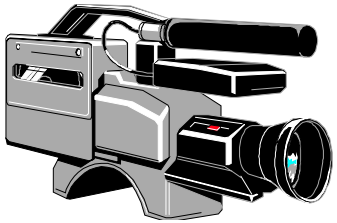
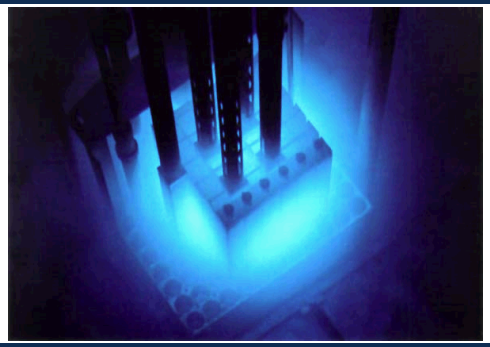
SAND2014-18029PE

Exceptional service in the national interest

Sandia National Laboratories





Authentication Approaches for Standoff Video Surveillance

George Baldwin, Shane Sickafoose, William Sweatt, and Maikael Thomas
Sandia National Laboratories

IAEA Safeguards Symposium
Vienna, Austria
October 23, 2014

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

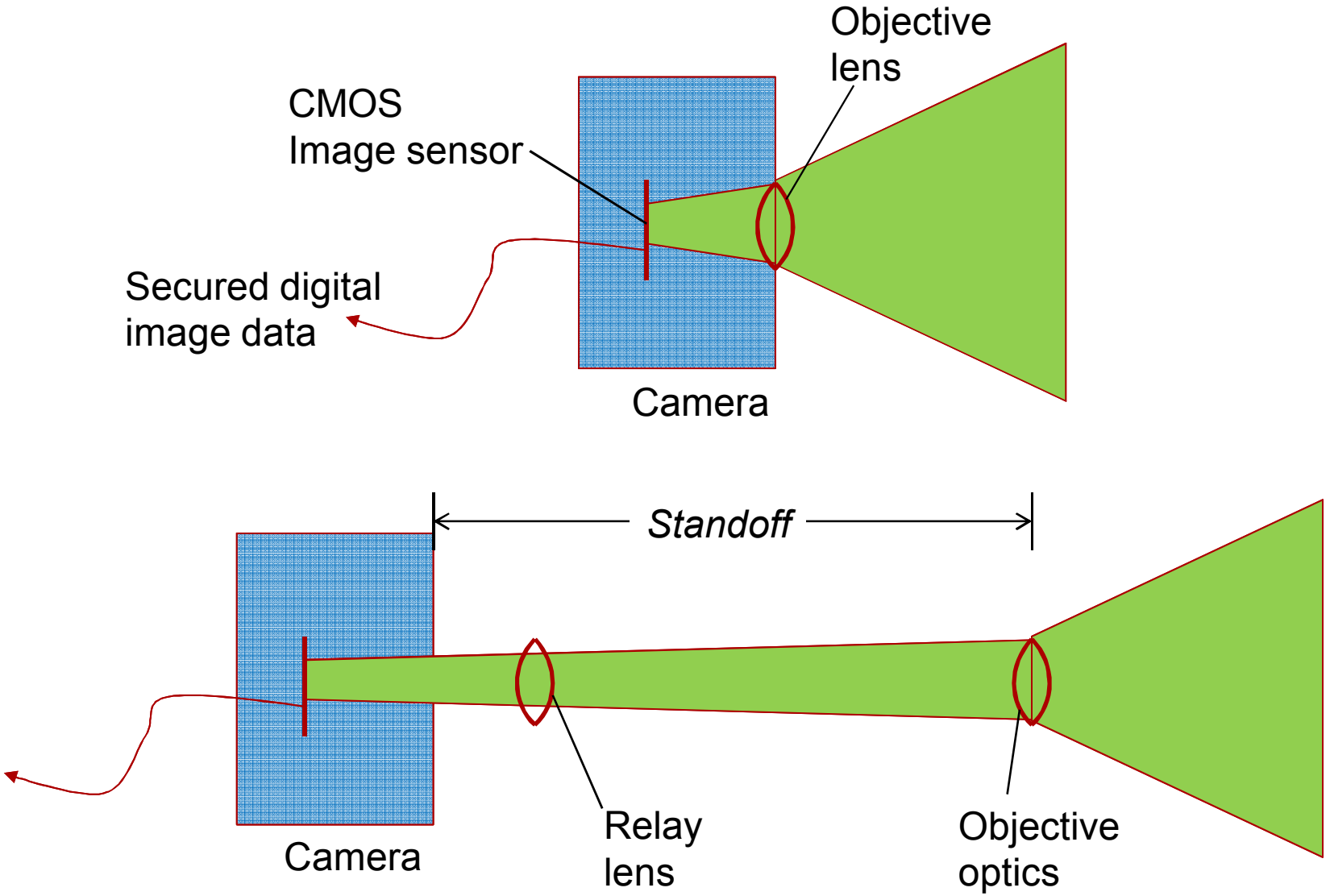
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Outline

Sandia National Laboratories

- Standoff video surveillance
  - What is it?
  - Where would it be useful for safeguards?
- Authentication of video images
  - The problem
  - Approaches
- Our work: scene interrogation
- Conclusions

What is standoff video?

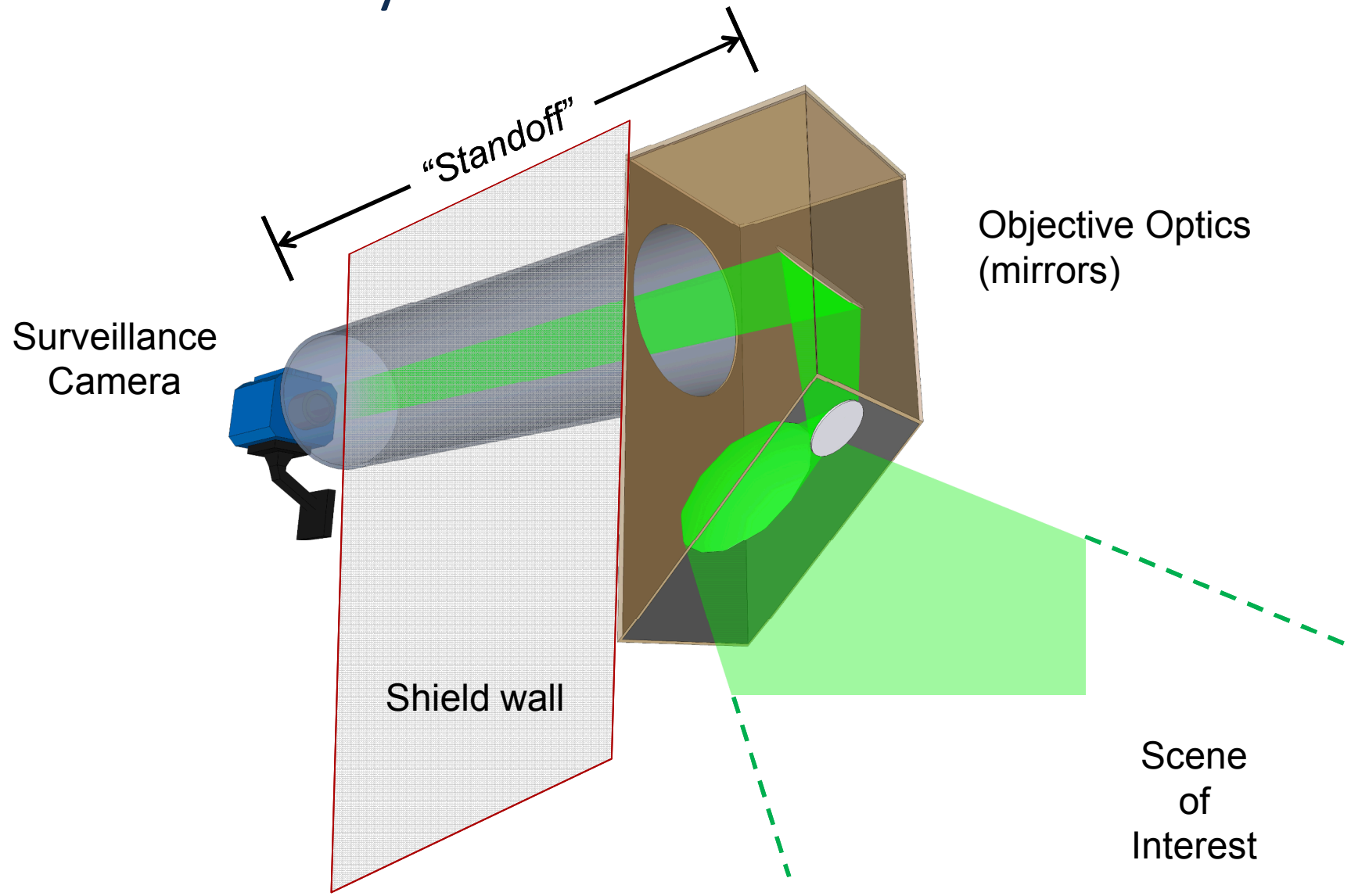


Technical approach for incorporating standoff between the camera and objective optics

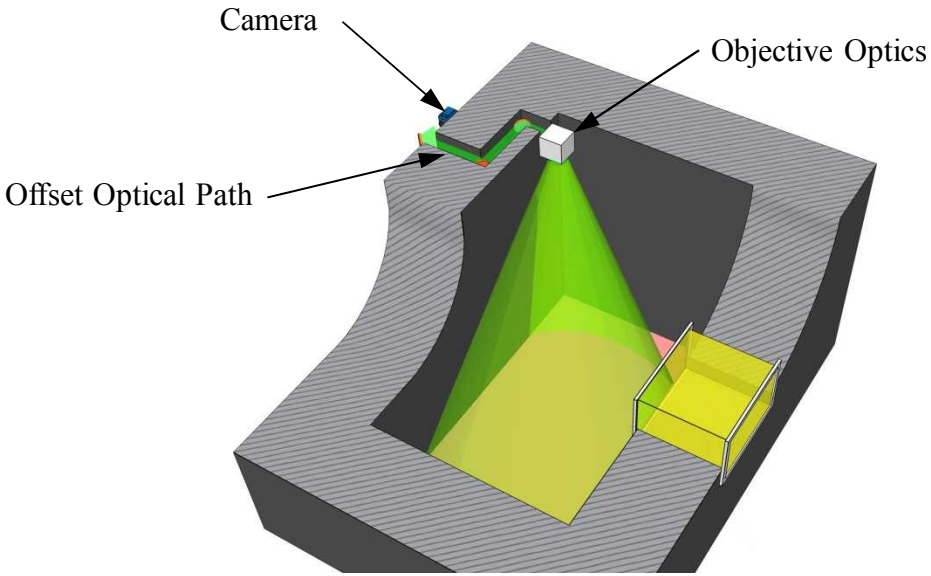
Sandia National Laboratories

- Avoid the use of transparent, refractive media at the front end
  - Such as optical fibers, lenses
  - Instead use curved-surface mirror(s) and air pipes
- Acquire a wide field of view
  - Capture a wide field of view with a curved-surface mirror
  - Acquired image will be distorted: Remove distortion in software
- Transport the image over the standoff distance
  - Exclude ambient light by enclosing in an opaque-walled pipe
  - 2”-diameter optics give adequate resolution and light through-put
- Couple the image to the camera’s CMOS image plane
  - “relay” lens (telephoto)
  - Requires a redesigned housing, lens distance to the image plane

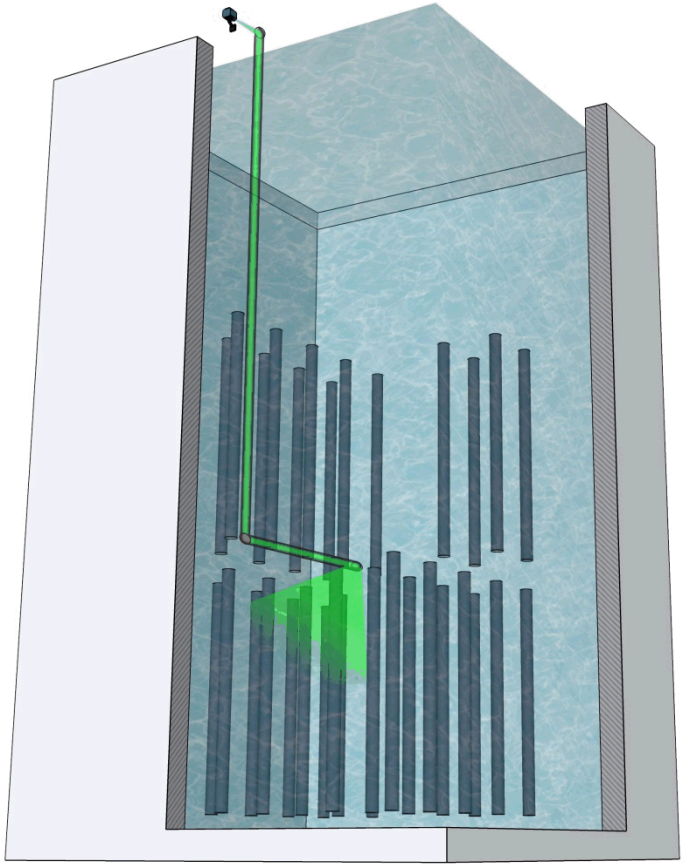
Standoff Video: put only a minimum part of the camera system close to the scene



Possible applications for standoff video



Hot Cell



Stacked Fuel in
Cooling Pond

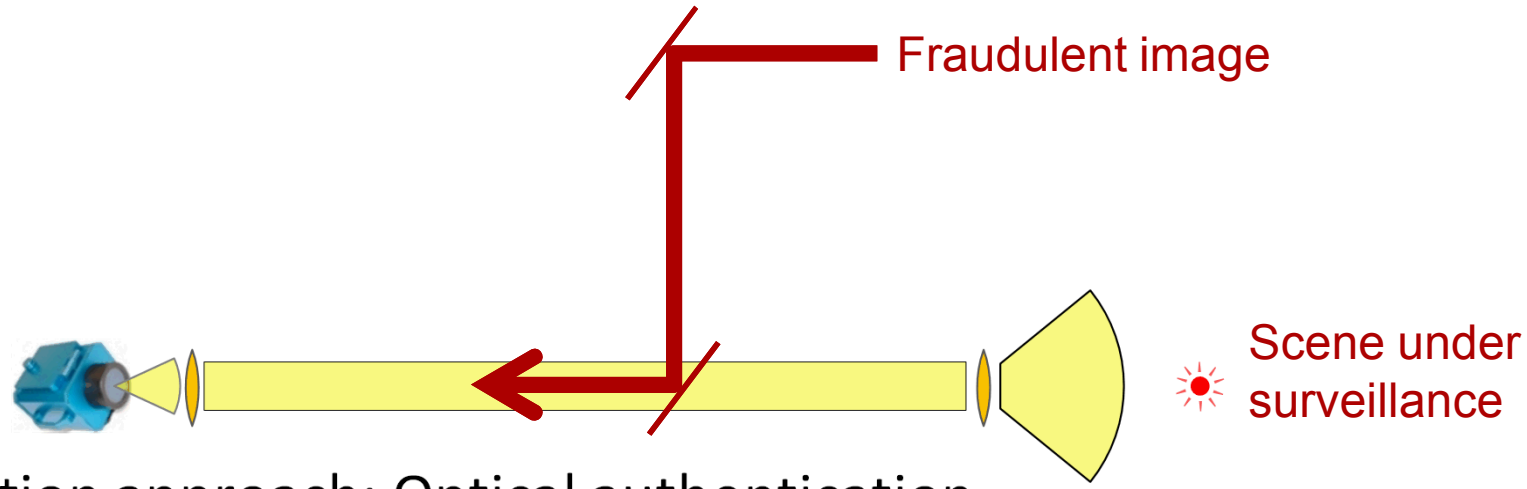
Image Authentication for Video Surveillance

Sandia National Laboratories

- The Surveillance Problem:
  How can we be sure we're looking at what we think we are?
- *Authentication* is what ensures that acquired surveillance data are truly valid images of the scene under surveillance
- Conventional Method:
  - Protect the security-critical components of the surveillance camera with a tamper-indicating enclosure (TIE)
  - Cryptographically sign the digital image data close to the CMOS sensor, within the TIE
- Does not address "before the lens" tampering
  - i.e., altering what the camera is able to see
  - For example, blocking the scene with a static photograph of the scene
  - To some extent, the risk can be mitigated with system approaches, e.g., use multiple cameras, each viewing another

Image Authentication for Standoff Video

- Standoff video exposes even more of the surveillance system to tamper, because of the extended optical path



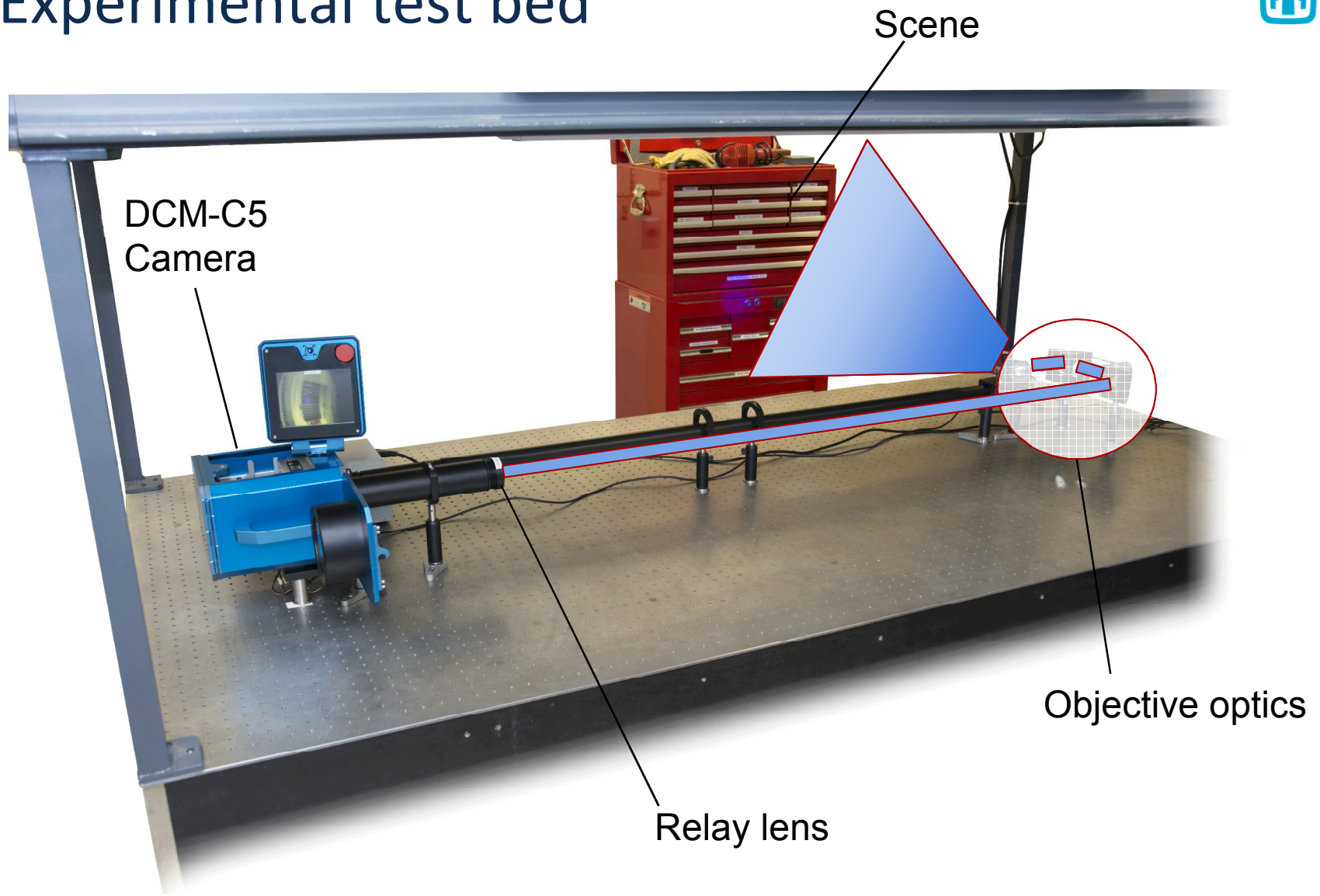
- Mitigation approach: Optical authentication
- Alternatives
  - We could just secure the standoff optical path within the system
  - Or, better, extend the authentication into the scene itself

In-Scene Image Authentication

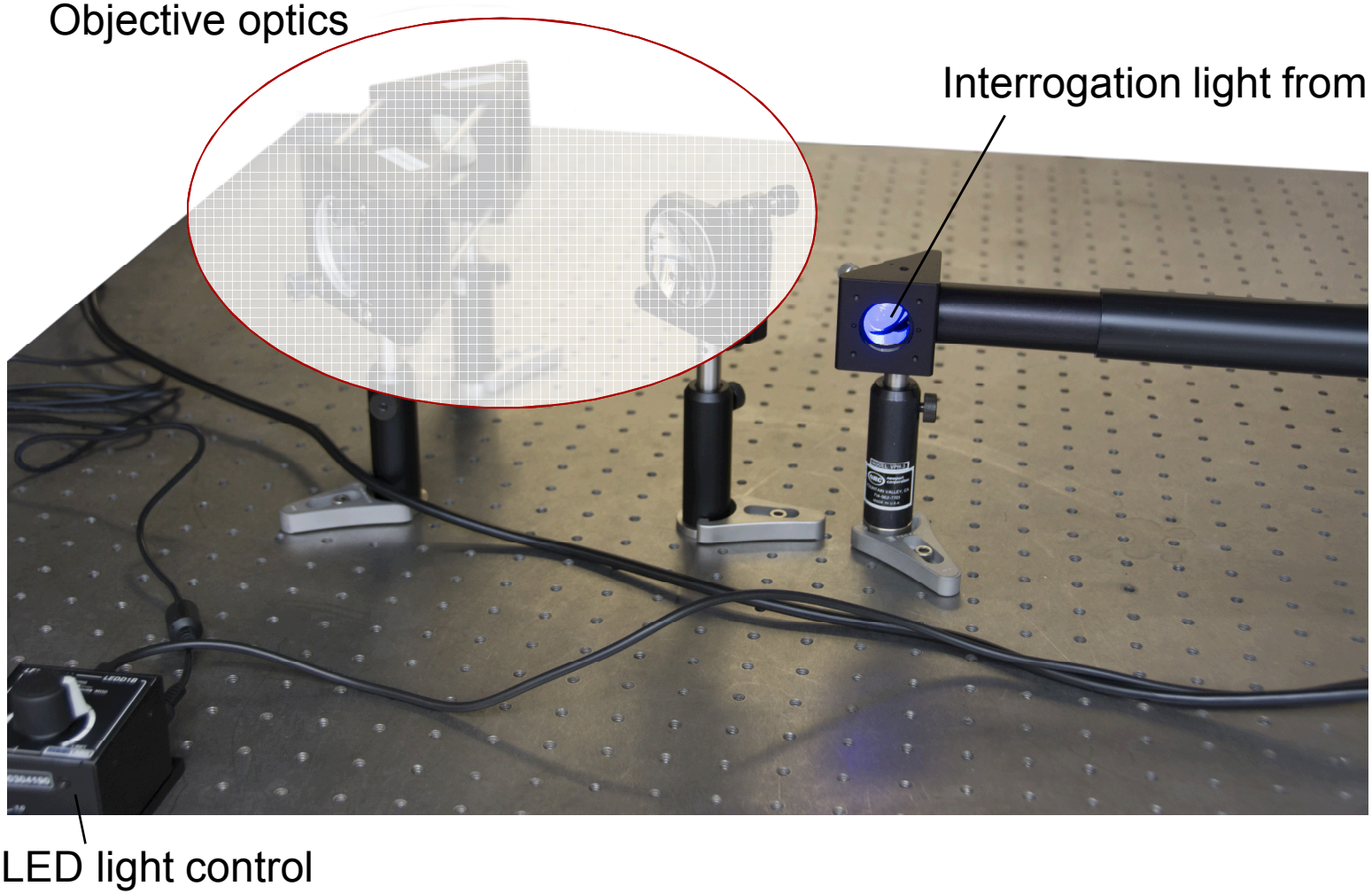
Sandia National Laboratories

- Time varying information is already in the scene (e.g., a clock)
- Something controllable can be inserted in the scene
- Our approach: scene interrogation
  - Shine light into the scene in a known fashion
  - Validate by observing an expected resulting effect in the scene
  - Especially effective if the interrogation can make use of shadows, reflective surfaces, and other scene features to complicate the effect
- The interrogation can be enhanced by controlling multiple factors
  - Color of the light
  - Intensity
  - Timing when off/on
  - Number, location, and size of illuminating spots

Experimental test bed



Experimental test bed: front end optics

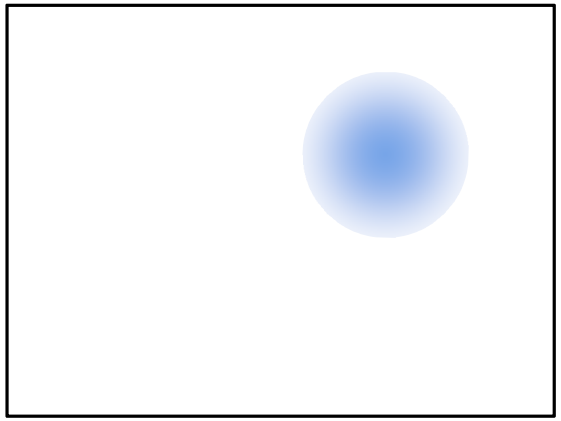


Interrogating illumination only needs to be detectable above ambient

Sandia National Laboratories

Scene without illumination

“Spot” illumination with LED



Computed Difference Image

Discussion

- LED vs laser illumination
  - LEDs do not introduce the eye hazards associated with lasers, but system implementation must deal with beam divergence (brightness issue)
- We are using nominally 1mW LEDs at 455nm, 565nm, and 625nm; could also investigate longer (IR) wavelength
- Various passive optical elements can be added to the interrogating light system to increase the complexity of the optical authentication

- It may be possible to do in-scene authentication by adding elements to the scene under surveillance (e.g. clock, “light bar”)
- Optical authentication has a significant advantage: *everything can be packaged with the surveillance camera system*

Where could we go from here?

- Further develop Standoff Video
  - Engineering: enclosed housing and window for the objective optical components
  - Underwater application (e.g., spent fuel pools): buoyancy issue
  - Fixed surveillance location, yet movable front end (pan/ tilt)
  - Movable surveillance location: objective optics on the end of a movable boom with a jointed surveillance “arm”
  - Multiplexed systems: multiple optical paths sharing a single camera
- Further develop Optical Scene Interrogation for authentication
  - Move to automated image processing to extract the image signature
  - Increase the sophistication of the projected spots in the scene, especially their temporal and spatial variation
  - Develop the capability for conventional video surveillance
- Future work needs to be application-driven

Conclusions

- Through this work we have explored new concepts for both
  - Video surveillance in hostile environments, using standoff
  - Optical authentication of video images

- Standoff video surveillance is a viable means to acquire images from hostile environments and protect camera electronics
- Scene interrogation is a promising approach for optical authentication of video surveillance images

We thank the DOE/NNSA Office of Nuclear Safeguards and Security for financial support of the standoff video surveillance project.