

# Laser Fault Injection System Enables Unprecedented Levels Of Smart Card Security Testing



- A new technique and testing platform which advances side channel fault injection testing of smartcards to completely new levels
- NIR diode laser microscope enabling silicon substrate penetration for back side attack
- Powerful red diode laser for front side attack, with extremely small laser spot footprint
- Fast multi glitching, accurate digital scaling with fast and predictable trigger pulse response
- Autoscanning of chip surface with integrated motorized XY stage
- Live camera inspection of laser spot and location on chip area

## Background

Protecting smartcard chips and other embedded microchips against unauthorised access is one of the main security challenges facing the smartcard industry.

**Riscure**, is an independent, market leading security testing laboratory specialising in the evaluation and intensive testing of smartcard and embedded chip products that are designed to operate securely in a hostile environment. Located in Delft, The Netherlands, Riscure has been pioneering advanced smart card security testing since its foundation in 2001. Riscure has a central focus on in-house design and development of state-of-the-art security testing tools for smart card and embedded technology

Today, Riscure remains at the very leading edge of smartcard testing, and in partnership with Opto, has pioneered a brand new technique and testing methodology, enabling it to push the envelope of smartcard testing to new levels. With the newly developed **Diode Laser Station** designed and built by Opto in collaboration with Riscure, it is now possible to perform advanced laser fault attacks that meet and exceed the highest international standards to assess if a smart card or other embedded chip is secured against attack.

## Task

The goal of the development was to create a video based, high power microscope instrument capable of delivering and imaging an extremely small, highly focused area of 2 wavelengths of laser energy to localised areas of a secure microcontroller, and then to give the possibility to reposition the chip with very high accuracy.

## Solution

In order to meet the demanding requirements of the project, Opto based its design for this system on one of its high resolution, multi-port microscope platforms. This configuration enabled optimised integration of the laser profile coaxially into the microscope.

In order to achieve the necessary levels of accuracy, Opto incorporated a unique adjustment mechanism into the system enabling the imaging CCD to be positioned perfectly into the laser and image path to micron accuracy in X & Y directions.

Laser integration was provided coaxially by a customised laser-in port incorporated into the main optical path of the microscope. This port incorporated mechanisms enabling high precision switchable beamsplitters and other filters to be introduced into the laser path in order to provide additional processing capability and a future upgrade path. A key element to the optical design of the system was the optimisation of the microscope to effectively transmit the 2 key wavelengths required by the system. The optical correction of the microscope to these wavelengths required the use of specialist glass optimised to give zero image and focus shift across the required optical bandwidth.

In addition to this, the Riscure system also incorporates a totally unique device able to control laser spot size according to user preference. With this device, laser spot sizes as small as  $6\mu\text{m} \times 1.4\mu\text{m}$  are possible.

Sample illumination was also provided coaxially, and was based on a long life, high power LED source. In order to offer maximum image contrast gains at the high magnifications required by the system,

Opto incorporated its unique 'Köhler' illumination delivery module, normally found only on high level research grade microscopes. The Köhler principle utilises a series of adjustable aperture diaphragms to create defined, parallel light rays to pass through the specimen. This results in significantly increased image contrast enhancement at magnifications of 20x and higher.

At the front end of the system, a rotating objective turret was integrated by Opto which was fitted with 3 long working distance NIR optimised microscope objectives offering 5x, 20x and 50x magnifications.

## Conclusion

Competing laser setups currently used for fault injection attacks on smart cards are typically based on laser cutting technology. Diode lasers have always been attractive but historically have lacked the power and small spot sizes necessary for effective chip manipulation. Every one of these issues has been effectively addressed by Opto in the Riscure Diode Laser Station by combining dedicated lasers with perfectly optimised optical design and by incorporating the very latest diode laser technology.

The Riscure Diode Laser Station has demonstrated itself to be highly effective in testing hardware and software countermeasures in smart cards. It automates the surface scanning process, and offers very high precision control over the laser power, injecting pulses with the small spot sizes required by emerging and next generation smart card technologies.

For more information, see:

<http://www.riscure.com/inspector/product-description/inspector-fi/diode-laser-station.html>

