DESIGN REQUIREMENTS OF SAFEGUARDS SEALING SYSTEM FOR REAL-TIME VERIFICATION

by

Jihyun AHN, Junsung PARK, Hayoung SIM, Geunyoeng AN, and Hee SEO*

Jeonbuk National University, Deokjin-gu, Jeonju-si, Jeollabuk-do, Republic of Korea

Technical paper
https://doi.org/10.2298/NTRP2104376A

To ensure the peaceful use of nuclear energy, nuclear safeguards are applied in member states of the International Atomic Energy Agency the Non-Proliferation Treaty. The two main goals of nuclear safeguards are effectiveness and efficiency. The International Atomic Energy Agency has a great interest in using a containment and surveillance technology to maintain continuity of knowledge. A representative means of a containment and surveillance technology is a sealing system to alert the user to tampering. The existing sealing systems used by the International Atomic Energy Agency are of limited utility for real-time verification purposes. To address this limitation, the present study analyzed the design requirements of a sealing system proposed by various institutions including the International Atomic Energy Agency, the U.S. Nuclear Regulatory Commission, a number of national laboratories, and companies. Then, we identified the appropriate design requirements of this system for real-time verification. The next step is to develop a real-time verification sealing system based on the design requirements identified and discussed herein. Such a system is expected to significantly enhance the efficiency of nuclear safeguards.

Key words: nuclear safeguard, sealing system, verification, real-time, design criteria

INTRODUCTION

For the peaceful use of nuclear energy, many countries have joined the treaty on the Non-Proliferation of Nuclear Weapons [1] and have signed a safeguards agreement with the International Atomic Energy Agency (IAEA). The technical objective of IAEA safeguards is *the timely detection of diversion of significant quantities of nuclear material from peaceful nuclear activities to the manufacture of nuclear weapons or of other nuclear explosive devices or for purposes unknown and deterrence of such diversion by the risk of early detection* [2-4]. Containment and surveillance (C/S), which is one of the various safeguard measures, is widely applied for improved safeguards efficiency. The C/S can reduce the number and duration of on-site inspection activities by maintaining continuity of knowledge (CoK) for previously verified nuclear materials or equipment. The sealing system for C/S [5] is a tamper-indicating device that is applied in such a way as to render difficult any access to the sealed contents without its being opened or destroyed. Such a device senses physical damage or access by unauthorized and/or unreported activities and provides evidence of these events.

* Corresponding author, e-mail: hseo@jbnu.ac.kr

The IAEA uses a metal cap seal [6] and adhesive seal [7] most commonly due to their simplicity and low cost, while, less commonly, an electronic sealing system with optical fiber loops [8] is employed. These seals can be used in a variety of safeguards applications such as nuclear materials previously verified through nuclear material accountancy (NMA), transportation of nuclear materials, and sensitive equipment. However, most of the existing seals provide only tamper-indicating features without any real-time verification functionality, whose lack is a limitation in terms of timely detection of abnormal situations; hence, the IAEA uses complementary real-time monitoring techniques including digital surveillance cameras, radiation monitors, and other sensors. Additionally, because most of the existing seals support only on-site inspection, a remote monitoring capability is required: to minimize the risk of radiation exposure of inspectors and to save inspection costs by shortening inspection time. For these reasons, we are developing a new safeguards seal for real-time verification based on a telecommunication technique used in the internet of things (IoT) applications. Safeguards seals do not necessarily require the same design requirements in cases where the requirements can vary depending on the application type, objectives, and environment. In the present study, by analyzing the relevant previous

studies, we identified the sealing-system design requirements proper for the purposes of real-time verification and remote monitoring.

ANALYSIS OF PREVIOUS STUDIES

Design requirements presented by the IAEA

The IAEA has provided safeguards implementation design guidelines for future nuclear power plants relevant to the state authorities, designers, and prospective purchasers [9]. The design requirements of a seal, as presented by the IAEA, are: the nuclear power plant applies C/S techniques to verify the presence of the unreported use of nuclear materials. The sealing system is one of the C/S techniques. Seals are used to record an abnormal situation that can be verified at a subsequent inspection. The sealing system should be easily accessible and installed so as to minimize radiation exposure of IAEA inspectors. Additionally, unique signatures that a dedicated seal reader can verify at an on-site inspection should be provided. The sealing system should include a method by which any attempt to tamper can be verified by IAEA inspectors, so as not to divert the operation of the seal. Based on these requirements, the IAEA has proposed a remote monitoring as a means of exposure control. The data collected from a remote monitoring device is forwarded to the IAEA headquarters and local offices for analysis. Any disruption of information flow between remote systems should be treated as a tamper attempt.

In another previous study [10], the IAEA has proposed design requirements for a new hybrid sealing system. Applicability, tamper indication, unique identity, and usability are proposed as performance design requirements of the system. A sealing system can be applied for various types of substances including nuclear materials, documents, and data storage devices, and can verify whether CoK has been maintained or not. The shape of a container to which the seal is applied may vary depending on the sealed object; hence, applicability is proposed as a design requirement. The seal should include tamper-indicating features as a means of proving that the sealed container has been continuously closed. In addition, tamper indication is an effective means of proving that the seal has been maintained between inspection visits. Meanwhile, the seal should indicate its identity. To this end, an authentication technology providing a unique identity confirmed by a signature is proposed as a design requirement. Finally, incorrect application of a sealing system can be minimized through easy-to-use procedures during application and removal, hence, usability is proposed as another design requirement.

Along with the performance design requirements of the sealing system, previously described, the following functional design requirements are proposed by the IAEA. The environmental impact should be considered for a seal that is applicable under a variety of environmental conditions. Therefore, the IAEA proposes seal robustness to the environment as a design requirement. In terms of radiation hardness, the IAEA proposes a seal to have robustness usually for two years of radiation exposure by spent nuclear fuel. Additionally, the seal function should be maintained within the temperature range of –40 °C to 150 °C. It should operate normally for up to two years in freshwater immersion and for up to one month in saltwater immersion with a typical seawater-salt concentration. Overall, the sealing system should have the integrity to be utilized as a safeguards measure. The tamper-indicating features are proposed as a design requirement to confirm the fact that each sealed component has been neither drilled nor damaged. The tamper-indicating features can be more useful when simple visual inspection is possible without the use of complicated verification devices. During the verification process, the seal data should be remotely verifiable. Therefore, remote communication functions such as the radio frequency communication are proposed as design requirements. Seal data, including tamper information and identity, should be communicable to at least 50 m of distance. In that case, the seal housing material should be selected such that communication is not impeded. The seal also needs to provide a unique identity for verification. Moreover, there are form requirements for usability of the designed sealing system: small size, lightweight, and easy portability.

Other previous studies conducted at the IAEA have proposed design requirements for the development of a new electronic seal [11]. Based on them, an active sealing system, the electronic-optical sealing system (EOSS), was developed. The design requirements for an electronic seal using fiber-optic loops proposed by the IAEA include proper wire length, sufficient memory size and tamper records, data security, wired/wireless communication with verification equipment, robustness, and usability.

Design criteria presented by the Sandia National Laboratory

Spent fuel casks are transferred to a storage facility for disposal. The IAEA requests to apply a seal to the containers containing spent nuclear fuel in order to maintain CoK for the containers and their contents when transferred and stored. The Sandia National Laboratory (SNL) proposed the design requirements of a sealing system capable of maintaining CoK for disposal and transportation castors [12, 13]. The structure of a typical electronic sealing system is shown in fig. 1.

The purpose of the sealing system is to detect containment failures such as opening, destruction, and penetration of containers and to provide a relevant re-

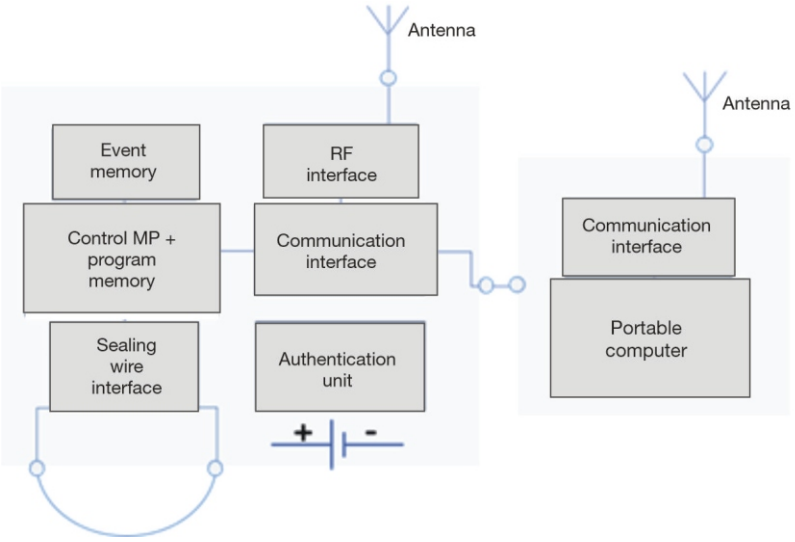

Figure 1. Structure of the electronic sealing system

cord to the national/international inspection agency. Consequently, the seal should be verifiable by the authorized person or agency. The SNL proposed design requirements including effective sealing system design, reliability, and usability. An electronic seal suitable for safeguards applications is a tamper-indicating device capable of multiple use and verification. A reusable seal should be able to be unsealed and resealed many times without requiring a replacement, while a multiple-verification seal should be verifiable without being destroyed during subsequent verification. A tamper-indicating device should record an event if there is unauthorized access or tampering with the sealed material and should include a unique identity of the seal. The seal should provide the inspector with reliability. In other words, the inspector should have confidence that the seal works properly as designed without any failure during the designed operation period. The SNL thus proposes seal failure resistance as a reliability factor. For example, reliability can be provided to inspection agencies through fault-tree analysis, which classifies electronic processes and components for investigation of potential failures of the sealing system. For safeguards implementation, the sealing process consists of four stages (initialization, application, verification, and removal stages) performed by the IAEA inspector; the user should be able to perform the sealing system's function easily and correctly for each process. To this end, one can use a dedicated tool, such as the EOSS Interface Tool (ESI) [13], which senses user errors and prevents incorrect verification processes.

Inspectors should be able to ensure that the data taken from the sealing system has not been altered or falsified. Additionally, the system should detect and prevent attempts to divert nuclear materials. In this regard, SNL proposed: tamper indication, tamper resistance, and data integrity as design requirements for a sealing system. Tamper-indicating features of the seal can use a unique pattern that is permanently changed by tampering. A tamper switch activated when a tamper event occurs or a micro-foil that is damaged when a housing is opened can be utilized. The possibility of successful diversion by malicious users should be reduced by the tamper-resistance characteristics. Additionally, electronic seals must ensure the integrity of the data, because it stores tamper information electronically within the equipment. Data integrity should be ensured throughout all of the processes, *i. e*., data generation, storage, transfer, external device storage, and recovery process. The data can be considered as reliable when it is generated by designated equipment. It should be regarded to have integrity when there has been no alteration, removal, or damage after data generation. Authentication and encryption techniques can be used to meet such design requirements. Moreover, data confidentiality could be included as a design requirement to ensure data integrity. It can be satisfied by encrypting and decrypting data using an encryption algorithm such as an advanced encryption standard (AES). Note also that the key to be used for encryption is required to have sufficient bit length.

The seal should reduce the need for direct access by inspectors, thus minimizing radiation exposure risk. Therefore, SNL proposed maintainability as a design requirement. The most frequent type of seal maintenance is battery replacement, hence, the battery should operate as long as possible before being replaced. In the case of a seal for transportation, an accidental situation may occur in which the battery should be replaced during transportation. Accordingly, then, the sealing system should be designed to facilitate easy access and maintenance. For example, a backup battery can be used to maintain the power supply of the seal in transportation, which battery can be designed to be replaced in the field. It was proposed that off-the-shelf batteries are most proper, in order to enable flexibility in the selection of seal batteries. The

seal case should be designed in consideration of environmental conditions so as to mitigate maintenance problems. Finally, up-to-date technology in seal software and firmware should be considered for the possibility of requiring updates or improving vulnerability management during the operating period.

The sealing system should operate as designed during the expected operation period under various environmental conditions. The SNL proposed environmental requirements as design requirements. Generally, the environment where the seal is applied could be a high radiation area wherein the radiation dose can be accumulated over the course of a long period of time. Functional degradation of some components of the seal is expected wherever long periods of use are anticipated. Therefore, damage due to environmental effects should be considered. In the case of transportation casks' seals, the environment may include land vehicles such as trucks and railways, or ships traveling in the ocean. Therefore, depending on each environment, the tolerance for the impact and shock affecting the seal during the transport process should be considered.

The sealing system should be able to collect data in the unattended mode and transmit the data to inspectors remotely. The SNL thus proposed remote verification and monitoring as design requirements. During remote verification, the seal and seal reader should transmit and receive data remotely, and inspectors should be able to verify the data in a safe place. Remote monitoring should include the capability of transmitting collected data to the IAEA headquarters over a wide-area communication network. Remote monitoring capabilities allow a single wireless station to communicate with multiple electronic seals and disconnect them without direct access of the seals. Although remote functions can implement effective safeguards measures, communication security must also be considered in this regard. Therefore, security plans including strong data authentication and encryption should be included in the design requirements.

Design criteria presented by other studies

The U. S. Nuclear Regulatory Commission (NRC) asks licensees who handle special nuclear materials (SNM) to comply with the requirements on their physical protection of facilities and materials under Part 71 of the Code of Federal Regulations [14]. To ensure the integrity of SNM, the NRC requires a seal to be used in containers or vaults. The seal must provide information on whether any attempt to tamper has occurred, and such information should be displayed immediately. Every seal is vulnerable to destructive removal and replacement with new seals. In such a situation, a seal is valuable only when it can be uniquely identified and in cases where this identification cannot be duplicated. Therefore, all tamper-indicating devices should provide a unique identity. Also, a seal usually can be easily re-applied after removal, hence, proper application of a seal is required to prevent this vulnerability. Consequently, the seal designer and provider should provide clear installation instructions explaining the appropriate ways to apply and use their seal. The seal is generally considered a weak obstacle that unauthorized persons can overcome with relatively little effort, however, it should provide an adequate level of resistance. For example, adhesive seals should not be removable simply by pulling on one end and should not be degraded in adhesive strength due to fluctuations in weather conditions.

The Los Alamos National Laboratory (LANL) proposes three essential design requirements for development of a graphite oxide (GO)-based seal [15].

– The seals should be sensitive to the common mechanisms that attackers use for tampering. In other words, the seals should show traces of irreparable damage whenever the attacker tries to restore them to their original configuration after they have been temporarily removed.
– At the same time, the seal should have a level of robustness to operate normally in any adverse environments where it is expected to be applied.
– Finally, the seal's uniqueness should be assured so as to prevent attempts to replace it with a counterfeit version. For example, the seal should be identifiable by a unique identity after any tamper attempt.

Canberra (currently, Mirion Technologies) has developed various safeguards measures and has proposed corresponding seal design requirements [16]. In designing a sealing system, it should be considered that they could be applied in adverse environments; hence, a system should be designed to be electrically independent, protected from damage, operable reliably in such environments.

Additionally, the SNL has presented design requirements for a ceramic seal [17]. The NIS Office of Nuclear Safeguards and Security [18], Pacific Northwest National Laboratory [19], and Uppsala University [20] also presented design requirements for a safeguards seal. The design requirements presented in these studies are similar generally to the previous, above-described studies.

IDENTIFICATION OF DESIGN REQUIREMENTS FOR A REAL-TIME-BASED SEAL

In the present study, the design requirements that need to be considered in developing a real-time-based sealing system were identified by consideration of the real-time verification environment and the previously proposed requirements in general. First, we identified

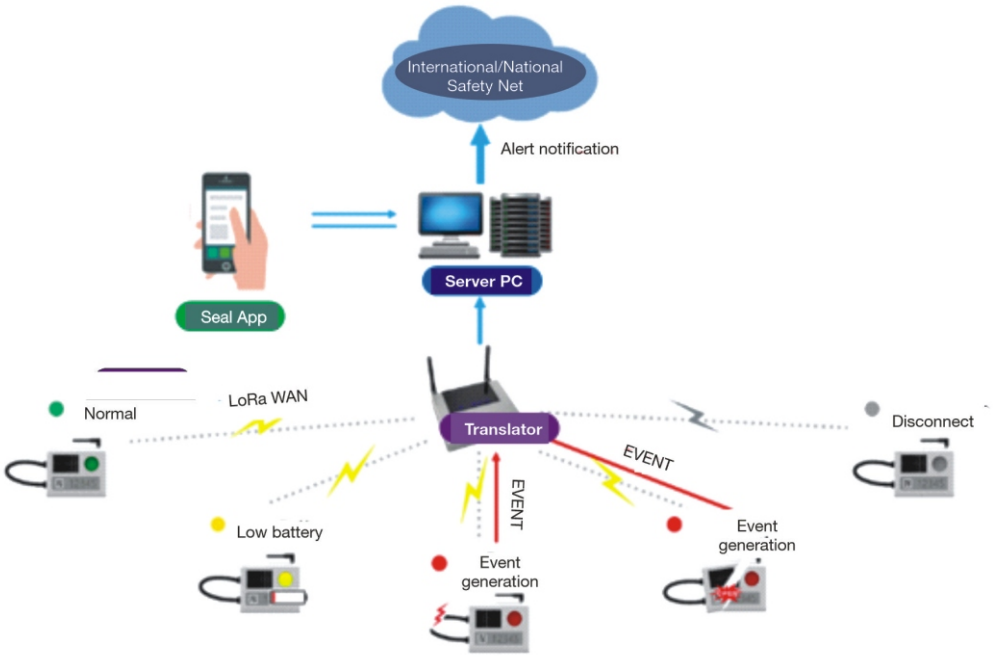

Figure 2. Schematic diagram of the sealing system for real-time verification

the general requirements that a real-time-based sealing system should satisfy. Then, the specific design requirements for each component, *i. e*., seal, transceiver, and verification device, were formulated.

The schematic diagram of the prospective sealing system for real-time verification is shown in fig. 2. The seal senses tamper events through various sensors and transmits relevant data to the transceiver using wireless communication. A transceiver can collect data from a number of designated seals in a specific area in real-time, and transmits that data to a server using wired communication, *e. g*., an Ethernet. A user, *i. e*., national/international authorities, can check the status of a seal and verify the seal integrity using a dedicated mobile application and a verification software in a real-time basis.

General requirements

As a general requirement, the seal should be verifiable. To this end: verifiability, reliability, and usability were identified as design requirements. A new seal is an electronic sealing system. For such a sealing system to be utilized as a verification device, it should be a tamper-indicating device with multiple-use and multiple-verification capability. Additionally, it should provide inspection data to inspectors in a timely manner. The user should also be able to verify the seal by the unique identity. These seal functions should be proven to work properly during the safeguards implementation process in order to provide the inspector with reliability. For example, a performance test by a qualified testing agency can be conducted to ensure reliability based on the quantitative/qualitative performance index. If the seal is improperly applied or removed by human error, failure to maintain the CoK will be the result. Therefore, usability during the safeguards procedures should be considered as a design requirement, hence, comprehensive and detailed procedures should be provided and approved by inspectors and designers. Moreover, adequate education and training on implementation of specific equipment is required. The user-friendliness of the verification software, for example, should be considered as a design requirement ensuring usability, as should small system sizes and light weights.

In order to operate the seal as a tamper-indicating device, its integrity must be assured, hence, tamper indication, tamper resistance, and data integrity were identified as design requirements of a sealing system for real-time verification. Dedicated visual information is required for a seal to recognize tampering events based on appropriate tamper-indicating means such as fiber optic wires. Additionally, analog and digital sensors, *e. g*., a tamper switch and internal micro-foil, should be used internally to detect the opening and closing of the seal housing. Tamper resistance to reduce the probability of success of tampering and to increase the financial burden of tampering attempts should also be considered as a design requirement. Finally, as an electronic seal stores data electronically in equipment used for verification, data integrity is the third general design requirement. In particular, the integrity of all stages of data generation, storage, transmission, and external storage should be considered, because the prospective seal transmits data via a com-

munication network for real-time verification. Common methods to secure data integrity are authentication and encryption.

For real-time verification, remote verification and remote monitoring were identified as design requirements. In terms of remote verification, the electronic seal should be able to communicate with a seal reader located outside the high-radiation area, access to which is prohibited due to the severe health risk posed by radiation exposure. The prospective sealing system aims to allow multiple seals to transmit data to one transceiver, hence, communication techniques suitable for many devices to communicate small amounts of data over long distances should be considered. Considering power consumption, the amount of data, and communication frequency and distance, LoRa (Long Range) communication, which is a representative communication technology used in the IoT, can be considered as a suitable communication protocol. LoRa could be the best option when the small amount of data needs to be occasionally communicated under the restriction of less power consumption. In terms of remote monitoring, transferring data collected in real-time from a seal to the National Nuclear Management and Control Agency (NNCA) is required. To this end, the proper and best way to access the servers of the NNCA by an authorized user should be provided.

In order to minimize inspectors' radiation exposure during the verification process, the minimization of procedures for seal maintenance was identified as a design requirement. First, battery capacity should be selected for proper operation during the design period. As required by the IAEA, an electronic seal should operate for at least two years. Additionally, the seal components should be made of appropriate materials in consideration of the environmental effects in which they are applied. Because maintenance is inevitable, ease of maintenance also was identified as a design requirement. For example, components requiring relatively frequent maintenance can be separated in external housings to ensure easy maintainability. Significantly, an external indicator of the seal itself, notifying of the necessity of maintenance, can also be included.

The seal could be applied in a variety of environments, *e. g*., high-radiation environments (inside of the hot cell or close to spent nuclear fuel), transportation of spent fuel casks, and dry storage of spent nuclear fuel. Therefore, proper operation under generally expected environmental conditions was identified as an additional design requirement. International standard ISO 18185-3 [21] defines the environmental conditions of electronic seals for transportation. The prospective seal should operate normally within the environmental conditions of low and high temperatures, mechanical shocks, vibration, humidity, rain and snow, salt fog, drop shock, sand and dust, and electromagnetism.

Design requirements of the seal

Six design requirements for the sealing system were identified:

– *Functionality*: The system should be developed in an electronic form capable of multiple-use and multiple-verification. The data should be stored in a non-volatile memory such as FRAM, wherein at least 100000 events should be recorded.

– *Reliability*: Performance tests by the authorized testing agency, as based on the international standard (ISO 18185-3), should be conducted and passed. Radiation resistance tests in consideration of the expected operating environment also should be performed.

– *Usability*: Minimization of the size and weight of the sealing system should be considered in the design stage, say, to 15 cm × 15 cm × 5 cm and less than 1 kg. In addition, the status of the seal should be immediately confirmable by an external display. A QR code could be used for extra convenience of identification. The user should be provided with detailed instructions that cover all of the functions of the seal.

– *Integrity*: The sealing system should function as a tamper-indicating device, to which end, fiber-optic wires should be used. The data should be encrypted and recorded in a non-volatile memory in order to render tampering or corruption by any unauthorized person impossible. Data encryption could be performed by an encryption algorithm such as the AES (Advanced Encryption Standard) [22] that can encrypt and decrypt the data and was developed by the U.S. National Institute of Standards and Technology.

– *Remote verification and monitoring*: A proper telecommunication technology, *e. g*., LoRa, should be applied. The data communication should be capable of transmitting and receiving up to a distance of a few km, considering the seal application of the dry cask storage of spent nuclear fuels. To ensure the integrity of data remotely transmitted and received, the data should be copied and stored in a physically separated memory, and the cyclic redundancy check (CRC) method [23] should be applied. The data encrypted independently and stored in each separated memory are compared to verify the data integrity. The CRC method, which is a method to include a calculated CRC value in the original data, can verify the integrity of data communication by comparing the CRC values of transmitted and received data.

– *Maintainability*: The parts that require frequent maintenance should be located in a separate external housing for ease of maintenance. To minimize the frequency of maintenance, moreover, the battery should have an operating period of at least five years and could use solar cells as an auxiliary power source. Ad-

ditionally, robustness in terms of resistance to the impact of environmental conditions must be considered.

Design requirements of the transceiver

Five design requirements for the transceiver were identified:
– *Functionality*: The transceiver should be capable of remote data collection and transmission. The data communication between the seal and transceiver should be performed by a wireless network (*e. g*., LoRa), while the communication between the transceiver and server should be performed by a wired network (*e. g*., Ethernet).
– *Reliability*: Tests for environmental impact and radiation damage should be performed, in the same manner as they will be for the seal.
– *Usability*: Minimization of the size and weight should be considered, say, to 25 cm × 20 cm × 10 cm and less than 2 kg.
– *Remote verification and monitoring*: The requirements would be the same as those for the seal.
– *Maintainability*: In order to eliminate the need for battery replacement, AC power could be useful. The rest requirements would be the same as those for the seal.

Design requirements of the verification device

In the case of the verification device, two design requirements were identified: functionality and usability. In terms of functionality, the verification device should be operable only by authorized users. To this end, a USB key (dongle) or biometric authentication techniques for user authentication should be applied. In addition, seal initialization and identification could be set by the verification device. In terms of usability, a dedicated user-friendly software with detailed instructions should be provided.

CONCLUSION

The IAEA uses C/S technology to improve the efficiency of safeguards implementation. A sealing system is a tamper-indicating device that detects attempts to tamper with the contents of containers by unauthorized acts for malicious purposes, and informs the designated authorities of any such attempts. The seal can be applied in a variety of environments, hence, the design requirements of a sealing system should be identified in consideration of both the system's purpose and the expected application environment. In the present study, the design requirements of a sealing system proposed by various organizations were surveyed and analyzed. Then, the design requirements of a prospective new sealing system for real-time verification were identified by taking into consideration the previously proposed system design requirements. The next step in this research will be the development of a real-time verification sealing system based on all of the identified requirements. We expect that this new sealing system with real-time verification capability could play an important role considering the IAEA's current and growing interest in remote and unattended safeguards systems.

ACKNOWLEDGMENT

This study was supported by the Nuclear Safety Research Program through the Korea Foundation of Nuclear Safety using financial resources granted by the Nuclear Safety and Security Commission of the Republic of Korea (2004024-0120-CG100). This study was also supported by the National Research Foundation of Korea funded by the Ministry of Science and ICT (NRF-2021M3I1A1097913). This research was a part of the project titled Development of Smart Processing Technology for Sea Foods, funded by the Ministry of Oceans and Fisheries, Korea. This study was supported by the Research Base Construction Fund Support Program funded by Jeonbuk National University in 2021.

AUTHORS' CONTRIBUTIONS

Analysis of previous studies were performed by J. Park, G. An, and H. Seo. Design requirements were identified by J. Ahn and H. Sim. The first draft of the manuscript was written by J. Ahn. All authors reviewed and approved the final manuscript.

REFERENCES

[1] ***, IAEA (International Atomic Energy Agency), The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons, Vienna, Austria, 1972
[2] ***, IAEA (International Atomic Energy Agency), International Nuclear Verification Series No. 3, IAEA Safeguards Glossary, Vienna, Austria, 2002
[3] Pesić, M., *et al*., Transport of High Enriched Uranium Fresh Fuel from Yugoslavia to the Russian Federation, *Nucl Technol Radiat, 17* (2002), 1, pp. 71-76
[4] El-Tayebany, R. A., *et al.*, Optimization of HPGe Detector Response Using Fast and Reliable Method, *Nucl Technol Radiat, 35* (2020), 3, pp. 253-260
[5] ***, IAEA (International Atomic Energy Agency), International Nuclear Verification Series No. 1, Safeguards Techniques and Equipment, Vienna, Austria, 1997
[6] Hymel, R., *et al*., Material Sealing and Monitoring, Sandia National Laboratories, Albuquerque, N. Mex., USA, 2014

[7] ***, IAEA (International Atomic Energy Agency), Safeguards Techniques and Equipment (2011 Edition). Vienna, Austria, 2011
[8] Goldfarb, M., *et al*., Electro-Optical Sealing System Remote Verification, International Atomic Energy Agency, Vienna, Austria, 2014
[9] ***, IAEA (International Atomic Energy Agency), Technical Report Series No. 392, Design Measures to Facilitate Implementation of Safeguards at Future Water Cooled Nuclear Power Plants, Vienna, Austria, 1998
[10] ***, IAEA (International Atomic Energy Agency), Provision of a New IAEA Integrated Hybrid Seal System Prototype. Vienna, Austria, 2020
[11] ***, IAEA (International Atomic Energy Agency), Development and Evaluation of New Electronic Seals at the IAEA, Vienna, Austria, 2001
[12] Smartt, H. A., *et al*., Developing Design Criteria for Safeguards Seals for Spent Fuel Transportation Casks, Sandia National Laboratories, Albuquerque, N. Mex., USA, 2018
[13] Rinch, R., *et al*., Developing Reliable Safeguards Seals for Transportation Casks to Be Applied, Verified, and Removed by State Operators, Sandia National Laboratories, Albuquerque, N. Mex., USA, 2017
[14] ***, U.S. Nuclear Regulatory Commission, Pressure-Sensitive and Tamper-Indicating Device Seals for Material Control and Accounting of Special Nuclear Material, Regulatory Guide 5.80, 2010
[15] Cattaneo, A., *et al*., A Graphite Oxide (GO)-based Remote Readable Tamper Evident Seal, Los Alamos National Laboratory, Los Alamos, N. Mex., USA, 2016
[16] Canberra, International Nuclear Safeguards Solutions (Nuclear Measurement Solutions for Safety, Security & the Environment), 2017
[17] Smartt, H. A., *et al*., Ceramic Seal, Sandia National Laboratories, Albuquerque, N. Mex., USA, 2016
[18] ***, NIS Office of Nuclear Safeguards and Security, Guidance for Research Reactors and Critical Assemblies. Next Generation Safeguards Initiative, Washington D.C., 2012
[19] ***, Pacific Northwest National Laboratory, Strengthening IAEA Safeguards for Research Reactors, Richland, Washington, D. C., 2016
[20] Fitzell, A., Concerns When Designing a Safeguards Approach for The Back-end of The Swedish Nuclear Fuel Cycle, Uppsala Universitet, Uppsala, Sweden, 2006
[21] ***, International Organization for Standardization. Freight containers - Electronic seals - Part 3: Environmental characteristics, International Organization for Standardization, Geneva, Switzerland, 2011
[22] Dworkin, M., *et al*., Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, Md., USA, 2001
[23] Arifin, M. M., *et al*., Design and Implementation of High Performance Parallel CRC Architecture for Advanced Data Communication, *Proceedings*, 4th International Conference on Electrical Information and Communication Technology (EICT), Khulna, Bangladesh, 2019, pp. 1-5

Received on May 5, 2021
Accepted on February 2, 2022

Ћихјуен АХН, Ћуенсунг ПАРК, Хајоунг СИМ, Геунјоенг АН, Хе СЕО

ЗАХТЕВИ ЗА ПРОЈЕКТОВАЊЕ ЗАШТИТЕ СИСТЕМА ЗАКЉУЧАВАЊА РАДИ ВЕРИФИКАЦИЈЕ У РЕАЛНОМ ВРЕМЕНУ

Да би се осигурала мирољубива употреба нуклеарне енергије, у државама чланицама Међународне агенције за атомску енергију примењује се нуклеарна заштита према Уговору о неширењу нуклеарног оружја. Два главна циља нуклеарне заштите су ефективност и ефикасност. Међународна агенција за атомску енергију има велики интерес за коришћење технологије контејмента и надзора како би се одржао континуитет увида. Репрезентативно средство технологије контејмента и надзора је систем закључавања који упозорава корисника на неовлашћено коришћење. Постојећи системи закључавања које користи Међународна агенција за атомску енергију ограничене су употребљивости за потребе верификације у реалном времену. Да би се одговорило на ово ограничење, у раду се анализирају захтеви дизајна система закључавања које су предложиле различите институције, укључујући Међународну агенцију за атомску енергију, Нуклеарну регулаторну комисију САД, бројне националне лабораторије и компаније. Затим су идентификовани одговарајући захтеви дизајна овог система за верификацију у реалном времену. Следећи корак је развој система верификације закључавања у реалном времену заснованог на захтевима дизајна који су идентификовани и о којима се овде расправљало. Очекује се да ће такав систем значајно побољшати ефикасност нуклеарне заштите.

Кључне речи: нуклеарна заштита, систем закључавања, верификација, реално време, критеријум пројектовања