Development of Additively Manufactured Cryptographic Structures for Tamper Detection

Francisco Gonzalez-Castillo, Dr. Derek Haas
The University of Texas at Austin
fragonz@utexas.edu, derekhaas@utexas.edu
ETI Annual Workshop, February 20 - 21, 2024
Poster # 3

Research Goals & Objectives

The goal of this work is to establish evaluation and development of tamper-detection systems (TDS) for applications in nuclear security. The objectives are the following:

- Evaluate state-of-the-art for TDSs
- Std. practices for development and deployment.
- Create TDS development\authentication techniques.
- Develop AM system for manufacturing TDSs.

Introduction

Tamper-detection is critical for ensuring nuclear compliance and security, and gaps in tamper-detection system development and deployment present a concern in tamper-detection research. Mapping principles of adjacent security research and additive manufacturing (AM) could prove useful in addressing these concerns.

By leveraging the expansive design space afforded by AM and inherent entropic properties of printed parts we can develop and evaluate different tamper-detection and part authentication techniques for applications in nuclear nonproliferation.

Images Source: Johnston RG, "Tamper-indicating seals : practices, problems, and standards." 2003, IAEA.org

Figure 1: Tamper-detection systems for ensuring continuity of knowledge to prevent counterfeiting, proliferation, etc.

Methods

While working towards developing an effective TDS, the following techniques are proposed to ensure comprehensive analysis of prior TDSs and effective development of future TDSs:

- Consult current/prior inspectors to understand TDS needs and opportunities.
- Catalog prior TDS specification, authentication, and evaluation metrics
- Implement design heuristics for TDS design
- Leverage AM process variability for reliable authentication and anti-counterfeiting measures.

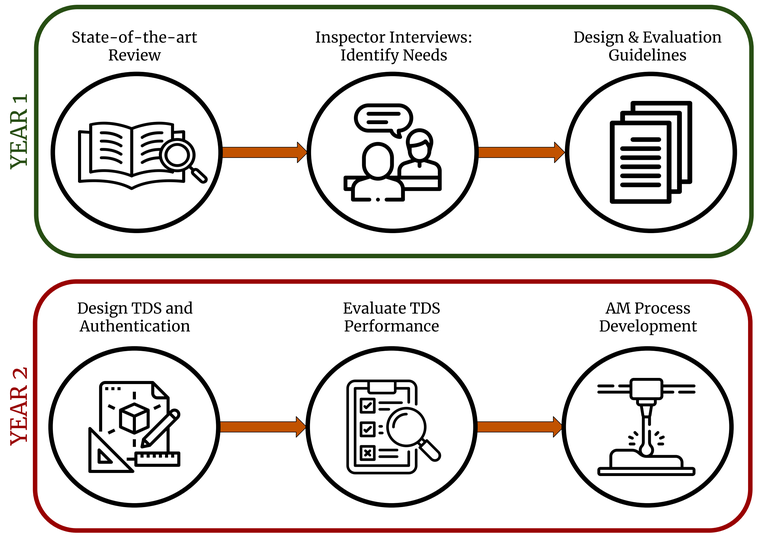
Major Findings

Although still in its early stages, great strides have been made towards developing tamper-detection design evaluation standards. A detailed literature review reveals the importance of developing TDS alongside their detection and authentication techniques.

Additionally, stochastic signatures inherent to AM processes can be leveraged to serve as an anti-counterfeit measure for TDSs in the field and can have varying degrees of security for various nonproliferation applications.

Discussion & Future Directions

This work is the principle effort in a Ph.D. dissertation and continued work on this project includes the development of tamper-detection "theory" development as well as standard evaluation techniques for the development and deployment of future tamper-detection systems. It is anticipated that leveraging inherent AM properties and the expansive design space afforded by AM will be central to development of novel TDSs.



Clipart/Icon Source: flaticon.com (various artists)

Figure 2: Project timeline for development of TDS research until completion of Ph.D. program.

Relevance to Program Objectives

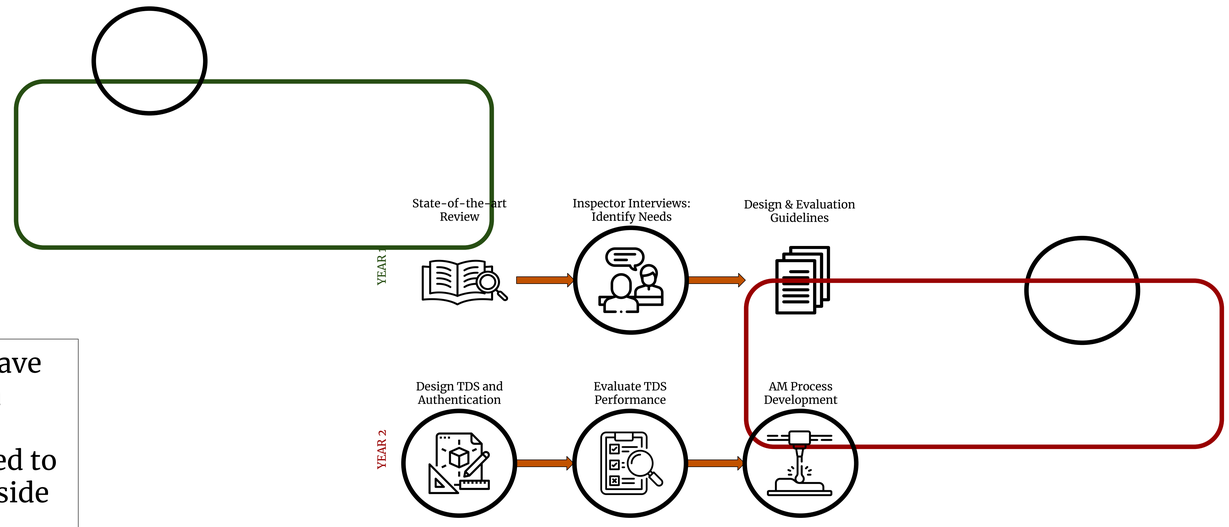
This research operates under thrust area 2 of the ETI consortium: Advanced Manufacturing and Nonproliferation. To advance the field of tamper-detection systems, it is critical to leverage the expertise and advanced manufacturing capabilities of a national laboratory.

Forming a synergistic relationship with subject matter experts promises to yield mutual benefits by propelling advancements in manufacturing while also contributing to nonproliferation efforts.

Aknowledgements

The researchers would like to thank the ETI consortium for their support of this work and expansive resources for connecting with researchers across the DOE complex and the multiple ETI-sponsored learning opportunities.

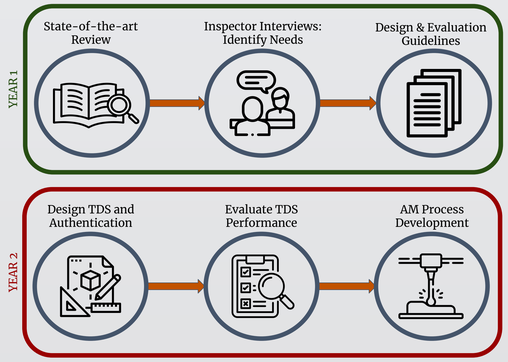
This material is based upon work supported by the Department of Energy / National Nuclear Security Administration under Award Number(s) DE-NA0003921.



Although still in its early stages, great strides have been made towards developing tamper-detection design evaluation standards. A detailed literature review of similar research has highlighted the need to develop tailored authentication techniques alongside TDS design.

Literature also revealed the potential for both polymer and metal AM processes to yield effective TDS for a range of applications in the nuclear nonproliferation regime.

Development of Additively Manufactured Cryptographic Structures for Tamper Detection



Francisco Gonzalez-Castillo
The University of Texas at Austin

Poster #3

National Nuclear Security Administration

The University of Texas at Austin