Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting
August 23-26 & August 30-September 1, 2021

DESIGNING A DYNAMIC, VERSATILE SAFEGUARDS SURVEILLANCE FLEET WITH MODERN TECHNOLOGY ADVANCEMENTS

A. Moore	K. Jenkins	J. Garner	J. Benz	J. Cree
PNNL	PNNL	ORNL	PNNL	PNNL
M. MacDougall	N. Moore	N. Smith	J. Hite	G. Westphal
PNNL	PNNL	PNNL	ORNL	ORNL

ABSTRACT The International Atomic Energy Agency's (IAEA) Next Generation Surveillance System (NGSS) maintains continuity of knowledge over nuclear material in and near storage areas and at transit points through which nuclear material can pass to supplement on-site visits [1]. Nearly 10 years after its initial development, rollout of the NGSS is approaching completion. Yet ensuring fleet effectiveness is optimized under current facility operations and IAEA surveillance needs at the time of roll out is a challenge, especially on systems that take years to design, deploy, and test. Maintaining and upgrading technology in this fleet, which in 2020 consisted of 1,530 cameras [2], is also a significant challenge. Recognizing the rapid advancements in commercial surveillance, consideration of a future generation of safeguards surveillance technology was undertaken by Pacific Northwest National Laboratory and Oak Ridge National Laboratory in 2020. The team investigated topics such as: infrared camera systems, time of flight cameras, multicamera integration and sensor fusion, self-healing encryption, in-field firmware updates, and modular platforms in an effort to identify both near-term and long-term advancements for safeguards surveillance. This paper will discuss the potential for these identified technologies to create dynamic, versatile surveillance systems, with remote, automated capabilities, as well as techniques to reduce inspector burden and enable in-field maintenance, while maintaining backwards and forward compatibility.

INTRODUCTION

Containment and surveillance (C/S) is a crucial facet of safeguards implementation around the world to supplement nuclear material accountancy by controlling and monitoring undeclared access to the nuclear material [1]. The International Atomic Energy Agency's (IAEA) Next Generation Surveillance System (NGSS) records activity around controlled nuclear material. Strategic placement of these cameras help maintain continuity of knowledge of nuclear material in a facility, specifically in storage areas and at facility boundaries to ensure material transfer only takes place at key measurement points, providing a cost effective solution for the IAEA to monitor unattended activities as a supplement to their on-site inspection visits. The research and development (R&D) community supports the IAEA in this mission by studying and developing technology to further improve these capabilities and anticipate future needs.

A surveillance system must be robust and adaptable to suit a diverse range of surveillance requirements. Some environments suffer from high radiation levels, such as spent nuclear fuel ponds or repositories; they might also be subject to extreme weather conditions and temperatures, and suffer from optical limitations such as field of view confines, light condition fluctuations, or complex background conditions in a facility. There is no one-size-fits-all solution for safeguards surveillance challenges. These various deployment environments, technological and infrastructure limitations, additional functionality in commercial off the shelf (COTS) products, eventual technology obsolescence and lifecycle costs, data security and tamper indication requirements, etc. all play large roles in complicating the development of a standard surveillance system for use in international safeguards. Nearly 10 years after its initial development, rollout of the NGSS is approaching completion. Ensuring the fleet's effectiveness will be optimized under current facility operations and IAEA surveillance needs at the time of roll out is a challenge for the scientific community,

especially on systems that take years to design, deploy, and test. Maintaining and upgrading outdated technology is also a significant challenge.

The Covid-19 pandemic also sparked consideration of additional desired system capabilities if inspectors and technicians were prevented from scheduled inspection and maintenance travel because of a pandemic, or for other reasons. Longer timespans between site visits could be managed with greater memory storage, possible remote access to the surveillance fleet, as well as in-field firmware updates to help with resiliency and to prevent lapses in coverage. Additionally, introducing greater cyber security methods, such as advanced encryption technology, as well as current image processing algorithms could help extend the capabilities of existing surveillance technology, while improving data transfer and analysis methods to help support even more remote and efficient automated operation.

Recognizing the rapid advancements in commercial surveillance, consideration of a future generation of safeguards surveillance technology has been undertaken by Pacific Northwest National Laboratory (PNNL) and Oak Ridge National Laboratory (ORNL). The team conducted a survey and preliminary evaluation of candidate commercial imaging technologies, as well as data security and image processing methods, for a follow-on to the NGSS to help inform available capabilities for the future development of versatile surveillance technology, with remote, automated capabilities; as well as techniques to reduce inspector burden and enable in-field maintenance, while maintaining backwards and forward compatibility. Some concepts from emerging technology were also studied in an effort to identify both near-term and long-term advancements for safeguards surveillance to further extend its effectiveness and ensure it remains dynamic (easily tailored to different environments, as well as easily modified and upgraded when needed) to help prevent obsolescence [3].

This paper outlines some of the promising technologies studied by PNNL and ORNL, including imaging techniques, multicamera integration and sensor fusion, self-healing encryption, in-field firmware updates, and a modular platform concept, that could be used to enhance the exiting NGSS suite or eventually be included in an NGSS replacement, or for incorporation in surveillance systems used by other agencies such as ABACC.

LEVERAGING TECHNOLOGY ADVANCEMENTS FOR SAFEGUARDS SURVEILLANCE

The R&D community is regularly seeking to advance the capabilities of current technologies to support the IAEA's verification work. It has been shown in previous C/S surveys that it is valuable to consider how developments in various non-safeguard technical fields could be applied to address current challenges. For example, a study performed to compare C/S technology used in safeguards vs transportation of nuclear materials [4] revealed that common types of active seals and closures, ageing research of various components, as well as the mutual development of the Global Identifier [5] were being developed in both groups, and advances on either side could be leveraged to inform the others' development for their specific purpose.

Similarly, numerous commercial security cameras have been developed to suit a variety of environments and applications like night vision infrared, high dynamic range (HDR), or depth processing for home surveillance, facility surveillance, or city security surveillance. Different camera types also exist for different light conditions and wavelength images for photography, optics research, medical procedures, and smart phones, to name a few. Commercial camera systems are often accompanied with an associated image processing software, but additional algorithms have been developed to enable machine learning at the camera, image reconstruction, improved image compression, and synergy in sensor fusion. The methods and technology implemented in these units could easily be applied to nuclear facility surveillance with the proper testing and modifications. Artificial intelligence could also assist with post-processing of image data to make surveillance review more efficient for inspectors and other analysts.

Since the NGSS was initially developed and deployed, advancements in communication and modularity have led to emerging technologies that can be leveraged to develop a customizable NGSS replacement. Modular platforms have been designed for innovations for smart city infrastructure such as Wi-Fiber Intelligent Station [6], Schréder Shuffle [7], and Waggle Platform [8]. This could help mitigate concerns about slow or difficult integration of new surveillance, ageing of the technology, or training burdens on staff for the introduction of new technology if the overall system still functions as before, but with new interchangeable sensors and data processing modules inserted into the platform to improve capability with a quick substitute. The ability to identify and route data by using a library to identify a peripheral device that is plugged in by a standard ID number is a common capability in many commercial devices, including phones, computers, and even some children's toys,. The same methods could be applied to these modular bases, associated sensors, and data processing units, to transmit data back to the agency rather than requiring the use of a SD card for memory during a site visit. To ensure the safety and security of these data, advancements made in self-healing encryption can be applied.

The concept of self-healing encryption, where the encryption key is updated every time a message or data packet is sent and received, has been around in various forms since the early 2000s. Self-healing encryption could easily be leveraged for transmitting other sensitive data such as surveillance images or to improve the confidence in security and tamper resistance in remote and unattended environments. Consequently, this could help address staffing limitations and concerns with site visit frequencies. More details on each of these concepts are given in the following sections.

Introducing existing technologies, either developed for a similar surveillance purpose (e.g. property security cameras) or for a different one entirely (e.g. self-healing encryption), could result in a shorter timeline from development to implementation of novel technologies and techniques, and aid in the overall lifetime of a surveillance system before it becomes obsolete. Repurposing existing technologies for another application also incites a different thought process, introducing new approaches to address challenges, or may improve the effectiveness of a solution by combining advantages from various fields of research. Lessons learned from implementation of the current fleet could also help reinforce positive capabilities to maintain, and lead developers to make modifications or additions to address surveillance challenges and desired future capabilities.

Working with different commercial partners ensures a certain level of state-of-the-art technology, as well as industry standards relating to safety and testing; however, it can lead to challenges with technology compatibility and proprietary information sharing. It restricts access and availability, as well as sustainability, of equipment since they are tied to whether the vendor supports the equipment into the future. Often, commercial technologies include various additional features that make their use for safeguards challenging, with need for extensive modification. It may be necessary to encourage a collaborative working group with multiple vendors and R&D organizations to find cost effective solutions that balance state-of-the-art technology and industry safety standards with securing and tailoring the system for safeguards (e.g. minimizing unnecessary functionality to make it easier to verify/validate).

MODULAR PLATFORMS AND MULTI- SENSOR INTEGRATION

A modular design for a NGSS replacement that uses a simple base module could provide flexibility to provide tailored functionality for virtually any deployment scenario. This proposed system would replace the existing NGSS platform due to the substantially different form factor and capabilities. This simple base would enable different plug ins for various sensors and data processing units. The simple base module would have little to no functionality by itself, beyond being able to route the appropriate data between various "capability modules" that are plugged into the board. Any functionality would originate from the capability modules themselves, while the base would only be capable of identifying a module and routing data appropriately. For example, if a system has a camera module and data storage module connected to it, the

base board would send the data from the camera to the data storage module. Adding an image analysis module, the base would direct the camera data first to the image analysis module, which may be intelligent enough to receive only raw data from the camera module. After processing and reducing the image data, the image analysis module could then send the data to the data storage module. Example capability modules could include:

- Video: standard optical camera, Infrared, 3D, time of flight, etc.
- Image/trigger analysis module: object detection, change detection, face/person detection, etc.
- Backwards compatibility: convert data from newer formats to older formats to support data transfers
- Sensor modules: Radiation/nuclear, chemical, explosive, biological, temperature, pressure, light, etc.
- Additional backup battery
- Compute module: capable of deploying other compute functions
- Data storage
- Data transmission
- External trigger devices
- Wireless module to provide wireless communications when/where/if allowed

A modular platform may also serve as a vehicle to enable multi-sensor integration, multi-spectral imaging, in-field reauthentication, and other needs. Multiple types of cameras and sensors could be integrated into each system such that the full applicable dynamic range of environmental conditions and surveillance requirements could be met, for deployment in a variety of facility types. Sensor or camera modules could be interchanged within the same form factor platform, selected specifically for each safeguards surveillance scenario or use case, to address high priority concerns. For example, if the power frequently goes out in a given facility, it may be a better trade off to have an additional battery capability module, as opposed to a specific sensor module on the board. If WIFI-connectivity is not allowed in a facility, it can easily be swapped with larger storage capabilities. This could minimize any unnecessary sensor inclusion and reduce costs associated with redesigning or manufacturing and developing specific installment and maintenance procedures for various systems.

Sensors and cameras could include multiple paired common-use cameras, specific night vision cameras, infrared cameras, other multispectral cameras, event cameras, or time of flight cameras, with image intensifiers and high sensitivity image sensors fused together in one system to provide complementary information for better resolution and performance in dynamic environmental scenarios, when needed. The relevant surveillance method could:

- be triggered to initiate recording depending on changing ambient conditions measured by the appropriate sensor in live time,
- be triggered if the image generated by the base surveillance is insufficient,
- be paired with local or remote algorithms designed to optimize brightness, contrast, and file size to enable simultaneous collection, combination, and stacking.

Testing will be needed to select the optimal combination of different sensors to reach the desired data quality, covering the full range of possible dynamic light conditions and operational environmental variations for safeguards surveillance.

There are many other added benefits that this approach provides, such as the ability for modules to be upgraded independently over time, without having to perform complete vulnerability assessment and other certification testing on the entire system, thus reducing the cost for module development and future upgrades. This may include alternative imaging solutions, new sensor designs, improved communication (beyond 5G), modern or new encryption methods, and other technological advances. Adapters may be developed to enable plug-and-play capability for older technologies, to make the overall system both backwards and forwards compatible.

The Wi-Fiber Intelligent Station is marketed as a smart, modular surveillance system, capable of connecting to city light poles and is equipped with LED lights, two-way microphones, speakers, cameras, facial and license plate recognition, in addition to various interchangeable sensors, such as gunshot detection [9]. The integrated 2G, 5G, and LTW connectivity in the modular enclosure furthers Wi-Fiber's goal is to enable a scalable, city-wide mesh network [6]. The Waggle Platform is an open source platform enabling researchers to make modifications for different projects, provided the researcher has proficiency in Linux (Ubuntu), internet networking, and web services [8, 10]. Waggle's increased complexity in its design, driven by relying on a single board computer, increases the challenges in its long-term adaptability, meaning that a redesign of the firmware and the base board may be necessary to incorporate newer sensors or expand its capabilities beyond the current suite. While the Schréder Shuffle or Wi-Fiber Intelligent Platform may be in a desirable form factor there are limitations in size, number of modules, and unknowns regarding its performance and adaptability that may not be suitable for safeguards surveillance. Furthermore, the proprietary hardware used in the Shuffle and the Intelligent Station further complicate modification for safeguards use, as well as potential unwanted functionality.

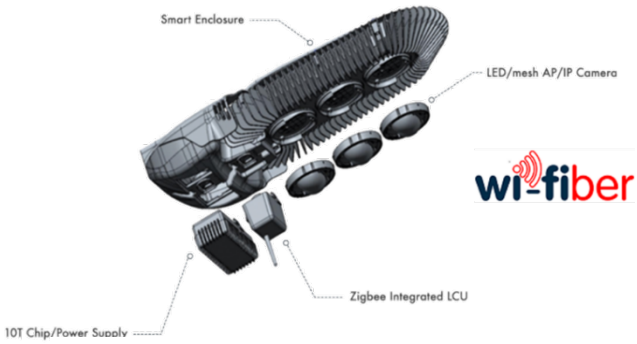

Figure 1. Wi-Fiber Intelligent Station [6]

These three products serve as examples of what can be done with existing technology and how industry has found a market for modular camera/sensor systems in smart cities, but more vetting and development would be required to determine suitability for an IAEA system. Furthermore, a modular system with limited base functionality tailored for safeguards surveillance provides an interesting challenge that industry will likely not need to tackle. Because of this, it may be necessary to design a NGSS modular platform replacement from the ground-up. An investigation into a simple base station, including data routing and communication methods, was recently completed by Texas A&M University, with input from a PNNL advising team [11]. The students created a motherboard that contained the necessary logic and circuitry to communicate with other ports and slots for multiple modules. The software on the base station would "address" other modules individually. This would prevent a third party from tapping into the base station and sniffing out "broadcast" transmissions. Each module slots into a 3D printed enclosure and is locked in place with a screw. Each screw can be covered with tamper evident tape to ensure validity of the data collected.

Smart phones, as well as commercially available cameras and surveillance, already take advantage of multicamera/multi-sensor integration on the same base module to provide better picture quality based on the need. Current models of the Apple iPhone, Google Pixel, Nokia 9, and Samsung Galaxy, among others, have two or more rear cameras that enable zoom, better HDR for high light scenarios, portrait mode that exploits background blurring post-processing, 3D photography using depth estimation, and low-light or night photography. Each camera has a different lens for its designated application and can be selected for use based on the menu option selected within the application or user interface, which deploys the appropriate post-processing technique. These concepts could be adapted and extended to meet the needs of the safeguards community. Alternatively, commercial stand-alone surveillance systems could be adapted for safeguards surveillance, including the necessary security measures currently in place for tamper indication and data transfer taken by the IAEA. More robust and radiation tolerant technologies or proper shielding methods would be needed for a safeguards surveillance system to increase physical security and prevent radiation damage in nuclear environments. The minimized form factor within smart phones is not a restriction for a safeguards application, and so an integrated multicamera system could incorporate robust

shielding as well as local processing hardware. However, these modifications could potentially negate some of the cost benefit obtained through mass-production from these vendors.

Various models of the AXIS Communications have multiple tiltable and exchangeable lenses for large fields of view, enhanced light sensitivity using an infrared cut filter that can be enabled or disabled based on the lighting condition, as well as wide dynamic range, thermal and visual surveillance cameras, pan, zoom, and tilt functionality in indoor or outdoor conditions, control over the compression, maximum frame rate, individual image alignment, brightness, saturation, sharpness, white balance, exposure, shutter speed, etc., where the video stream may be accessed through its IP address with respective password protection. Camera tampering alarms may also be enabled on some systems. Some commercially available security surveillance systems also implement HDR capabilities to address the need for reliable surveillance in changing light conditions [12, 13, 14, 15]. If financially viable, a multi-sensor or multicamera system could substantially improve the capabilities of surveillance in the field.

If multi-sensor integration is not possible due to technical requirements and cost restrictions, existing NGSS system settings could be evaluated for their impact on current system performance. HDR cameras, when combined with respective post processing algorithms, can provide images similar to what the human eye can perceive, adapting to a broader range of environmental luminance. It is possible that the NGSS may have the ability to operate in HDR. If HDR could be enabled, this would lengthen the lifetime if paired with new sensors to address dynamic operation concerns. The computational capabilities would need to be expanded beyond what is currently available in the NGSS, in order to perform the different post-processing tasks to produce the desired data and image compressions. Alternatively, post-processing of raw images could be pushed to a separate system which receives data from the integrated camera, either through hardwiring or by leveraging wireless communication capabilities (including those still being researched, including advanced wireless communication protocols enabling edge computing and other over-the-air functionality).

OPTICAL ADVANCEMENTS: CAMERAS AND IMAGE PROCESSING ALGORITHMS

Over the last decade (and previously) there have been large strides in optics research for various applications. The associated ORNL paper [16] reports on several technologies for their application to optimize safeguards surveillance. Here, one example imaging technique, leveraging polarization, is presented. Many polarization cameras have been marketed for laboratory use or for conditions that are relatively constant, due to polarization cameras strengths in seeing changes in material properties (texture, strain, etc.) against a uniform background. However, commercial markets for medical and surveillance applications are emerging. There are different commercial polarization cameras manufacturers including: Lucid Vision Labs, FLIR, Allied Vision, PixeLINK, Polaris Sensor Technologies, and Bossa Nova. In addition to the different styles of polarization image acquisition mentioned above, many companies have proprietary image analysis software.

Polarization Cameras

Standard optical surveillance systems record a scene through wavelength (color) and intensity information. Polarization cameras add an additional dimension, recording the polarization of incoming light (the filtering of light to confine its oscillations to one or more specified directions) to provide additional contrast of targets of interest and increase the effective resolution [17, 18, 19]. These types of cameras can work in multiple ways, including employing a fixed polarization filter, using a rapidly switching LCD polarizer lens, polarized camera arrays using fixed polarizers, or by integrating polarizing filters directly onto the camera's charge-coupled device (CCD) array [20]. Using a fixed polarization filter is the lowest cost option, but it generally requires manual orientation of the filter, only filters light reflected on a narrow range of angles, does not work well with wide field of view (fisheye) lenses, and does not work well in low light

conditions. Polarized camera systems are generally less sensitive in low light situations due to the polarizer reducing the intensity of light by half (due to the nature of light waves where the electric field and magnetic field components of the wave are always perpendicular to each other). Additionally, polarized imaging does not generally work well with wide field of view cameras because the high curvature of the lens alters the polarization of incoming light [21]. This effect can be mitigated with image processing but it is an additional complication.

The benefit of a polarization camera is maximized by a camera system able to record multiple polarizations; however multiple lenses or integrated filters are more expensive than a traditional camera and may require postprocessing for optimal image storage. A polarized CCD array is the most common type of polarization camera. By measuring multiple orthogonal polarizations on the CCD detector, one can increase target contrast, especially with the use of post processing for further detail. This can be especially useful to distinguish objects with similar color and intensity of light and different reflective properties including texture, index of refraction, orientation, etc. The use of polarization can clarify images in nearly all environments, thus aiding in useful surveillance features such as object recognition and triggering. Having already been studied for its potential use in nuclear safeguards swipe sampling inspections and tamper indication [22], this technology shows promise in its applicability for surveillance.

Additional potential benefits include reducing glare and reflected light on objects such as spent fuel pools, reducing the intensity of external light (e.g., sunlight, in outdoor environments and providing a clearer image in such situations), and limiting the oversaturation of images/video in dynamic lighting environments such as surveillance in a covered outdoor area with both shade and sun. Rejection of reflected light can improve the viewing of a reflective surfaces that may overwhelm a traditional camera or reduce haze [18, 23]. The high degree of polarization from reflective surfaces generally leads to an easier distinction between liquids and solids, which would allow easier detection of situations such as identifying leaks from containers at due to changes in the effective smoothness of the container (or floor) when covered in a liquid.

CYBER SECURITY

Cyber security is a critical component of current and future safeguards applications. As the world progresses to a more virtual, remote landscape to improve efficiency, and cyber attacks become more prominent, having the proper security in place to prevent breaches becomes increasingly significant. Additionally, the cyber security in place on systems must be continually evaluated and updated to be effective against emerging threats. Existing security features for stored surveillance data include measures to ensure access to the stored files is granted only to an authenticated user; the DSA 2K cryptographic authentication and AES 128-bit cypher block chaining (CBC)-mode image encryption [24] provide robust data security equating to 3.4·10^38 possible combinations, which cannot be defeated by any practical methods due to the amount of data storage required to perform a brute force attack. However, additional measures will further improve security, as well as techniques to reduce inspector burden and enable in-field maintenance.

Self-Healing Encryption

Where the self-healing approach really finds value is when there are large numbers of messages being transmitted between two entities, either uni- or bi-directionally. Additionally, the encryption algorithm at the heart of self-healing encryption can also be used as a secure mechanism to distribute keys to many users over untrusted or unreliable networks. Forward security and post-compromise security were developed, along with encryption algorithms to implement, to prevent an attacker from obtaining access to historical information as well as future information secured by compromised keys. Forward security means that previous communications remain secure in the event of key compromise. Post-compromise security means that future communications remain secure in the event of key compromise. These are accomplished in self-

healing encryption algorithms by updating the encryption key every time a message or data packet is sent and received.

The self-healing algorithm approach may potentially alleviate the need to rekey a system with a visit, and more importantly generate trustable data by limiting the impact of a tamper event through limiting the window in which data is compromised to the time between subsequent messages. Self-healing encryption can mitigate the damage (reputation, resources to fix, data integrity) from compromised keys used on equipment in untrusted environments. In future equipment, implementation of this approach could allow equipment to securely communicate within a group, enhancing the capability for triggering off events or actions by or on other equipment.

A potential weakness is the amount of computation power required to implement this process, based on the number of entities in the group where messages are being exchanged [25]. Another potential issue requiring further research is the ability to integrate the algorithm into existing equipment security and communication protocols and infrastructure. The outstanding unknowns pertain to if such approaches are compatible with existing equipment to maintain backwards compatibility, and if so, how would such approaches be implemented in a cost and resource effective manner while enabling full security capabilities of previous and future message protection if a key is compromised. The implementation must accommodate a variety of message types like state of health, video, still images, etc. If properly implemented, a self-healing encryption has the potential to significantly benefit data security and key control, supporting the use of unattended and remote monitoring at facilities worldwide.

In-Field Firmware Updates

Firmware updates are currently performed at IAEA Headquarters. Inspectors are tasked with uninstalling the existing camera system, and replacing it with an updated system, then transporting the outdated system back to the IAEA for its own update. In-field firmware updates can be as simple as inserting a USB stick with the appropriate updates, however, it has the possibility of requiring advance coding experience from the installer to troubleshoot errors. Furthermore, security is a concern, including alteration to the provided firmware update, replacing the intended firmware with unauthorized firmware, using the authorized update on unauthorized equipment, and reverse engineering [26].

In-field update techniques would allow inspectors to update the firmware of their equipment in-situ rather than requiring it to be sent back to IAEA headquarters. In-field update processes are used for many commercial products, with a variety of tools used to perform the task. Securing in-situ routine maintenance like firmware updates is so commercially prevalent and documented that it may be possible to find or develop a similar process for IAEA equipment like the NGSS. This process would reduce the need for the inspector to transport the camera and installation equipment (reducing the physical burden), reduce the time needed for an inspector to be onsite or at least the time dedicated to this maintenance activity, and reduce the overall required camera inventory needed to maintain up to date functionality. Furthermore, in-situ techniques could potentially eliminate the need for an inspector to be on site by enabling a securable method for the host to install the firmware and receive the stored data files via encryption. In order to begin moving update procedures to the field, commercial implementation of in-field firmware updates should be understood to determine feasibility for components within the NGSS or integrated into a future design.

Integrity Scanning of Secure Digital (SD) Cards

Currently, data stored from the NGSS are offloaded using an SD card. The SD card is typically retrieved from the system when operating in a stand-alone configuration, with a new SD card inserted to replace the old. The stored data files are later downloaded to a computer for review. Despite robust security measures taken to control access to the stored data, there is no implemented method to ensure malware has not compromised the SD card during the reading of the internal storage. Because the current data collectors

operate on embedded processors without an operating system, they are immune to potential corruption that could impact the server; however, depending on future needs and data analysis methods for the next generation of surveillance, this may not remain the case. Therefore, prior to offloading data from the SD or reinserting it into the camera or some other device, it should be scanned for malware or corruption.

Malware detection scans could be performed both when entering and leaving the computer for verification that neither device will be compromised, whether that's a local computer at the site, a laptop carried by an inspector, or a computer used for analysis at the Agency, or within the NGSS in-situ to protect the system through routine checkups. The integrity of the card can then be verified with minimal steps from the user, with detailed logs of the scanning results for future reference should the need arise to investigate. A simple, commercially available solution for this problem may be found by turning to existing cybersecurity scanning technology implemented in media kiosks already deployed in nuclear facility environments and national laboratories. The components may be modified to fit the form factor and needs of the NGSS, such that the scanning hardware and malware detection software could be adapted to fit within the existing housing or within an associated computer. Or, with little modification, existing commercial systems could be deployed at the Agency or through a mobile platform provided to inspectors for onsite scanning. Various vendors, such as OPSWAT [27], Tresys/Owl Cyber Defense [28], Odix [29], GateScanner [30], among others, offer different malware scanning technologies as well as supportive servers, clouds, data vaults, and centralized management platforms; they also offer customizable options for their commercial systems. However, the security requirements to which these technologies have been tested may not match the requirements, as currently designed, for the desired criteria of the IAEA.

CONCLUSION

Each of these technologies or approaches may serve as a stand-alone improvement to existing surveillance methods, however, many of these solutions have the potential to be combined to address multiple challenges or enhancement strategies. These different topics aim to address current concerns of cyber security, inspector, and fiscal burdens, while introducing advanced optic capabilities, robust and sophisticated image processing algorithms, to develop a fleet of surveillance technology that is easily tailored to different environments, as well as easily modified and upgraded when needed, with remote, automated capabilities for a variety of nuclear facility environments. Ultimately, these features would provide improved performance, security, cost effectiveness, and an extended lifecycle for the next generation of surveillance.

ACKNOWLEDGEMENT

The work presented in this paper was funded by the National Nuclear Security Administration of the Department of Energy, Office of International Nuclear Safeguards.

REFERENCES

[1] I. A. E. Agency, "International Nuclear Verification Series No. 1 (Rev. 2). Safeguards Techniques and Equipment: 2011 Edition," Vienna, 2011.

[2] IAEA, "IAEA Safeguards in 2020," [Online]. Available: https://www.iaea.org/sites/default/files/21/06/sg-implementation-2020.pdf.

[3] IAEA, "Safeguards in practice," [Online]. Available: https://www.iaea.org/topics/safeguards-in-practice. [Accessed 2021].

[4] K. A. Jenkins and A. S. Moore, "Gap Analysis of Material Control Technologies for Safeguard Applications. PNNL-29442.," Pacific Northwest National Laboratory, Richland, WA, 2019.

[5] J. White-Horton, "Establishing a Global ID for UF6 Cylinders: 2009-Present," in *19th International Symposium on the Packaging and Transportation of Radioactive Materials*, New Orleans, LA, 2019.

[6] Wi-Fiber, "Next Generation Smart Lighting," [Online]. Available: ttp://www.wi-fiber.us/edge_compute.pdf. [Accessed 2020].

[7] Schreder, "Shuffle," [Online]. Available: https://www.schreder.com/en/products/shuffle-smart-multifunctional-column. [Accessed 2020].

[8] Waggle, "About," [Online]. Available: https://wa8.gl/. [Accessed 2020].

[9] C. Moore, "Wi-Fiber is creating safer cities by combining wireless tech, smart streetlights," 2018.

[10] R. Sankaran, P. Beckman, C. Catlett, R. Jacob and K. Keahey, "Waggle: A Framework for Intelligent Attentive Sensing and Actuation".

[11] SIDE-Technology, *Simple Base Station User Manual,* 2021.

[12] AXIS, "AXIS Q3708-PVE Network Camera," [Online]. Available: https://www.axis.com/files/manuals/um_q3708pve_1525419_en_1604.pdf. [Accessed 2020].

[13] AXIS, "AXIS Q3709-PVE Network Camera," [Online]. Available: https://www.axis.com/products/axis-q3709-pve. [Accessed 2020].

[14] AXIS, "AXIS Q6010-E Network Camera," [Online]. Available: https://www.axis.com/products/axis-q6010-e. [Accessed 2020].

[15] AXIS, "AXIS Q87 Bispectral PTZ Network Camera Series," [Online]. Available: https://www.axis.com/en-us/products/axis-q87-series. [Accessed 2020].

[16] J. Garner, K. Jenkins, J. Hite and G. Westphal, "Contemporary Optical Surveillance Technologies," in *INMM & Esarda Joint Annual Meeting*, 2021.

[17] Get-cameras, "Polarization camera whitepaper explains how polarizaiton filters work," [Online]. Available: https://www.get-cameras.com/polarization-camera-whitepaper. [Accessed 2020].

[18] X. Wang, J. Ouyang, Y. Wei, F. Liu and G. Zhang, "Real-time vision through haze based on polarization imaging," *Appl. Sci.,* vol. 9, no. 1, 2019.

[19] J. Smoke, "Comparison of Polarirametric Cameras," 2017.

[20] L. V. Labs, "Going Polarized: Polarization Adds a New Perspective," 2020. [Online]. Available: https://thinklucid.com/polarization-white-paper/.

[21] S. S. Lin, K. M. Yemelyanov, E. N. Pugh and N. Engheta, "Polarization enhanced visual surveillance techniques," in *IEEE International Conference on Networking, Sensing and Control*, 2004.

[22] M. Bliss, B. Bernacki and K. Kaplan, "Polarization Imaging for International Safeguards: Fiscal Year 2019 Report. PNNL-29702," 2020.

[23] Y. Zhao, Q. Peng, C. Yi and S. G. Kong, "Multiband Polarization Imaging," *J. Sensors,* vol. 2016, 2016.

[24] SNL, "The NGSS, an Overview and Discussion," 2012. [Online]. Available: https://www.osti.gov/servlets/purl/1116295.

[25] *The Messaging Layer Security (MLS) Protocol, draft-ietf-mls-protocol-03.*

[26] T. Instruments, "Secure In-Field Firmware Updates for MSP MCUs, Application Report SLAA682," November 2015. [Online]. Available: https://www.ti.com/lit/an/slaa682/slaa682.pdfts=1600457904949&ref_url=https%253A%252F%252Fwww.google.com%252F. [Accessed 2020].

[27] OPSWAT, "OPSWAT Comparison Guide MetaDefender Kiosk," [Online]. Available: https://www.opswat.com/uploads/assets/files/OPSWAT_ComparisonGuide_MDKiosk-global_20200403_USLetter.pdf. [Accessed 2020].

[28] O. C. Defense, "XD Air," [Online]. Available: https://owlcyberdefense.com/product/xd-air/. [Accessed 2020].

[29] odix, "odix Kiosk," [Online]. Available: https://www.odi-x.com/odix-kiosk/. [Accessed 2020].

[30] GateScanner. [Online]. Available: https://www.sasa-software.com/products/. [Accessed 2020].