SAND2014-15052C

Standoff Video Surveillance for High Radiation Applications

George Baldwin, William Sweatt, and Maikael Thomas
Sandia National Laboratories
Albuquerque NM USA
gtbaldw@sandia.gov; wsweatt@sandia.gov; mthomas@sandia.gov

ABSTRACT

Video surveillance cameras used for safeguards applications have grown progressively more sophisticated and costly. It would not be prudent to deploy such high-value equipment directly in high radiation areas, contamination areas, confined spaces, or other harsh environments. International nuclear material safeguards could easily desire video surveillance of activity within hot cells, spent fuel shearing operations for reprocessing, or in storage facilities. Camera performance and life could be compromised; moreover, the camera would be difficult to maintain and service.

We consider instead a practical means to deploy a high-value safeguards camera some distance removed from the scene of interest. Video surveillance would still be possible if an image could be piped to the camera. Likely an image pipe will incorporate shielding windows and/or offset paths using mirrors to penetrate a shield wall. Practical implementations will differ from case to case, but in this work we pose a generalized application scenario. The scenario simplifies the problem for the purpose of determining requirements, developing an approach, and eventually demonstrating a feasible solution for “standoff” video surveillance.

The three primary technical challenges for standoff video are (1) devising an optical architecture for relaying images from the scene of interest to the camera, (2) ensuring the authenticity of those images, and (3) ensuring that optical components closest to the scene are “radiation hard.” For the first problem, various transparent optical-quality plastic light guides and/or fiber bundles might be considered, but these can fail in radiation environments. In our baseline scenario, we instead replace the camera objective lens with a relay lens system that transmits images over a straight path in air. The camera sensor and the surveillance objective lens are arbitrarily chosen to be two meters apart. The second problem recognizes that digital authentication at the camera’s image sensor is insufficient; that the extended optical path is vulnerable to tamper. We therefore devise a means to test authentication approaches to ensure the image integrity through the extended surveillance system. Eventually we will evaluate the front-end optical components and in-scene authentication devices for radiation hardness, but that is beyond the scope of this paper.

1. INTRODUCTION

Because human resources are often limited and costly, onsite inspection must be supplemented with automated systems for information collection. Such technology-intensive monitoring and verification can encompass a variety of sensors, but video cameras are still relied upon as the primary tool providing the “eyes” (if not the ears) of a human inspector. Cameras have limitations, of course. They are usually tied to fixed locations, they rely on external scene lighting, their view can be blinded or blocked, and they would produce unmanageably large data streams unless a large fraction of the acquired time history is discarded. Moreover, they are at risk of being spoofed, such as the live scene being replaced instead by a picture of the scene, so-called "before the lens" tampering. Nevertheless, video cameras are widely used in remote monitoring for nuclear material safeguards.

In some situations, video surveillance also may be desirable to "go" where a human inspector cannot go, or even where it is better not to go, such as into high radiation areas, contamination areas, confined spaces, or other hazardous environments. However, many of those same hazardous environments are also not ideal places for technologically sophisticated and expensive camera electronics. In this paper, we explore "standoff" approaches, which are ways to employ video surveillance while keeping the camera safely out of a hazardous environment. Only minimal "front end" image collection optics would be exposed to the hazards. The task is then how to relay the image truthfully from the scene to the camera.

A hot cell is one example where video surveillance may be desired because of safeguards interest. High radiation and radioactive contamination are the primary hazards. Viewing the hot cell from the outside, with a camera looking through an existing shield window, would be complicated. Typically the space immediately in front of the window must be kept free for an operator working with a master-slave manipulator. So as not to interfere, the camera would have to be situated behind the operator, where the field of view is limited and easily blocked. Such constraints are likely not acceptable for surveillance. Presently, locating the camera inside the hot cell is the only alternative, assuming that a camera would be able to function there.

We instead consider installing within the hot cell the *least* amount of optical hardware necessary for surveillance, i.e., only the objective optics that gathers an image. We relay an image to a camera on the outside, via an optical path through the shield wall. Figure 1 illustrates such a hypothetical application where the surveillance would be from an upper corner of the room. The

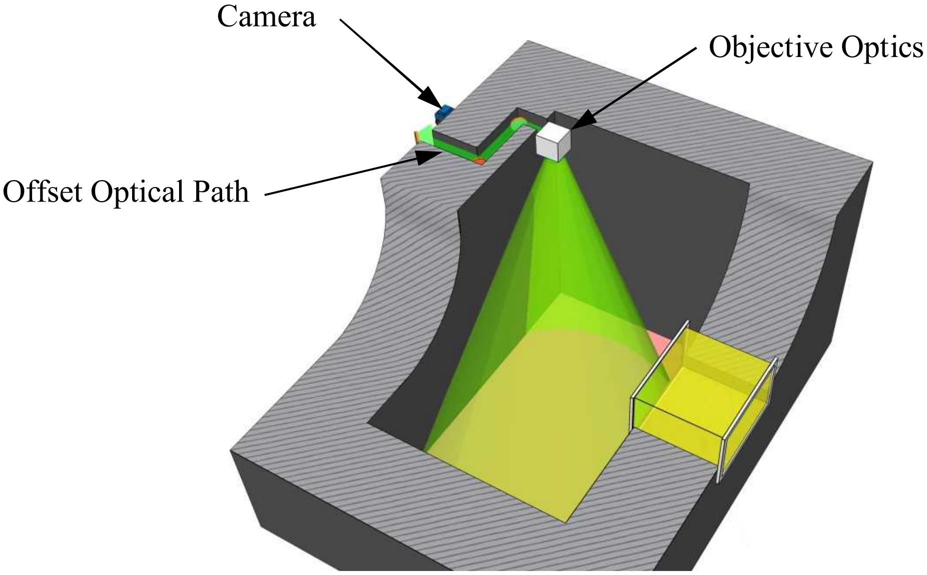

Figure 1. Surveillance of hot cell

image relay uses mirrors and an air pipe, with an offset to reduce radiation streaming and perhaps also a window for a contamination seal.

Another safeguards application might be for underwater spent fuel storage, particularly where fuel may be obscured by stacking arrangements, as depicted in **Error! Reference source not found.**. Depending on the purpose of the surveillance in this case (e.g., to inspect particular assemblies, or count the number of assemblies present), it may also be necessary to be able to move the objective optics within the space between the fuel storage levels.

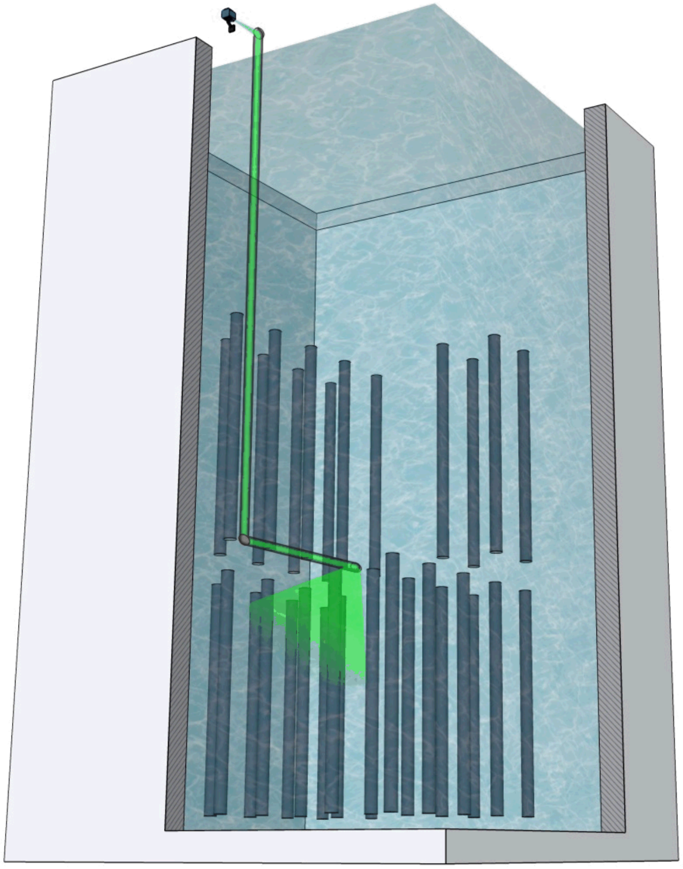

Figure 2. Schematic of standoff surveillance of vertically-stacked fuel assemblies in a cooling pond

2. PROBLEM DEFINITION

2.1. Generalized Application Scenario

Practical implementations will differ from case to case, so for the purposes of this work we define a "baseline" scenario to represent a generalized application. Actual applications likely introduce additional complexity, but the baseline scenario, illustrated in Figure 3, allows us to isolate the fundamental issues common to most all applications. The scenario simplifies the problem for the purpose of determining requirements, developing an approach, and eventually demonstrating a feasible solution.

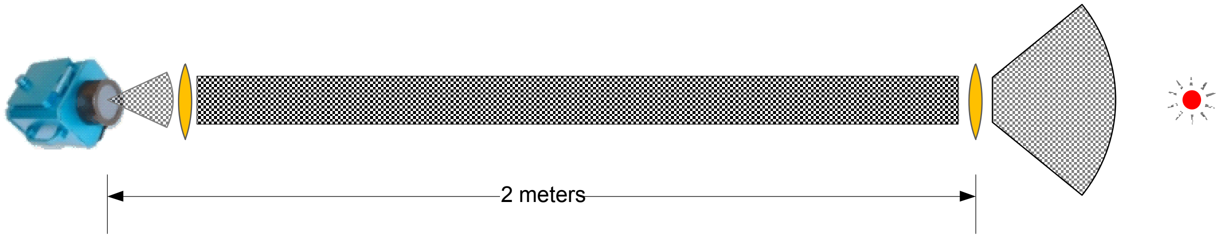

Figure 3. Baseline scenario for standoff image collection

The common features for standoff video include (1) objective optics at the “front end” of the surveillance system, where the image originates, (2) an appreciable separation distance between the objective optics and the camera’s image plane, and (3) a coupling of the piped image to the image plane of the camera.

The objective optical elements comprise the only parts of the system that must exist in the hazardous environment. Although conceivably one could consider selecting a radiation-hard glass lens for this purpose, we suggest that reflective mirrors, which are inherently radiation-hard, would be a more robust alternative. In Figure 4, we illustrate a system including a concave mirror that subtends a field of view of at least 45 degrees. Image distortion can be corrected in software.

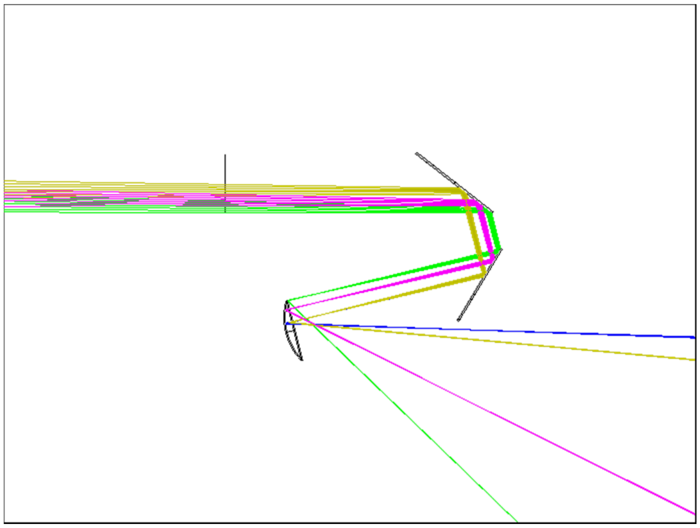

Figure 4. Front end objective mirror system for image collection, subtending 45-degree or greater field of view

The separation distance could vary considerably depending on the particular situation. In the baseline scenario, we have arbitrarily assumed a straight two-meter optical path, a scale representative of a typical concrete shield wall thickness. We have further assumed that the path is in air. To exclude ambient light, we enclose the path in an opaque-walled pipe.

For the camera, we use the model “NGSS DCM-C5” available from Canberra Industries.[1] The DCM-C5 has a 5-megapixel CMOS image sensor, processed to one of three output resolutions, 320x240, 640x480, or 1280x960 pixels.

For typical video surveillance applications, the DCM-C5 uses one of two lenses, standard (58mm) or fisheye. Such focal lengths are not well-suited for the standoff application. Instead, a telephoto lens is required to couple the piped image to the camera. We have chosen a 225mm focal-length relay lens for demonstrating the baseline scenario. Such a "long" lens also is generally not compatible with the camera housing, either, and custom hardware is necessary for connecting the camera to the optical pipe.

2.2. Image Authentication

There are two basic approaches we considered for image authentication: 1) establishing the continuity of the standoff optical path, and 2) in-scene authentication.

In the first approach, the authentication measure would assure us that the extended optical system is intact, between the front-end objective optics and the camera. In other words, whatever enters the front-end objective optics is identically what is relayed to the camera's image plane. No substitute image has been "patched in."

Such an approach can be realized by incorporating an active light source at the front end that can be controlled remotely by the camera owner (inspector). The light source itself might be located at the camera end and conducted to the front end via an optical fiber, and there merged with the image signal. The front end components would need to be radiation hard. Observing the artificially-superimposed source in the image would confirm the integrity of the standoff optical path. The active source could involve various combinations of spectral, timing, and intensity modulation.

When combined with the cryptographic authentication of digital data originating from the camera, continuity of the standoff optical path provides the same level assurance as conventional video surveillance systems without standoff.

In the second approach, in-scene authentication, the assurance extends to the scene under surveillance itself. In-scene authentication further protects against so-called "before the lens" tampering, which in principle is a defeat scenario even for conventional video surveillance systems. The basic approach is to create some controlled modification of the actual scene, confirmed in the recorded image, to provide assurance of image authenticity.

The specific means for authenticating the standoff video image is the subject of continuing research. Our first step is to create an experimental setup that readily permits us to test authentication approaches, e.g., against identical image scenes lacking authentication. With such a setup, it is possible to demonstrate why authentication is essential for us to trust the surveillance images.

2.3. Multiplexed image sources

We therefore incorporate one additional "feature" into our baseline scenario to enable comparative tests. We create two identical optical paths, and join them with an optomechanical switch, as shown in Figure 5. By thus multiplexing two sources, potentially conveying the same apparent scene, we can readily explore and demonstrate image authentication.

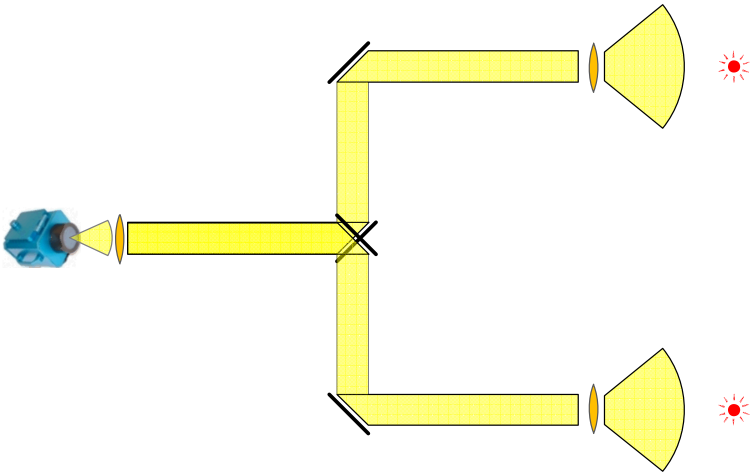

Figure 5. Selectable optical path for testing authentication.

3. DISCUSSION

3.1. Benefits

Several benefits accrue from a practical standoff surveillance capability. One is the ability to do video surveillance in certain situations (e.g., within hot cells) that otherwise would not be possible or practical without standoff. Servicing and maintenance are facilitated when the camera is readily accessible. In-scene authentication methods for standoff video might easily be adapted to standard video surveillance applications, which would strengthen the authentication assurance. The multiplexing of various optical paths to a camera might also be explored as a means to leverage an expensive camera installation for multiple image sources.

3.2. Alternative approaches

The generalized scenario we have pursued assumes a fixed surveillance location. There may be cases where it would be desirable to change the view. If it is only a matter of pointing (e.g., pan and tilt), it may be possible to work with the same basic approach using air pipes and mirrors, yet incorporate remote control of the front end surfaces to change the view. In a practical sense, optical zoom would not be possible with the air pipe and mirror approach, because it would require changing the curvature of the objective mirror.

In other situations, such as the spent fuel cooling pond example described in the Introduction, there may be a need to move the location of the surveillance, as well as its pointing. This may still be possible with suitable remote manipulation of the optical pipe sections and their coupling mirrors. Again, any part of the system within the hazardous environment must be able to perform reliably under remote control.

A coherent fiber optic bundle to that is tethered to the camera is another idea that is tempting to consider for a flexible, movable standoff. However, optical fibers will blacken with radiation exposure, so the approach may have limited utility. The fiber bundle requires an objective lens coupled to its front end to create the image. Both the fiber bundle and image-forming lens would need to be of radiation-hard glass, but the glass transparency may still degrade over time. Flexibility of the glass fiber bundle may be limited. At the camera end, the end of the fiber bundle needs to be fixed very close to the camera's digital sensor for good coupling, because the light from the individual fibers spreads (and the image thus blurs) with the separation distance.

3.3. Next Steps

A variety of image authentication ideas will be tested over the next several months using the baseline scenario for standoff video surveillance. Assuming that we identify a satisfactory image authentication option, the laboratory-scale tests will be followed by a field demonstration. The development is possible even without deploying in an actual high radiation or other hazardous environment, since the front end mirror components are not susceptible to radiation degradation.

4. CONCLUSION

The eventual capability for authenticated standoff video surveillance would facilitate safeguards implementation in hostile environments, such as hot cells and spent fuel pools. We have developed a stepwise approach to investigating image authentication for standoff video surveillance, featuring a mirror-based image collection system coupled via air pipe to a remote camera. The first step is to demonstrate that an image from the surveillance field of view can be acquired at a distance from the camera. The second step introduces measures for authenticating the image over that standoff separation distance. A third step incorporates a more complicated optical path allowing offsets to prevent radiation streaming. At this stage, the system is able to switch readily between different image sources for comparing authenticated and non-authenticated images. A fourth step develops options for in-scene authentication of the surveillance images. In future work, we could consider movable standoff paths.

ACKNOWLEDGMENT

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration (NNSA) under contract DE-AC04-94AL85000. The authors gratefully acknowledge funding support from the NNSA Next Generation Safeguards Initiative.

SAND2014-XXXXX.

[1] http://www.canberra.com/products/safeguards_surveillance_seals/pdf/DCM-C5-Camera-C38711.pdf