

Engineering Solutions for Military and Aerospace

DEFENSE®

TECH BRIEFS

Airflow and Thermal Analysis of UAV Deicing Systems

Designing a New Generation of Rugged Military Electronics

System Interconnects for Today's Military Vehicles



INSIDE:

RF & Microwave
Technology

Embedded Technology

Supplement to *NASA Tech Briefs*

www.defensetechbriefs.com



Using Laser Direct Structuring (LDS) to Create Robust Hardware Security Devices

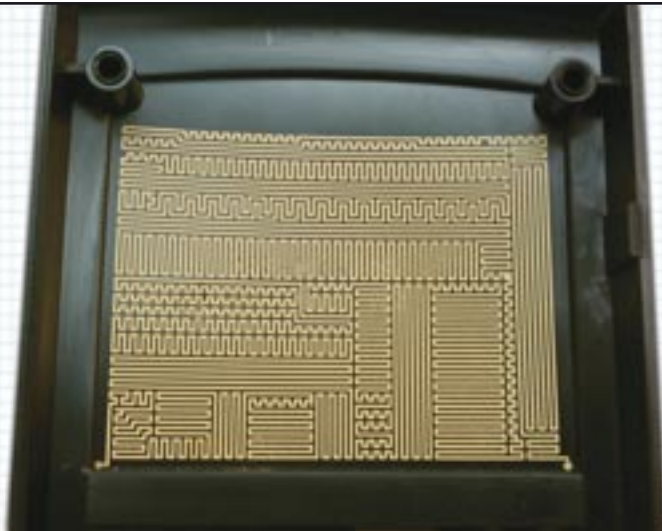


Figure 1. LDS security circuit integrated with enclosure.

A wide range of devices are designed to handle, convey and store sensitive information that requires varying degrees of security from protecting low level administrative to classified and top secret information. In addition, the information and data can reside in an equally wide range of locations and environments from protected and guarded facilities to unsecured desks and offices and over a wide range of environmental conditions including temperature, humidity, shock and vibration.

The National Institute of Standards and Technology (NIST), in conjunction with industry, developed security requirements for cryptographic modules to protect sensitive information on computer and telecommunications systems. The standards are known as The Federal Information Processing Standard (FIPS) Publication 140-2.¹

FIPS 140-2 provides four levels of increasing security to allow the appropriate level of security to be applied depending on the sensitivity of the information and the use environment.

- **Security Level 1** provides the lowest level of security for a cryptographic module and includes at least one approved algorithm or security function but requires no specific physical security mechanisms.
- **Security Level 2** adds the requirement for physical security mechanisms such as tamper-evident seals, coatings, or pick resistant locks on removable covers and doors in addition to the requirements of Security Level 1.
- **Security Level 3**, in addition to the tamper-evident physical security mechanisms required in Security Level 2,

seeks to prevent intrusion and access to critical security parameters (CSP) incorporated within the cryptographic module by means such as reinforced enclosures, tamper detection, and response circuitry that zeros all plain text CSPs when the covers/doors are tampered with or opened.

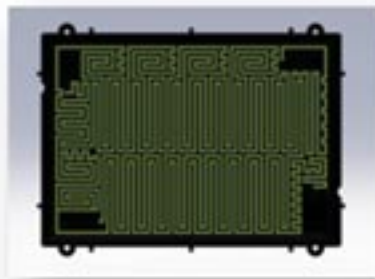


Figure 2. LDS Security Shield Circuitry on the inside of a component protection cover.

- **Security Level 4** provides for the highest level of security requiring physical security mechanisms to completely encase the cryptographic module, detect and respond to unauthorized attempts of physical access that may come at the cryptographic module from any direction by zeroing all plain text CSPs. Level 4 devices must also protect the cryptographic module from compromise due to environmental conditions and changes outside of the modules normal operating values for voltage and temperature. The cryptographic module must contain features to detect environmental fluctuations outside the design range and zero all CSPs should those parameters be

exceeded or must undergo environmental failure testing to validate the module will not be affected by outside fluctuations beyond its normal operating range.

Depending on the required level of security and the operating environment, designers must consider both electronic and physical barrier protection against intrusion and environmental conditions as part of a comprehensive data protection strategy.

Package Protection

Package or envelope protection is a first line of defense in protecting sensitive data and electronic components from attackers trying to access content. Tampering techniques are classified into four major techniques.

- **Microprobing**, where attempts are made to access the chip or bus circuits by physical connection or contact. Microprobing is an invasive attack.
- **Eavesdropping**, a technique used to monitor the analog characteristics of electromagnetic radiation produced by processors and components.
- **Software attacks**, that attempt to exploit flaws in algorithms and protocols through communications interfaces.
- **Fault generation** seeks to create an abnormal environmental condition that will cause a malfunction in protected components.

Eavesdropping, software attacks and fault generation are non-invasive attacks, where once the vulnerability is uncovered it may rapidly be used against other devices of the same kind.

Constructing a non-invasive attack requires specific knowledge of the



Intro

Cov

ToC



device's construction and is made significantly easier if known. Invasive micro-probing, on the other hand, does not require any advance knowledge of the device and attacks often start with attempts to reverse-engineer security elements and then use those results to develop faster, lower cost methods of non-invasive techniques.²

Invasive attacks typically start with removing smartcard processor chips from the package so that they can be deconstructed by physical and chemical means to expose and map bus layouts and probe logic circuits. Preventing access to the processors and other electronic components, including the cryptographic module, is therefore paramount to protecting data.

Historically, package protection has been accomplished by methods that were costly and laborious or that provided less than expected performance. Early attempts included epoxy potting the device, which could be compromised by scraping away the material to expose the devices within. Higher end anti-tamper schemes included a sensing circuit composed of fine wire or mesh wrapped around processors, potted with epoxy and connected to a sensing circuit

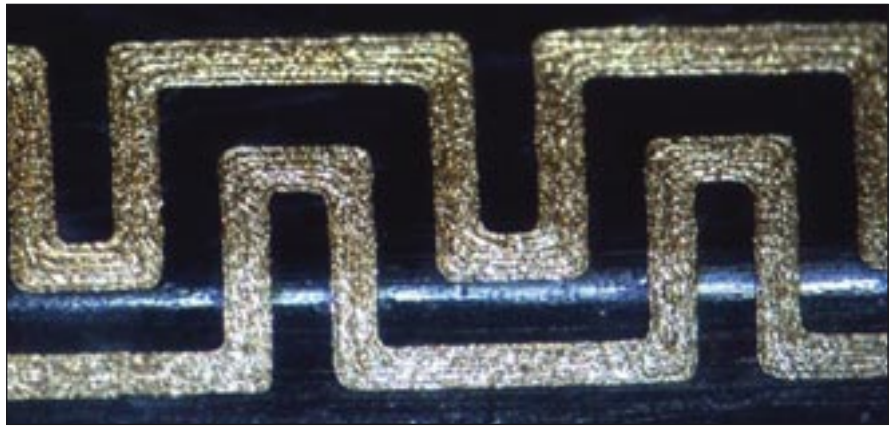


Figure 3. 8 mil lines/10 mil spaces.

that would destroy the contents if a wire was broken.

Laser Direct Structuring

Now a physical barrier package created by Laser Direct Structuring (LDS) fulfills a critical requirement of an active package protection strategy that is easy to adopt and works in conjunction with electronics and software solutions for volume tamper protection.

An LDS created circuit pattern is a critical element of a high performance Level 3 or 4 cryptographic module used to protect

against physical intrusion and tampering of circuits, memory, electronic components, displays and to mitigate problems caused by operating outside environmental design requirements. These types of modules are commonly used to protect USB type memory devices, ATM machines, security tokens, bank crypto keys, telecommunication crypto keys, defense electronics, aerospace, medical devices and next generation electronics.

The Laser Direct Structuring process was commercially developed in Germany by LPKF Laser and Electronics

Touch me 'cause you can!

ISAQ 100

Secure Data Acquisition

- **High precision measurements**
18 bit resolution, 2 Mbit/s
- **Potential free measurements**
Up to 3 km optical data transfer
- **Absolute safety**
Galvanic Isolation > 1 MV
On-desk operation up to 1000 V
- **Wide input range**
±250 V max. input range
- **Outstanding portability**
8000 hours battery power
Light weight and compact design
- **Simple integration**
OLE automation interface

The perfect choice for EMC critical areas and high voltage applications!

Find out more at: www.omicron-lab.com/daq

Laser Direct Structuring

over twenty years ago. The process is used in high-volume production of mobile handset antennas and to produce three-dimensional circuitry on injection molded enclosures, housings and carriers, called 3-D Molded Interconnect Devices (3D-MID).

A Laser Direct Structured barrier achieves a high level of physical security where space is often limited. Circuit barrier functionality is enabled by adding a unique pattern of complex circuitry comprised of fine lines and spaces with widths on the order of 0.005 – 0.010

inches, to the inside of the volume protection enclosure that is almost impossible to breach without detection (Figures 1, 2 and 3).

LDS circuit patterns are ideal for volume tamper solutions because of the 3-dimensional nature of the circuitry that follows the exact contour of the enclosure, the achievable fine pitch and the ability to easily and rapidly make new patterns and changes to existing patterns.

LDS circuitry, as part of an active protective circuit and used in conjunc-

tion with software and other electronic components to form a critical protection barrier, can detect and respond to physical intrusions by sensing attempts to open, remove or penetrate the enclosure with drills, probes, or by chemical attack. If the fine lined and closely spaced traces of the LDS circuit on the inside of the cover are compromised, the circuitry can be programmed to zeroize the contents of memory or programmable devices rendering them useless and the contained data unreadable.

Laser Direct Structuring is a process to selectively mark and plate circuit patterns onto injection molded parts made from engineering grades of thermal plastic resins doped with an organometallic catalyst material.

Laser ablation activates the catalyst in the plastic, making it active towards electroless copper plating, and creates a rough surface providing physical anchor points for the plating (Figure 4).

The laser defined pattern is plated with electroless copper followed by electroless nickel, and an optional immersion gold layer to enhance the electrical and assembly characteristics of the circuits.

Electroless plating chemistries do not require electric current, which means the parts can be plated in barrels or on simple, high capacity racks at minimal cost.

A wide range of engineering grade resins are available in LDS formulations containing the metallization catalyst.⁴ Material selection is done to meet mechanical and environmental requirements in addition to dielectric properties important to the design.

Higher melt index materials like LCP (Liquid Crystal Polymer), nylons, PET, PBT and PET/PBT alloys are amenable to reflow-soldering techniques for attaching ASIC, Flip-Chips and electronic components providing an opportunity to eliminate printed circuit boards and flex circuitry.

LDS enclosures for tamper proofing are designed on any of the available 3-dimensional, computer aided design (CAD) systems by creating a solid model of the package and including the circuit traces as a surface on the solid model. The file is exported to a laser readable file format and then imported into an LPKF laser marking system where the data set is converted or hatched into laser marking coordinates.

Laser parameters, consisting of power output, pulse frequency, pulse duration and linear velocity are then

EVANSCAPS EVERYWHERE



Phased array radar



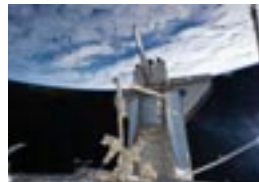
Laser targeting



Avionics, communications, and power hold-up



Displays, mission computers



Space systems



JTRS software-defined radio

Evanscaps are proven in over 100 ratings and configurations to have the highest power density in hermetic tantalum packages.

Evanscaps were delivered to 120 aerospace and defense customers in 2011. They're everywhere.

10V to 125V • Low ESR • >100 Amp Discharge • Unlimited Cycle Life
High Shock and Vibe • 5 Million Hour MTBF • -55°C to 125°C Operation



EVANS

The Evans Capacitor Co.



72 Boyd Avenue • East Providence, RI 02914 USA • 401.435.3555

Since 1996

FAX 401.435.3558 • chasd@evanscap.com



www.evanscap.com for specs and pricing



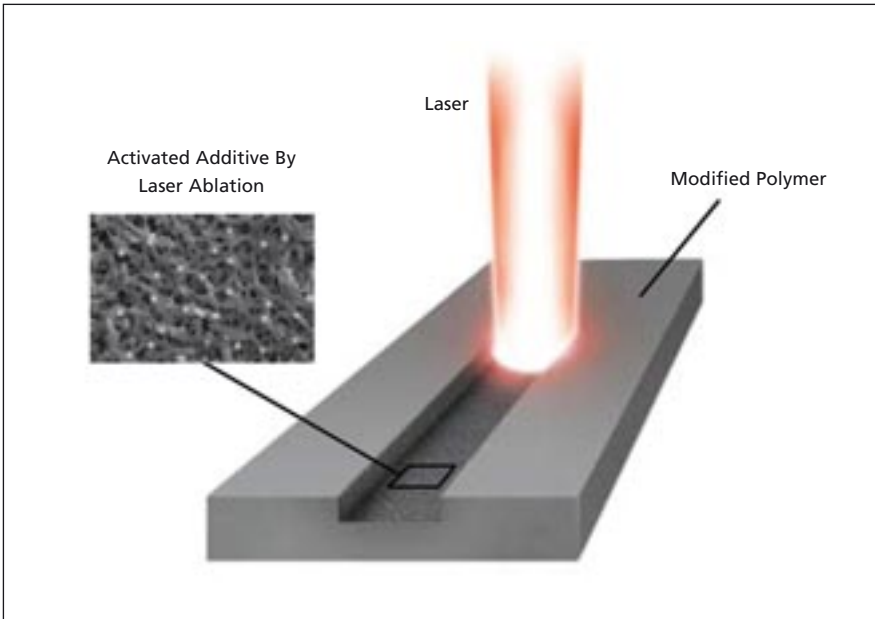


Figure 4. Laser ablation activates a micro-particulate catalyst contained in the thermal plastic and roughens the surface aiding copper plating adhesion.

programmed into the LPKF Nd:Yag 1064nm laser system. The parameters differ depending on the type of material being processed.

Laser marking is fast, which supports a wide range of production volumes,

including high volume production. As an example, a part with 2-in² of circuit traces can be lazed in less than twenty seconds.

Laser Direct Structure created volume protection enclosures can provide com-

plete 360 degree volume protection as part of a Level 3 or Level 4 cryptographic module. The injection molded enclosures are easily designed to protect almost any geometry and are cost effectively produced in both small and large numbers. The method provides for simple revisions to security circuit patterns and rapid implementation of pattern design changes.

This article was written by James Liddle, Director of Business Development, SelectConnect Technologies (Palatine, IL). For more information, contact Mr. Liddle at jliddle@selectconnecttech.com, or visit <http://info.hotims.com/40438-400>.

Reference

- 1.) csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf (FIPS Publication 140-2).
- 2.) <http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf> (Page 1, Design Principles for Tamper-Resistant Smartcard Processors, Oliver Kömmerling, Advanced Digital Security Research and Markus G. Kuhn, University of Cambridge Computer Laboratory).
- 3.) www.cl.cam.ac.uk/~rja14/Papers/SE-14.pdf (Security Engineering: A Guide to Building Dependable Distributed Systems, Chapter 14).
- 4.) LPKF web site; <http://www.lpkfusa.com/mid/materials.htm>
- 5.) Security Engineering: A Guide to Building Dependable Distributed Systems, Ross J. Anderson Page 487.

MODULAR VIDEO GRAPHIC SOLUTIONS

Mil-810, IPC class-3, RIAC, Extended Temperature (-40°C to 85°C)

XMC-E6760-VO Graphics Processing Module:

Parallel Processing OpenCL1.2 and CUDA

576 GFLOPS GPGPU Processing

Conduction Cooled

Custom Fitted Heatplate

Up to 6 Independent DisplayPort Outputs

ANSI/VITA 46.9 Pattern Map



WOLF

WOLF Industrial Systems Inc.
1.905.852.1163 www.wolf.ca

North American Toll-Free: 1.800.931.4114

Celebrating 20 years of Innovation!

XMC

MXC

CompactPCI-S.0

COM Express

VPX

PMC

MXM

ATCA

AMC

A Complete COTS Solution in XMC!

For more detailed descriptions of WOLF's modules and their cutting-edge advances in video graphics functionality, go to www.wolf.ca/products/xmc-e6760-vo/



Intro

Cov

ToC

