PROCEEDINGS OF THE INMM & ESARDA JOINT VIRTUAL ANNUAL MEETING
AUGUST 23-26 & AUGUST 30-SEPTEMBER 1, 2021

EXPLORING NOVEL PHYSICAL SECURITY ENHANCEMENTS FOR INDUSTRIAL IRRADIATORS THROUGH GOVERNMENT-INDUSTRY PARTNERSHIPS

Meghan Van Den Avyle
Sandia National Laboratories

Michael Bolduc
Sandia National Laboratories

Garril Smith
Nordion (Canada) Inc.

ABSTRACT

Government and industry are committed to securing radiological material against theft or sabotage—even in the harsh environments and operational conditions of industrial irradiators. The U.S. Department of Energy/National Nuclear Security Administration's Office of Radiological Security (ORS) supports a unique program that facilitates collaborative partnerships with radiological device manufacturers, with the goal of enhancing device security. This program, the In-Device Delay (IDD) program, works with U.S. and international manufacturers to develop and integrate additional delay and detection capabilities into the company's commercial products through security-by-design (SbD) and retrofitted means.

This overview will highlight one such government-industry partnership that currently exists between ORS and Nordion (Canada) Inc. Throughout their long-standing relationship, the two organizations have sought to identify opportunities to further enhance the security of various radiological devices and then to develop and implement new security technologies. ORS supports this partnership by providing security expertise—from concept design to testing and implementation. Nordion brings a deep understanding of their technologies and their customers' operational needs to this partnership. Together, these two organizations have the tools and resources needed to develop practical and effective physical security solutions for radiological devices.

Industrial irradiators are highly secure to ensure their radiological material are not subject to theft or sabotage. However, this potential threat establishes the continued need for additional security solutions for these devices. ORS and Nordion are collaborating on a project to explore this issue. This effort will focus on developing security technologies to be applied directly at the irradiator pool and radiological source rack. Due to the complexities of securing radiological material within the irradiator environment, traditional security technologies are not always suitable, and novel concepts are required. This overview will feature industrial irradiator delay and detection concepts developed by Sandia National Laboratories through the ORS-Nordion partnership and will describe the project's vulnerability testing approach. Plans for future pilot testing will also be discussed.

Ultimately, this partnership and project will bring valuable new tools to the effort to further secure radiological materials world-wide.

INTRODUCTION

The U.S. Department of Energy/National Nuclear Security Administration's Office of Radiological Security (ORS) has a global mission to protect, remove, and replace radioactive sources used for medical, research, and commercial applications. ORS executes this mission through various programs and partnerships. Once such program is the In-Device Delay (IDD) program, which is managed by Sandia National Laboratories. The IDD program is a strong proponent of commercial partnerships and works with various radiological device manufacturers to promote enhanced security within their devices. Specifically, IDD helps partner companies to design, test, and integrate additional security technologies into device designs. These technologies can be developed as security-by-design (SbD) features for new product models and installations, or to retrofit existing devices and installations.

ORS has maintained a long-standing partnership with Nordion (Canada) Inc., a Sotera Health Company. Nordion is a global supplier of Cobalt-60 (Co-60) and a manufacturer of irradiation systems. It develops and installs large-scale custom gamma irradiation facilities throughout the world–with over 200 facilities in operation in 40 countries. (Nordion, n.d.) These two organizations have a shared commitment to the safety and security of radiological material. Together, ORS and Nordion established a joint project to explore the development of practical and effective security solutions for radiological devices, with a specific focus on industrial irradiators.

This joint project launched in 2018 with a charter between ORS and Nordion directing the IDD program to collaborate on the analysis of an existing radiological device, to jointly develop new security concepts for this device, to fabricate a prototype of a selected concept, and then to conduct vulnerability testing and analysis of the prototype. The project charter called for the security solutions to increase the time it might take an adversary to steal or sabotage the radioactive sources within an industrial irradiator and to decrease the time to detect a potential theft or sabotage. If successful, these two requirements would maximize likelihood of preventing a theft or sabotage scenario. The final goal of the project is to pilot the concept and ultimately make the security technologies available for integration into irradiator designs and for use by irradiation service suppliers. The designs are to be owned by Nordion and may be offered as part of new irradiator installations and potentially as retrofits for existing facilities. To date this project has successfully down selected a security concept and is currently preparing to conduct the vulnerability testing. This partnership and project will be further explored in this paper.

PROJECT OVERVIEW

ORS has a long history of partnering with industrial irradiator facilities across the globe by providing physical security enhancements throughout their facility buildings. In contrast, this IDD-Nordion partnership project is focusing on developing security technologies to be applied directly at the radiological device components–the irradiator pool and source rack.

Industrial Irradiator Overview

Industrial irradiators use high levels of ionizing radiation to sterilize, modify, or decontaminate various products. They can use either a radioactive isotope (gamma irradiation) or electron beams (beta irradiation) in their operation. Gamma irradiators are the devices of interest for this project based on their use of a radioactive source, Cobalt-60 (Co-60), and ORS's mission to secure radioactive materials.

Gamma irradiators emit a constant source of radiation. The radiation from the Co-60 sources is controlled by raising and lowering the sources into a large pool of water. While in the water, the radiation is absorbed. When the sources are exposed, the radiation is used to irradiate anything within the irradiation chamber–a room made of thick concrete walls (Fig. 1). The radioactive sources are typically positioned on a rack that moves vertically in and out of the water. The irradiator pool is uncovered.

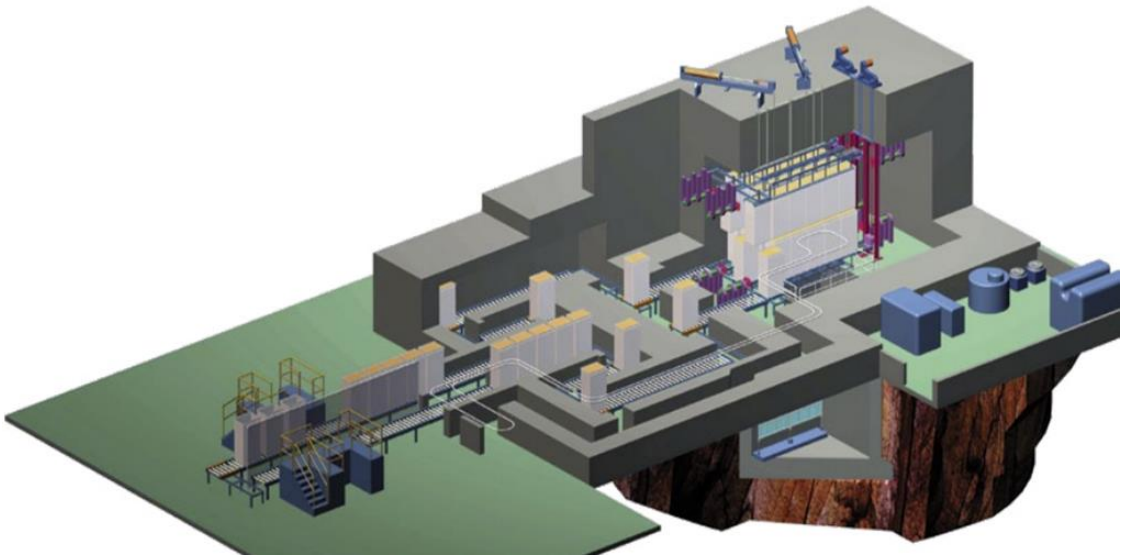

Figure 1. Industrial irradiator cut-away view

Material Threat

The radiological material used in industrial irradiators is of particular interest to potential adversaries for purposes of theft or sabotage due to the millions of curies of Co-60 required to execute the irradiation process. Fortunately, industrial irradiators are innately very secure. When the sources are not being shielded in the pool, they are emitting a very high dose of radiation within the irradiation chamber. Anyone exposed to these sources for even a short period of time would likely experience severe injury or death. When stored in the pool, the sources are located under 3.5-m of water and are therefore difficult to access.

Despite the general self-securing nature of industrial irradiators, a strong threat does exist. This project assumes that persistent adversaries willing to die for their cause pose a true threat and therefore focuses on developing security technologies to prevent an attack or to make an attack significantly more difficult, and ultimately unsuccessful.

Project Phases

This project is following a typical technology development process to create the new security technologies. The process steps include baselining the system, developing conceptual designs, and verifying and validating the modified system. The IDD team brings unique testing approaches to the baselining and verification/validation phases through its established competencies in vulnerability testing. The team also has a long and successful history of developing delay and detection concepts for various security applications.

The first step in this project was to gain a thorough understanding of the existing system–an industrial irradiator. System input was gathered from Nordion and from an earlier assessment of irradiator designs by Pacific Northwest National Laboratory and Sandia National Laboratories. This information informed the project team's effort to identify opportunities to further enhance the security of industrial irradiators. Once the opportunities were identified, IDD and Nordion worked together to develop a requirements package for the project. The requirements set included a time limitation for facility operators to assemble and disassemble the security technologies for routine system maintenance and the ability to modify the design for various system configurations, amongst many other requirements. Various security concepts were then developed that could satisfy these requirements. The project team assessed the various concepts and selected an approach that included the development of an irradiator pool cover and rack locking mechanism that employed both delay and detection components. The analysis showed a significant increase in the time requirement and difficulty level to access the radioactive sources when these two security elements were simultaneously deployed at an industrial irradiator.

Following the selection of the concepts, the IDD team collaborated with Nordion on the design specifics. During this phase fine design details were discussed, and requirements were further refined. Multiple iterations of component bench-scale testing also occurred during this phase to demonstrate the concept and to mature the prototype design. Once the design was agreeable to all parties, the IDD team fabricated and assembled the lab-scale prototype.

The validation and verification testing of the new security concepts has not been completed and is expected to occur in late 2021. The primary activity in this phase includes a vulnerability test series that will compare the baseline performance of the irradiator security against the improved state and will verify whether requirements have been met. If requirements are not met or the concept does not meet expectations, revisions to the design will be made and retested. Details of IDD's testing methodology are described in greater depth in the next section.

Testing Methodology In-Depth

The IDD program conducts vulnerability testing to support the verification and validation of system requirements. The purpose of vulnerability testing within this project specifically, is to determine the effectiveness of preventing the removal of the Co-60 sources from an industrial irradiator following the addition of the newly developed security technologies, which includes the irradiator pool cover and rack locking mechanism.

As previously mentioned, the enhanced security technologies are aimed at lengthening the adversary timeline so that they are unsuccessful in their goal of theft or sabotage of the radiological sources. This involves increasing the time required for an adversary to gain access to the sources and also detecting unauthorized access to the sources at an earlier point in the attack. Delay and detection times were estimated for the various new security elements and for

the system during the project's concept development phase. Vulnerability testing will be used to validate or revise these estimates.

Vulnerability testing will be conducted at Sandia National Laboratories' Gamma Irradiation Facility (GIF). The GIF maintains a 5.5-m deep pool of water which can be used to simulate an irradiator pool. Although the GIF has the capability of producing a wide variety of gamma irradiation environments, the test facility will only be used for its layout which is comparable to an industrial irradiator. No live sources will be used in the testing. The pool contains an irradiation fixture near the bottom of the pool and a typical irradiator source rack will be attached for the testing of the rack lock. The pool cover will simultaneously be placed over the GIF pool for testing.

Vulnerability testing of the system will be conducted by two attack teams acting as the adversary: A-Team and B-Team. The A-Team attack represents a higher-level attack team with a greater knowledge of industrial irradiators, newly developed security technologies, and the installation procedures. The B-Team attack represents a lower-level attack team with a limited knowledge of industrial irradiators and the newly developed security technologies. These teams will use varying tools, knowledge, and skills to attempt to remove the radiological sources from the rack and pool.

The attack teams will use various attack scenarios, or paths, to determine the most successful attack approach. Success will be defined by the timeline to remove the sources. The best scenario will have a combination of the shortest timeline to retrieve the source and the greatest period detection avoidance. If the attackers can remove the sources before the time requirement for law enforcement to respond and to interrupt the attack, then the security concepts may need further improvement. However, if the system is successful in thwarting the attack, it should be ready to move into the pilot phase.

All stakeholders have been invited to attend the vulnerability testing to ensure the testing approach is understood and to increase familiarity and comfort with the new security concepts.

TESTING RESULTS

As discussed, testing of the enhanced security components has not been completed. However, some hypotheses can be made about the testing results based upon the component testing and historical knowledge. It is expected that the testing will show that the new security concepts substantially increase the difficulty for an adversary to gain access to the radioactive sources within the irradiator. The A-Team is likely to be more successful than the B-Team in their attack based on their increased knowledge of the system and attack capabilities; however, the system should still "win".

Vulnerability testing results will be thoroughly recorded throughout the testing process and will be documented in the project's vulnerability testing report.

NEXT STEPS

Some design revisions are expected following the completion of the vulnerability testing. This would include any adjustments needed to improve or refine the designs following testing and any necessary modifications to improve manufacturability. The manufacturability improvements will be identified through discussions with Nordion and other stakeholders. These changes will ensure that the design can be manufactured in an efficient and effective manner for the pilot installation and once in full-scale production.

While the designs are being revised for manufacturability, the project team will also be working with industrial irradiation facility stakeholders to identify the facility at which to pilot the new security technologies. It is preferred that a new facility be selected for a security-by-design integration of the security concept; however, an existing facility may be used based on availability. The team will partner with the selected facility to customize the design to fit the irradiator layout. Once all manufacturability and facility design changes are implemented, the designs will be submitted for fabrication and assembly.

The project team will assist with the installation at the pilot facility and will continue to monitor the performance as the irradiator and security technologies are exercised. All final drawings will be transferred to Nordion. It is desired that these security technologies be integrated into future industrial irradiator installations and be offered to existing facilities as retrofits.

CONCLUSIONS

This project demonstrates the benefits of establishing strong government-industry partnerships. Each organization brings a unique perspective and toolset to the project which strengthens the approach. This project has shown the thoughtful and thorough process and efforts of the various organizations involved to develop new security technologies that provide additional security to industrial irradiators. Ultimately, this partnership and project will bring valuable new tools to the effort to further secure radioactive materials world-wide.

ACKNOWLEDGEMENTS

The Office of Radiological Security and Sandia National Laboratories' In-Device-Delay program would like to acknowledge and thank Nordion (Canada) Inc. for their commitment to radioactive material security through this collaborative partnership. Nordion's voluntary dedication to enhance the robustness of industrial irradiators will contribute positively to global security for many years and demonstrates to other manufacturers that incorporating enhanced delay and detection methods can be achieved. The programs would also like to recognize STERIS and Sterigenics International Inc. for their contributions to the project.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of

Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2021-9110 C

References

Nordion. (n.d.). *Gamma Irradiation Systems*. Retrieved from Nordion: https://www.nordion.com/products/irradiation-systems/

Nordion. (n.d.). *JS-10000 Hanging Tote Irradiator.* Retrieved from https://www.nordion.com/wp-content/uploads/2018/11/Nordion_Irradiator_JS-10000_2018.pdf