SAND2019-8231C

Physical Encryption of Sensitive Gamma-Ray Templates

PRESENTED BY

Michael Hamel, PhD

INMM 60th Annual Meeting
July 16, 2019
Palm Desert, CA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.

Background

Treaty Accountable Item (TAI) Verification Concepts

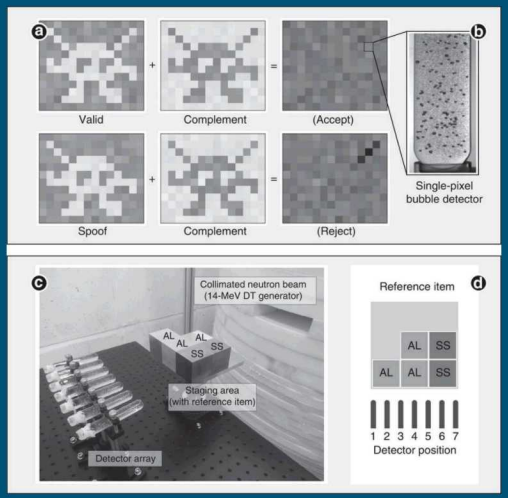
- Attribute Measurements
  - Measure physical signatures to confirm or not confirm an agreed upon unclassified attribute
  - E.g. Minimum mass estimate of fissile material
- Template Matching
  - A reference template is created from a trusted TAI
  - The reference template is compared with subsequent measurements on other TAIs to confirm or not confirm
- Information barrier
  - A combination of technology (hardware and software) and procedures (administrative controls) to prevent the release of classified information while allowing meaningful measurements and independent conclusions [Close, 2001]
  - A combination of physical and/or encryption mechanisms that preclude acquisition of sensitive, quantitative information [Bachner, 2013]

***Challenge**: Ensure that measurement systems protect information considered sensitive by the host party while providing confidence in the monitoring of sensitive items to the monitoring party*

Background

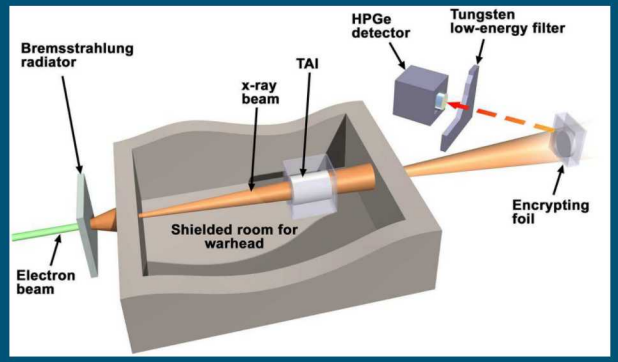
Zero Knowledge Protocol and Physical Encryption

- These methods and techniques attempt to verify TAIs by collecting and analyzing only non-sensitive information
- Intended to reduce the risk of sensitive information loss
- Examples of system based on these principles
  - Physical zero-knowledge object-comparison system (Princeton)
  - CONFIDANTE (Sandia National Laboratories)
  - Physical cryptographic verification (MIT)



S. Philippe et al., "A physical zero-knowledge object-comparison system for nuclear warhead verification," Nature Communications 7, 12890, 2016.

CONFIDANTE (SNL)

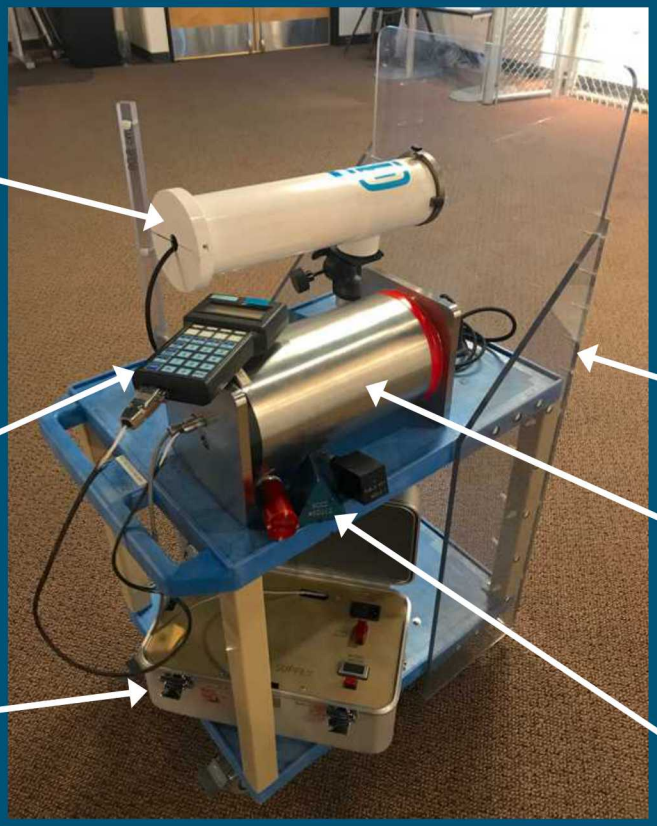


S. Kemp et al., "Physical cryptographic verification of nuclear warheads," PNAS 113(31), 8618-8623, 2016.

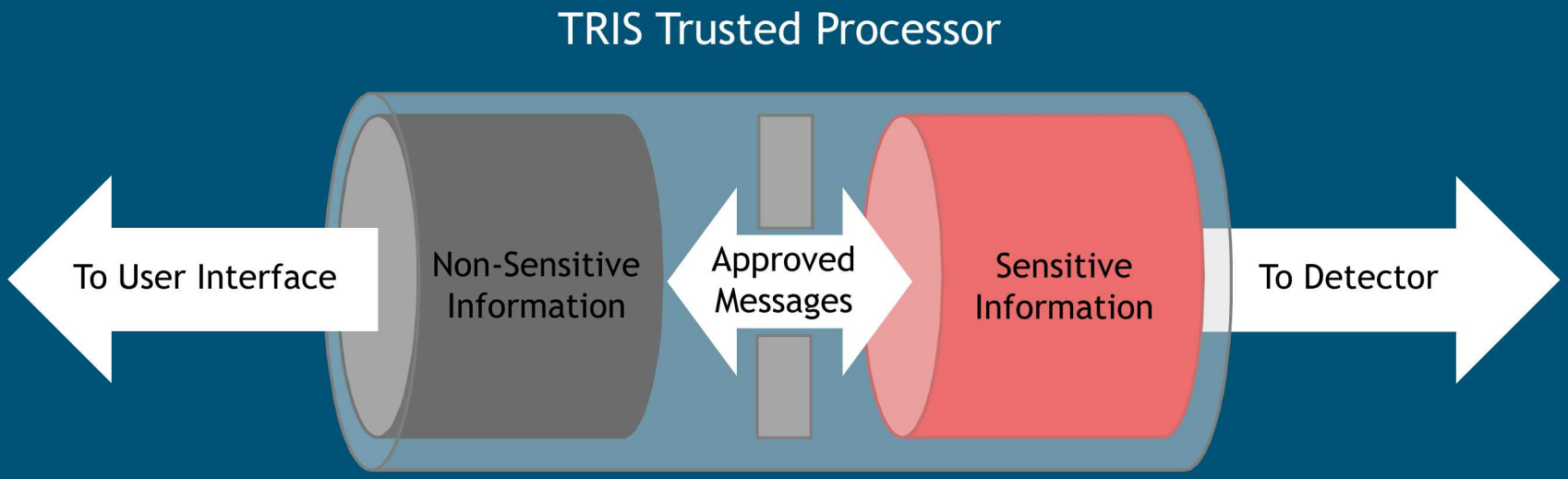
Trusted Radiation Identification System (TRIS)

Can a physical encryption concept be used with a template matching device such as TRIS so that a sensitive signal is never recorded?

- Concept represents an additional approach to protecting sensitive information



Trusted Radiation Identification System (TRIS)



The black side processor is an information barrier showing only approved messages and results from the red side

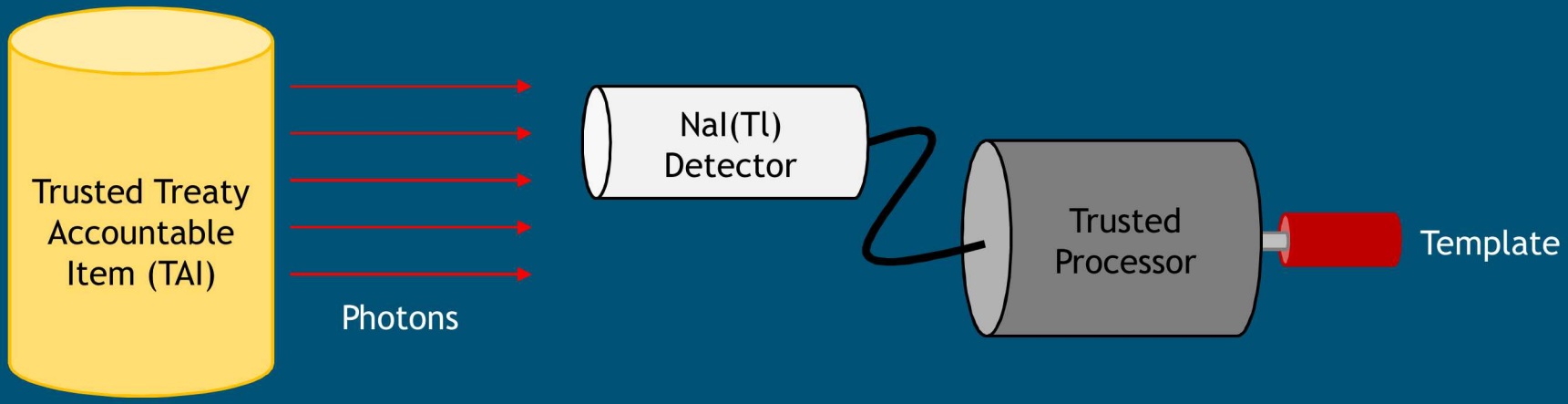
Other features that provide host/monitor confidence

- Digitally signed template (public/private key pair)
- Firmware authentication with a hash key
- Physical tamper protection

Trusted Radiation Identification System (TRIS)

Template matching for TAI verification

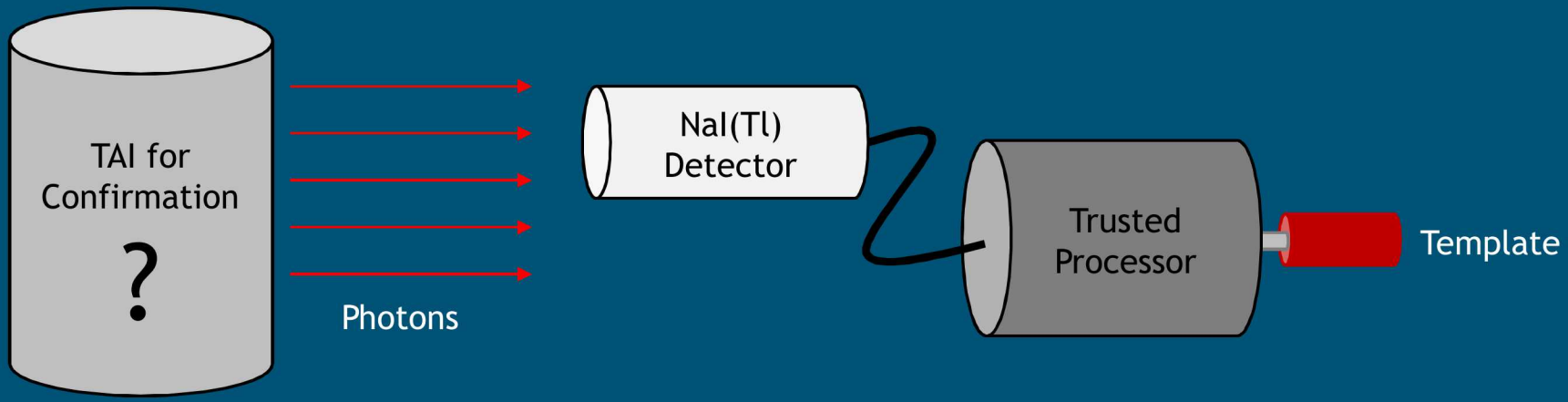
- Template Generation



Trusted Radiation Identification System (TRIS)

Template matching for TAI verification

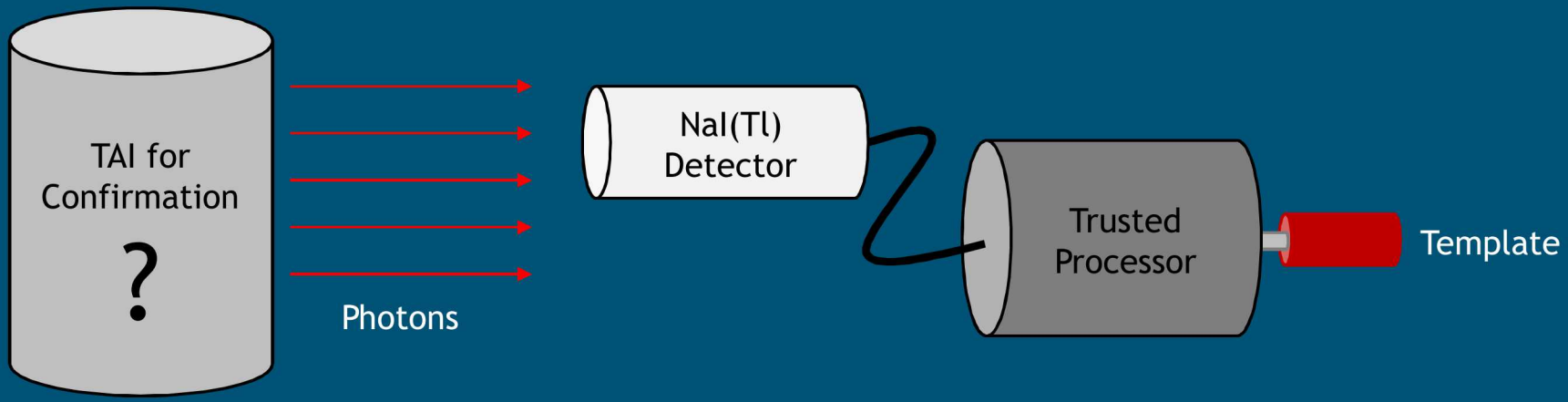
- Confirmation Measurement



Trusted Radiation Identification System (TRIS)

Template matching for TAI verification

- TAI is confirmed or not confirmed

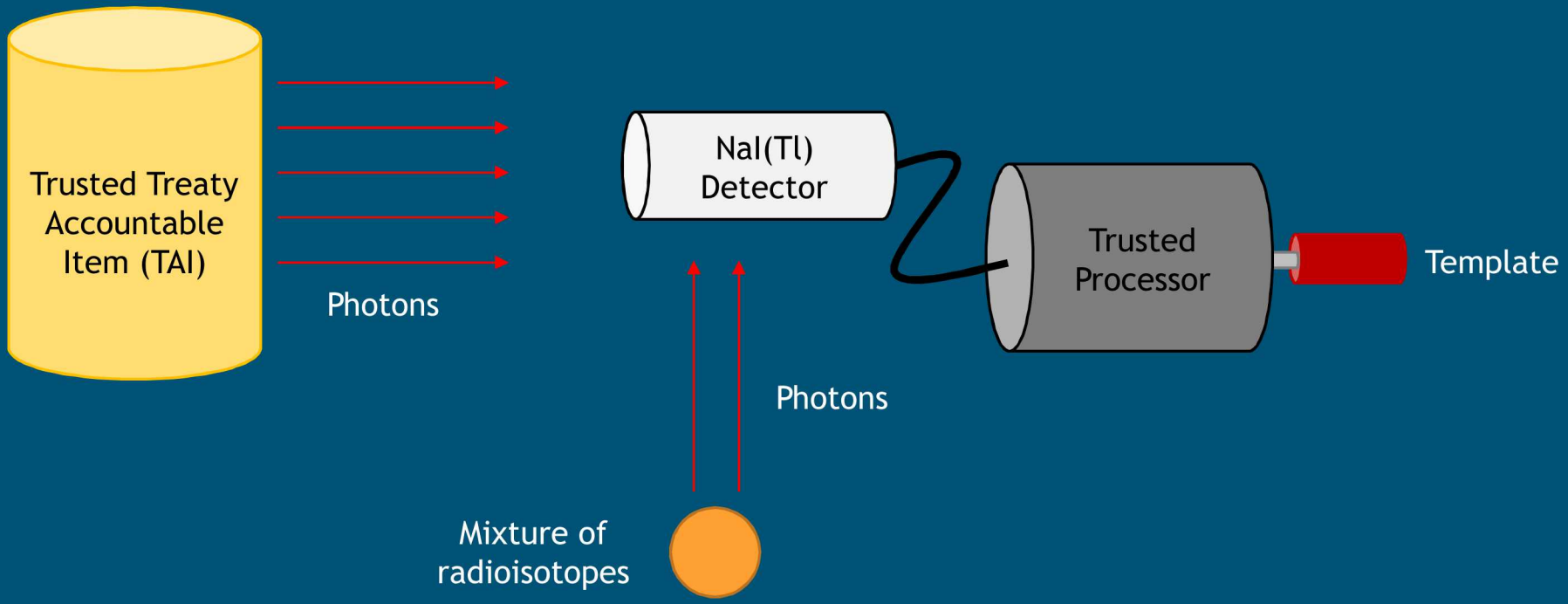


✓ or X

Signal Encryption Methods

Masking with radioisotope mixture as an "encrypting source"

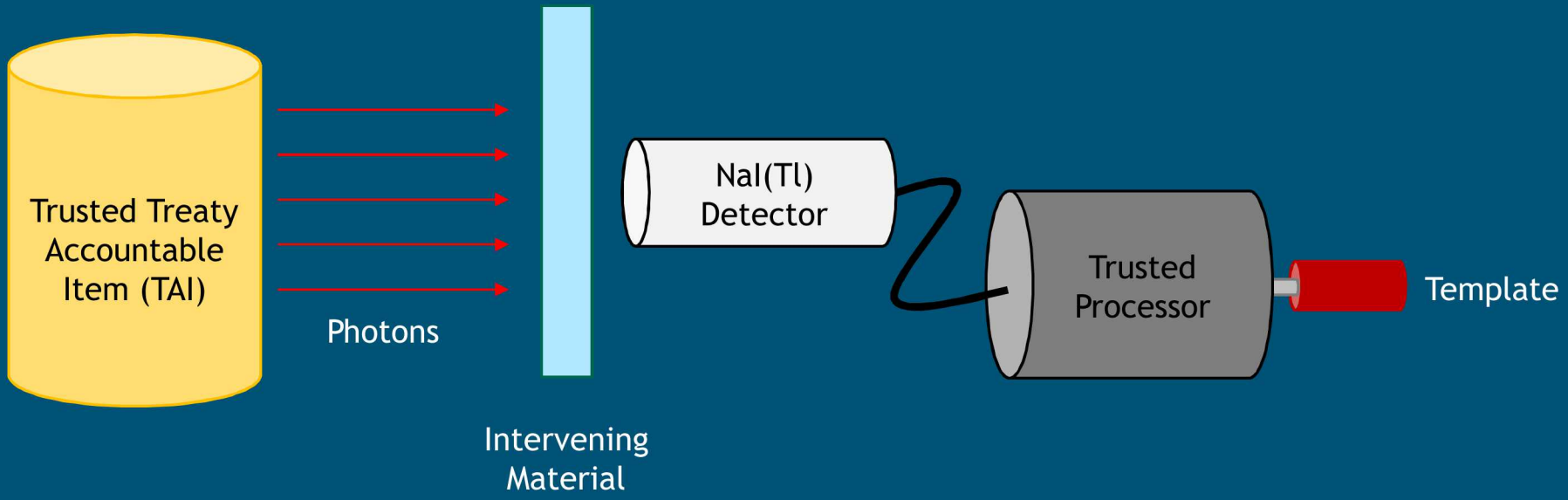
- Signal measured is a combination of the TAI and encrypting source
- Encrypting source would be designed to potentially make the generated reference template non-sensitive
- The same encrypting source would be used again for confirmation measurements
- Composition of the encrypting source would be unknown to monitor



Signal Encryption Methods

Masking with intervening material

- Material placed between the TAI and detector will change the spectrum
- The attenuated TAI spectrum would potentially make the generated reference template non-sensitive
- Amount and composition of material would be unknown to monitor



Signal Encryption Methods

Considerations for feasibility and procedures

- A spectrum of the TAI with encrypting source and/or intervening material could be considered non-sensitive
- In this scenario, a spectrum of the encrypting source would be sensitive since it could be used to derive the TAI spectrum from the combined spectrum
- Template matching algorithm must still work with addition of other sources/intervening material
- Encrypting source must not dominate entire signal
- Encrypting source spectrum will change over time due to radioactive decay

Constraints and Monitor Verification

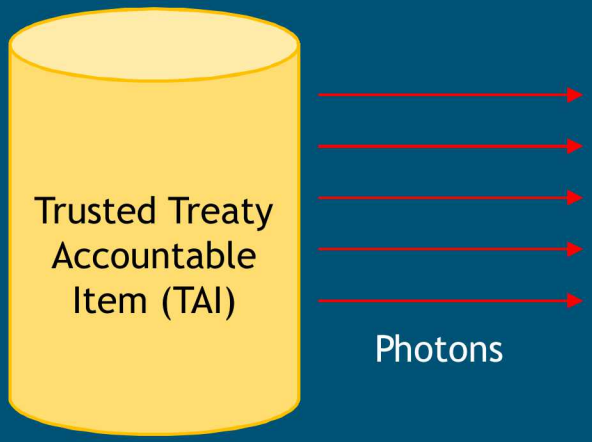
Encrypting source and intervening material in this scenario would be host provided and constrained

- Intervening material in a container of agreed upon size
  - Container of a specific size that can have dimensions measured by monitor
  - Materials and their amounts would be unknown to the monitor, but constraining the container size places constraints on maximum amount of attenuation
- Encrypting source
  - Simple count rate detector could be used to determine if encrypting source activity is allowable
  - A non-spectroscopic detector such a Geiger–Müller tube may be feasible for this task
  - Lack of spectroscopic capability could aid host certification of instrument

Proposed Procedures

Template Collection Procedures

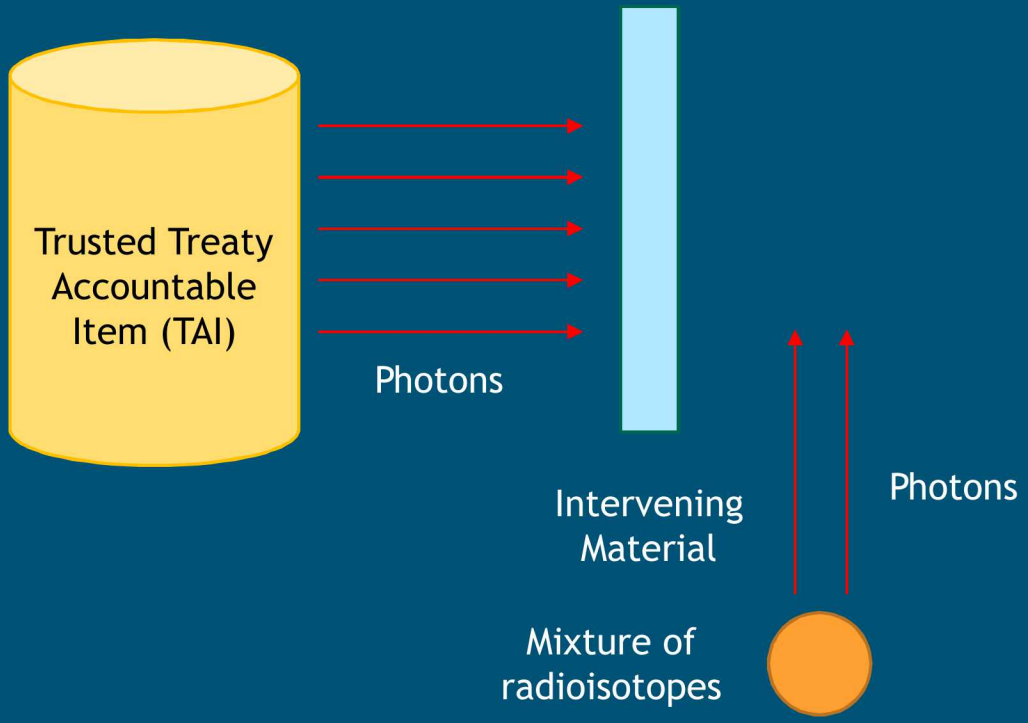
- Set-up procedures are implemented before template collection



Proposed Procedures

Template Collection Procedures

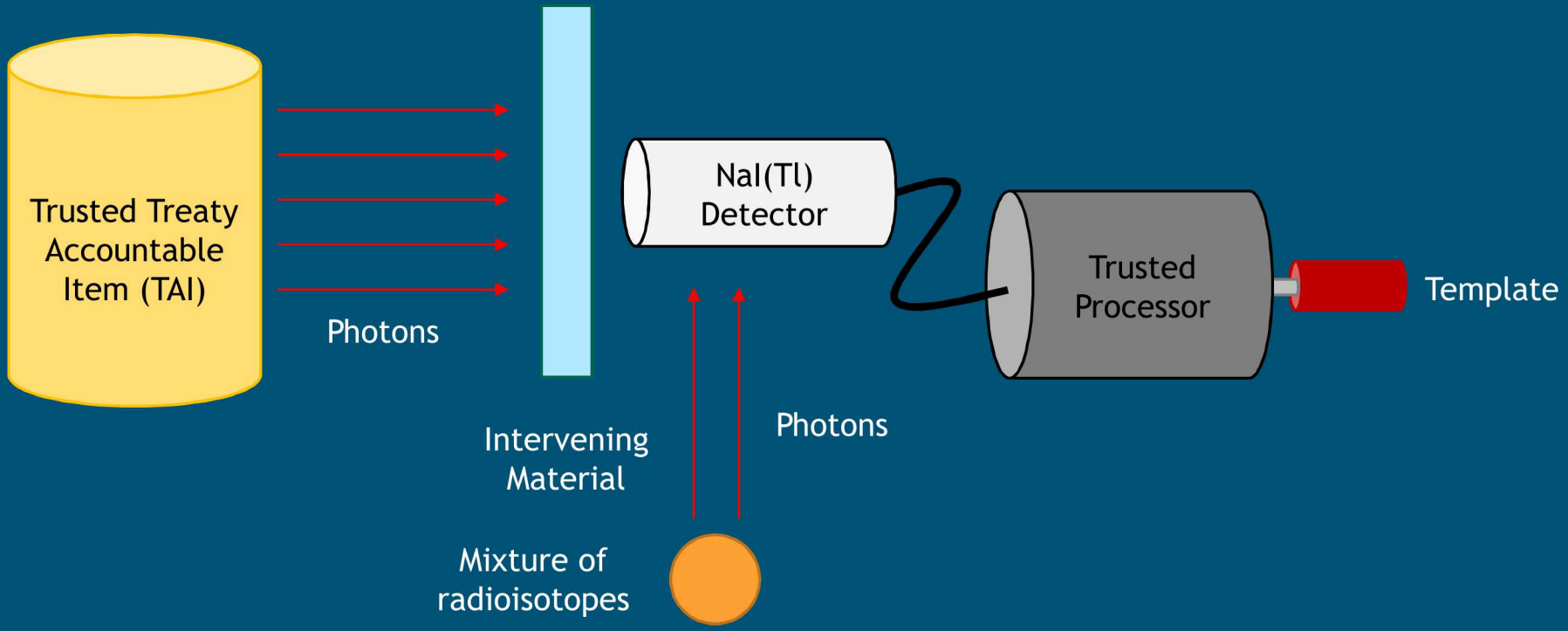
- Set-up procedures are implemented before template collection



Proposed Procedures

Template Collection Procedures

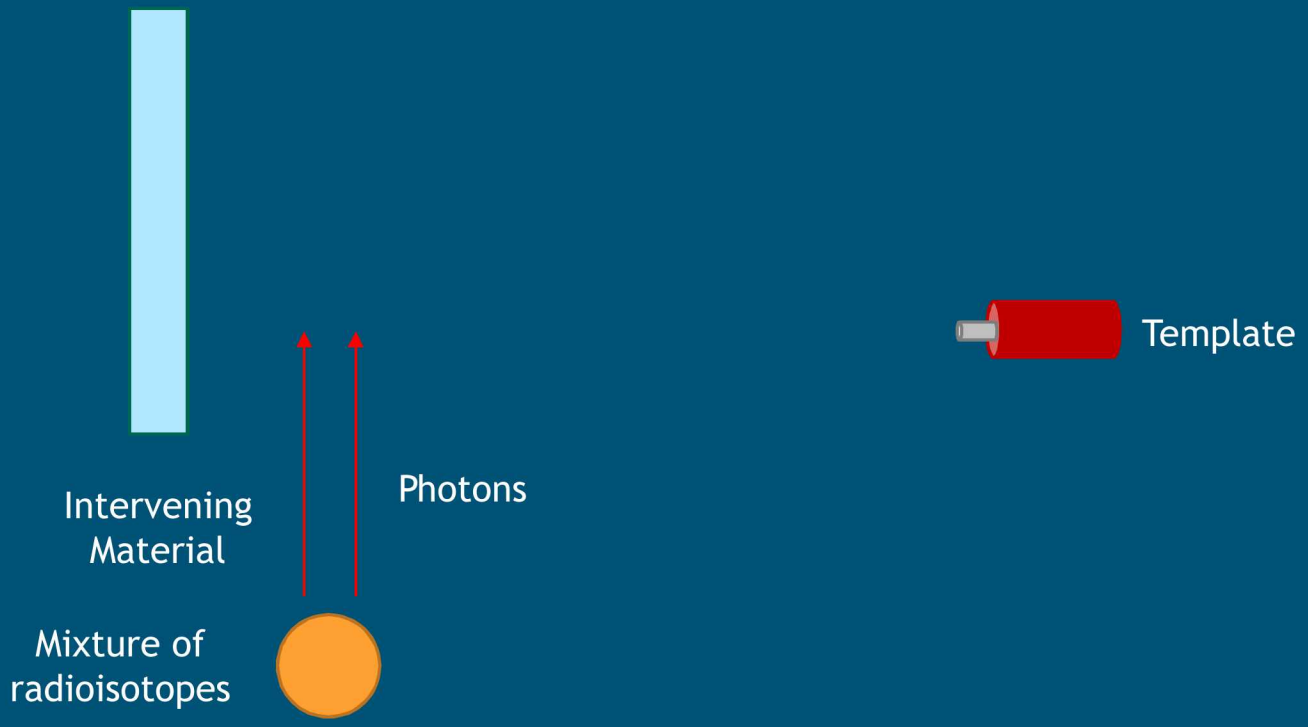
- Template of TAI, encrypting source, and intervening material is collected



Proposed Procedures

Template Collection Procedures

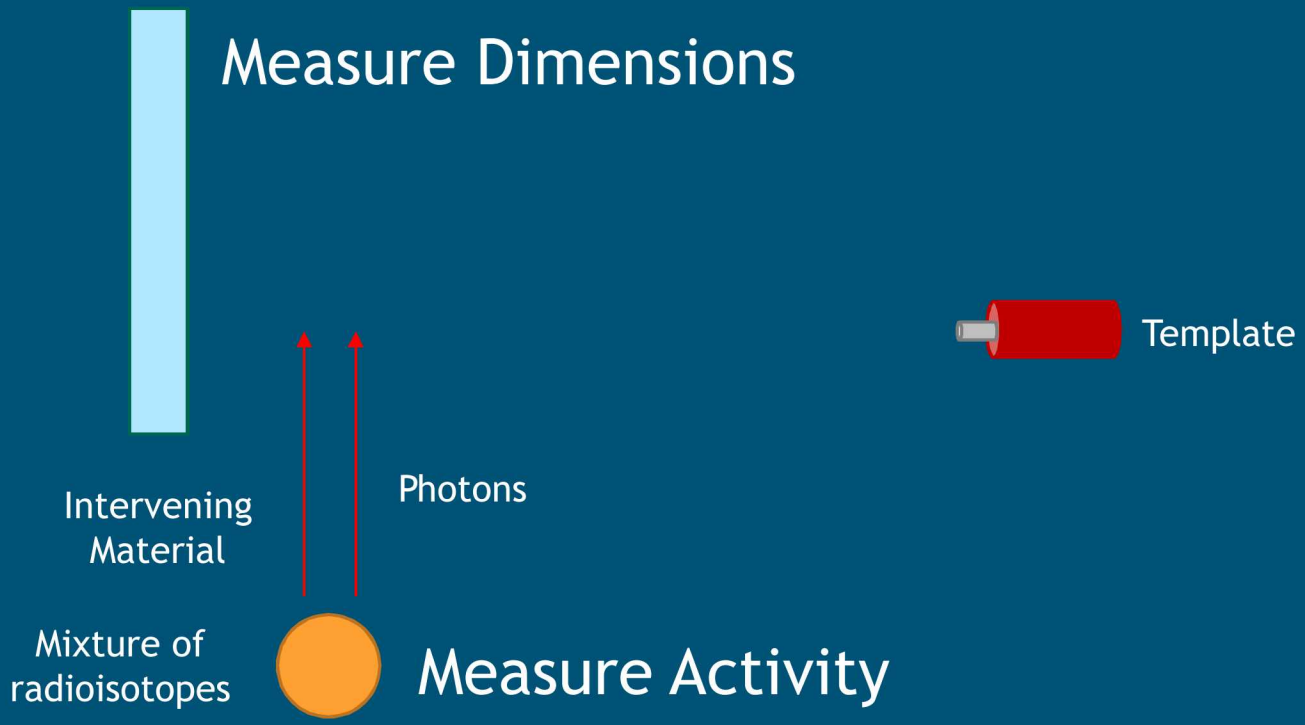
- The TAI and TRIS are removed



Proposed Procedures

Template Collection Procedures

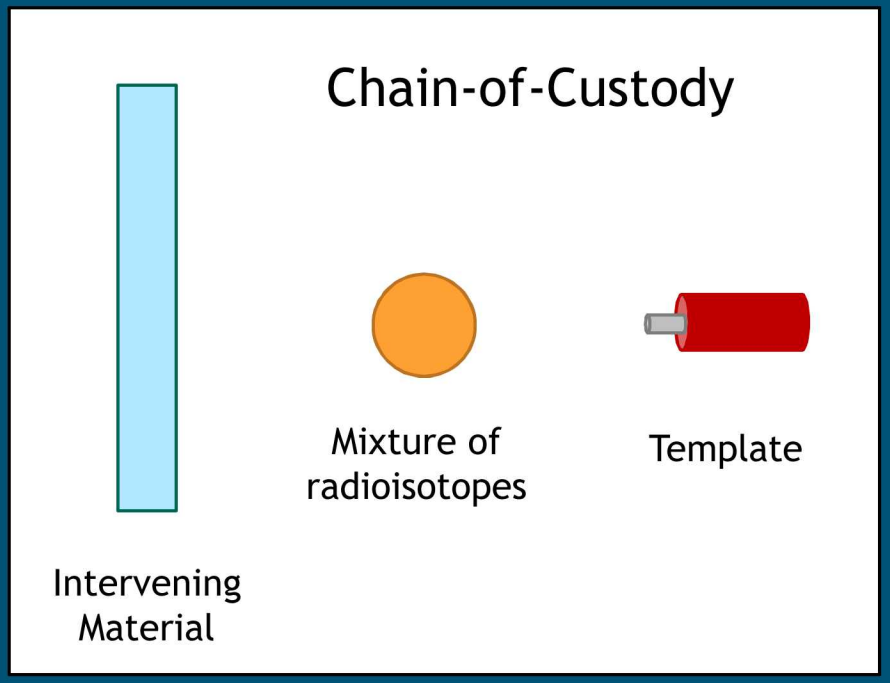
- The monitor verifies that the intervening material and encrypting source are allowable



Proposed Procedures

Template Collection Procedures

- The intervening material, encrypting source, and template are placed under Chain-of-Custody

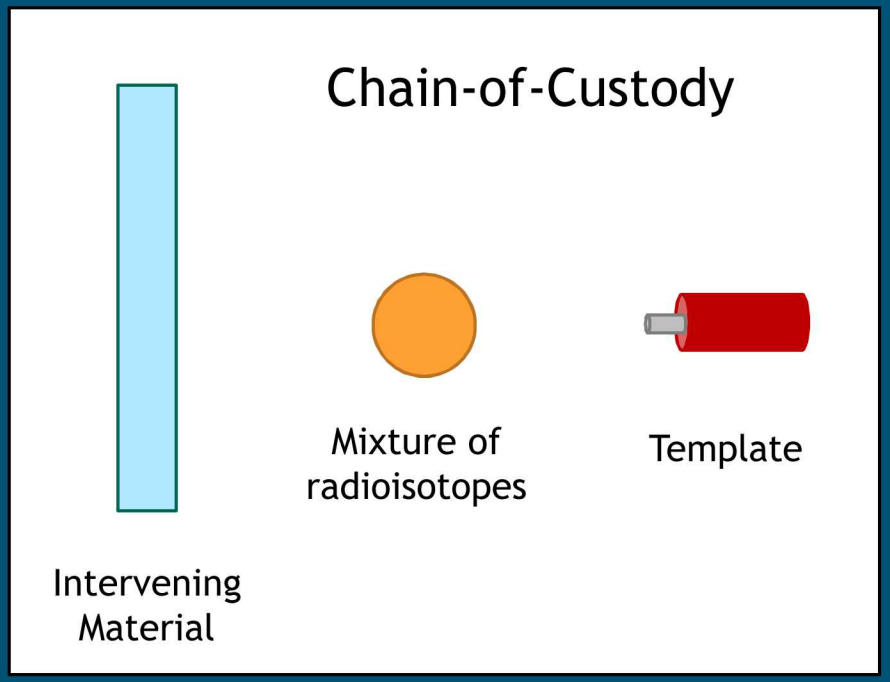


Proposed Procedures

Confirmation Measurement Procedures

- The monitor verifies CoC

Verify CoC



Proposed Procedures

Confirmation Measurement Procedures

- The monitor re-verifies that the intervening material and the encrypting source are allowable

Measure Dimensions

Intervening Material

Measure Activity

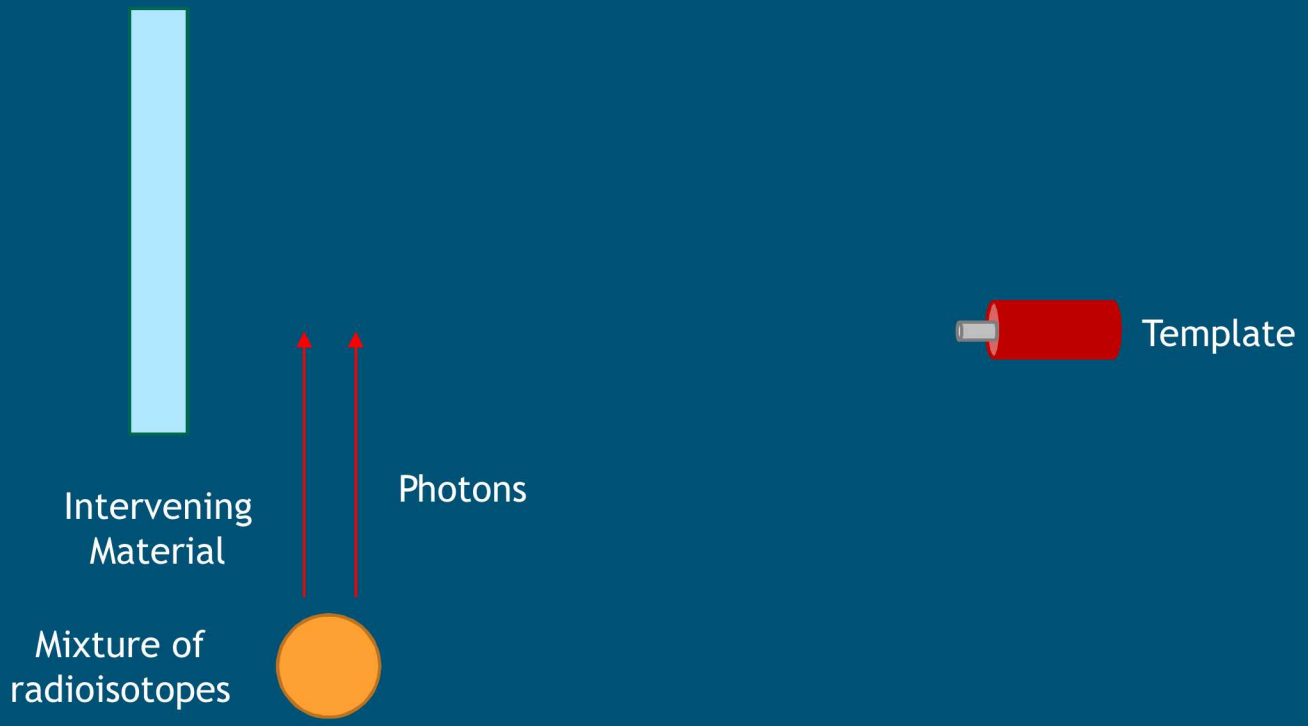
Mixture of radioisotopes

Template

Proposed Procedures

Confirmation Measurement Procedures

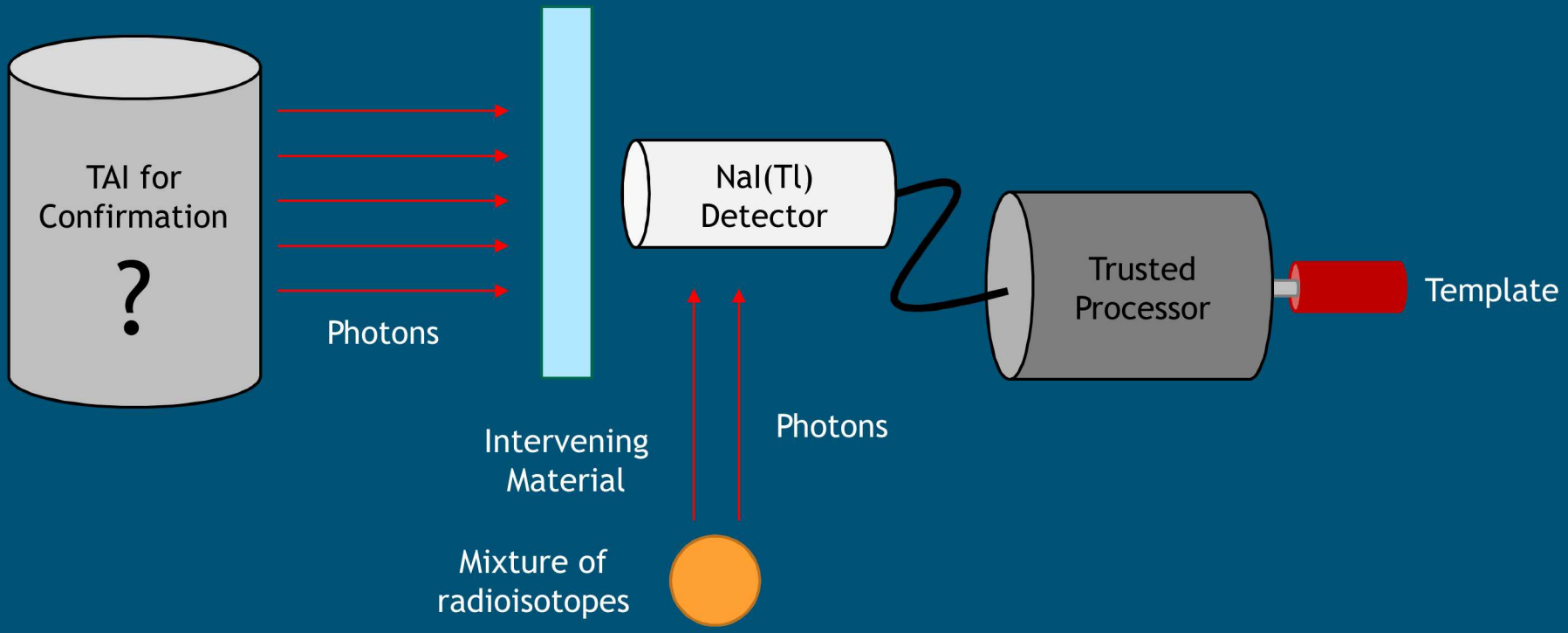
- Set-up procedures are implemented before confirmation measurements



Proposed Procedures

Confirmation Measurement Procedures

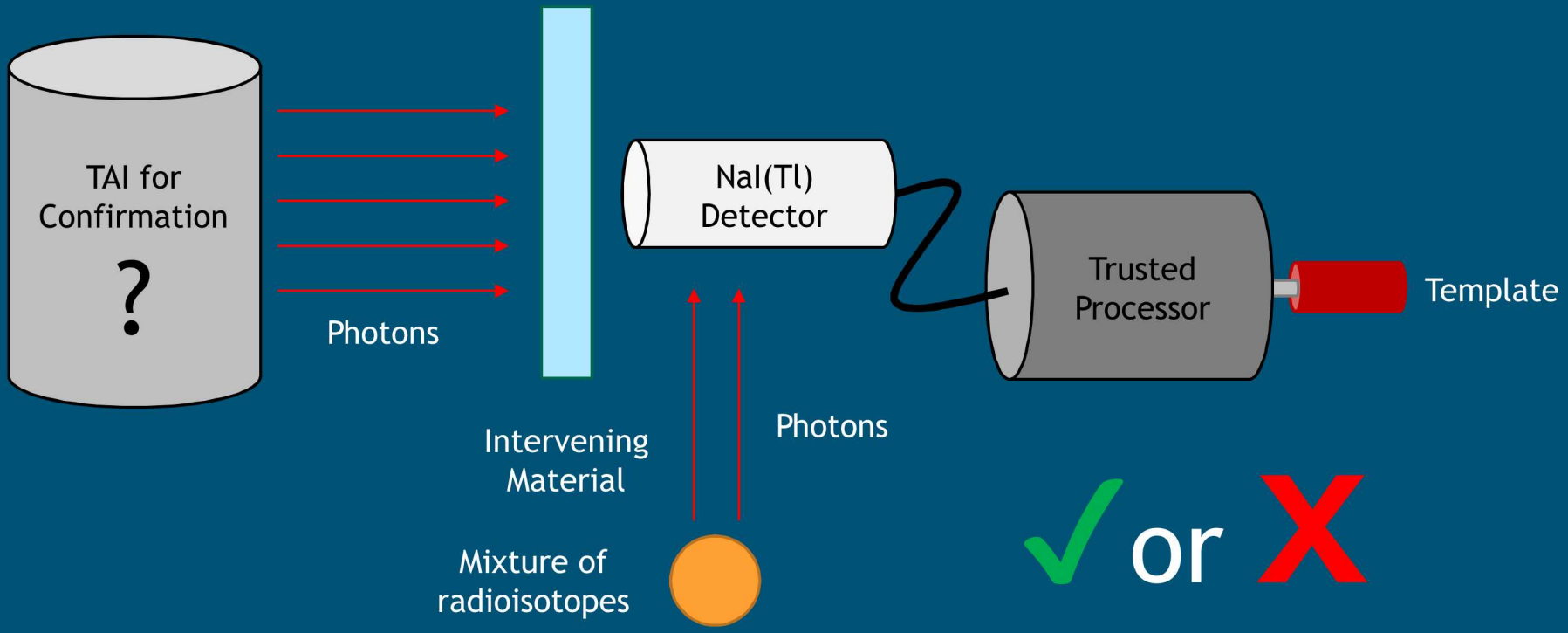
- The TAI is measured with the intervening material and encrypting source



Proposed Procedures

Confirmation Measurement Procedures

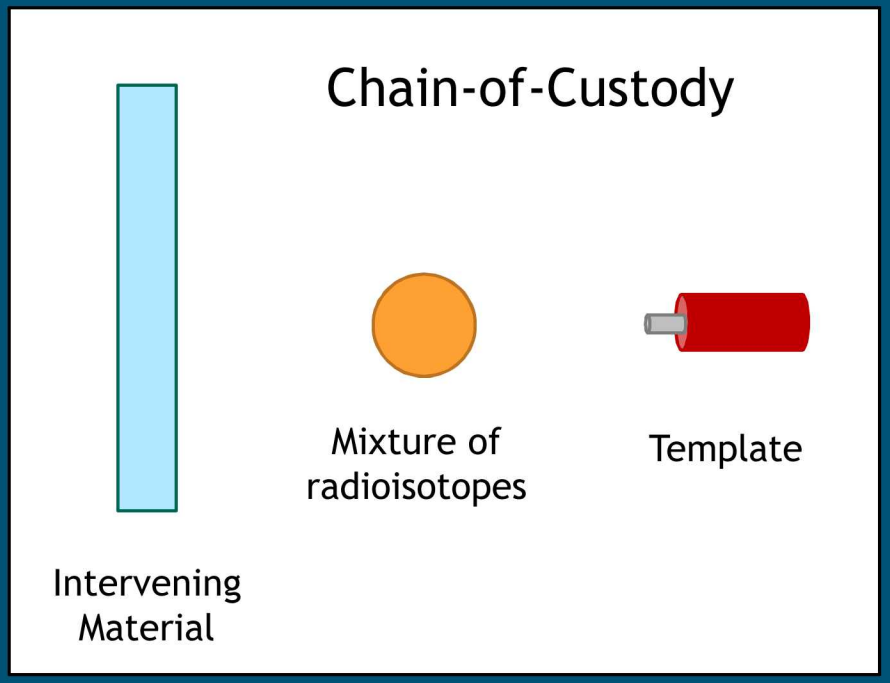
- The TAI is either confirmed or not confirmed



Proposed Procedures

Confirmation Measurement Procedures

- The intervening material, the encrypting source, and the template are placed back under chain-of-custody



Summary and Future Work

- Combine physical encryption with a gamma-ray template matching system
- Template spectrum can include other contributions or modifications as long as it can be matched for subsequent TAI measurements
- TAI spectrum could be encrypted using other radioactive sources and intervening material
- Monitor would need to ensure that signal from TAI is not dominated by encrypting sources or intervening material
  - Could limit activity of encrypting source and monitor could verify with a simple gamma counter
  - Container size for intervening material could be bounded and measured by monitor

- *Next Steps:* Perform feasibility study on presented method

Acknowledgements

Work funded through the NNSA's Office of Nuclear Verification as part of the Warhead Verification Program

Physical Encryption of Sensitive Gamma-Ray Templates

PRESENTED BY

Michael Hamel, PhD

INMM 60th Annual Meeting
July 16, 2019
Palm Desert, CA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & 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.