Summary of Key Findings Regarding Machine-Vision Technologies and Counterfeit EEE Parts Policy Review

On June 12th, 2023, the Defense Microelectronics Activity (DMEA) released the Final Report on Machine Vision Pilot (MVP) and Microelectronic Authenticity and Security, Evaluation and Research (MASER).

> *The stated purpose of the pilot program was to test the feasibility and reliability of using machine-vision technologies to determine the authenticity and security of microelectronic parts in weapon systems. The primary focus of the project is the prevention and detection of counterfeit microelectronics from entering the supply chain. For the purposes of this effort, the term "Machine Vision" was defined as systems which detect signals within the electromagnetic (EM) spectrum, not only the frequencies visible to the human eye. Systems which rely on image comparison are referred to as "Image Analysis" within this effort. The program included an evaluation of two types of Machine Vision: Image Analysis, and Side Channel, and included conventional standards-based testing methods as applied to counterfeit microelectronics detection.*

The project team was made of contributors from The Defense Microelectronics Activity (DMEA), the Center for Advanced Life Cycle Engineering (CALCE) at the University of Maryland at College Park, the University of Maryland College Park, and SMT Corp.

In addition to the evaluation of machine vision technologies, *a policy analysis was conducted to identify potential impediments to effective implementation of existing laws and regulations, and to indicate steps that can enhance the effective application of such rules, regulations, or processes to mitigate counterfeit microelectronics proliferation throughout the DoD.*

A summary of key findings and recommendations regarding the use of machine-vision technologies for counterfeit EEE parts detection include:

- *Through an assessment of the key Image Analysis (IA) and related Side Channel (SC) technologies for counterfeit detection and prevention it was found that some IA and SC technologies have shown promise. However, in their current stage of development, Machine Vision technologies do not provide satisfactory solutions for counterfeit prevention and detection in the real-world environment (TRL 7), despite demonstrating promising results in controlled laboratory environments (TRL 4).*
- *Standards-based Conventional Testing remains the most effective form of counterfeit detection but is time consuming.*
- *Applying Machine Vision technologies can add additional layers of risk mitigation, but no "silver bullet" currently exists to mitigate the threat of counterfeit microelectronics.*
- *Careful source selection and the application of Standards-based Conventional Testing, commensurate with the appropriate level of risk mitigation for the application, remains the industry best practice.*
- *Standards-based Conventional Testing is consistently accurate, though time consuming, in the detection of variations between authentic and counterfeit parts and demonstrated the ability to determine which parts were counterfeit in the absence of an exemplar, based on detection of physical defects.*
- *The findings of the Blind Study support the recommendation that DoD should continue to rely upon standards-based testing for counterfeit detection.*

Summary of Key Findings Regarding Machine-Vision Technologies and Counterfeit EEE Parts Policy Review

- *The DoD should take a more active role in standards organizations that are developing anti-counterfeit standards, for both awareness within DoD as well as influencing development of standards in a way that addresses DoD's needs.*

Regarding the policy analysis related to counterfeit electronics parts that was completed as part of the study, some of the key observations and recommendations included:

- *The DFARS requires Cost Accounting Standards (CAS) covered contractors to establish and maintain an acceptable counterfeit electronic part detection and avoidance system, which must include risk-based policies and procedures…*
- *SAE AS6171A, in particular, provides a risk assessment model to quantify the level of risk associated with use of a part obtained from an unauthorized supplier, followed by recommended testing sequences based on a resulting risk score.*
- *An agreed-upon definition of "counterfeit" is needed. The DFARS, DoD Issuances, industry standards, and other laws provide conflicting definitions, and agreement needs to be reached on the criteria for identifying a counterfeit electronic part.*
- *A uniform, DoD-wide set of policies and procedures to address prevention, detection, and avoidance of counterfeiting is needed.*
- *DoD should require compliance with the SAE AS6171 standards for risk-based testing to determine authenticity and reliability of electronic parts.*
- *Integration of counterfeit microelectronic part preventions and avoidance strategies into a broader hardware assurance framework that addresses cyber-physical system security is needed.*
- *DoD should include tampered parts and clones in its approach to counterfeiting.*
- *GIDEP reporting: to what extent are counterfeit parts being reported as non-conforming, and what are the reasons that contractors or DoD components may prefer to avoid reporting parts as suspect counterfeit? GIDEP reports should be analyzed and subject matter experts within contractors and DoD components should be interviewed to gain insight into reporting practices and whether GIDEP reporting is serving the notice function that it was intended to serve. An analysis is needed to determine why alternative reporting platforms, such as ERAI, are preferred by some contractors, and what actions are needed to make GIDEP reporting more effective.*
- *Legislative intent and DoD and industry response regarding counterfeit prevention: how did the requirement to eliminate all counterfeits in the 2012 NDAA evolve into the use of risk-based methodologies for counterfeit avoidance? How did responses from contractors, industry associations, suppliers, and the legal community shape DoD's implementation of Congress's instructions in Section 818 of the 2012 NDAA?*