SAND2019-14032C

DEVELOPING SECURITY-BY-DESIGN ENHANCEMENTS FOR A STEREOTACTIC DEVICE WITH HIGH-ACTIVITY RADIOACTIVE SOURCES

M. Kuca
Sandia National Laboratories
Albuquerque, New Mexico U.S.A.
Email: mkuca@sandia.gov

M. Potter
Sandia National Laboratories
Albuquerque, New Mexico U.S.A.

Abstract

Radioisotopes such as cesium-137 (Cs-137) and cobalt-60 (Co-60) are used in various medical, industrial, and research applications. This radiological material can be a theft or sabotage target that requires increased security for adequate protection. The presented work provides an overview of a collaboration between the United States Department of Energy/National Nuclear Security Administration Office of Radiological Security's In-Device Delay (IDD) project and Xcision Medical Systems, LLC (Xcision) to integrate access-delay and intrusion-detection security enhancements for the GammaPod™. The Xcision GammaPod™ is a fairly new stereotactic radiotherapy device for the treatment of breast cancer. It uses multiple Co-60 sources to deliver high radiation doses to affected tissue. A collaborative Security-by-Design solution was sought so that Xcision could install security enhancements as part of their routine device setup on all newly-manufactured units. Since Co-60 decays with a half-life of 5.26 years, periodic source reloading is necessary. This can be a challenge when designing robust, device-level, sustainable protection elements, as those elements must not significantly impact the reloading process by creating excessive device downtime or additional hardware costs. The paper will discuss these design criteria and how the project team addressed them.

Following successful verification of the design solution, a pilot installation was conducted to address unforeseen procedural, technical, security, or logistic issues. The pilot included integration of a tamper detection component with the facility's alarm system. In addition, the security stature of the device, sources, and enhancements during the installation process needed to be addressed. This required coordination between Xcision, the Sandia National Laboratories' IDD team, the ORS program team, the medical facility, and onsite security/response elements. The paper will also discuss these challenges associated with conducting the pilot.

1. IN-DEVICE DELAY (IDD) OVERVIEW

The In-Device Delay (IDD) program, which is managed by Sandia National Laboratories (SNL), supports the United States Department of Energy/National Nuclear Security Administration Office of Radiological Security's (ORS) mission to enhance global security by preventing high-activity radioactive materials from being used in acts of terrorism. An effective physical protection system requires that the response arrival time is less than the adversary's attack timeline. To obtain this, the system must either sense the attack early in the timeline, reduce the time needed for detection and assessment, reduce the response time, or increase adversary delay once detection and assessment occur (refer to Fig. 1). It is this last element, increase adversary delay, that IDD strives to influence.

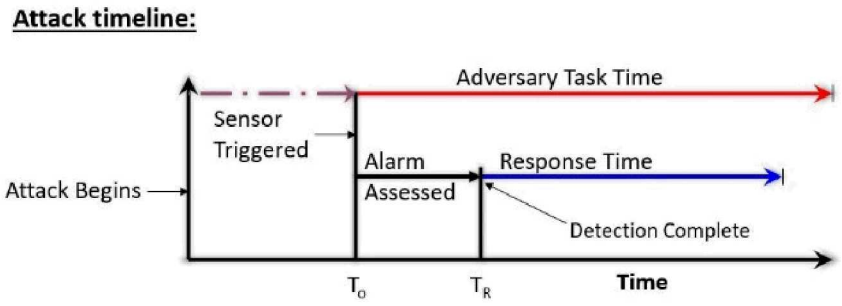

Fig. 1. Attack Timeline in a Physical Protection System

Delay is focused at the target level (i.e., device) by way of hardened barriers and unique fasteners that create an obstacle an adversary must overcome to access the radioactive material within irradiators or medical treatment devices. Therefore, IDD partners with manufacturers of irradiators and medical devices that contain high-activity cesium-137 (Cs-137) and cobalt-60 (Co-60) sources to design enhancements that harden the device against illicit source removal. If feasible, detection components are integrated into the delay elements so that the facility is alerted of any attempts to tamper with the device's hardened areas. Since 2007, IDD has partnered with more than ten manufacturers, and more than 650 devices have been hardened.

Two primary IDD design goals are to design delay enhancements that will not significantly impact the overall cost of the device or excessively prolong the time a device is out of service while the security enhancements are installed. In addition, IDD kits are designed to:

— Provide enough additional source access delay to improve the likelihood that response forces will arrive in time to contain the adversary

— Not affect device performance, operation, or safety

— Be field-installable or easily incorporated into the device manufacturing process

— Not affect the manufacturer's warranty

— Be consistent with and complementary to existing regulatory security requirements

Incorporating access delay and early detection into the initial design phase of radiological facilities or devices automatically reduces the probability of radiological material theft and increases the probability that an adversary is detected with sufficient time for response forces to interdict. This front-end design approach, called Security-by-Design (SbD), more effectively addresses facility or device vulnerabilities. Whenever possible, IDD and the partner manufacturer will strive for a SbD solution that allows the manufacturer to incorporate security enhancements as part of their regular device manufacturing or setup processes, ensuring that all newly-sold devices have effective, robust hardening built in. This approach also allows for considerable cost savings over a retroactive, onsite application of device-hardening components. When radioactive sources are installed prior to shipping the unit to the facility, hardening occurs at the factory. When sources need to be loaded into the unit at the facility, device hardening is installed by the manufacturer just after source loading is finished.

A typical collaborative IDD project consists of three general phases, as shown in Fig. 2. A description of each phase follows.

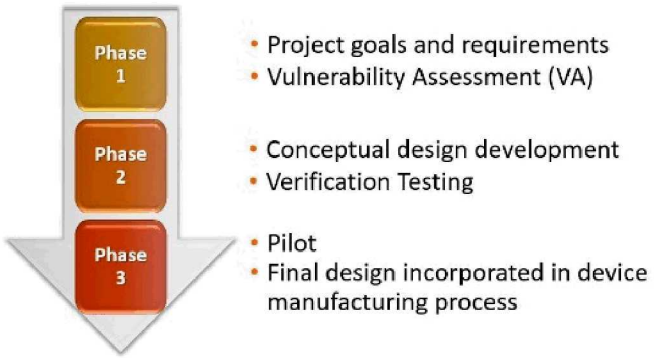

Fig. 2. IDD Collaborative Project Phases

1.1. Phase 1

A project team made up of IDD access-delay engineers and security-sensor experts, along with engineers and decision-makers from the partner company, confirm project plans and requirements. To begin the partnership, a Non-Disclosure Agreement (NDA) is signed by both parties. The NDA specifies that IDD will only share partner device design details with personnel within SNL or ORS programs who have a need-to-know. Occasionally, and with written permission from the other party, general information is provided to country regulatory bodies for the purposes of demonstrating that device safety is not affected and that a facility's physical security system can take credit for additional delay and tamper detection elements.

Project goals, requirements, and expectations are discussed and agreed-upon. One of the primary goals/expectations of these projects is to have the manufacturer adopt the final design concept as part of their routine device manufacturing or setup process. With agreements in place, a vulnerability assessment (VA), which includes device attack testing, is conducted by IDD delay experts to determine the likely attack path(s) and baseline (i.e., inherent) delay. The manufacturer is encouraged to attend device attack testing, as this is the best way for IDD to convey attack mitigation needs and allows for real-time input on facility or device considerations. A sound understanding of potential source access points as well as existing, or inherent, delay facilitates decisions regarding appropriate and adequate security design concepts. The final VA report is reviewed with the device manufacturer, and then the project team discusses potential enhancement concepts that will meet the stated project goals and requirements. With the overall goal of developing a cost-effective solution, conceptual design strategies include the following:

- Sufficient delay along attack path(s)
- Delay concentrated at the source
- Barrier materials that are difficult to cut or overcome with a variety of tools
- Use of multiple barrier materials together to create synergy and require the need for unique attack tools
- Two-person control incorporated when possible
- Tamper detection integrated into delay barriers early in the attack path, if feasible
- Removal of device components that aid an adversary's attack approach

1.2. Phase 2

This phase begins with further development of agreed-upon conceptual design(s) by the IDD access delay experts in conjunction with input on device or facility designs from the manufacturer. As delay concepts are evolving, the project team also evaluates possible tamper detection solutions and determines whether it is feasible to integrate detection into the delay elements. The detection feasibility decision is dependent upon several factors, among these are device operation requirements or limitations, additional cost, ability to interface with varied facility security systems, potential maintenance needs, etc. Refined concept designs are reviewed with the manufacturer, who will ultimately incorporate the final design specifications into their existing internal design software and processes. This ensures that all product requirements and industry standards are observed. The manufacturer provides IDD with a design package that includes drawings and design information so that prototypes of the security enhancements can be fabricated for verification testing. Prototype fabrication can be simplified as long as key elements of the security enhancement and the device are sufficiently simulated. Verification testing includes hardware fit check and attack testing to ensure that all delay and detection design goals and device operation requirements have been met.

Fig. 3. Verification attack testing

As with the initial, baseline attack testing, the manufacturer is encouraged to attend verification attack testing so that additional design modifications can be discussed and agreed upon as needed. Any changes are incorporated into a final design package, and an estimate of the cost difference for manufacturing a device with these new security features is completed. The manufacturer also ensures that all regulatory and medical-use device change approvals are secured.

1.3. Phase 3

During this phase, also called the pilot phase, the delay and detection (if feasible) solution "kit" is installed onto a new or existing device so that installation procedures, fit, and logistical considerations can be assessed and validated. If the IDD solution must be applied to a unit already in use at a facility or after sources are initially loaded on site for a new unit, coordination between the IDD team, manufacturer, end-user, ORS program team, and site security is essential to ensure that all parties are aware of roles, logistics needs, and site security-integration assistance. To protect both the manufacturer's proprietary device design information as well as security-sensitive barrier installation information, room access is limited to those with a need-to-know during the pilot. If important post-installation details are necessary, such as the need to secure only the manufacturer to handle device reload operations that involve the removal and reapplication of IDD elements, this is provided to the appropriate facility personnel. Throughout the pilot, installation issues or process improvements are captured by the IDD team and the manufacturer so that lessons learned can be incorporated into procedure or process steps for future installations. Assuming there are no significant issues that require further design modification, a pilot summary report is prepared, and the manufacturer incorporates the final design solution into their regular process so that industry quality control measures are in place. This SbD approach, therefore, facilitates the implementation of device security enhancements wherever and whenever new units are deployed.

2. XCISION GAMMAPOD™ SECURITY-BY-DESIGN PROJECT

The Xcision GammaPod™ is the first of its kind stereotactic radiotherapy system for the treatment of breast cancer. Multiple Co-60 sources within a collimated bowl continually rotate underneath the patient during treatment to produce thousands of directed beam angles. The patient table moves in all directions, which allows radiation dose to be administered across the focal spot in three dimensions.[1][2]

Fig. 4. GammaPod™ Stereotactic Radiotherapy System

When the IDD team learned of Xcision's new device, they contacted the company to see if they were willing to engage in a collaborative security partnership, to which Xcision agreed. At the time, only one GammaPod™ unit was deployed, as the company was working to complete all of the necessary medical and device approvals. The timing was perfect for device-hardening design modifications that would roll out as the GammaPod™ hit the marketplace, and an NDA was signed by SNL's IDD program and Xcision. It should be noted that IDD partnerships are voluntary, and the manufacturer's engineering resources are needed at key points to complete the project. The IDD team does its best to accommodate fluctuating or strained partner resources by sharing information through secure communication or meeting our partners at their facilities. Even as a start-up company, Xcision was able to devote the necessary engineering efforts to support the design of concept solutions. This greatly facilitated timely progress on the project.

IDD design development proceeded normally through the various project phases, concluding with a successful pilot security upgrade installation in June 2018. Attack pathways were analysed as part of the VA, and Xcision engineers were instrumental in the conceptual design process to mitigate source access vulnerabilities. Given the need to periodically resource the GammaPod™ Co-60 sources, the team went through several conceptual design iterations to address the trade-off between accommodating Xcision's need to remove and reapply delay hardware during reload operations and trying to maximize the amount of additional delay that could be gained. Xcision incorporated another device design change as well, a collimator offset feature that prevents sources from lining up directly within the collimator when the device is not in treatment mode. Due to proprietary- and security-related restrictions, actual test data and specifics about the hardening and detection solutions cannot be provided in this paper; however, the final design solution more than doubled the inherent delay of the unit, and the integrated detection indicated tamper at the start of the attack as intended.

The length of IDD projects vary but typically run about three years. From start to finish, the Xcision GammaPod™ project continued nearly four years. The reason this project ran slightly longer than average was because the team needed to complete a fit check prior to source load on a new unit and then complete the final installation of IDD hardware once the sources were in place. In addition, because the pilot would be on a newly-purchased unit, there was a good deal of coordination needed on the independent efforts being taken care of by Xcision, the site, and the site security contractor. Xcision had to complete device procurement and delivery steps that were dependent upon the end-user facility finishing room renovations at the same time room-level security system upgrades were being installed. All things considered, the coordination of efforts went smoothly.

The access delay hardware with integrated detection (called the IDD kit) was installed without significant issue or need to modify the design, and IDD has not received notification of any issues from the end-user. In April 2019, Xcision announced that the GammaPod™ radiotherapy system received CE marking, paving the way for sales in Europe. As new units are setup in hospitals around the world, they will include the security upgrade features that Xcision and the IDD team designed.

3. FURTHER INFORMATION

3.1. Author affiliation

Michal Kuca, Sandia National Laboratories, mkuca@sandia.gov, United States
Michelle Potter, Sandia National Laboratories, mrpotte@sandia.gov, United States

3.2. Xcision Medical Systems, LLC contact information

Michelle Crawley, Vice President of Operations and Sales, service@Xcision.Com

ACKNOWLEDGEMENTS

Sandia National Laboratories' In-Device-Delay program would like to acknowledge and thank Xcision Medical Systems, LLC, and in particular Dr. Cedric Yu, Peter Maton, Michelle Crawley, and Brent Webb for their commitment to radioactive material security through this collaborative partnership. Xcision's voluntary dedication to enhance the robustness of the GammaPod™ will contribute positively to global security for many years and demonstrates to other manufacturers that incorporating low-cost enhanced delay and/or detection methods can be achieved.

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.

REFERENCES

[1] XCISION, GammaPod: The Technology (2019), https://www.xcision.com/index.php/gammapod/the-technology
[2] XCISION, GammaPod Treatment Demonstration (2019), https://www.youtube.com/watch?v=_c237pfc50c