sellafield site is kept under video surveillance at all times; the door is also fitted with a radiation monitor (neutron monitor and NaI detector). The security door is sealed with an EOSS seal and remains closed except for when the operator accesses the store for unloading or maintenance operations. The EOSS seal is connected to the local EURATOM network for remote interrogation, which in turn is linked to EURATOM headquarters in Luxembourg (Persson, Synetos, et al. 2014a).

Another facility at Sellafield for storage of plutonium (Pu) is under dual C/S and monitored remotely by EURATOM. Both EOSS and COBRA seals are applied on storage channels for redundancy and arranged to reduce common-mode failures. The C/S system has been modified and connected to the network to make data available remotely to both EURATOM and the IAEA (Persson, Synetos, et al. 2014b). Surveillance data are recorded locally, and the surveillance data, as well as the EOSS seals, can be accessed remotely by EURATOM inspectors. Data can also be accessed from Luxembourg and data can be transmit further to IAEA headquarters in Vienna, according to agreement between EURATOM, UK authorities and the IAEA. Data is transmitted via a Virtual Private Network (VPN) for which agreed equipment is used. Transmitting images requires that a security sensitivity (classification) of the field of view for the camera is approved by the operator (Persson, Synetos, et al. 2014b).

This arrangement for RDT has reduced the number of inspections at the Sellafield Pu store by half, from one per month to one inspection every two months. Every other month, when there is no on-site inspection, EURATOM and IAEA review from their respective headquarters signals from all EOSS seals that constitute the boundaries of the Pu store, as well as data from cameras inside the store.

Both UK examples illustrate the crucial role of RDT and RSI in reducing inspector presence and allowing increased operator management of C/S systems. Considering the possibility of an operator applying and removing seals from transportation casks bearing disposal canisters destined for disposal, the role of RDT and RSI in maintaining CoK on casks and canisters will likely be of paramount importance.

Intentionally Left Blank

3. REVIEW OF OPERATOR NEEDS

The ability and willingness of an operator to routinely manage safeguards seals on transportation casks used to ship disposal canisters for spent fuel must take into account operational demands of the disposal process. Such demands include the frequency (potentially daily) at which disposal canisters are inserted into transportation casks (e.g., at an encapsulation plant) and the comparable frequency at which disposal canisters will be removed from transportation casks (e.g., at the repository). The projected timeline for disposing each canister for the Swedish program is two weeks from final PDV to emplacement (Hildingsson and Andersson 2017).

A crucial consideration will be the inability to re-verify disposal canisters or their contents after canisters have been emplaced underground. This sharply distinguishes disposal from spent-fuel storage, because the latter allows continued access to inspectors for possible reverification of materials in storage, whereas disposal does not.

The examples of operator-managed seals described in Section 2.3 above illustrate several criteria that an operator may require in order to take on the responsibility of managing safeguards seals and sealing systems, whether applying them or removing them (or both), including those related to RSI and RDT. As neither example pertains specifically to transportation casks used to ship disposal canisters for permanent disposal in a repository, we also interviewed staff from SSM in Sweden to glean their input about operator needs relevant to the disposal process (Hildingsson and Andersson 2017). Thus several operator criteria have been identified, as well as suggestions for streamlining the process of operator-managed safeguards seals for spent fuel transportation casks.

Sealing System – operation: An operator-managed sealing system must be applied in a "fool-proof" manner, either automatically applied upon cask closure (similar to the prototype system described in Section 2.1.1 above) or according to agreed-upon procedure with possible special equipment (similar to German case described in Section 2.3.1 above). Such a sealing system benefits both operator and inspectorate if designed to be user friendly (Brotz, et al. 2016). Once applied, a sealing system should operate in unattended mode and comprise one or more electronic seals that are remotely monitored and can transmit safeguards-relevant data to the inspectorate. Seals should provide timely information to both operator (on site) and inspectorate (off site) as follows.

- The correctness (or lack) of a seal's application and closure,
- Remote transmission of seal status, including SoH information and other agreed-upon data (e.g., location),
- Timely information to both operator and inspectorate of a seal's integrity (or its lack) upon arrival at the receiving end,
- If and when a seal has been opened or removed in an acceptable manner (or not).

The signal must provide a timely alert for any "hold" or "do not open" warning for any cask on which a seal indicates a problem.

Sealing System – containment: A sealing system must ensure that any breach of a cask's containment, whether by opening a lid, cutting through another location on the cask, or any other penetration of the cask, is detected and recorded, and that the information is transmitted in a timely manner to the inspectorate. This eliminates a sealing bolt (only) as an acceptable sealing system, as this only detects

opening of a cask's lid. If two independent sealing systems are used to satisfy dual C/S, then both must assure the same level of confidence in a cask's containment integrity.

Time and Distance: Although transportation casks will be shielded, the radiation field will be such that applying seals must be accomplished without undue exposure to any individual, especially as the application, verification and removal of seals will occur on a regular basis. These operations need to be done as quickly as possible or from as great a distance as possible (or both). Most promising would be a seal that can be applied, verified and removed without exposing an individual to the radiation field near a cask or canister; e.g., by means of a remote-handling operation.

Location – Application: Seals would be applied to transportation casks at the shipping point where, in the Swedish case, disposal canisters are placed into casks at the encapsulation plant for shipment to the repository. In the Finnish case, the final safeguards accountancy measurement will be performed at the NPP where assemblies are loaded into transportation casks for shipment to the encapsulation plant; Finnish transportation casks would therefore need to be sealed at the power plant.[20]

Location – Verification & Removal: These operations occur at the receiving end of a shipment (repository or encapsulation plant). The Swedish operator expressed a strong preference for a seal than could be interrogated (verified) before a transportation cask enters the repository's underground workings (e.g., at an entrance ramp) and be removed underground where the cask would be opened and the disposal canister extracted for final emplacement (Hildingsson and Andersson 2017). That is, that there be no potential for a disposal canister that has not been verified and approved for final disposal to enter the repository. A complementary option is to consider implementing a "station" to interrogate seals when each transportation cask arrives at the repository site. This might be envisioned as a "docking station" under IAEA control that would have the capability to transmit information about a seal's status to a database. Such a docking station could be located at a surface holding, storage, or staging area where canisters would be held until they are ready for disposal. In any case, seal removal is likely to be conducted under video surveillance.[21]

Burden of proof must be on the IAEA: An operator must know that (1) the correct seal has been applied correctly, (2) that a seal has not been compromised, (3) whether a seal can be removed and (4) that IAEA will not require reverification after an operator has received authorization that a seal can be removed and the canister emplaced. In other words, before a seal can be removed by an operator, the IAEA must acknowledge that CoK has been maintained on the transportation cask and its contents during shipment (a disposal canister and the spent fuel it contains). Authorized removal of a seal by an operator must also be conducted in such a way that the IAEA can confer authorization to an operator to proceed with emplacing the disposal canister that will be removed from the cask from which a seal is to be removed – or can notify an operator in a timely fashion not to proceed if there is a problem.

---

[20] The Finnish Disposal Facility at Olkiluoto will consist of two co-located sections: (1) the above-ground encapsulation plant where spent nuclear fuel will be received, dried and packed into disposal canisters, and (2) the underground repository directly underneath the encapsulation plant. Disposal canisters will be lowered to the repository directly from the encapsulation plant by using a lift (http://www.posiva.fi/en/final_disposal).

[21] Implementing video surveillance, or any safeguards measures underground is controversial and alternative measures above ground may need to be considered

Timeliness: IAEA concurrence on all aspects of the process, the application, verification and removal a seal, must be timely. SSM suggests only a "few hours" will be available for the IAEA to notify an operator of any irregularities and whether or not to proceed to the next step in the process (Hildingsson and Andersson 2017).

Remote Data Transmission (RDT) and Remote Safeguards Inspections (RSI): Successfully implementing operator-managed seals – both their application and removal – will require successfully implementing unattended RDT in support of RSIs, complemented by random interim inspections, as part of an IS approach (IAEA 2010b, p. 13). As described in Section 2.3, RDT systems operating in unattended mode, which enable RSI, must meet certain operator criteria, including security concerns. Remote transmission of sensitive image data, for example, may require that the associated RDT system meet an operator's security requirements, such as the 24-hour delay required in the German example described in Section 2.3.1 (Jussofie, van Bevern, et al. 2014); however, data-transmission delays, may need to be shortened or suspended when sealing a cask at the shipping end and, especially, unsealing a cask at the receiving end, so that the inspectorate can approve (or not) canister emplacement underground.

Efficiency gains under IS largely depend on the condition that re-verification of NM inventory will not be necessary and also require remote transmission of safeguards equipment SoH between an inspection notification and an inspection. For example, in the UK example, EOSS seals are connected to the local EURATOM network and can be interrogated remotely, allowing inspectors to remotely check safeguards equipment SoH before any NM transfers, and so that problems or defects can be reported to an operator as soon as possible (Persson, Synetos, et al. 2014b). Potential interruptions to data transmission must also be anticipated and should not adversely affect operations; this was addressed in the German example by including local data-storage for the RDT system along with automatic synchronization of the system following an interruption (Jussofie, van Bevern, et al. 2014). Successfully implementing RDT and RSIs therefore requires close coordination with an operator so that these systems can be included as part of a facility's design process ("safeguards by design").

Intentionally Left Blank

4. DESIGN CRITERIA[22]

This section identifies assurance features, remote verification, and data transmission and authentication for potential seals technologies for use on transportation casks. By implementing design features described here, it should be possible to enable an operator to manage IAEA seals without compromising safeguards requirements for maintaining CoK on disposal canisters and transportation casks. Design criteria below apply to all safeguards sealing systems; special considerations for seals on (or part of) transportation casks are noted.

- Establish a method (or methods) to ensure that the correct seal is applied correctly. This might be a measure that can ensure that a seal's loop is threaded properly through a hasp on a container, combined with an active approach that ensures that all parts of a container (e.g., lid and body) are in proper contact by using a switch, a fiber, a continuous conductive path, self-sealing methods, weld integrity, or some intrinsic property of the container that unambiguously establishes that a cask is closed.
- Unique identifier for each seal to ensure that the correct seal has been applied. For a loop seal, this could be a feature on a seal such as a unique readable pattern, or an electronic authenticated signature. If a seal is integrated into a transportation cask, separate unique identifiers for seal and cask may not be required if the integrated seal cannot be removed from the cask.
- Tamper-indication: Whatever method is chosen, the inspectorate(s) must be confident that a seal has not been tampered, breached or defeated without detection.
- Remote verification: The inspectorate should be able to determine remotely that a seal has been properly attached, that a seal has not been tampered with, that a seal is functioning properly (state-of-health), and that a seal being monitored is the correct seal.
- The communications path by which the inspectorate receives information about a seal should include authentication measures to ensure that the data stream is valid. For example, seal data may be collected by a data-acquisition computer at either the location of attachment or downstream at the location of verification; consolidated seal data is then sent via VPN over the Internet to the inspectorate. Specifications about requirements for remote-monitoring systems have been provided by the IAEA (IAEA 2014b).
- To avoid holding an operator liable for improper installation, there must be a method that assures the operator and inspectorate that the correct seal has been attached correctly, as well as being verified and removed correctly. An operator should retain a record of this assurance. Further, an operator should be trained on properly performing the installation procedure. Specialized equipment may be needed to help ensure that proper procedure has been followed by an operator, such as the ESI used to apply EOSS sealing systems by German NPP operators (Section 2.3.1 and Figure 6).
- A seal must be both reliable and robust, especially as a seal will be exposed to the elements during transportation; e.g., on a container by ship. A seal should have long mean time between failures.

[22] Information in this section draws substantially on the analysis by (Brotz, et al. 2016).

- Before acceptance and deployment, a seal must undergo a vulnerability assessment (VA) and undergo periodic vulnerability reviews during the design process.

Consolidated technical needs for an operator-managed seal are based on the needs of all stakeholders: inspectorate(s), operator(s), State and regional regulatory authorities. In the following sections, we assume that remote monitoring of an operator-managed sealing system is electronic in nature. There may be other options for remotely monitoring operator-managed sealing systems for transportation casks; however, we consider that an electronically based system is the most likely type to be used.

4.1. Verifiability

Perhaps the most important attribute of an electronic sealing system is the degree of confidence it gives an inspectorate that a quantity of NM under safeguards has not been diverted or substituted. This confidence comes from the following sources.

- *Valid seal design*: A sealing system is designed according to appropriate requirements.
- *Correct seal application and operation*: A sealing system has been applied and operates according to requirements.
- *Seal integrity*: A sealing system has not been compromised by an attack.
- *Seal data integrity*: Data produced by a seal has not been compromised.

Each of these attributes is discussed below, including how each contributes to an inspectorate's confidence.

4.1.1. Validation of a Seal's Design

As discussed in the report, "Development and Evaluation of New Electronic Seals at the IAEA" (Tzolov, Goldfarb and Penot 2001), an electronic seal is a *multiple use*, *multiple verification, tamper-indicating device (TID)* with the capability to *store information* about its handling history.

A *multiple use* seal can be unsealed and resealed multiple times without damaging, permanently altering, or otherwise needing to refurbish a seal between uses.

A *multiple verification* seal can be verified non-destructively (by an inspector, or in the case of an operator-verified sealing system, by an operator).

A *TID* creates a record of tampering, both of the item under containment and of the seal itself[23].

Information stored by an electronic seal can be retrieved for later use by an inspector in order to gain confidence that there has been no undetected access to, or tampering with, the asset in containment and under seal.

The use-case for our analysis here is for sealing transportation casks that contain disposal canisters of spent fuel, and tampering in this use-case refers to any unauthorized opening of a transportation cask. Therefore, an electronic seal for this use-case must indicate (create a record of) any opening of a transportation cask under seal, including opening a transportation cask at any location on the cask (that is, not just opening a sealed cask lid). In order to meet these criteria and be accepted for use, such a sealing

[23] In the case where a seal has been tampered with, the record of tampering should be irreversible.

system must indicate tamper with a high degree of reliability and credibility, as discussed further in subsections 4.1.2 and 4.1.3 below.

4.1.2. Reliability

In order for a seal to give an inspectorate confidence in the integrity of an item under containment, a seal must operate as designed throughout its service life. The *reliability* of an electronic seal refers to the likelihood that a seal will not fail over a specified time period or, more generally, the degree to which a seal is resistant to failures during its service lifetime. Failure of a seal may result in a loss of CoK on the contents of a sealed containment. A number of factors can contribute to reliability, including seal construction materials, design of safety margins, redundancy of critical components, integrity of software or firmware, and environments in which a seal must operate (e.g., mechanical stress on a fiber-optic connector caused by an unsupported seal body could reduce reliability of the fiber-optic connector and, therefore, the associated seal and sealing system). Seal reliability can be addressed during the design process through a fault-tree analysis, which examines potential failures of a system by decomposing the system into subsystems and components. Understanding failure likelihoods for each subsystem and component is typically based on previous observations and experiments with similar components in other comparable systems. After design and manufacturing are complete, thorough reliability testing is commonly conducted on production units; however, the cost and time involved usually leads to a selective subset of environmental tests aimed at achieving an acceptable level of reliability.

Reliability is often viewed as being inversely proportional to complexity. While this may be overly simplistic, minimizing the number of components in a system's design may improve a system's overall reliability.

4.1.3. Usability

As described in Section 3, implementing an operator-applied sealing system will require that it meet several operator needs, including that it can be installed, verified and removed without errors by an operator. Usability refers to the degree to which users (inspectors or operators) can readily perform necessary sealing functions, including initializing, attaching, verifying, and detaching a seal. A maximally usable seal minimizes human error and thereby reduces situations that can cause a seal to operate incorrectly or malfunction. In addition, a highly usable seal provides greater confidence in verifications over a seal's service lifetime. Usability of a seal includes a verification (or reader) system as well, if that system is separate from the seal. An example of a useable sealing system is the operator-applied sealing system used by German NPP operators (Section 2.3.1) which employs a specially design tool (the ESI) that walks an operator through the sealing process and prevents an operator from continuing the sealing process if an error is detected by the ESI. Such a sealing system benefits both operator and inspectorate when it is designed to be user friendly (Brotz, et al. 2016).

4.2. Seal Integrity

In order for an inspectorate to have confidence in an electronic seal, a seal needs to deter and detect attempts to subvert the seal's function. Seal integrity is generally provided by security features and a design that makes it difficult (and/or costly) to bypass those security features. Thus, in addition to providing tamper indication for sealed containment, a secure seal design generally includes tamper indication for the seal itself, as discussed in more detail in the next section

4.2.1. Tamper Indication

The primary function for a sealing system is to provide tamper indication for the containment to which a seal is attached (e.g., by monitoring a fiber-optic loop seal). In addition, a seal should also contain tamper-indicating features that record attempts to physically alter the seal, perhaps with the intent to counterfeit a desired outcome. For example, disabling a seal wire's sensing mechanism so that a seal wire always seems to be closed, even when open. Tamper-indicating features can be as simple as a case switch; more complex tamper-indicating features include conductive foil that surrounds all security-critical seal components. The performance of tamper-indicating features on a seal is typically evaluated by an independent VA.

Tamper-indicating features on seals can be active, such as a tamper switch, or passive, such as a unique pattern that is altered permanently during tampering. Passive features must be inspected, often with a set of special tools, whereas active features commonly include recording tampering attempts and may remotely transmit that information, either automatically or when queried (e.g., by an inspector). The latter feature is likely to be requisite for operator-managed seals used on spent-fuel transportation casks.

4.2.2. Tamper Resistance

As distinguished from tamper-indicating features, *tamper resistance* refers to design features that might help reduce the likelihood that an adversary will attempt to defeat a seal. Such features might include thick metal enclosures and potted electronics designed to make targeted subversion attempts more difficult and to increase the cost of such attacks. The performance of tamper-resistance features can also be evaluated by an independent VA. Although potentially beneficial, a seal's tamper resistance is not as valuable as its tamper-indicating features, which are crucial to all seals. [24]

4.2.3. Mitigation or Absence of Physical Vulnerabilities

As discussed in previous subsections, a VA can identify paths that an adversary might use to defeat a seal or to mislead an inspector into having false confidence in the integrity of a breached containment. Key contributors to an inspectorate having confidence in an electronic sealing system include a system with few identified vulnerabilities along with mitigations for those vulnerabilities. All vulnerabilities constitute risks to be eliminated, mitigated, or accepted. High-security electronic seals are used by the IAEA and EURATOM to provide trustable containment of highly valuable assets critical to achieving their international safeguards missions. Therefore, vulnerabilities, even if mitigated, will only be acceptable if the cost to exploit or defeat them is considered unacceptably high to an adversary (Brotz, et al. 2016). An additional vulnerability concerns the robustness of a seal to resist accidental breakage (see Section 4.5 below).

4.2.4. Integrity of Seal Data

All electronic seals collect and record data used to gain and maintain confidence in a sealed containment. In addition to functions that enhance the trustworthiness of a seal as an effective TID, data created by those functions must also be trusted during the several potential stages of data management. These stages

[24] Also see footnote 18 in (Johnston 2001) for one view about the degree to which seals can be considered effectively tamper-resistant.

include (1) data creation, (2) data storage in a seal's internal memory, (3) data transmission (e.g., from seal to receiver), (4) data storage on another device external to a seal, and (5) data recovery for analysis (which may be days, months or even years after data was created). Criteria for meeting IAEA data-security requirements for all stages of data management for remotely monitored safeguards systems, including electronic seals, is discussed further elsewhere; e.g., (Capel, et al. 2004). We present some specific recommendations below.

4.2.4.1. Data Authenticity and Integrity

Data is considered *authentic* when it originated in a seal from which that data was expected to have originated. Data is considered to have *integrity* when data (or information) has not been altered, removed or otherwise corrupted since its creation. If data-authentication measures are not used, false data could be substituted for valid data, or a false seal could be made to seem like a valid seal such that the false seal could be used to create false (unauthentic) data. If data integrity measures are not used, parts of a data stream could be altered; for example, by changing a seal's status (its state value) from "open" to "closed".

Both data authenticity and data integrity are commonly protected by using cryptographic authentication, employing a mechanism such as a digital signature appended to valid data. By using cryptographic authentication, data (or an associated message) are used as input to a cryptographic algorithm, such as a Digital Signature Algorithm (DSA). A digital signature is represented in a computer as a string of binary digits. The signature is computed by using an algorithm such that the identity of the data-generating entity, the signatory, that signs the data (in our case, an electronic seal) – as well as the authenticity of the original data – can be verified. The signature is generated by using a *private key* known only to the signatory.

If a *symmetric key* is used to create an authentication signature, the same key is used to verify the authenticity and integrity of that data. If an *asymmetric key* (the private key in a public-private key pair) is used to create a signature, a seal's public key is used to verify the authenticity and integrity of the data. The public key corresponds to, but is not the same as, the private key. A signatory possesses both a private and public key pair. Public keys may be known by the public; whereas, private keys are kept secret. Only a valid signatory (a valid seal) can generate a valid digital signature (NIST 2013). A cryptographic authentication mechanism such as a DSA can be validated immediately upon retrieving data from a seal or it can be validated later; e.g., at a location away from the seal (such as inspectorate headquarters or a regional office).

While both symmetric and asymmetric algorithms protect data authenticity and integrity, an asymmetric algorithm imposes a smaller burden on the inspectorate to protect keys. The private key in a public-private key pair can be engineered to never exist outside a seal's electronics, for example, if the key is automatically generated within a seal upon the application of power or some other initialization step; however, this requires a true random-number generator in order to be secure. A public key can be freely transmitted without protection, since it is used only to verify data, not to sign data. A single key used in a symmetric algorithm needs to be protected, not only on the seal, but also on the reader device, at inspectorate offices, and anywhere else data might need to be verified. IAEA and EURATOM may need to verify seals data independently and require separate keys. If an operator needs to verify a seal's authenticity, the operator might require yet another separate key, although verification requirements may differ among stakeholders (operator vs. inspectorates) and will need to be developed. Public-key

encryption and pairing-based cryptography, including identity-based encryption (IBE), have been the subject of a great deal of research, as well as recent efforts at standardization (Moody, et al. 2015).

Assuring data authenticity and integrity from operator-managed seals on transportation casks will be crucial to the inspectorate for maintaining CoK on disposal canisters with spent fuel and avoiding re-verification of fuel assemblies after a seal has been removed.

4.2.4.2. Data Confidentiality

Safeguards data is considered *confidential* if it can be read only by the inspectorate. Data confidentiality, or secrecy, prevents a host from seeing event logs on the seal or the reader device. While this may not always be necessary, knowledge of seal data may be considered proprietary by the inspectorate. Some data collected for safeguards purposes may be considered sensitive or proprietary by an operator or State and therefore require it be treated as confidential by the inspectorate (Capel, et al. 2004). Details about sharing safeguards-relevant information from operator-managed seals, and among which parties, will require careful consideration; however, an operator most urgently needs authorization from the inspectorate to remove/open a seal in order to remove a canister from a transportation cask and may not require detailed information about confidential safeguards data.

Data confidentiality is provided by encrypting data by using a cryptographic algorithm, such as the Advanced Encryption Standard (AES) (NIST 2001). The key used for encryption must be protected, both within a seal for encryption and outside of a seal for decryption. A mechanism can be used to reduce the inspectorate's burden for the protection of encryption keys if a public-private key pair exists on a seal and an associated device is used to read seal data. With an IBE based on a Diffie-Hellman key exchange (Diffie and Hellman 1976), the private key of one side (the seal) can be combined with the public key of another (the reader), creating a symmetric encryption key that is shared only between that seal and that reader. As public keys are the only keys transmitted outside of their respective devices, no transmitted keys are vulnerable, and once a session is complete, a combined key can be erased (upon initiation of the next session, the key will be created again).

As discussed in Section 3 above, surveillance data may contain sensitive or proprietary information that an operator will require be encrypted in order to maintain its confidentiality; such data cannot be shared (e.g., by EURATOM to IAEA) without an operator's or State's approval. In addition, information about the location of spent-fuel disposal canisters may be considered a security concern, and such information could require encryption as well as, potentially, a transmission delay (see Section 2.3.1). IAEA Member State requirements for data confidentiality are addressed in the Model Additional Protocol (IAEA 1998, Articles 14b & 15a) and by IAEA's Policy Paper on Remote Monitoring (Capel, et al. 2004).

4.2.4.3. Potential Vulnerabilities in Cryptographic Firmware or Software

As with physical vulnerabilities, vulnerabilities in either firmware or software (both within a seal and in a reader device) should be eliminated or mitigated. In addition to the use of recommended cryptographic algorithms of sufficient bit strength, a VA is commonly performed to identify potential vulnerabilities. However, potential new and currently unknown vulnerabilities may arise due to advancements in technology.

4.2.4.4. Potential Obsolescence of Cryptographic Firmware or Software

Another consideration for firmware and software used to authenticate or encrypt safeguards data is the potential advent of quantum cryptography during the extended period over which a repository will operate, and whether that could impact or compromise operator-managed seals if current conventional methodologies are used in their design.[25]

4.3. Joint-Use Capability

Both the IAEA and EURATOM perform safeguards functions for Sweden and Finland (States in which the first geologic repositories are likely to be operating within the next decade). Both inspectorates commonly use the same sealing systems for similar items under containment. Both inspectorates should therefore approve any operator-managed electronic seal designed for transportation casks. Although most sealing functions would be performed by an operator, each inspectorate would also have a compatible reader device and could use separate cryptographic keys to verify authenticity of such a seal and its data. If a public-private key pair is used for data authentication, both inspectorates could verify data independently without sharing secrets. In addition, a public-private key pair would allow both inspectorates to encrypt data with two different encryption keys by using a Diffie-Hellman key exchange, as described above. A public-private key pair makes it easier for each inspectorate to independently verify its own data authentication and encryption methods, should that be necessary. As noted above (Sections 4.2.4.1 and 4.2.4.2) if an operator needs to verify a seal's authenticity, the operator might require yet another separate key; however verification requirements may differ among stakeholders (operator vs. inspectorates) and those requirements will need to be developed.

4.4. Maintainability

An electronic seal should require minimal maintenance throughout its lifetime, and any maintenance that is necessary should be straightforward and relatively easy to perform. The primary maintenance required by electronic seals is battery replacement. The battery should last as long as possible before needing to be replaced. If replacing the battery causes a seal to lose power, the seal will need to be re-initialized. A seal is most commonly re-initialized at the inspectorate headquarters in order to maintain security; however, an operator-managed seal may need to take into account the potential for on-site re-initialization, especially if a seal is integrated into a transportation cask. Indeed, maintaining such an integrated seal could be a problem if designed without considering such maintenance concerns. For example, if a seal on a loaded transportation cask requires maintenance or repair, maintaining CoK on the cask and its contents could be a challenge, and planning for such contingencies will be necessary before implementation.[26] As an example, an on-site (or on-transport) backup battery could be used to maintain power to an electronic seal during transfer of the primary battery, thereby enabling battery replacement in the field. Other parts that might need replacement over a seal's lifetime should also be readily available throughout the operational phase of a repository. A long-term parts purchase might also help prevent technical obsolescence (and long or permanent downtimes), especially considering decades-long periods expected

[25] See for example the NIST announcement at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[26] Dual C/S measures may help to mitigate such concerns to some extent, but a systematic approach to addressing these issues is recommended.

for repository operations (Hildingsson and Andersson 2014). The degree to which an operator would be authorized to perform such maintenance activities is not certain, but would likely entail an agreement among the operator, the state regulatory agency, and the inspectorate (IAEA 2014b, Section 7.3 and Annex 9).

Flexibility in the choice of batteries that can be used for a given seal is also desirable. Commercial off the shelf (COTS) batteries are most readily procured. Flexibility in the type of batteries that can be used in a seal is also beneficial, although implementing such flexibility may be difficult due to voltage limitations. The likelihood that COTS battery designs and specifications may change over the operational period will also need to be considered. Years-long storage of many batteries is not feasible, so that long-term procurement of COTS batteries may not be an option.

Other seal components to consider are plastics and other potentially degradable materials that may need replacement. Understanding the environmental conditions to which a seal will be exposed during its expected service lifetime will help mitigate or prevent potential maintenance problems caused by using materials inappropriate or inadequate for a seal's expected use. In addition to common environmental conditions, such as temperature and humidity, the radiation field to which a cask-mounted or cask-integrated seal will be exposed is a potentially important consideration, as will the decades of frequent handling that a re-useable transportation cask will experience. Considerations for seal performance under expected environmental conditions is discussed further in Section 4.5 below.

A final note on maintainability is to mention the possibility that software and firmware will need upgrades or develop vulnerabilities over their service lifetimes due to future technological advances (see Section 4.2.4.4). Attention to such possibilities should be part of future seal-design considerations, especially for sealing systems that could be integrated into transport casks intended for many decades of use.

4.5. Operation in Expected Environments

A sealing system attached to a transportation cask must be designed to operate effectively over its service lifetime under the range of environmental conditions that a transportation cask can be expected to experience during shipments. In addition, a transport cask, and associated seal, will experience handling operations in preparation for, during, and after each shipment. Shipping conveyances may include land-based vehicles, such as trucks and railcars, and ocean-going vessels, and shipments may include modal transfer points between conveyances. Shipping and handling will therefore expose a transportation cask and seal(s) to some level of shock and vibration. The period between repeated use of an individual transportation cask could be on the order of four weeks (Hildingsson and Andersson 2017), and the service lifetime of a re-usable transportation cask may be several decades. Sealing systems built/integrated into such long-service transportation casks would need to operate over the same service lifetime.

A transportation cask, and an associated sealing system, will experience variations in temperature (both ambient and radiation-induced), humidity and radiation dose (primarily gamma radiation). Depending on shipping venues and storage locations, casks and seals may also be exposed to corrosive salt-sea air and salt-sea spray. The Swedish case provides a design basis for a transport cask, including requirements for anticipated environmental conditions (SKB 2010). The Swedish cask design will be designed to fulfil criteria for a Type B cask in accordance with IAEA requirements (IAEA 2012).

Transportation casks will experience heat generated internally by spent fuel due to decay heat. The Swedish design requires that the temperature on the surface of the copper canister (inside the transportation cask) not exceed 100°C, and the maximum temperature on the exterior of the cask is likely to be considerably lower. In fact, transportation casks used in both Sweden and Finland may experience external cask temperatures well below freezing during winter months. Of course, Sweden's design basis is not universal, and each country's design criteria will need to be considered when designing a sealing system for transportation casks to be employed in a specific country.

A sealing system will need to perform as designed over an extended service lifetime, during which it will accumulate radiation dose over many decades, and some degradation of electronics and plastic components might be anticipated. Decay heat and radiation dose rate are related, and the maximum acceptable radiation dose rate at the surface a Swedish canister is 1.0 Gray per hour (Gy/hr). This is considerably more than the maximum dose rate expected (less than about 0.2 Gy/hr), based on Sweden's selection criteria for assemblies (SKB 2010, pp. 33 & 57), which are based on decay-heat criteria (designed to maintain canister temperature below 100°C, as noted above). Again, these criteria and conditions apply to the Swedish case, and each country's design criteria will need to be considered when designing a sealing system for transportation casks employed in a specific country0.

Decades of frequent handling that a re-useable transportation cask will experience will be a further consideration for a sealing system, which must not fail during shipment. A seal must not break or be removed accidentally at any place or time between the shipping point and the receiving point, as this could lead to an unacceptable loss of CoK. Thus a sealing system for a transportation cask will need to be robust against breakage or unintentional removal. Given the potential for environmentally driven degradation of some system components over a seal's service lifetime, unintentional breakage could become an increasing concern over time – and may be of particular concern for a seal integrated into the cask design (*cf*. Section 4.4). The inspectorate will also levy requirements for environmental testing to be performed on a sealing system before it is put into use.

4.6. Remote Verification Capability

Multiple transportation casks in a single storage, holding or staging area can generate a collective radiation field, increasing the threat to human health; access to such areas must be minimized. Verifying, reading, or otherwise inspecting a seal that requires a direct (and close) connection to a seal can expose inspectors and operators alike to unacceptable radiation levels. Such concerns can be mitigated through remote verification, which is the capability for an electronic seal to communicate to a reader device outside a hazardous area, and which can be accessed without undue exposure to radiation.

A seal and a reader device can communicate in a variety of possible ways, including cables and wireless telemetry; however, options may be limited because of the mobile nature of transportation casks. For example, attaching (and removing) cables to seals on transportation casks in a storage or holding area risks exposing individuals to radiation fields that should be avoided. The fact that seals on transportation casks might need to be attached and removed frequently further obviates this method. There are other disadvantages to connecting multiple seals to wired communication links (Brotz, et al. 2016).

Wireless communications provide an attractive alternative to monitoring and verifying seals on multiple transportation casks. A single wireless base station can communicate with multiple electronic seals, and such connections (and disconnections) can be accomplished without necessarily accessing the seal to be

monitored. Nevertheless, wireless communications can pose security concerns (e.g., unauthorized access to a wireless signal may allow data to be intercepted, altered or otherwise corrupted). Such concerns can be mitigated with strong data authentication and encryption (see Section 4.2.4 above).

4.7. Remote Monitoring Capability

Somewhat related to remote verification is remote monitoring. But, whereas remote verification refers to on-site communications between safeguards equipment such as seal and readers, *remote monitoring* (in a safeguards context) refers to transmission to an inspectorate of safeguards data that has been collected from sealing systems, UMS, and optical surveillance systems (IAEA 2011, Section 5, p. 78-84).

As discussed in Section 2.2.1.1, remote monitoring has played an increasingly important role in the successful implementation of IS. Remote monitoring provides the capability to encrypt data and communicate with inspectorate offices over communication links such as public switched telephone networks (PSTN), integrated services digital networks (ISDN), asymmetric digital subscriber lines (ADSL), and satellite services (Figure 8). The IAEA's main central data collection and communications controllers for field deployment are server-based surveillance systems, such as digital-image surveillance (SDIS) and digital multi-camera optical surveillance (DMOS); however, the use of UMS continues to expand under remote monitoring, most notably for monitoring spent fuel in storage (IAEA 2011). Nevertheless, as demonstrated in the examples described in Section 2.3 above, remote, unattended monitoring of seals and seals data has also been successfully implemented at a number of facilities.

Such systems provide useful models for UMS applied to remotely monitoring seals on transportation casks. However, unlike stationary seals (e.g., at spent-fuel storage facilities), transportation-cask seals will need to be monitored throughout each shipment: from the time a seal is attached at the shipping point, throughout all transport and handling operations, until final verification and removal at the receiving point. This will likely limit communications links to satellite systems.

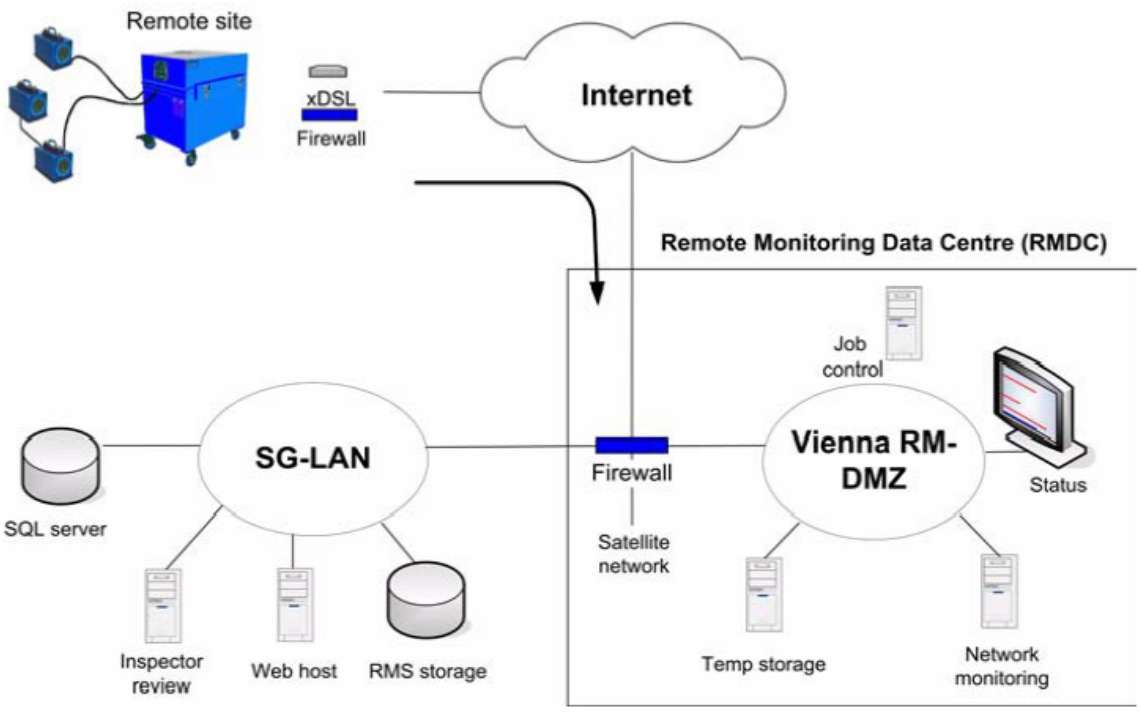

Figure 8. Schematic diagram of remote monitoring system (IAEA 2011, Fig. 42, p. 82).[27]

4.8. Procedural Implementation

In the absence of an inspector, an operator that applies or removes a seal needs confirmation that the correct seal has been applied correctly or has been verified and removed correctly. This avoids operator liability for improperly applied or removed seals, and provides assurance to the inspectorate that the procedure has been executed properly. A crucial aspect of proper execution requires comprehensive and detailed procedures, fully approved by both inspectorate and operator, to be followed by an operator, as well as sufficient training of operators on properly executing those procedures and on the use of any special equipment. In the German example described above (Section 2.3.1) the operator received instruction manuals for both sealing procedures implemented by the NPP operator as well as training on the procedures and the use of the ESI.

The ESI used in the German NPP example guides the operator step-by-step through the EOSS sealing procedure. By contrast, the JRC prototype for an operator-applied seal on a cask can be sealed without any special procedures after an inspector has attached that sealing system to a cask and lid (Section 2.1.1). A similarly transparent operator-managed sealing system would be ideal for transportation casks

[27] See the Abbreviations & Acronyms for definitions of acronyms shown in Figure 8. Note that the term demilitarized zone (DMZ) in Vienna Remote Monitoring – Demilitarized Zone (RM-DMZ) refers an Ethernet connection that is logically and physically separated from both the internal (secure) network and the external (insecure) network.

containing disposal canisters, but such a seal might require fully integrating the sealing system into the transportation cask's design. However, if such a transparent sealing system cannot be implemented, appropriate training of an operator in executing sealing (and unsealing) procedures and any use of special equipment will be necessary. Additional arrangements and agreements about how the inspectorate will handle or respond to unexpected or off-normal events should also be negotiated.

5. CONCLUSIONS AND RECOMMENDATIONS

Following the final NMA determination on spent fuel destined for permanent disposal, a critical objective of safeguards is to maintain continuity of knowledge (CoK) on the verified fuel assemblies by using highly reliable, redundant C/S measures. The transportation link is one of the more challenging stages of the disposal process when it comes to maintaining CoK on encapsulated fuel assemblies, which will rely on C/S measures to a degree unprecedented in other stages of the nuclear fuel cycle. Dual C/S measures will be applied to maintain CoK during transport, one component of which could be effective containment by a transportation cask to include a sealing system that can assure a cask's containment integrity. This may require a specially designed sealing system (or systems), as no current sealing system can assure containment integrity of a transportation cask. Furthermore, if seals on spent fuel transportation casks could be applied, verified and removed by an operator with IAEA approval, this could significantly reduce the burden on the inspectorate to perform such duties during repository operations.

IAEA policy has been that the IAEA must be involved in either the application or the removal of a seal. In the case where an operator applies a seal, IAEA's removal of that seal verifies that the operator had applied the correct seal correctly, and the containment can be inspected to assess whether its integrity has been maintained. If an operator is to remove safeguards seals, the IAEA must be confident that the correct seal had been applied correctly at the shipping end (currently performed by a trained IAEA inspector), that the operator uses an approved verification measure at the receiving end, and that the sealing system (including containment) has not been tampered. This assurance is especially crucial for transportation casks containing spent fuel for disposal, as there will be no opportunity to re-verify spent fuel once it has been emplaced underground. To date, no seal for a transportation cask can provide that level of containment assurance; however, a sealing system that is fully integrated with a transportation cask might provide such assurance.

A sealing system for a transportation cask that can be fully managed by an operator, including applying, verifying, and removing such seals, may need to be specifically designed for that application, and may entail developing auxiliary equipment to ensure that the sealing and unsealing procedures are performed appropriately. One example auxiliary system used to ensure proper application of seals is the ESI used by German NPP operators (Section 2.3.1). Another sealing system that requires no auxiliary interface between operator and sealing system (but requires one-time installation by an inspector) is the prototype sealing system for casks described in Section 2.1.1. Both systems provide models for developing a sealing system for transportation casks that could be fully managed by an operator.

Remote monitoring will likely be a crucial component of successfully deploying operator-managed sealing systems for transportation casks. IAEA has been expanding its remote monitoring capabilities and increasing its use of UMS that can operate in remote-monitoring mode, and in monitoring operators performing IAEA functions, including the application or removal of electronic seals. A seal must have the capability to provide the inspectorate sufficient confidence to confer approval to the operator to proceed with emplacing a disposal canister that will be removed from its cask after a seal is removed – or can notify an operator in a timely fashion not to proceed if there is a problem; these decisions will need to be made remotely and will therefore require RDT from seals to the inspectorate.

Regardless of the eventual design and use of a successfully implemented operator-managed sealing system for transportation casks, remotely monitored video surveillance will be needed to record the application and removal of seals by operators. Such systems are already common at many facilities and

generally include information-sharing agreements, along with appropriate infrastructure with agreed-upon maintenance arrangements (IAEA 2014b).

5.1. Recommendations

Establish methods to *ensure that the correct seal is applied correctly*. An example might be to combine measures, one that ensures that a seal's loop is installed properly with an active approach that ensures all parts of a cask are in proper contact.

Each sealing system must have a *unique identifier*. This could be a feature on the seal (e.g., a unique readable pattern or an electronic authenticated signature), but if a seal is integrated into a transportation cask, separate unique identifiers for seal and cask may not be required if the integrated seal cannot be removed from the cask.

Tamper-indication. A sealing system must provide the inspectorate(s) with confidence that a seal cannot be tampered, breached or defeated without detection.

Remote verification. The inspectorate should be able to determine remotely that a seal has been properly attached, that a seal has not been tampered with, that a seal is functioning properly (state-of-health), and that a seal being monitored is the correct seal.

Data authentication. The communications path by which the inspectorate receives information about a seal should include authentication measures that ensure the validity of a data stream. For example, seal data may be collected by a data-acquisition computer at either the location of attachment or downstream at the location of verification; consolidated seal data is then sent via VPN over the Internet to the inspectorate. Specifications about requirements for remote-monitoring systems have been provided by the IAEA (IAEA 2014b).

A seal must be reliable and robust under the range of environmental conditions in which it will operate over its service lifetime, with a long mean time between failures. A sealing system used for a transportation cask, especially if it is to be used for the lifetime of the cask (such as an integrated seal) will probably need to operate in a wider range of environments than most seals and to tolerate handling operations during shipping (including handling accidents such as dropping a cask or, potentially, more severe accidents such as collisions).

Sealing System – operation: An operator-managed sealing system must be applied in a "fool-proof" manner, either automatically applied upon cask closure (similar to the prototype system described in Section 2.1.1) or according to agreed-upon procedure with possible special equipment (similar to German case described in Section 2.3.1). Once applied, a sealing system should operate in unattended mode and comprise one or more electronic seals that are remotely monitored and can transmit safeguards-relevant data to the inspectorate. Seals should provide timely information to both operator (on site) and inspectorate (off site) as to the correctness (or lack) of a seal's application and closure, remote transmission of seal status, including SoH information and other agreed-upon data (e.g., location), timely information to both operator and inspectorate of a seal's integrity (or its lack) upon arrival at the receiving end, and when a seal has been opened in an acceptable manner (or not). The signal must provide a timely alert for any "hold" or "do not open" warning for any cask on which a seal indicates a problem.

Sealing System – containment: A sealing system must ensure that any breach of a cask's containment, whether by opening a lid, cutting through another location on the cask, or any other penetration of the

cask, is detected and recorded, and that the information is transmitted in a timely manner to the inspectorate. This eliminates a sealing bolt (only) as an acceptable sealing system, as this only detects opening of a cask's lid. If two independent sealing systems are used to satisfy dual C/S, then both must assure the same level of confidence in a cask's containment integrity.

Time and Distance: Although transportation casks will be shielded, the radiation field will be such that applying seals must be accomplished without undue exposure to any individual, especially as the application, verification and removal of seals will occur on a regular basis. These operations need to be done as quickly as possible or from as great a distance as possible (or both). Most promising would be a seal that can be applied, verified and removed without exposing an individual to the radiation field near a cask or canister; e.g., by means of a remote-handling operation.

Location – Application: Seals would be applied to transportation casks at the shipping point. For the Swedish case, this occurs at the encapsulation plant for shipment to the repository; whereas, in the Finnish case this occurs at the NPP. Each country with a repository program will develop transportation criteria and plans specific to that country.

Location – Verification & Removal: These operations occur at the receiving end of a shipment (e.g., repository or encapsulation plant). Verification may occur before a transportation cask enters the repository's underground workings and the seal removed underground where the cask would be opened and the disposal canister extracted for final emplacement.[28] In this case, there can be no potential for a disposal canister that has not been verified and approved for final disposal to enter the repository. A complementary option might be to consider implementing a "station" to interrogate seals when each transportation cask arrives at the receiving point. This might be envisioned as a "docking station" under IAEA control that would have the capability to transmit information about a seal's status to a database. In any case, seal removal is likely to be conducted under video surveillance.

Remote Data Transmission (RDT) and Remote Safeguards Inspections (RSI): Successfully implementing operator-managed seals – both their application and removal – will require successfully implementing unattended RDT, which must meet certain operator criteria, including security concerns. Remote transmission of safeguards equipment SoH allows inspectors to remotely check safeguards equipment SoH before transfers of NM so that problems or defects can be reported to the operator as soon as possible. Potential interruptions to data transmission must also be anticipated and should not adversely affect operations; e.g., by including local data storage for an RDT system along with automatic synchronization of the system following interruptions.

Timeliness: IAEA concurrence on all aspects of the process, the application, verification and removal of a seal, must be timely, perhaps as short as a few hours for the IAEA to notify an operator of any irregularities and whether or not to proceed to the next step in the process.

Burden of proof must be on the IAEA: An operator must know that (1) the correct seal has been applied correctly, (2) that a seal has not been compromised, (3) whether a seal can be removed and (4) that IAEA will not require reverification after the operator has received authorization that a seal can be removed and the canister emplaced. That is, before a seal can be removed by an operator, the IAEA must acknowledge that CoK has been maintained on the transportation cask and its contents during shipment (a disposal

[28] Implementing safeguards measures underground in a repository is potentially contentious (Murtezi, et al. 2015).

canister and the spent fuel it contains). Authorized removal of a seal by an operator must also be conducted in such a way that the IAEA can confer approval to the operator to proceed with emplacing the disposal canister that will be removed from the cask from which a seal is to be removed – or can notify the operator in a timely fashion not to proceed if there is a problem.

6. REFERENCES

Araujo, J., C. Charlier, D. Hatt, A. Lebrun, N. Muroya, P. Rance, I. Tsvetkov, R. Zarucki, and M. Zendel. 2010. "Enhancing and Optimizing Safeguards Implementation by Remote Safeguards Inspections." *International Safeguards Symposium: Preparing for Future Verification Challenges.* Vienna: IAEA. Accessed August 2017. https://www.iaea.org/safeguards/symposium/2010/Documents/PapersRepository/266.pdf.

Araujo, J., G. Morris, I. Tsvetkov, Z. Vukadin, B. Wishard, W. Kahnmeyer, and W. Trautwein. 2014. "Verification of Spent Fuel Transfers in Germany- Linking Strategy, Implementation and People." *Symposium on International Safeguards: Linking Strategy, Implementation and People, 20–24 October 2014.* Vienna: International Atomic Energy Agency. 426. Accessed August 2017. https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-slides/000025.pdf.

Baldwin, George, Risa Haddal, and Robert J Finch. 2016. "Containment and Surveillance as a Primary Approach for Safeguarding Geological Repositories." *Annual Meeting of the Institute for Nuclear Materials Management, July 25-28, 2016.* Atlanta, Georgia: INMM.

Brotz, J., H. Smartt, R. Haddal, K. Aymanns, M. Durr, I. Niemeyer, and A. Rezniczek. 2016. *Lifecycle Study of the Electronic Optical Sealing System (EOSS): Assessment of Technical Challenges and Needs.* Technical Report SAND2016-2352, Albuquerque: Sandia National Laboratories.

Capel, Tony, Keith Tolk, Cesare Liguori, and Peter Button. 2004. "A Systematic Approach to Data Security for Unattended and Remote Monitoring Systems." *Proceedings of the 45th Annual Meeting, Institute of Nuclear Materials Management, July 18, 2004.* Orlando, Florida: INMM. Accessed September 2017. https://www.inmm.org/INMM/media/Archives/Annual%20Meeting%20Proceedings/2004/0267.pdf.

Diffie, Whitfield, and Martin Hellman. 1976. "New directions in cryptography." *IEEE Transactions on Information Theory* IT-22 (6): 644-654. Accessed September 2017. doi:10.1109/TIT.1976.1055638.

Drobysz, Sonia, and Bernard Sitt. 2011. "Optimizing the IAEA Safeguards System." *EU Non-Proliferation Consortium.* CESIM (Centre d'Études de Sécurité Internationale et de Maîtrise des armements). September . Accessed September 2017. http://www.nonproliferation.eu/web/documents/other/soniadrobyszbernardsitt4ecd0b3738cb3.pdf.

Hildingsson, Lars, and Camilla Andersson. 2014. "Safeguards aspects regarding a geological repository in Sweden." *IAEA Symposium on International Safeguards: Linking Strategy, Implementation and People, 20-24 October 2014.* Vienna: International Atomic Energy Agency. p. 236. Accessed September 2017. https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000166.pdf.

Hildingsson, Lars, and Camilla Andersson, interview by R. Finch and H. Smartt. 2017. *via Skype* (January 12).

IAEA. 1998. *INFCIRC/540 (Corrected) Model Protocol Additional to the Agreement(s) between State(s) and the IAEA for the Application of Safeguards.* Information Circular, Vienna: International Atomic Energy Agency. Accessed September 2017. https://www.iaea.org/sites/default/files/infcirc540c.pdf.

—. 2001. *Safeguards Glossary.* 2001 Edition. International Nuclear Verification Series No. 3. Vienna: International Atomic Energy Agency. Accessed August 2017. https://www.iaea.org/sites/default/files/iaea_safeguards_glossary.pdf.

—. 2003. *Policy Paper 15: Safeguards for Final Disposal of Spent Fuel in Geological Repositories.* Safeguards Manual, Safeguards Policy Series, SMR 2.15, Section 3.1.1, Vienna: International Atomic Energy Agency.

—. 2005. *Safeguards Manual - Safeguards Criteria.* SMC, SGCP-PST, Vienna: International Atomic Energy Agency.

—. 2010a. *Model Integrated Safeguards Approach for a Spent Fuel Encapsulation Plant.* International Atomic Energy Agency, Vienna: IAEA Department of Safeguards (SGCP-CCA), SG-PR-1305 (ver. 1, 18 October 2010).

—. 2010b. *Model Integrated Safeguards Approach for a Geological Repository.* SG-PR-1306, SGCP-CCA, Vienna: International Atomic Energy Agency.

—. 2011. *Safeguards Techniques and Equipment.* 2011 Edition. International Nuclear Verification Series No. 1 (Rev. 2). Vienna: International Atomic Energy Agency. Accessed August 2017. http://www-pub.iaea.org/MTCD/Publications/PDF/nvs1_web.pdf.

—. 2012. *Regulations for the Safe Transport of Radioactive Material.* Specific Safety Requirements No. SSR-6, Vienna: International Atomic Energy Agency. Accessed September 2017. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1570_web.pdf.

—. 2013. *Partnership Approach Under Integrated Safeguards For Spent Fuel Storage Facilities.* Vienna, May 15.

—. 2014a. "Safeguards Statement for 2013." *International Atomic Energy Agency.* International Atomic Energy Agency. Accessed September 2017. https://www.iaea.org/safeguards/symposium/2014/images/pdfs/Statement_for_SIR_2013_GOV_2014_27.pdf.

—. 2014b. *Safeguards Implementation Practices Guide on Facilitating IAEA Verification Activities.* Safeguards Implementation Practices (SIP) Guide, Services Series 30, Vienna: International Atomic Energy Agency, x + 96 pp. Accessed September 2017. http://www-pub.iaea.org/MTCD/Publications/PDF/SVS-30_web.pdf.

—. 2015a. "IAEA Safeguards Serving Nuclear Non-Proliferation." *IAEA Safeguards Serving Nuclear Non-Proliferation.* International Atomic Energy Agency. June. Accessed August 31, 2017. https://www.iaea.org/sites/default/files/safeguards_web_june_2015_1.pdf.

—. 2015b. "STATUS LIST." *International Atomic Energy Agency.* International Atomic Energy Agency. July 3. Accessed September 2017. https://www.iaea.org/sites/default/files/sg_agreements_-_status_list_-_3_july_2015.pdf.

Johnston, Roger G. 2001. "Tamper detection for safeguards and treaty monitoring: fantasies, realities, and potentials." *The Nonproliferation Review* (James Martin Center for Nonproliferation Studies) Volume 8 (Spring 2001): 102-115. Accessed August 2017. https://www.nonproliferation.org/wp-content/uploads/npr/81john.pdf.

Jussofie, A., K. van Bevern, M. Hahn, and W. Trautwein. 2014. "Germany's Accelerated Exit from Nuclear Energy: Challenges and Perspectives with Regard to Safeguards." *IAEA Symposium on International Safeguards: Linking Strategy, Implementation and People, 20-24 October 2014.* Vienna: IAEA. p. 269. Accessed August 2017. https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000123.pdf.

Jussofie, A., R. Graf, and W. Filbert. 2010. "German Approach to Spent Fuel Management." *IAEA Symposium on International Safeguards: Preparing for Future Verification Challenges, 1–5 November 2010.* Vienna: IAEA. Accessed August 2017. http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/42/081/42081472.pdf.

Mongiello, Risa, Robert J Finch, and George Baldwin. 2013. *Safeguards Approaches for Geological Repositories: Status and Gap Analysis.* Technical Report SAND2013-5185P, Albuquerque: Sandia National Laboratories.

Moody, Dustin, Rene Peralta, Ray Perlner, Andrew Regenscheid, Allen Roginsky, and Lily Chen. 2015. "Report on Pairing-based Cryptography." *Journal of Research of the National Institute of Standards and Technology* (NIST) 120 (2015): 11-27. Accessed September 2017. doi:http://dx.doi.org/10.6028/jres.120.002.

Moran, Bruce, interview by R. Finch. 2017. *via email* (June).

Murtezi, M., W. Kahnmeyer, C. Koutsoyannopoulos, P. Schwalbach, and A. Zein. 2015. "Euratom Perspective on Safeguarding Final Disposal: the Finnish Baseline." *Presented at the 11th ASTOR Experts Meeting, 20 – 22 April 2015.* Gyeongju, Republic of Korea: International Atomic Energy Agency.

NIST. 2001. *Announcing the Advanced Encryption Standard (AES).* Federal Information Processing Standard (FIPS) 197, Information Technology Laboratory, National Institute of Standards and Technology, Gathersburg, Maryland: US Department of Commerce. Accessed September 2017. https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf.

NIST. 2013. *Digital Signature Standard (DSS).* Federal Information Processing Standard (FIPS) 186-4, Information Technology Laboratory, National Institute of Standards and Technology,

Gaithersburg, Maryland: US Department of Commerce, 130 pp. Accessed September 2017. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

Persson, L., S. Synetos, A. Ozols, K. Ruuska, R. Leslie, H. Du Preez, C. Martinez, K. Payne, A. Polkey, and M. Beaman. 2014b. "Use of electronic seals and remote data transmission to increase the efficiency of safeguards applied in a static Plutonium store." *Symposium on International Safeguards: Linking Strategy, Implementation and People. 20–24 October 2014.* Vienna: International Atomic Energy Agency. p. 426. Accessed September 2017. https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000027.pdf.

Persson, L., S. Synetos, A. Ozols, M. Ayranov, Y. Lahogue, A. Kiewiet, D. Ancius, et al. 2014a. "Consolidation of NM in the UK: Optimising the EURATOM approach." *Symposium on International Safeguards: Linking Strategy, Implementation and People, 20-24 October 2014.* Vienna: IAEA. p. 257. Accessed August 2017. https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000176.pdf.

SKB. 2010. *Design, production and initial state of the canister.* Svensk Kärnbränslehantering AB, Stockholm: SKB Technical Report TR-10-14, 111 pp.

Tzolov, Rouman, Michael Goldfarb, and Laurent Penot. 2001. "Development and evaluation of new electronic seals at the IAEA." *IAEA Symposium on International Safeguards: Verification and Nuclear Material Security, 29 Oct - 2 Nov 2001.* Vienna: International Atomic Energy Agency. p. 115. Accessed August 2017. https://inis.iaea.org/search/search.aspx?orig_q=source:"IAEA-SM--367/7/07".

DISTRIBUTION

National Nuclear Security Administration

Attn:

1	Melissa Einwechter (Melissa.Einwechter@NNSA.DOE.Gov)	NNSA/NA241 (electronic copy)

Sandia National Laboratories

Attn:

1	MS 0899	Technical Library, 9536 (electronic copy)
1	MS 1371	Risa Haddal, 6832 (electronic copy)
1	MS 1371	Tina Hernandez, 6832 (electronic copy)
1	MS 1371	Dianna Blair, 6830 (electronic copy)
1	MS 1371	Robert Finch, 6832 (electronic copy)
1	MS 1373	Heidi Smartt, 6832 (electronic copy)
1	MS 1375	Rodney Wilson, 6800 (electronic copy)


Sandia National Laboratories