SANDIA REPORT
SAND2018-10552
Unclassified Unlimited Release
Printed September 2018
NOT FOR DISTRIBUTION Tracking Number 819777

Developing Design Criteria for Safeguards Seals for Spent Fuel Transportation Casks – Final Report

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

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

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-NA0003525.

Sandia National Laboratories

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

Printed in the United States of America. This report has been reproduced directly from the best available copy.

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

SAND2018-10552
Printed September 2018
Unclassified Unlimited Release

Developing Design Criteria for Safeguards Seals for Spent Fuel Transportation Casks

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

Abstract

Current designs for spent fuel transportation casks cannot ensure a cask's integrity during shipment, nor is there any verifiable means of maintaining continuity of knowledge (CoK) on a cask's contents. Spent fuel destined for encapsulation plants or geological repositories requires additional containment and surveillance (C/S) measures during shipment. Following final safeguards accountancy measurements on spent fuel assemblies, the shipment of verified assemblies will require unprecedented reliance on maintaining CoK on the fuel inside transport casks. Such increased reliance is due to the lack of reverification of spent fuel following encapsulation into disposal canisters and by meeting the requirement of dual C/S measures during such fuel shipments according to recommendations made by the Application of Safeguards to Geological Repositories (ASTOR) International Atomic Energy Agency (IAEA) expert group. By designing spent fuel transportation casks with effective seals integrated into their design, CoK can be more effectively maintained than by ad hoc C/S measures because seal integration ensures that a cask has not been tampered with. Externally applied seals might not be able to provide such assurance for currently designed spent fuel transportation casks, although some combination of seals, detectors, and/or a technology that can verify canister integrity might provide this assurance. This paper examines the design criteria for integrating safeguards seals into transportation casks and provides recommendations for near-term applications.

ACKNOWLEDGMENTS

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.

The authors thank Bruce Moran for helpful comments and discussions.

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

ABBREVIATIONS & ACRONYMS

AES	Advanced Encryption Standard
BNFL	British Nuclear Fuels Limited
BMG	British Nuclear Group
BWR	Boiling water reactor
C/S	Containment and surveillance
CoK	Continuity of knowledge
COTS	Commercial off the shelf
DSA	Digital Signature Algorithm
EOSS	Electronic Optical Sealing System
Euratom	European Atomic Energy Community
GNS	Gesellschaft für Nukleaire Services
IAEA	International Atomic Energy Agency
JRC	Joint Research Centre
MUND	Mobile Unattended Neutron Detector
NAC	Nuclear Assurances Corporation
NGSS	Next Generation Surveillance System (NGSS)
NM	Nuclear material
NMA	Nuclear material accountancy
NPP	Nuclear power plant
PWR	Pressurized water reactor
RMSA	Remotely Monitored Sealing Array
SFA	Spent fuel assembly
SKB	Swedish Nuclear Waste Management Company
SNF	Spent nuclear fuel (also “used nuclear fuel”)
SoH	State of health
SSM	Swedish Radiation Safety Authority
TID	Tamper-indicating device
UMS	Unattended monitoring system
VA	Vulnerability assessment (or analysis)

1. INTRODUCTION

The disposal of spent nuclear fuel in geological repositories presents an entirely new challenge for international nuclear safeguards. Conventional safeguards approaches for other stages of the nuclear fuel cycle rely on nuclear material accountancy (NMA) supplemented by containment and surveillance (C/S); however, this conventional approach cannot be strictly applied to the disposal process.

Unlike conventional safeguards approaches that reverify NMA if supplementary C/S measures fail, reverifying NMA of spent fuel that has been permanently encapsulated in disposal canisters is not realistic, and in fact 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, International Atomic Energy Agency (IAEA) policy requires that after a disposal canister has been permanently closed, dual C/S measures be applied to maintain CoK on the disposal canister and its contents, and that CoK continue to be maintained during the transport of the disposal canisters to the geological repository [1]. The transportation link, such as from an encapsulation plant to the repository, represents one of the more challenging stages of the disposal process for maintaining CoK on the encapsulated fuel assemblies, which will rely on C/S measures to a degree unprecedented in other stages of the nuclear fuel cycle [2, 3].

Once a geological repository's operations have begun, the encapsulation and disposal of spent fuel will be performed as a continuous, industrial scale series of processes [3]. 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 [1] and could include one or more sealing systems for disposal canisters or transportation casks, plus complementary surveillance or monitoring, such as video cameras or radiation monitors (which will not be discussed in detail in this report). 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. Seals on transport casks almost certainly will need to be both applied and removed by an operator as recommended by the Application of Safeguards to Geological Repositories (ASTOR).

Current designs for spent fuel transportation casks cannot ensure a cask's integrity during shipment, nor is there any verifiable means of maintaining CoK on the contents of transportation casks—that is, spent fuel destined for encapsulation plants or repositories—without employing additional C/S measures during shipment. By designing spent fuel transportation casks with seals integrated into their design, CoK may be more efficiently and effectively maintained. An integrated cask seal would reveal tampering of a cask (beyond removing a bolted lid, for example, such as cutting through the unsealed end of a cask), and thereby rigorously maintain CoK on a cask's contents during shipment. Furthermore, an integrated cask seal may allow operators to maintain sealing operations, which would reduce inspectorate burden.

Drawing in part on the results from a previous study [4], this paper examines design criteria for integrating tamper-indicating seals into the design of spent fuel transportation casks. A crucial requirement for a built-in tamper-indicating seal would be that it can ensure that no part of a transportation cask has been accessed or otherwise compromised. Ideally, this seal would be engaged immediately upon closing a cask, record and transmit state of health (SoH), record a timestamp of closure, and when opened, provide unique and verifiable identification, possibly transmitting location information. Data transmission would be authenticated and potentially encrypted. If designed to be installed and removed by a State operator, the seal could also include remote transmission of the seal's integrity upon application and before removal.

2. SWEDEN'S FINAL DISPOSAL SYSTEM – TRANSPORTATION AND FINAL DISPOSAL (BASE CASE)

In Sweden, the Swedish Nuclear Fuel and Waste Management Company (SKB) is responsible for developing the disposal concept and ultimately spent nuclear fuel (SNF) disposal. Owned by Swedish nuclear power plant (NPP) companies, it uses the KBS-3 design for final disposal (Finland also uses this design). Sweden will dispose of SNF from three reactor sites: Oskarshamn, Forsmark, and Ringhals. Sweden decided to locate the final disposal repository, SFK, at Forsmark, thus necessitating transportation between the NPPs, the encapsulation plant, and the repository. SNF is transported from the NPPs to interim storage at Clab in Oskarshamn, encapsulated at Clink (also in Oskarshamn), then transported using the specially designed ship M/S Sigrid to the geological repository SFK in Forsmark. See Figure 1 for the flow of materials.

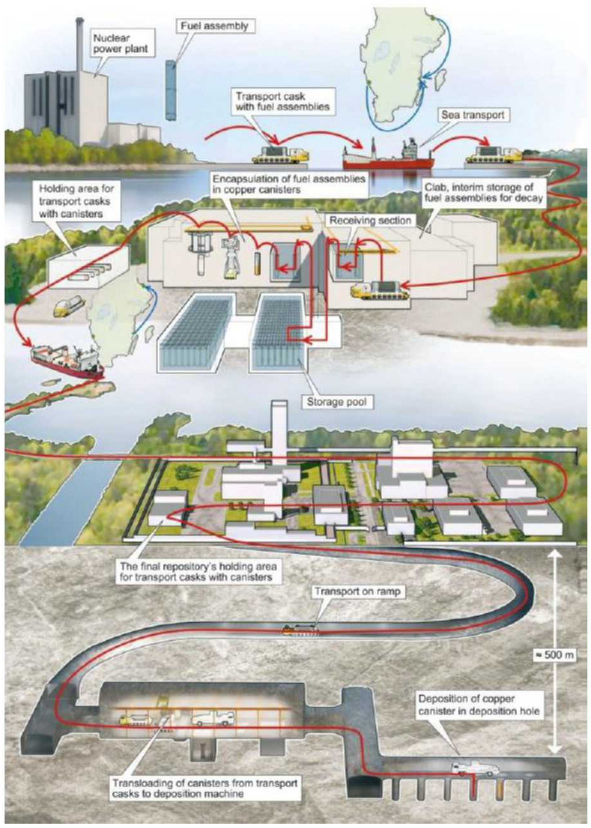

Figure 1: Sweden's disposal process. Image taken from [5].

After approximately five years of cooling in pools at NPPs, SNF is transferred from NPPs to Clab, where they are stored until ready for disposal. Note that the transportation casks used to transfer SNF from the NPPs to Clab may be current transportation cask designs because the SNF is not yet encapsulated and will undergo final NMA in the handling pool at Clab. SNF is stored in underground pools built in rock caverns that are approximately 30 meters below ground. The fuel is cooled in the pools for approximately 30 to 40 years before being encapsulated for permanent disposal. The encapsulation plant Clink will be an aboveground extension to Clab. When deemed ready for disposal, spent fuel assemblies (SFAs) are moved from Clab storage pools to the handling pool where final safeguards accountancy is conducted.

The SFAs are moved to the handling cell (hot cell), dried, then emplaced in disposal canisters using robotics and remote operations. At this point, SFAs cannot be reverified and thus the C/S measures must be robust, as shown in Figure 2 [6].

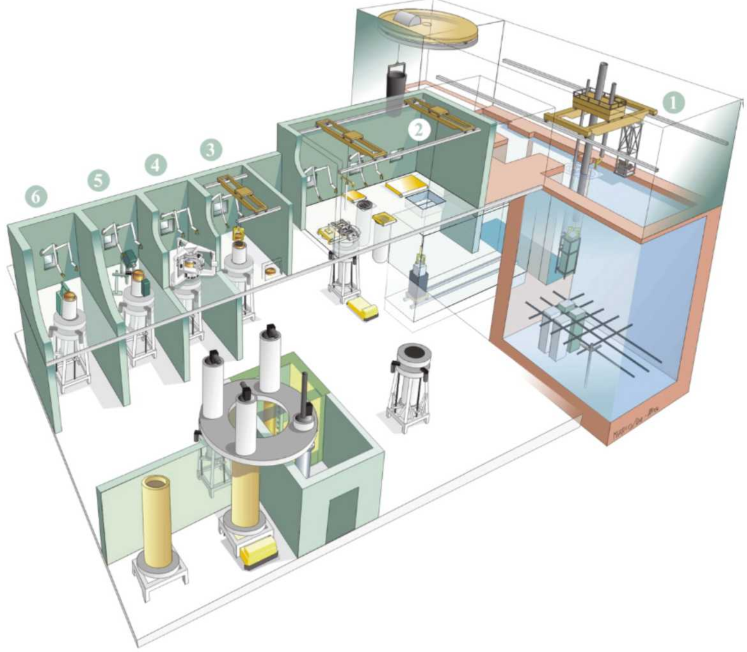

Figure 2: (1) Handling Pool, (2) Handling Cell, (3) Inerting, (4) Welding, (5) Non-destructive testing, (6) Machining [7]

During most years, Sweden expects that the encapsulation plant will produce 150 disposal canisters annually. During operation, it is expected to load one disposal canister each working day, corresponding to material flow of 12 boiling water reactor (BWR) or 4 pressurized water reactor (PWR) assemblies per day. Once assemblies are encapsulated into the disposal canister, they are moved to the canister handling machine and loaded into transportation casks (the payload for disposal canisters filled with SFAs instead of individual SFAs has not yet been designed). Maintaining CoK on each cask and its contents is crucial from this point until the canister is removed from its transportation cask at the SFK repository. Tags/seals must be applied to the cask or engaged at this point to ensure verification of the cask’s integrity. If deemed difficult-to-access, dual C/S would be required and may include video surveillance or radiation monitoring. Because one cask is loaded per day, there may be an increased inspection burden if an IAEA or European Atomic Energy Community (Euratom) inspector must be present. Operator-applied seals under surveillance may be necessary at this location. After sealing and applying a unique identifier (which may be integrated), transportation casks are moved to a buffer storage area at the nearby terminal building, which can hold up to 12 casks. Loaded casks are stored temporarily in the terminal building while awaiting transfer via the dedicated spent fuel cargo ship M/S Sigrid on the Baltic Sea from Clink in Oskarshamn to the SFK repository in Forsmark. Following receipt at the SFK repository, transportation casks will be placed in temporary buffer storage on the surface. Seals and tags may be verified in the buffer storage at the terminal building at the repository. If CoK has failed, the transportation cask can be set aside until a decision is made about go/no-go.

When a disposal canister is scheduled for emplacement underground, the corresponding transportation cask is transported from the terminal building to the repository's ramp entrance. Seals may be removed here, or possibly not until the casks reach the underground receiving gallery. If seals are removed at the ramp, the transportation casks would also be opened, the canisters removed, and then the canisters moved down the ramp. This approach has the benefit that the canisters outside the transportation cask would be better detected using radiation monitors. If the seals are not removed aboveground, the transportation casks would move down the main ramp to the underground receiving gallery, where the seal would be removed under surveillance, the transportation cask opened, and the disposal canister removed.

3. TRANSPORTATION CASKS

This section reviews both generic and specific transportation cask designs. Note that the current cask designs are for SFA payloads and have not yet been designed for a disposal canister payload. The design criteria and analysis below assumes that new cask designs would be similar to current SFA casks.

3.1. Generic Cask Designs

Type B casks are used for SNF and range in size and in what types of spent fuel can be inserted within the cask [8]. Casks can be licensed for storage, transportation, or both. The focus here is on casks that are licensed for transportation or for both storage and transportation. Cask design is determined by the characteristics of the spent fuel within the cask (which will differ for disposal canisters). Factors that characterize spent fuel include physical design/dimensions, initial enrichment, burnup, and cooling period [9].

Generally, a transport cask contains the following components: integral internal basket for SFAs, neutron shielding, inner steel shell, outer steel shell, gamma shielding, an impact limiter, and a closure lid [10]. Figure 3 shows a cask's general components.

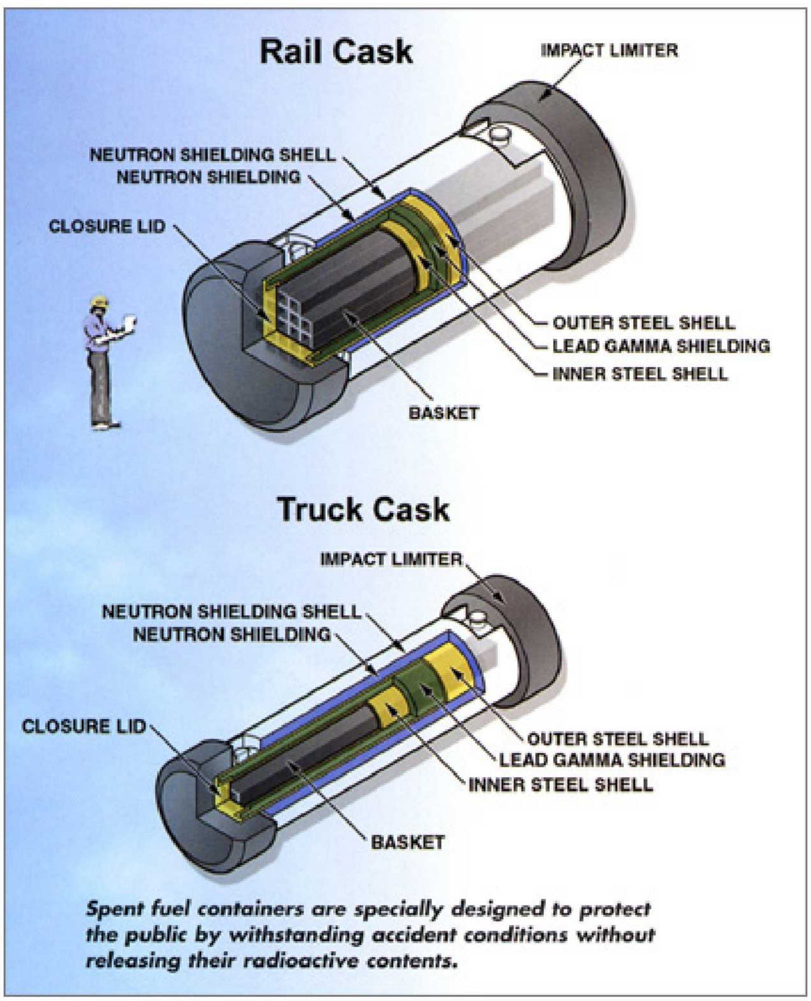

Figure 3: Generic diagram of casks [11].

Each country in which a cask is licensed may have monitoring requirements for casks, including temperature, over pressure (of inter-lid-space or inter-seal-space), leak testing, dose rate, surface contamination (i.e., after fuel loading in the pool), gas sampling, and visual inspection. Again, these requirements may differ for casks containing disposal canisters.

3.2. Detailed Cask Designs

This section provides detailed cask designs where information is available. From the research, it appears that many cask companies no longer design and fabricate casks, and companies are now defunct or have consolidated with other companies. This makes it difficult to track the origin and current manufacturer of many of the casks described.

3.2.1. AREVA Transnucleaire/Orano TN

Orano TN (formerly Areva TN before January 2018) [12] is a major global manufacturer of casks for transportation and storage and has locations in France, the U.S., and Japan. It has a fleet of about 40 casks that are licensed for transportation [13]. These generally fall under the TN family of casks, or the NUHOMS family.

As shown in Figure 4 and Figure 5, there are many versions of the TN cask, each holding a different number and type of fuel. The TN24 is a newer version of this cask series (licensed for both storage and transportation), and there are 20 different models of the TN24 depending on the fuel type [14]. The concept for the design is main gamma shielding provided by a forged steel body, neutron shielding via a layer of boronated resin enclosed between the forged steel and the external shell, longitudinal heat conductors made of copper or aluminum plates that carry the heat of fuel assemblies from the forged steel body to the external shell through the resin, and an inner basket for the spent fuel assemblies. This basket is made of boronated aluminum and/or stainless steel and guarantees the sub-criticality of its contents.

THE TN®24 CASK FAMILY

Model	Number of Fuel Assemblies	Max Burn up MWd/tU	Cooling Time (years)	Max Enr. (%)
TN®24 D	28 PWR	36 000	8	3.4
TN®24 DH	28 PWR	55 000	7	4.1
TN®24 XL	24 PWR	40 000	8	3.4
TN®24 XLH	24 PWR	55 000	7	4.3
TN®24 SH	37 PWR	55 000	5	4.25
TN®24 G	37 PWR	42 000	10	3.81
TN®24 (F1)	37 BWR	40 000	4	3.2
TN®24 (F1)	52 BWR	40 000	4	3.2
TN®24 E	21 PWR	65 000	5	4.65
TN®32	32 PWR	45 000	7	4.05
TN®40	40 PWR	45 000	10	3.85
TN®24 P	24 PWR	33 000	5	3.5
TN®52 L	52 BWR	55 000	min. 2.5	4.95
TN®24 SWR	61 BWR	70 000	min. 5.5	5.0
TN®68	68 BWR	60 000	7	4.7
TN®97 L	97 BWR	35 000	10	4.0
TN®24 BH	69 BWR	50 000	6	5.0
TK®69	69 BWR	40 000	10	3.2
TK®26	26 PWR	47 000	15	4.3
TN®24 ER	32 BWR (th)	13 700	40	5.2

Figure 4: The TN24 cask family [14].

Figure 5: TN cask family [14].

New casks include the TNG3S (short), TNG3L (long), and the TN17 Max. These are all high-performance casks that can transport SNF with short cooling time, high burn-up, and high initial enrichment [13].

Orano TN also offers the NUHOMS MP197HB transportation cask, a universal cask capable of transporting nine different types of spent fuel. It is used for offsite transportation of up to 61 or 69 intact or damaged BWR fuel assemblies, and 24, 32, or 37 PWR assemblies. The cask can handle a maximum of 32kW heat load. External fins are required for heat loads greater than 26kW. The cask has a stainless steel shell, gamma shielding of stainless steel and lead, neutron shielding of aluminum-encased resin, impact limiters of balsa and redwood encased in stainless steel shells, and carbon steel closure bolts [15]. Figure 6 shows the design of the Orano TN NUHMOS cask.

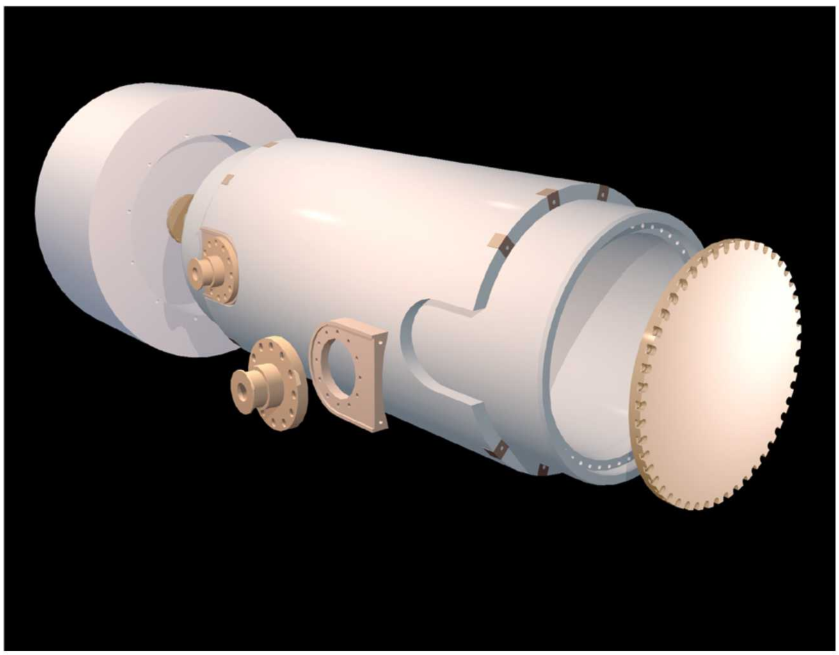

Figure 6: Orano TN NUHMOS cask [16].

3.2.2. British Nuclear Group

British Nuclear Group (BNG) was a major subsidiary of British Nuclear Fuels Limited (BNFL), owned by the Government of the United Kingdom. In the mid-2000s, BNFL restructured and sold the companies comprising BNG. BNFL ceased operations in May 2009.

Since 2005, the NTL-11 cask [17] has been considered the workhorse of BNFL's European spent fuel commercial transport.

Figure 7 shows the design of the NTL-11 cask. A lead liner provides gamma shielding, and the shock absorbers are steel-encased balsa. Orifice plugs are identified below:

- A = vent orifice in lid
- B = drain orifice
- D = ullage orifice

- E, F = two lid seal interspace test points
- G, H = water connections to bagging ring to prevent contamination in reactor ponds

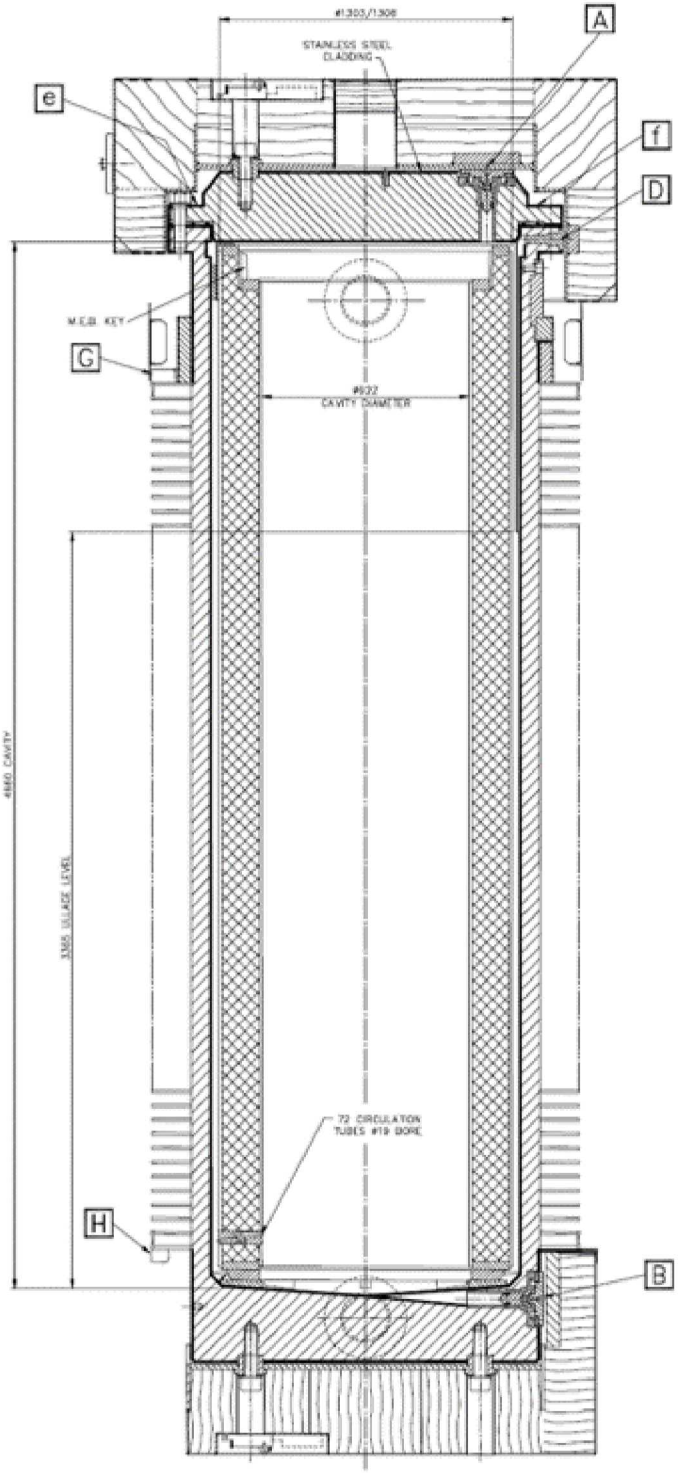

Figure 7: NTL-11 cask design [17].

3.2.3. Nuclear Assurances Corporation International [18]

Nuclear Assurances Corporation (NAC) International offers the NAC-LWT (1 PWR or 2 BWR) and NLI-1/2 (1 PWR or 2 BWR) and NLI-10/24 (10 PWR or 24 BWR). The NAC-LWT, shown in Figure 8, is the workhorse for U.S. commercial SNF transportation casks.

Figure 8: NAC-LWT cask [19].

3.2.4. Holtec International [20]

U.S.-based Holtec International manufactures the HI-STAR 100, a high-capacity multi-purpose canister that can store or transport SNF. It is made up of three shells: an innermost shell that acts as the containment boundary, a series of thick steel intermediate shells for gamma shielding, and an outer shell that houses neutron shielding material. Figure 9 shows the HI-STAR 100 canister. During transport, the HI-STAR 100 is fitted with AL-STAR Impact Limiters [20].

Figure 9: The HI-STAR 100 canister [20].

3.2.5. Gesellschaft für Nukleaire Services [21]

Gesellschaft für Nukleaire Services (GNS) is fully owned by the German utilities and is responsible for the management of Germany's SNF. GNS has designed and developed the CASTOR® series of casks for transportation and interim storage of SFAs. The casks all share the same general design, but vary in the type and number of SFAs contained, as shown in Figure 10. The general design comprises a monolithic cask body made of ductile cast iron with machined cooling fins for passive heat dissipation, deep drilled boreholes filled with polyethylene as a neutron moderator, a basket for SFAs, a bolted double lid system made of stainless steel with pressure monitoring of the interspace for leak tightness, and trunnions for handling and lifting.

- Geo – 37 PWR or 69 BWR
- V/19 – PWRs
- V/52 –BWRs
- 1000/19 – VVER 1000

Figure 10: CASTOR® series of casks. From left to right: geo, V/19, V/52, 1000/19 [21].

3.2.6. Mitsubishi Heavy Industries [22]

Japan's Mitsubishi Heavy Industries (MHI) MSF cask series features a boron-containing aluminum alloy basket made with powder metallurgy, a forged low alloy steel main body shell, a double lid closure system, epoxy resin neutron shielding material, and a high performance shock absorber. Figure 11 shows an overview of MHI's MSF cask. Specifically, the MSF-21P holds 21 PWR assemblies and the MSF-57B holds 57 BWR assemblies.

For these casks, a pressure monitoring port located on the side of the top flange allows continuous monitoring of pressure changes in the interspace between the primary and secondary lids. Details of the double lid design are shown in Figure 12.

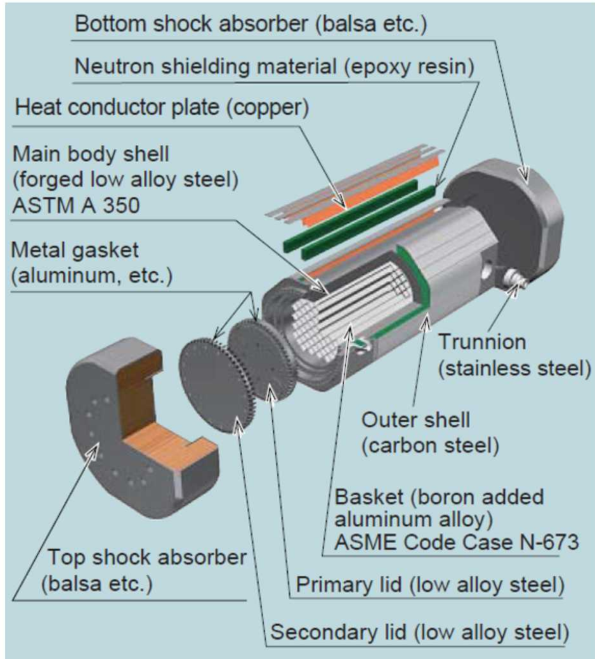

Figure 11: An overview of the MSF cask [23].

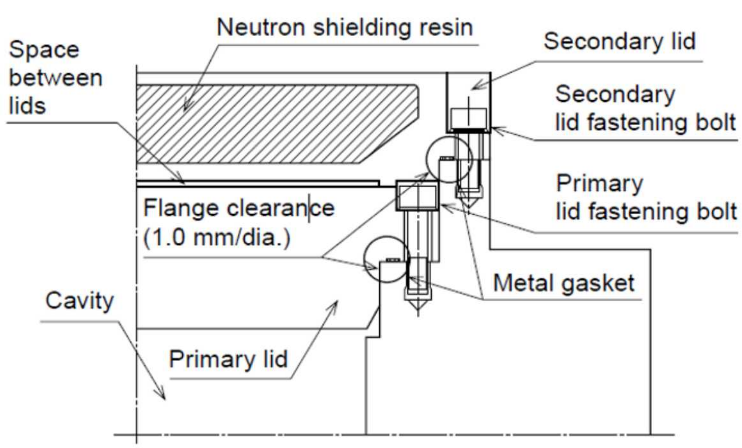

Figure 12: Details of the double lid closure system [24].

3.2.7. Nuclear Fuel Transport Co., Ltd. [25]

Japan's Nuclear Fuel Transport Co., Ltd (NFT) engineers and fabricates transportation packages. The casks currently listed on their website include the NFT-38B (holds 38 BWR SFAs) and the NFT-14P (holds 14 PWR SFAs). These casks are designed with current and future SFAs in mind and with increased SFA capacities. They are also designed for sending spent fuel from Japan to overseas reprocessing facilities.

3.2.8. Hitz or Hitachi-Zosen [26]

Hitz is a large Japanese company that designs and manufacturers casks for storage and transportation. They don't list specific models or designs of their casks on their website; however, the HZ-75T cask has been associated with Hitz. Hitz acquired all shares of the U.S.-based NAC International Inc. in 2013, and now includes NAC products in their product line.

4. DESIGN CRITERIA FOR SEALS[1]

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, fiber optic cable), and (3) the containment[2] enclosing nuclear material (NM), safeguards equipment, or other protected items [27]. All three components must be examined 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. Transportation casks require a sealing system, not just the seal itself. An integrated sealing system combines the seal, a way to apply the seal, and verification of the containment.

A seal is verified when it is inspected and either shows evidence of tampering or an absence of tampering.[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* [28] and CoK on the contents of the containment has been 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. However, re-verifying spent fuel inside a welded canister would delay its disposal. Before a suitable determination can be made, the canister must be cut open, an operation that needs to be performed at an appropriate facility (e.g., the encapsulation plant). This, in turn, requires additional transportation, which results in further delay. It also requires appropriate *additional* C/S measures be applied. Such a scenario should be avoided if at all possible.

As discussed in [29], an electronic seal is a *multiple use*, *multiple verification*, *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. This may be required as applied to transportation casks due to the daily operations of attaching and removing seals.

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[5].

---

[1] Information in this section draws substantially on the analysis in [30], p. 13-18.

[2] The IAEA defines containment as "structural features…used to establish the physical integrity of…items" and to maintain CoK on items [28], p. 66.

[3] This is known as an "attributes test" and results in a "yes" (no tampering) or a "no" (possible tampering) [28], p. 83.

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

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

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

In this analysis, the use case begins with *sealing transportation* casks that contain disposal canisters of spent fuel and *tampering* refers to any unauthorized opening of a transportation cask (whether at the separable parts of the cask or by penetrating the containment). 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). To meet these criteria and be accepted for use, such a sealing system must indicate tampering with a high degree of reliability and credibility.

By designing spent fuel transportation casks (in particular, future casks with disposal canister payloads) that have effective tamper-indicating features integrated into their design (essentially deploying a single integrated sealing system that includes containment verification), CoK can be more effectively maintained than by current ad hoc C/S measures. Ad hoc C/S measures may result in multiple components, each reporting their status separately to the IAEA, whereas an integrated seal may reduce burden by reporting status as a single component.

Another anticipated benefit of an integrated seal may be the ability of an operator to manage the seal. 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 [31]. 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, 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. Based on the assumption that an operator will be required to either apply, remove, or both apply AND remove, this analysis includes only systems that have the ability for remote data transmission. Data transmission implies that at least some of the sealing system will be active.

This section reviews the design criteria, including assurance features, remote verification, and data transmission and authentication, for an integrated transportation cask seal, and discusses the additional possibility of an operator-managed (integrated) seal.

4.1. Seal Integrity

For an inspectorate to have confidence in a 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 a sealed containment, a secure seal design generally includes tamper indication for the seal itself, as discussed in more detail in the next section.

4.1.1. *Tamper Indication*

The primary function for a sealing system is to provide tamper indication for the containment (note that most sealing systems tend to ignore the containment past the separable parts) 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. An example is 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. In the case of an integrated cask seal, tamper-indicating features will be required throughout the whole volume of the containment including any seal on the moveable parts (cask lid). The performance of tamper-indicating features on a seal is typically evaluated by an independent vulnerability assessment (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.

4.1.2. *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-resistant features can also be evaluated by an independent VA. Although potentially beneficial, a seal's tamper-resistant features are not as valuable as its *tamper-indicating* features, which are crucial to all seals. [6]

4.1.3. *Mitigation or Absence of Physical Vulnerabilities*

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 a 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 [30].

4.1.4. *Integrity of Seal Data*

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

[6] Also see footnote 18, p. 111, in [32] for one view about the degree to which seals can be considered effectively tamper-resistant.

functions must also be trusted during the several potential stages of data management. These stages 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., [33]. Some specific recommendations are presented below.

4.1.4.1. 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, changing a seal's status from "open" to "closed."

Both data authenticity and data integrity are commonly protected by *cryptographic authentication*, which uses 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 using an algorithm that verifies both the identity of the data-generating entity (the signatory) that signs the data (in this case, an electronic seal) and the authenticity of the original data. 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 not and must be kept secret. Only a valid signatory (a valid seal) can generate a valid digital signature [34]. A cryptographic authentication mechanism such as a DSA can be validated immediately upon retrieving data from a seal or it can be validated later 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, such as 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 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 seal 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 versus 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, including recent efforts to standardize the cryptography schemes [35].

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

4.1.4.2. 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 [33]. Details about sharing safeguards-relevant information from seals and among which parties will require careful consideration; however, an operator most urgently needs authorization from the inspectorate to remove or open a seal 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) [36]. 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 [37], 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).

Surveillance data may contain sensitive or proprietary information that an operator will require be encrypted 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. IAEA Member State requirements for data confidentiality are addressed in the Model Additional Protocol [38] and by IAEA's Policy Paper on Remote Monitoring [33].

4.1.4.3. 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.

4.1.4.4. 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 seals if current conventional methodologies are used in their design.[7]

4.2. Reliability

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. 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., on a truck or ship in route to a repository). 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.

4.3. Usability

Usability refers to the degree to which users (inspectors or operators) can readily perform necessary sealing functions, including initializing, attaching (or engaging), verifying, and detaching (or unengaging) 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 also includes a verification (or reader) system if that system is separate from the seal.

4.4. Joint Use Capability

Both the IAEA and Euratom perform safeguards functions for Sweden. Both inspectorates commonly use the same sealing systems for similar items under containment and should, therefore, approve any 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

---

[7] See, for example, NIST, "Post-Quantum Cryptography," Last modified January 3, 2017, Accessed on June 25 2018, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

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 in Section 4.1.4.1. 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, 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 versus inspectorates) and those requirements will need to be developed.

4.5. 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 it needs 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 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 it is 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.[8] A battery could be replaced in the field by using an on-site (or on-transport) backup battery to maintain power to an electronic seal during transfer of the primary battery. Energy harvesting may be another approach that can extend the life of batteries or enable continuous operation with batteries only as backups.

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 the decades-long periods expected for repository operations [31]. 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 [39].

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 the 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

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

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 4.6 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. 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.

4.6. 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 transportation cask and its 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. 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 up to four weeks [40], 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 [41]. The Swedish cask design will be designed to fulfil criteria for a Type B cask in accordance with IAEA requirements [42].

Transportation casks will experience heat generated internally by spent fuel decay heat. The Swedish design requires that the temperature on the surface of the disposal canister (inside the transportation cask) not exceed 100°C. 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.

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; 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 [40], which are based on decay heat criteria (designed to maintain canister temperature below 100°C, as noted above).

The 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. 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 4.5 above). The inspectorate will also levy requirements for environmental testing to be performed on a sealing system before it is put into use.

4.7. Unattended and Remote Monitoring Capability

Unattended monitoring systems (UMSs) are defined as "a special mode of application of non-destructive assay or C/S measures or a combination of these that operates for extended periods without inspector intervention." [28]. These systems must be reliable, i.e. operate without loss of safeguards relevant data over extended periods and at times when facility power is interrupted. They are comprised of a tamper-indicating cabinet with a computer, data acquisition module, and an uninterruptable power supply to cover short-term power outages. Data may come from a variety of types of detectors and sensors, and are forwarded by the data acquisition module to the computer for secure storage. For unattended monitoring, data authentication is required [27].

Remote monitoring is defined as:

> [A] technique whereby safeguards data collected by unattended C/S, monitoring and measurement systems are transmitted off-site via communication networks for review and evaluation. The system's internal recording capability is used for backup purposes. Remote monitoring may provide better utilization of equipment, better planning of inspections and a reduction in the inspection effort needed to meet verification requirements. These systems transmit data ranging from equipment state of health data to verification data. The use of redundancy is particularly applicable for unattended C/S and monitoring devices. For data sent over unsecured transmission lines, authentication and encrypted are required [28].

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 [43]. 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.

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 to unacceptable radiation levels. Such concerns can be mitigated through use of UMS and remote monitoring.

4.8. Operator Needs

As mentioned earlier in this section, it will be almost certain that operators will manage seals on transportation casks.

The ability and willingness of an operator to routinely manage 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 partial defect verification to emplacement [40].

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. The latter allows continued access to inspectors for possible reverification of materials in storage, whereas disposal does not.

The authors interviewed staff from Swedish Radiation Safety Authority (SSM) in Sweden to glean their input about operator needs relevant to the disposal process [40]. Several operator criteria have been identified, as well as suggestions for streamlining the process of operator-managed safeguards seals for spent fuel transportation casks. Note that some of these criteria are the same for the operator as the inspectorate.

Sealing System – operation: An operator-managed sealing system must be applied in a fool-proof manner, either automatically applied upon cask closure or according to agreed-upon procedure with possible special equipment. Such a sealing system benefits both operator and inspectorate if designed to be user friendly [30]. 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. 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 since the application, verification and removal of seals will occur regularly. 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 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.

Location – Verification & Removal: These operations occur at the receiving end of a shipment. The Swedish operator expressed a strong preference for a seal that 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 [40]. There would 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.[9]

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.

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 [40].

Remote Monitoring: Successfully implementing operator-managed seals—both their application and removal— will require successfully implementing UMS with remote monitoring, complemented by random interim inspections [44]. Systems operating in unattended mode, with remote monitoring, must meet certain operator criteria, including security concerns.

4.9. Procedural Implementation for Operator-Managed Seals

In the absence of an inspector, an operator who 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

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

well as sufficient training of operators on properly executing those procedures and on the use of any special equipment.

5. CANDIDATE CONTAINMENT AND SURVEILLANCE APPROACHES

5.1. Integrated Seal Approach

An integrated sealing system will combine the seal, a way to apply the seal, and verification of the containment as a single component. No such sealing system currently exists for transportation casks. The critical concern is ensuring that the encapsulated SFAs within the cask have not been accessed without detection. To determine if a monitored item has been accessed, a classic approach is to seal the moveable parts (such as the lid), and separately ensure the container has not been opened in locations other than the moveable parts (often through a visual inspection). If material is extracted, inspectors will either detect the material directly, perhaps through radiation emitted from the SFAs through the disposal canister, or they will know the container has been opened by some other mechanism. It may be difficult to rely only on radiation detection as an adversary could shield a detector during material extraction. However, can we develop a solution that relies completely on determining if a container has been opened, no matter from where this occurs?

While many designs may be possible, we considered the following ideas: (1) fiber optics embedded in a cask layer with electronics to control the light pulses that travel through the fiber, store messages, perform cryptographic functions, and communicate from the sealing system to a data acquisition system or reader, (2) Smart bolts that incorporate sensors that indicate a change in the internal environment of the cask. These sensors could detect changes in pressure, gas, or light. An issue with the first approach, embedded fiber optics, is that transportation casks are certified for safety, and integrating anything into the cask walls may not be acceptable. It may be possible, however, to replace one of the bolts of the cask with a special smart bolt. This bolt can be designed according to the requirements from Section 4. Tamper is detected by a change in environment, indicating breach. The tamper must be recorded and be irreversible. Note that no such bolt currently exists and would require design and development.

The smart bolt (Figure 13) would have the following components:

- Verification that the bolt is completely screwed in (properly installed, i.e., lid is attached to base) and provide indication if bolt is removed.
- Electronics in bolt that provide state-of-health of bolt, detect environmental sensor conditions, provide a unique ID for bolt, storage of events in internal non-volatile memory, transmission of state-of-health, and events to a nearby reader.
- Cryptographic algorithms in electronics to ensure data integrity, data authentication and confidentiality (if required).
- Tamper indication of bolt.
- Tamper indication of containment (via change in internal environment).

In the following table, we take some of the criteria from Section 4 and comment on how these approaches may satisfy or relate to the criteria.

Table 1: Comparing design criteria between integrated fiber optics and smart bolt.

Criteria/ Possible approaches	Integrate fiber optic cables into cask body with electronic seal	Smart bolt with environmental sensor (light, pressure, gas) integrated into a bolt
Correct seal application and operation	Design would need to ensure that fiber continuity is achieved when lid is attached (aligning ends of fiber between lid and bottom of cask).	Seal should indicate that it is attached properly (and that lid is correctly attached and aligned with bottom of cask). Torque or tension indicator possible.
Seal integrity • tamper indication • tamper resistance • mitigation of physical vulnerabilities	All seals should be designed to mitigate vulnerabilities of any kind and undergo an assessment prior to deployment; tamper indication is via disruption of the light pulses through the fiber; electronic components must also have tamper indication.	Tamper indication is via change in internal environment of cask (i.e., pressure, gas, light) if cask is breached, or recording when bolt is disengaged or loosened; must protect internal sensors, bolt, and bolt electronics from tamper.
Seal data integrity • data authenticity and integrity • confidentiality • potential vulnerabilities in cryptographic firmware or software • potential obsolescence of cryptographic firmware or software	Implement cryptographic algorithms (for data authenticity, integrity, confidentiality) for SoH and event messages. Mitigate potential vulnerabilities and/or perform an analysis and accept risks.	Implement cryptographic algorithms for SoH and event messages. Mitigate potential vulnerabilities and/or perform an analysis and accept risks.
Reliability	Consider degradation of fiber within casks – not possible to replace once embedded. What effects will radiation have on fiber or associated seal electronics? Where will electronics package be located and will transportation cause issues with reliability?	Sensors within bolt may be somewhat protected from the environment. Bolt seal will require long mean-time-between-failure and reliable components. Bolt can be replaced if it fails over time. Will radiation affect electronic components?
Usability	Need to line up ends of fiber from the bottom and top of casks (to provide continuous path).	Smart bolt would replace standard lid bolt – need an indicator that bolt is inserted and engaged correctly (tension or torque).
Joint use capability	Consider public key cryptography so that each entity has own key set.	Consider public key cryptography so that each entity has own key set.
Maintainability	Very difficult for embedded fiber. Electronics may require changing batteries – consider photovoltaic energy harvesting with backup battery.	Can replace or repair smart bolt if needed. Electronics may require changing batteries – consider photovoltaic energy harvesting with backup battery.

Criteria/ Possible approaches	**Integrate fiber optic cables into cask body with electronic seal**	**Smart bolt with environmental sensor (light, pressure, gas) integrated into a bolt**
Operation in expected environments	Embedded fiber may be well protected, but uncertain where to locate electronics. Electronics will need to survive extreme temperatures, humidity, saltwater and vibration.	Better shielding from environmental conditions due to bolt form. Electronics will need to survive extreme temperatures, humidity, saltwater and vibration.
Unattended monitoring	Likely need wireless communication (secured) to a data acquisition system nearby. Send SoH on set intervals, and send event messages immediately. During transport, store messages on seal until data acquisition system is available. Data also stored on seal.	Likely need wireless communication (secured) to a data acquisition system nearby; smaller electronics needed. Send SoH on set intervals, and send event messages immediately. During transport, store messages on seal until data acquisition system is available. Data also stored on seal.
Remote monitoring	Send SoH and event messages from unattended monitoring system to IAEA Headquarters or regional offices.	Send SoH and event messages from unattended monitoring system to IAEA Headquarters or regional offices.
Operator needs	Seal should not interfere with operations. Seal should indicate proper attachment. Seal installation, deployment, maintenance, verification, should minimize radiation doses to operators.	Seal should not interfere with operations. Seal should indicate proper attachment. Seal installation, deployment, maintenance, verification, should minimize radiation doses to operators.

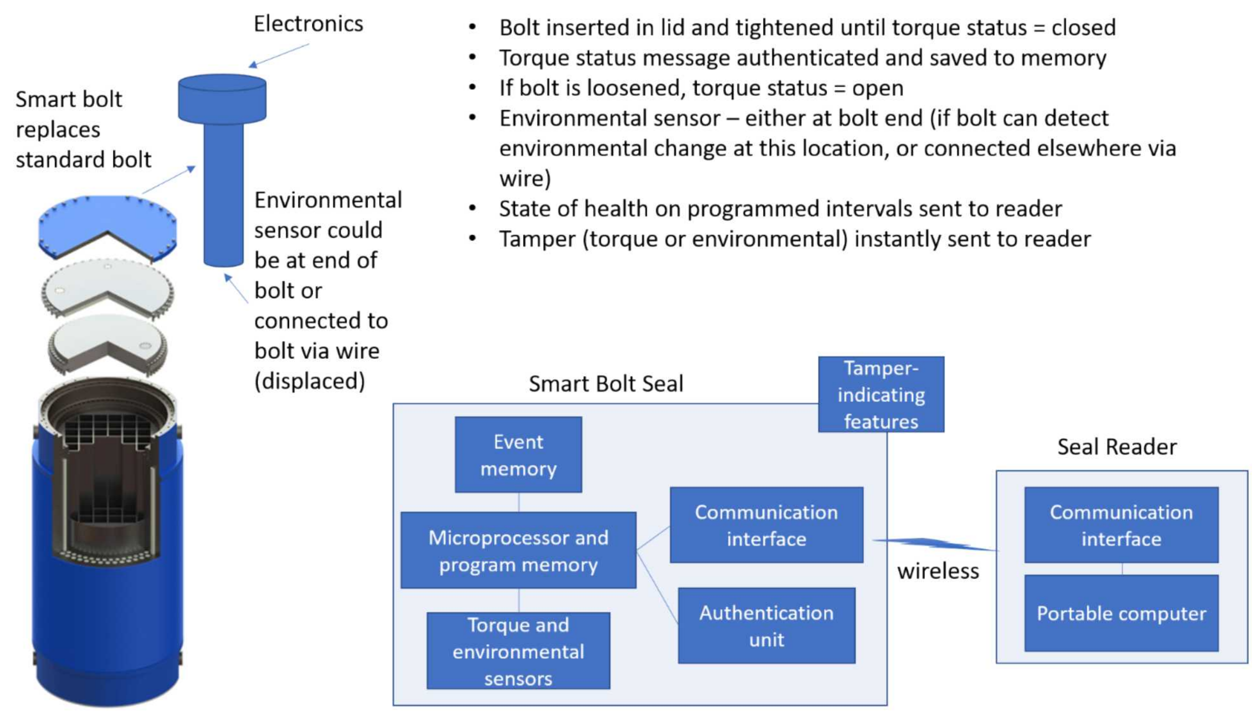

Figure 13: Smart bolt conceptual diagram.

5.2. Ad Hoc Seal Approach

If an integrated seal approach is not feasible for application to a transportation cask, a combination of seals, detectors, and/or a technology that can verify cask integrity might provide assurance that the cask has remained closed and CoK has been maintained. The seal (for the moveable parts of the cask) and the tamper-indicating enclosure approach for the cask volume, combined, should meet the criteria outlined in Section 4. Based on these criteria, seals will need to have electronics to fulfill functions such as unattended and remote monitoring. Some contenders include the Electronic Optical Sealing System (EOSS) [45], though this seal is slowly being phased out; the Remotely Monitored Sealing Array (RMSA) [45]; other active fiber loop seals under development; and a prototype from the Joint Research Centre (JRC) that uses small pairs of tags to ensure the lid is closed.

To ensure that the cask has not been opened at locations other than the lid, a secondary method/technology is needed. Options include a pressure, gas, or light monitor that ensures the cask has not been opened; fiber optics embedded within the cask; and the mobile unattended neutron detector (commonly referred to as MUND). Other seals and tamper-indicating enclosures may be used as well.

5.2.1. Seals

5.2.1.1. EOSS

The EOSS seal is a reusable fiber optic seal approved by the IAEA for routine use in 2005. It registers sealing wire events, case events, and state-of-health in non-volatile memory. It uses secret key cryptography to authenticate and encrypt messages. The seal case includes tamper-indicating features—

the inner part contains all security sensitive components, and the outer part houses the batteries, as well as electrical and fiber optic connectors to facilitate repair. The EOSS is verified by physically connecting a reader which comprises a laptop running special software, as shown in Figure 14.

Figure 14: EOSS seal (bottom yellow item) with reader (laptop). (Courtesy Canberra, www.canberra.com)

5.2.1.2. RMSA

The reusable RMSA actively monitors a fiber optic loop to determine if the seal wire is open or closed and is able to send this status, as well as device health information, to a local data consolidator (called a translator) via secure RF communication. The RMSA uses secret key cryptography and is embodied in a tamper-indicating enclosure. RMSA is based on the Sandia National Laboratories-developed Secure Sensor Platform (SSP), a technology structure providing common security, communication, cryptography, and power capabilities for sensors. The main components of an RMSA system are the seal, translator, and a review station.

Figure 15: RMSA seal. Picture courtesy SNL.

Figure 16: RMSA translator.

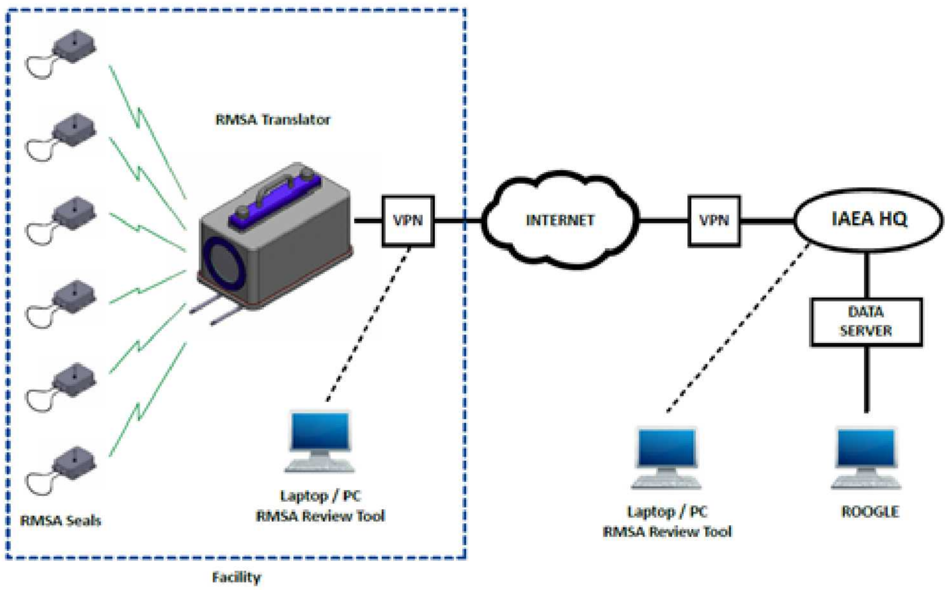

Figure 17: RMSA system topology.

5.2.1.3. Joint Research Centre prototype

The European Union's 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 [46]. The system consists of three anchors fixed to the cask body, three tags fixed to the cask lid, and a master unit fixed to the cask body, as shown in Figure 18. Each tag and anchor has an ultra-wideband module that transmits and receives time-of-flight data. They also have a crypto module to store a private key and digitally sign data packages. The tags and anchors 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 unit 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 not need to perform any special operation to install or activate the system. The sealing system is patent pending in the European Union, although 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. We will not compare this system to the design requirements since the prototype features are not thoroughly known.

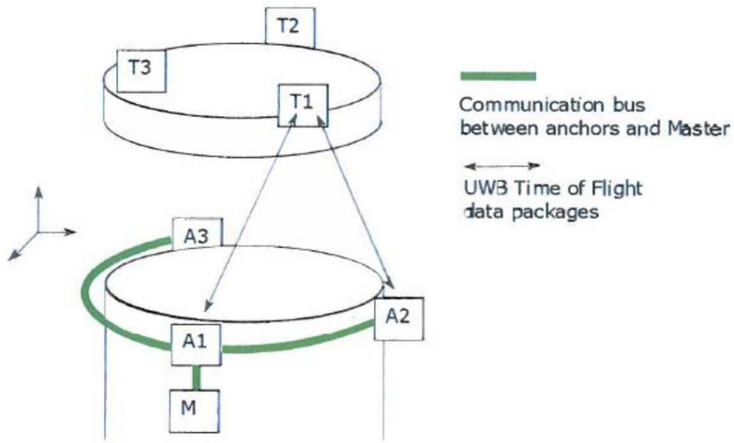

Figure 18: Proposed sealing system for sealing a container lid to a container body. The system comprises the anchors (A1, A2, A3) fixed to the cask body, three tags (T1, T2, T3) fixed to the cask lid, and a master unit (M) fixed to the cask body.

Table 2: Comparing design criteria between EOSS and RMSA fiber optic loop seals.

Criteria/ Possible approaches	EOSS	RMSA
Correct seal application and operation	Fiber optic loop needs to be properly threaded so that the lid is sealed to the cask bottom	Fiber optic loop needs to be properly threaded so that the lid is sealed to the cask bottom
Seal integrity • tamper indication • tamper resistance • mitigation of physical vulnerabilities	The EOSS seal has undergone a vulnerability assessment and is approved for use by the IAEA. Tamper indication of the seal is via conductive foils surrounding security-sensitive components, as well as case switches. Tamper indication of the monitored item is via recording the opening/closing of the fiber optic loop.	The RMSA seal has undergone a vulnerability assessment and is approved for use by the IAEA. Tamper indication is via a case switch, as well as optional tempered glass within the case. Tamper indication of the monitored item is via recording the opening/closing of the fiber optic loop.

Criteria/ Possible approaches	**EOSS**	**RMSA**
Seal data integrity • data authenticity and integrity • confidentiality • potential vulnerabilities in cryptographic firmware or software • potential obsolescence of cryptographic firmware or software	Secret key cryptography is used for data authenticity, integrity, and confidentiality. The seal has undergone a VA but should occasionally be re-evaluated as new technological capabilities emerge.	Secret key cryptography is used for data authenticity, integrity, and confidentiality; public key cryptography is an option. The seal has undergone a VA but should occasionally be re-evaluated as new technological capabilities emerge.
Reliability	Potential issues with radiation fields	Battery issues have been reported, but are being addressed.
Usability	Easy to install seal. Easy to verify seal.	Easy to install seal. Easy to verify seal via review station.
Joint use capability	Only one authentication key is available, and is typically provided to the IAEA; hence, Euratom is unable to independently verify data integrity.	Public key cryptography is an option and would allow joint use capability.
Maintainability	Batteries can be changed via a separate compartment. Battery switch will be activated. Backup battery provided.	Batteries will need replaced periodically. Energy harvesting is a potential feature (on-going research and development).
Operation in expected environments	Not intended for harsh environments	Not intended for harsh environments, although some field trials in harsh conditions have been performed.
Unattended monitoring	Events (opening/closing of fiber, case tamper), and SoH are stored on the seal and are later retrieved using a physically connected reader.	Events (opening/closing of fiber, case tamper), and SoH are stored on the seal, as well as transmitted on-site to the translator.
Remote monitoring	Some use cases have the EOSS seal physically attached to the Next Generation Surveillance System (NGSS), which allows remote monitoring. Without the NGSS, remote monitoring is not possible for the EOSS seal.	As events and SoH are securely transmitted to the translator, remote monitoring is possible. A computer with Internet attached to the translator can send data to inspectorates. For transport cases, the seal could be read by translators on both ends (before shipment and after arrival), or a translator and computer could accompany the transport for continuous monitoring capability.

Criteria/ Possible approaches	EOSS	RMSA
Operator needs	Seal should not interfere with operations. The EOSS is relatively small but operators may need to take care to protect the seal from incidental rough handling during transport. Seal should indicate proper attachment. EOSS has an LED that flashes briefly when the fiber optic cable is properly closed, but there is no mechanism to ensure the fiber is threaded correctly. Seal installation, deployment, maintenance, verification, should minimize radiation doses to operators. Once installed, the seal will need to be verified by physically connecting the reader, unless is it permanently attached to the NGSS.	Seal should not interfere with operations. Operators may need to take care to protect seal from incidental rough handling during transport. Seal should indicate proper attachment – fiber optic closure can be verified using review software. There is no mechanism to ensure the fiber is threaded correctly. Seal installation, deployment, maintenance, verification, should minimize radiation doses to operators. Once the RMSA is installed, verification can be performed remotely. Battery maintenance will periodically be required unless energy harvesting is implemented.

5.2.2. Containment integrity

5.2.2.1. Environmental sensors

An environmental sensor could be used to monitor pressure, gas, or light in the cask interior. Unlike in the integrated seal approach, this sensor would be separate from a seal that ensures the lid is not removed without knowledge. The environmental sensor would need to address design criteria separate from the seal, potentially adding complexity and additional burden to inspectorates for verification and maintenance.

5.2.2.2. Fiber optics within cask

Fiber optics could be embedded in the cask to determine if unauthorized entry was attempted. However, this approach suffers from the same issues as in the integrated seal section in terms of cask certification, and would require additional complexity and burden to inspectorates. We will not address this option in terms of design criteria.

5.2.2.3. MUND

The MUND[10] is a neutron detection system that runs on battery power. It comprises a ^{3}He detector inside a polyethylene moderator slab integrated with electronics, all within a single sealable enclosure [27]. It can collect data for more than eight weeks, after which the unit is replaced with a fully charged one. This

[10] Note that the IAEA spells the acronym MUND Mobile Unattended Neutron Detector, while others [47] refer to it as Mobile Unit for Neutron Detection.

device could be attached to the outer surface of the cask and collect data indicating if the cask had been opened. MUND can be used with a docking station and a virtual private network for data security. Additional details on MUND have not been found during an open literature search, and thus we will not compare MUND to the criteria. However, it should adhere to the requirements of Section 4.

6. CONCLUSIONS

Following final safeguards accountancy measurements on spent fuel assemblies, the shipment of verified assemblies will require unprecedented reliance on maintaining CoK on the fuel inside transportation casks. Such increased reliance is due to the lack of reverification of spent fuel following encapsulation into disposal canisters.

Transportation casks have not yet been designed for disposal canisters as a payload, but they likely will be similar to transportation casks for spent nuclear fuel assemblies. Integrating seals into the design of transportation casks could ensure the proper closure of the lid and the containment integrity, and possibly allow operators to manage seals. A promising approach is the design and development of a smart bolt that would replace one of the cask bolts on the lid. One data stream for inspectors would provide information regarding the integrity of the entire transportation cask.

If an integrated cask seal is not feasible due to time constraints in the design process or hesitation to modify casks due to safety concerns, ad hoc approaches could also be implemented. In an ad hoc approach, a seal such as the RMSA or EOSS would ensure cask lid closure, and a separate technology such as internal environmental sensors or the MUND would ensure volumetric cask integrity. This approach would result in two separate data streams, and may satisfy dual C/S requirements. Either the integrated or ad hoc approach will require adherence to a set of design criteria specific to international nuclear safeguards regimes. An approach should be determined in the near-term as geological repositories will begin operations in the next few years.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY. IAEA Department of Safeguards (SGCP-CCA), SG-PR-1305 (ver. 1, 18 October 2010).

[2] Baldwin, R., Haddal, R. & Finch, R. J. (2016). Containment and Surveillance as a Primary Approach for Safeguarding Geological Repositories, presented at Annual Meeting of the Institute for Nuclear Materials Management, Atlanta, 2016. Atlanta, Georgia: Institute of Nuclear Materials Management.

[3] Mongiello, R., Finch, R. J., & Baldwin, G. (2013). *Safeguards Approaches for Geological Repositories: Status and Gap Analysis* (SAND2013-5185P). Albuquerque, New Mexico: Sandia National Laboratories.

[4] Finch, R., Smartt, H. A., & Haddal, R. (2017). *Developing Reliable Safeguards Seals for Transportation Casks to be Applied, Verified, and Removed by State Operators*. (SAND2017-11187). Albuquerque, New Mexico: Sandia National Laboratories.

[5] Clementi, C., Littman, F., & Capineri, L. (2017). Ultrasonic identification & authentication of copper canisters. In *European Safeguards Research and Development Association (ESARDA) Joint Meeting on Geological Repositories*. Ispra, Italy: European Safeguards Research and Development Association.

[6] Finch, R., Baldwin, G., & Haddal, R. (2017). *A Safeguards Methodology for the Swedish System of Spent Fuel Disposal*. (Pending). Albuquerque, New Mexico: Sandia National Laboratories.

[7] Stål, J-O. (2015). Status of the Encapsulation Plant and the Geological Repository in Sweden. In *European Safeguards Research and Development Association (ESARDA) Joint Meeting on Geological Repositories*. Ispra, Italy: European Safeguards Research and Development Association.

[8] World Nuclear Association. (2017, July). Transport of Radioactive Materials. Retrieved from www.world-nuclear.org/information-library/nuclear-fuel-cycle/transport-of-nuclear-materials/transport-of-radioactive-materials.aspx

[9] Operation and Maintenance of Spent Fuel Storage and Transportation Casks/Containers. (2007). Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/te_1532_web.pdf

[10] Transport of Radioactive Materials - World Nuclear Association. (2007). Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/te_1532_web.pdf

[11] Transportation of Spent Fuel and Radioactive Materials. (2016). Retrieved from https://www.nrc.gov/docs/ML0504/ML050480314.pdf

[12] Nuclear Transport and Used Fuel Solutions. (n.d.). Retrieved from http://us.areva.com/EN/home-2271/areva-inc-transnuclear.html

[13] Valenzano, M. (2015). The Future of Used Fuel Transportation in the US. Institute for Nuclear Materials Management, presented at the 30th Spent Fuel Management Seminar, Arlington, Virginia, 2015.

[14] Metal Casks for Used Fuel Transport and Storage. (2013). Retrieved from http://us.areva.com/home/liblocal/docs/Catalog/AREVA-TN/AREVA_TN24_Metal%20Casks.pdf

[15] NUHOMS® MP197HB Transport Cask. (2014). Retrieved from http://us.areva.com/home/liblocal/docs/Catalog/AREVA-TN/ANP_U_354_V3_14_ENG_MP197HB_TC.pdf

[16] NUHOMS® MP197HB Universal Transport Cask. (2017). Retrieved from http://us.areva.com/home/liblocal/docs/Catalog/AREVA-TN/ANP_U_354_V5_17_ENG_NUHOMS_MP197HB_.pdf

[17] Cory, A. (2004). NTL 11 Spent Fuel Flask – Meeting the Challenge of Regulatory and Technological Change. Retrieved from http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/37/088/37088560.pdf

[18] Site and Transportation Services. (2015, August 25). Retrieved from http://www.nacintl.com/site

[19] Transport Services. (2014). Retrieved from http://www.nacintl.com/transport

[20] Dry Cask and Storage Transport. (2016). Retrieved from https://holtecinternational.com/productsandservices/wasteandfuelmanagement/dry-cask-and-storage-transport/

[21] GNS. (n.d.) Retrieved from http://www.gns.de/language=en/24394

[22] Mitsubishi Heavy Industries, Ltd. (n.d.). Mitsubishi Heavy Industries, Ltd. Global Website. Retrieved from https://www.mhi.com/

[23] Yamamoto, T., Hode, S., Kamiwaki, Y., Tamaki, H., Matsuoka, T., & Hojo, K. (2006). Developments in Spent Fuel Transport and Storage Casks. *Mitsubishi Heavy Industries, Ltd. Technical Review, 43*(4). Retrieved from https://www.mhi.co.jp/technology/review/pdf/e434/e434050.pdf

[24] Akamatsu, T., Matsuoka, T., Ohsono, K., & Hode, S. (2002). Sealing Technology for Transport and Storage Casks. *Mitsubishi Heavy Industries, Ltd., Technical Review 39*(1). Retrieved from https://www.mhi.co.jp/technology/review/pdf/e391/e391036.pdf

[25] NFT. (n.d.). Retrieved from http://www.nft.co.jp/english/business/packages.html

[26] Hitachi Zosen Corporation. (n.d.). http://www.hitachizosen.co.jp/english/

[27] SAFEGUARDS TECHNIQUES AND EQUIPMENT: 2011 EDITION. (2011). *International Nuclear Verification Series,* 1st ser., 69. (Rev2). Retrieved from https://www-pub.iaea.org/MTCD/Publications/PDF/nvs1_web.pdf

[28] IAEA SAFEGUARDS GLOSSARY 2001 Edition. (2002). *International Nuclear Verification Series No. 3*. Vienna: International Atomic Energy Agency. Accessed June 2018. https://www.iaea.org/sites/default/files/iaea_safeguards_glossary.pdf

[29] Tzolov, R., Goldfarb, M., & Penot, L. (2001). DEVELOPMENT AND EVALUATION OF NEW ELECTRONIC SEALS AT THE IAEA. Retrieved from http://www.iaea.org/inis/collection/NCLCollectionStore/_Public/33/006/33006947.pdf?r=1

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

[31] Hildingsson, L., & Andresson, C. (2014, October). Safeguards aspects regarding a geological repository in Sweden. In the *IAEA Symposium on International Safeguards: Linking Strategy, Implementation and People*. Vienna. Retrieved from https://www.iaea.org/safeguards/symposium/2014/home/eproceedings/sg2014-papers/000166.pdf

[32] Johnston, R. (2001). Tamper detection for safeguards and treaty monitoring: fantasies, realities, and potentials. *The Nonproliferation Review, 8* James Martin Center for Nonproliferation Studies. Retrieved from https://www.nonproliferation.org/wp-content/uploads/npr/81john.pdf

[33] Capel, T., Tolk, K., Liguori, C., & Button, T. (2004). A Systematic Approach to Data Security for Unattended and Remote Monitoring Systems. In the *Proceedings of the 45th Annual Meeting, Institute of Nuclear* Materials. Orlando, Florida: Institute of Nuclear Materials Management. Retrieved from https://www.inmm.org/INMM/media/Archives/Annual%20Meeting%20Proceedings/2004/0267.pdf

[34] NIST. (2013). *Digital Signature Standard (DSS).* Federal Information Processing Standard (FIPS) 186-4, Gaithersburg, Maryland: US Department of Commerce. Retrieved June 2018. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[35] Moody, D., Peralta, R., Perlner, R., Regenscheid, A., Roginsky, A., & Chen, L. (2015). Report on Pairing-based Cryptography. *Journal of Research of the National Institute of Standards and Technology, 120*, 11-27. doi:http://dx.doi.org/10.6028/jres.120.002

[36] NIST. (2001). *Announcing the Advanced Encryption Standard (AES).* Retrieved June 22, 2018, from https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

[37] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644-654. doi:10.1109/TIT.1976.1055638

[38] IAEA. (1998). INFCIRC/540*, Model Protocol Additional to the Agreement(s) Between State(s) and the International Atomic Energy Agency for the Application of Safeguards*. Retrieved June 22, 2018, from https://www.iaea.org/sites/default/files/infcirc540c.pdf

[39] IAEA. (2014, September). *Safeguards Implementation Practices Guide on Facilitating IAEA Verification Activities.* Retrieved June 22, 2018, from http://www-pub.iaea.org/MTCD/Publications/PDF/SVS-30_web.pdf.

[40] Hildingsson, L., & Andresson, C. (2017, January 12). Personal interview.

[41] SKB. (2010) *Design, production and initial state of the canister.* (SKB Technical Report No. TR-10-14). Stockholm: Svensk Kärnbränslehantering AB.

[42] IAEA. (2012). *Regulations for the Safe Transport of Radioactive Material.* Specific Safety Retrieved June 22, 2018 from http://www-pub.iaea.org/MTCD/publications/PDF/Pub1570_web.pdf

[43] Araujo, J., Charlier, C., Hatt, D., Lebrun, A., Muroya, N., Rance, P., Tsvetkov, I., Zarucki, R., & Zendel, M. (2010). Enhancing and Optimizing Safeguards Implementation by Remote Safeguards Inspections. In *International Safeguards Symposium: Preparing for Future Verification Challenges.* Vienna: Retrieved June 22, 2018 from https://www.iaea.org/safeguards/symposium/2010/Documents/PapersRepository/266.pdf

[44] IAEA. (2010). *Model Integrated Safeguards Approach for a Geological Repository.* SG-PR-1306, SGCP-CCA, Vienna.

[45] Electronic Optical Sealing System (EOSS). (2017). Retrieved from http://www.canberra.com/products/safeguards_surveillance_seals/seals.asp

[46] Electronic ranging seal for unattended sealing of spent fuel transport casks. (2016). Retrieved from https://ec.europa.eu/jrc/en/patent/2964-electronic-ranging-seal-unattended-sealing-spent-fuel-transport-casks-0

[47] MUND – Mobile Unit for Neutron Detection. (n.d.). Retrieved from https://www.quaestainstruments.com/mund-mobile-unit-for-neutron-detect

DISTRIBUTION

National Nuclear Security Administration

Attn:

1	Wayne Mei (Wayne.Mei@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)