AURA TrustedAM™ Mark I Endpoint Assessment Activity

TrustedAM™

ATO on DoD networks

and/or via air gap

Trusted Side PKI, AAA, UI, R/O media, receipts

Untrusted Side (Isolated)

Sole trust assumption: DM machine faithfully executes fab. instructions.

DM machine (AM, CNC, waterjet…) (UNTRUSTED)

Low-level ctrl. interface (serial, USB, TCP/IP, etc.)

Data-driven config. of untrusted side for each machine type.
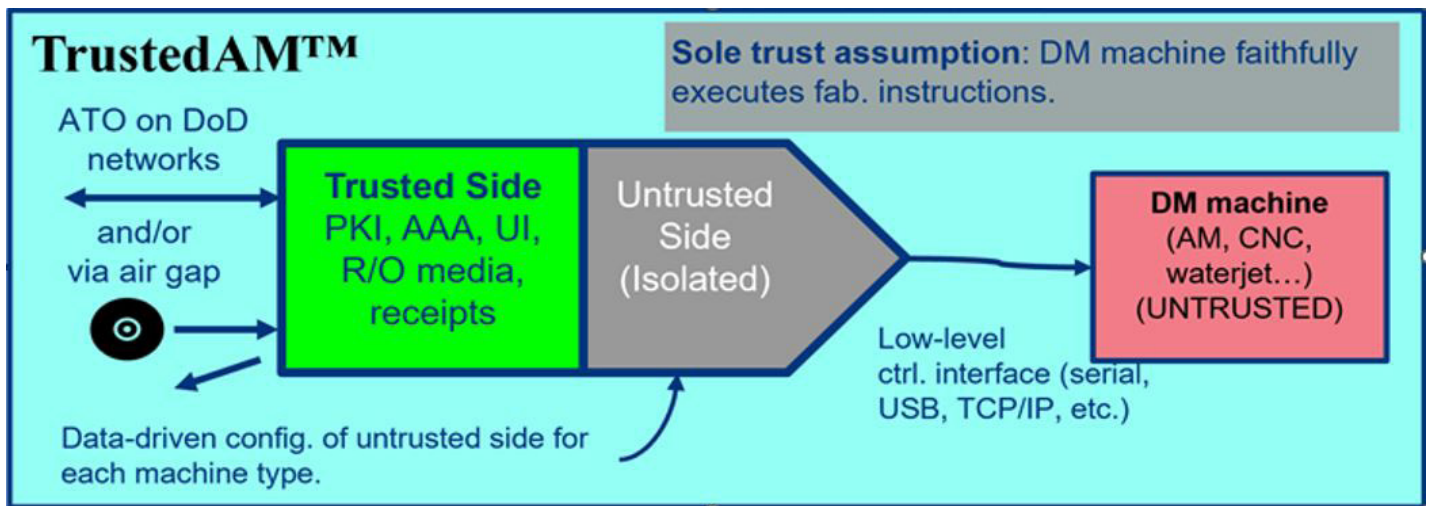
TrustedAM™ establishes trust in devices connecting to resources containing sensitive information.

PROBLEM

Additive manufacturing (AM) machines are problematic from a cybersecurity standpoint; they typically contain sophisticated computer systems designed for industrial/commercial deployment but are not designed to meet the rigorous certifications required for authority to operate (ATO) on Department of Defense (DoD) networks and/or are not trusted more generally. As a result, most AM machines are "air-gapped" from DoD networks and AM artifacts are transported via read-only media (such as CD-ROMs). The process itself is cumbersome and inconvenient for the user compared, for example, to the user clicking "print" in a web portal and printing the part on any (authorized) machine similar to networked printers.

OBJECTIVE

The goal of the project is to provide a means for AM machines in the DoD to connect to an IT system using an encrypted secure digital device without having to qualify or certify via ATO/RMF (risk management framework) every AM machine in the DoD's inventory. TrustedAM™ provides a secure transactional integrity across air gaps and enables key digital twin functionality and process and policy controls, including support for third-party intellectual property. This project seeks to utilize the TrustedAM™ endpoint, which is a hardened, embedded system that provides trusted connectivity between the repository and the AM machine. These endpoints are available off-the-shelf and are being adapted for DoD use.

AMERICA MAKES TECHNOLOGY DEVELOPMENT ROADMAP

This project aligns to:

VALUE CHAIN

TECHNICAL APPROACH

AURA Technologies is selecting two AM machines from a list of ten candidates provided by the Government to install trusted endpoints and run assessment testing. The next step is to configure, deliver, and install two COTS trusted endpoints at an Army facility and two COTS trusted endpoints at a USMC facility. AURA is conducting interoperability and integration testing and assessments of the commercial-off-the-shelf (COTS) trusted endpoint with each selected AM machine. The company is also providing a one-year limited warranty on Mark I trusted endpoint hardware, as well as remote technical support and firmware and software maintenance throughout the project duration.

PROJECT START DATE
October 1, 2021

EXPECTED END DATE
April 30, 2023

EXPECTED DELIVERABLES
- AM machine selection
- Presentation at AM Community Conference
- (4) Mark I TrustedAM™ endpoints
- Final project report

FUNDING
$832,007 total project budget
($832,007 public funding)

PROJECT PARTICIPANTS
Project Principal:
AURA Technologies

Public Participants:
U.S. Department of Defense