



Universidad de Sevilla.
Escuela Politécnica Superior de Sevilla.



Trabajo Fin de Grado en Ingeniería Electrónica Industrial.

Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.

Autor: Ricardo Soto

Tutores: Carlos Jesús Jiménez Fernández

José Miguel Mora Gutiérrez

Departamento de Tecnología Electrónica

Junio 2022



Universidad de Sevilla.
Escuela Politécnica Superior de Sevilla.



AGRADECIMIENTOS

Mi más sincero agradecimiento a Carlos Jesús Jiménez Fernández y José Miguel Mora Gutiérrez, por su interés, orientación y ayuda prestada.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página I

RESUMEN

La inserción de fallos por láser pulsado es una técnica bastante precisa que permite simular los efectos de la radiación, conocer vulnerabilidades de circuitos u obtener información considerada como privada o secreta que se encuentra almacenada internamente en el circuito como pudiera ser las claves en circuitos de encriptación. Este tipo de proyecto es importante ya que están aumentando el número de datos informáticos que se está transfiriendo por el mundo y se necesita más seguridad en los sistemas de encriptación.

El presente Trabajo de Final de Grado tiene como objetivo estudiar la inserción de fallos en flip-flops de un circuito integrado con un equipo láser. Para poder obtener un dato se realiza una serie de disparos con el láser y se compara la respuesta del circuito con la interacción del láser y sin el láser. Con esto se puede sacar ciertas conclusiones y llegar a sacar datos y claves e incluso posiciones de los componentes de un circuito criptográfico. Para dicho estudio se va a necesitar una interfaz que facilite al usuario el diseño del ensayo, la visualización de los datos y el control de los equipos de laboratorio. La interfaz se ha desarrollado con el lenguaje de programación Python y los ensayos se han realizado en los laboratorios del Instituto de Microelectrónica de Sevilla (IMSE, del Centro Nacional de Microelectrónica, CNM-CSIC, Universidad de Sevilla).

Al final del trabajo se realizan ensayos sobre flip-flops de un circuito integrado que contiene varios cifradores de flujo Trivium, se analiza los resultados y se diseñan unas pautas para poder obtener información del circuito.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página II

ABSTRACT

The laser fault injection attack is a quite precise technique that allows us to simulate the effects of radiation, to know vulnerabilities of circuits or to obtain information considered as private or secret that is stored internally in the circuit such as the keys in a cryptographic circuit. This type of project is important because the amount of computer data being transferred around the world is increasing and more security is needed in cryptographic systems.

The objective of this work is to study the laser fault Injection attack in some flip-flops of an integrated circuit with a laser equipment. We need to do some tests with the laser in the circuit and compare the result with laser and without laser to get some information. Also, we can draw some conclusions and get the keys and data or the localization of the component in a cryptographic circuit.

For such a study, an interface will be needed to facilitate the user to design the test, visualize the data, and control the laboratory equipment. The interface was developed with Python language, and the tests were carried out in the laboratories of the Instituto de Microelectrónica of Sevilla (IMSE, del Centro Nacional de Microelectrónica, CNM-CSIC, Universidad de Sevilla).

At the end of the work, tests are performed on flip-flops of an integrated circuit containing several Trivium stream ciphers, the results are analyzed and guidelines are designed to obtain information from the circuit.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 1 de 72

Índice

1.	Introducción	6
1.1.	Introducción de fallos con laser.....	7
1.2.	Aplicaciones.....	8
1.3.	Estudios sobre laser pulsado	9
1.4.1	Búsqueda de bibliografía y adaptación al proyecto.....	10
1.4.2	Bibliografía	10
1.4.3	Adaptación de la programación	11
2	Equipos de laboratorio.....	13
2.1	Perspectiva general	13
2.2	Módulo <i>PulSys</i>	14
2.2.1	Microscopio	15
2.2.2	Monitor	16
2.2.3	Eje Z.....	16
2.2.4	Plataforma motorizada de desplazamiento ZRANGE200.....	17
2.3	Módulo <i>PulsBox</i>	17
2.3.1	Control del laser	18
2.3.2	Fuente del laser.....	20
2.4	Analizador Lógico	21
2.5	Osciloscopio Digital.....	22
2.6	Fuente alimentación.....	22
2.7	Preparación del láser pulsado.....	24
2.7.1	Activar la regleta trasera.....	24
2.7.2	Activar regleta delantera, encender los instrumentos.....	25

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 2 de 72

3	Descripción del circuito integrado	28
3.1	Arquitectura del circuito de prueba	29
3.2	Generación de patrones y adquisición de datos	30
4	Descripción de la interfaz del programa	33
4.1	Introducción	33
4.1.1	Iniciación del programa	34
4.1.2	Colocar en la posición inicial el puntero laser.....	37
4.2	Desarrollo de las aplicaciones de programa.	38
4.2.1	Ventana de inicio y ventana de ejecución	38
4.2.2	Creación de ruta de puntos	41
4.2.3	Ajustes del laser	43
4.3	Modo Prueba	44
4.3.1.	Funciones generales (Bombardeo_manual)	45
4.3.1.1	Base de datos	45
4.3.1.2	Función manual.....	46
4.3.1.3	Automatización.....	50
4.3.2.	Código de la interfaz gráfica (Bombardeo_personalizado)	51
5	Resultados experimentales	54
5.1	Ensayos preliminares.....	55
5.2	Resultados	59
5.2.1	Análisis de las áreas de exposición.....	59
5.2.2	Análisis a baja energía	61
5.3	Ensayo con flip-flop de solo lectura	62
6.	Conclusión.....	64
6	Bibliografía.....	65

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 3 de 72

Índice de Figuras

Figura 1: Union P-N	8
Figura 2: Captura página principal US Figura 3: Captura Libros US	11
Figura 4: Página Pulscan Figura 5: Página Digilent.....	11
Figura 6: Librería PyQt5.....	12
Figura 7: Visión general del sistema Láser	14
Figura 8: Microscopio.....	15
Figura 9: Monitor.....	16
Figura 10: Ejemplo del sistema de control del eje Z.....	16
Figura 11: Marcador ajustable y controlador.....	17
Figura 12: Ajuste de la cabeza en el eje Z.....	17
Figura 13: Panel frontal PULSCAN.....	18
Figura 14: Fuente del laser	21
Figura 15: Digital Discovery y Waveform	22
Figura 16 : Parte frontal de la fuente de alimentación.....	23
Figura 17: Regleta trasera	25
Figura 18 : Parte de debajo de la mesa	25
Figura 19: Modulo PulsBox y PC	26
Figura 20: Pantalla de información PulsBox a) preparación b) modulo listo	27
Figura 21: Registro de desplazamiento y carga paralelo	30
Figura 22: Patrón creado en WaveForm	31
Figura 23: Cronograma de patrones de entrada	32
Figura 24: Programas de escritorio	34
Figura 25: Consola de PulSys.....	35
Figura 26: Interfaz grafica del módulo pico	36
Figura 27: Nueva interfaz	37
Figura 28: Texto dibujado en el circuito	37
Figura 29: Controlador eje Z y controlador eje X, Y	38
Figura 30: Ventana inicio ruta	39

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 4 de 72

Figura 31: Ventana ejecución.....	40
Figura 32: Ventana Datos	41
Figura 33: Ventana crear rutas.....	42
Figura 34: Ventana ajustes	43
Figura 35: Código inicio ventana.....	51
Figura 36: Código de la barra del Eje x.....	52
Figura 37: Punto con cambio 0->1 Figura 38: Punto con cambio 1->0.....	52
Figura 39: Clase punto.....	53
Figura 40: Códigos ejemplo Qt Design	53
Figura 41: Apertura orificio en el circuito ASIC y placa de prototipado	54
Figura 42. R90 R27 MY90 MX90	55
Figura 43: Recorrido flip-flop.....	56
Figura 44: Ventana inicio	58

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 5 de 72

Índice de Tablas

Tabla 1: Características de las lentes	15
Tabla 2: Características PulsBox	18
Tabla 3: Diferentes combinaciones del M0, M1, M2 para los modos trigger	20
Tabla 4: Entradas y salidas del módulo PulsBox	20
Tabla 5: variables base de datos	45
Tabla 6: Función manual.....	46
Tabla 7: Tablas función manual	50
Tabla 8: Automatización.....	50
Tabla 9: Análisis por zona.....	60
Tabla 10: Análisis de los flip-flops a baja energía	61
Tabla 11: Análisis de los flip-flops de lectura	62
Tabla 12: Análisis flip-flop baja energía	63

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 6 de 72

1. Introducción

El objetivo de este trabajo fin de grado es estudiar la inserción de fallos en flip-flops de un circuito integrado con un equipo láser. Para dicho estudio se va a necesitar una interfaz que facilite al usuario el diseño del ensayo, la visualización de los datos y el control de los equipos de laboratorio. Antes de la realización de este proyecto existía un programa que permitía realizar pruebas con el equipo de laser pulsado, el cual necesitaba algunas mejoras para evitar confusiones y modificar parámetros que daban lugar a fallos en el programa. Además, en este trabajo se ha desarrollado una metodología para, usando la posición de errores, localizar flip-flops sin conocer sus posiciones y extraer el valor lógico almacenado de estos flip-flops.

Para poder hacer los ensayos se han usado los equipos del Instituto de Microelectrónica de Sevilla (IMSE, del Centro Nacional de Microelectrónica, CNM-CSIC, Universidad de Sevilla). En esta memoria se describen todos los equipos y componentes utilizados además del circuito integrado utilizado para los ensayos y que ha sido utilizado como vehículo de test.

Aunque se ha tenido como punto de partida los códigos desarrollados por otras personas que ya habían trabajado antes con estos equipos, se han tenido que crear nuevos ficheros y programas para poder crear funciones más sencillas y mejorar el proceso de diseño del ensayo.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 7 de 72

1.1. Introducción de fallos con laser

La inserción de fallos se basa en usar una técnica para alterar el funcionamiento de un circuito, produciendo algún error con el objetivo de cambiar sus salidas. Existen diversos tipos de técnicas a aplicar para introducir fallos: el control de la tensión de la alimentación del circuito, la introducción de picos o perturbaciones en la frecuencia del reloj, el aumento de la temperatura de operación, la inserción de perturbaciones electromagnéticas, la utilización de un láser pulsado, entre otras. Todas ellas se basan en modificar el entorno de operación del circuito. También hay muchos trabajos basados en estudiar la respuesta ante estos fenómenos y como mitigarlas. En este trabajo vamos a utilizar un láser pulsado como mecanismo de introducción de fallos en un circuito.

El primer reporte sobre el uso de un haz láser para modificar el estado interno en un circuito integrado fue en 2002 realizado por S. Skorobogatov and R. Anderson [1]. En este trabajo se comprobó que el efecto de la radiactividad y el del láser tenían ciertas similitudes físicas y por tanto el efecto del láser se podía usar como simulación para el efecto radiactivo.

La inserción de fallos con esta técnica se basa en intentar inducir una corriente en una unión P-N de un semiconductor. Para ello el láser produce pares electrón hueco a lo largo de su recorrido (Figura 1). Cuando hay suficientes pares electrón hueco se absorben los electrones sobrantes produciendo una corriente inducida y haciendo que el circuito produzca una respuesta errónea. Si no se le aplica un láser muy potente, el propio semiconductor se regula produciendo un efecto transitorio. Si se aplica con demasiada energía este fallo se puede volver permanente [2].

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

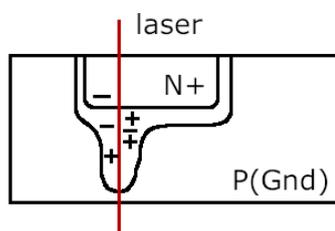


Figura 1: Unión P-N

Desde esta primera publicación ([1]), la inserción de fallos por láser se ha considerado un método bastante eficiente ya que en los ensayos se puede controlar tanto la variable de la posición donde insertar el fallo como el momento exacto para disparar el láser. Además, permite cambiar los valores bit a bit haciéndolo un experimento bastante preciso. Sin embargo, la capacidad de insertar fallos bit a bit puede estar limitado por la escala nanométrica de la tecnología ya que tecnologías demasiado pequeñas pueden producir que el haz del láser influya en dos o más flip-flops a la vez [3].

1.2. Aplicaciones

El estudio de la introducción de fallos por láser pulsado se utiliza para obtener datos, por ejemplo, en criptografía y en diseños que operan en entornos de alta radiación (por ejemplo, diseños localizados en aplicaciones espaciales), siendo muy útiles para localizar posibles vulnerabilidades en el circuito.

En la encriptación, por ejemplo, los ataques de fallos permiten obtener la clave secreta. Esto podría ser relevante en el caso de uso de tarjetas inteligentes las cuales llevan un microcontrolador y tienen la función de almacenar, cifrar y descifrar datos. En este tipo de tarjetas se pueden obtener sus datos si no están protegidas ante este tipo de ataques.

En el caso de su uso en entornos de alta radiación se intenta prevenir y estudiar aquellos errores que se puedan producir debido a la exposición del circuito a partículas de alta radiación cuando se manda un circuito a entornos con alta radiación tales como el espacio o centrales nucleares u otros tipos de

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 9 de 72

entornos hostiles. Estas radiaciones degradan el funcionamiento de los circuitos produciendo cambios transitorios o permutantes. En algunos casos, las técnicas experimentales se combinan con simulaciones para prevenir posibles fallos y crear sistemas más robustos.

1.3. Estudios sobre laser pulsado

A día de hoy existen algunos estudios que han realizado ensayos de laser pulsado con diferentes tecnologías. Algunos han intentado analizar la imagen que deja un mapa de errores en una zona donde hay un flip-flop [4] [5]. También se han probado en diferentes tecnologías, como en CMOS 28 nm [6] [7], 90 nm [8] y en memorias SRAM (*Static Random Access Memory*) [9]. En otros trabajos se ha llegado a simular el efecto de un láser pulsado para predecir las vulnerabilidades de un circuito [10].

A nivel de funcionamiento y seguridad existe un estudio basado en el análisis de la encriptación RSA (*Rivest, Shamir y Adleman*) el cual analiza su operación principal basada en un exponente seguido de un módulo $R = A^D \text{ mod } c$. Después de encontrar algunos defectos y descubren el proceso de la operación el cual sería más óptimo para obtener la clave (D). También exploran ciertas soluciones para intentar dificultar la obtención de la clave [11].

A nivel hardware existe un artículo que colocó una serie de contramedidas basadas en la detección y la reacción ante un ataque. Este trabajo estaba basado en unos sensores de corriente de inducción y un actuador el cual borra los datos en el instante en el que se detecta algún ataque, realizando también pruebas de errores para comprobar su eficiencia [12].

Para el caso de los efectos de radiación existe un estudio el cual recoge una gran cantidad de información sobre los efectos de un circuito fuera de la atmosfera terrestres [13].

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 10 de 72

Otra de las aplicaciones, además de la seguridad en un circuito y el buen funcionamiento, es usar el láser para simular efecto de la radiación, ya que ambos efectos tienen bastante similitud [14].

1.4.1 Búsqueda de bibliografía y adaptación al proyecto

1.4.2 Bibliografía

La bibliografía utilizada en el desarrollo de este proyecto se ha sacado en su mayoría de la página web de la biblioteca de la universidad de Sevilla, usando como base el trabajo fin de grado de Fernando López Orellana, [15] (alumno que se encargó el año 2021 de estudiar el uso del *Digital Discovery* y crear la primera interfaz de los ensayos del láser pulsado y realizar ensayos con el láser). De entre los artículos utilizados cabe destacar un artículo llamado *Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model*, [7] además de otros artículos buscados e bibliografía relacionados con el tema en cuestión. Otros apoyos bibliográficos están referenciados en esta memoria.

El uso de la página web de la biblioteca de la universidad de Sevilla el cual su dirección es <https://bib.us.es/> es bastante intuitivo.

1.- Primero una vez dentro tiene un buscador en el centro de la pantalla en el cual se puede buscar los títulos de los artículos, pero antes hay que marcar la opción de (Todo (artículo/idus/catalogo)) (Figura 2).

2.- Una vez encontrado el artículo en cuestión se hace clic en título del artículo. Esta abrirá una nueva ventana en el cual habrá diferentes apartados. El que nos interesa es Ver en línea (Figura 3).

3.- Este apartado primero pide el usuario y contraseña del UVUS y luego nos redirige a la página web donde está publicada el artículo (IEEE Xplorer, Springer link, etc...).

	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

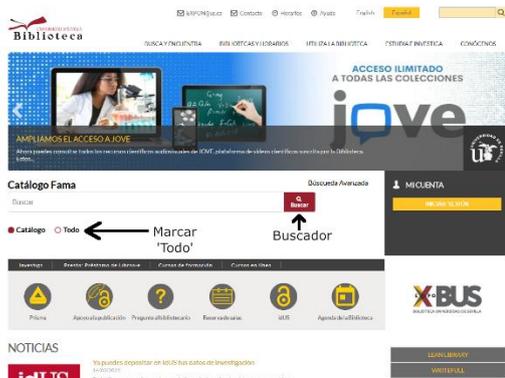


Figura 2: Captura página principal US

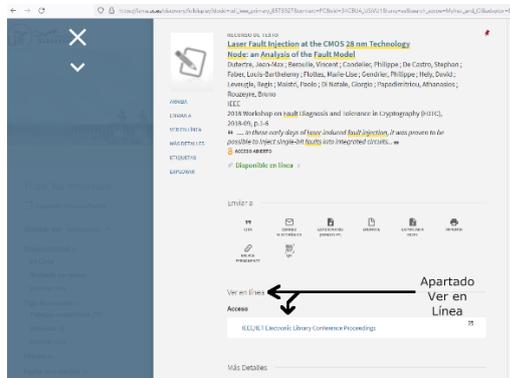


Figura 3: Captura Libros US

Para los equipos electrónicos del laboratorio el procedimiento usado ha sido guardar el nombre de las marcas de la mayoría de los equipos del laboratorio y buscar en sus páginas correspondientes las fichas técnicas de dichos equipos (Figura 4 y Figura 5).

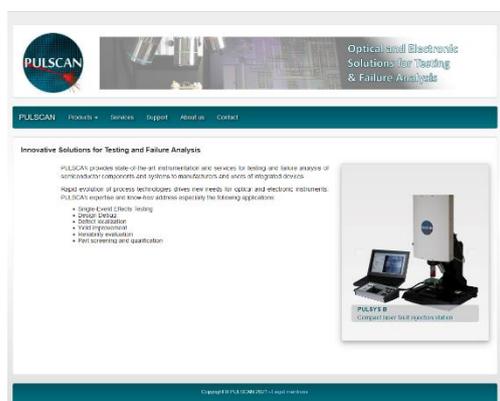


Figura 4: Página Pulscan



Figura 5: Página Digilent

1.4.3 Adaptación de la programación

La programación de todo el software se ha llevado cabo en el lenguaje Python, puesto que los programas de partida estaban escritos en ese lenguaje.

Para aprender a programar en *PyQt5* al ser una herramienta bastante utilizada se utilizaron diferentes foros tanto en español como en inglés donde se explicaban sus funciones, aunque las funciones se pueden encontrar buscando la librería de *PyQt5* en C++ [16] (Figura 6) ya que lo que se utiliza

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 13 de 72

2 Equipos de laboratorio

2.1 Perspectiva general

Los equipos del laboratorio utilizados permiten realizar el estudio de cómo afecta a un flip-flop el ataque con el haz del láser pulsado a diferentes energías y si es posible modificar su valor lógico almacenado de manera controlada con este sistema. En la Figura 7 se pueden observar los diferentes equipos utilizados en el laboratorio del sistema laser. Los principales son:

- Un sistema de laser pulsado el cual se compone a su vez de dos módulos, *PulsBox* (es el encargado de generar el pulso láser) y el módulo *PuISys* (engloba todos los sistemas encargados del desplazamiento de la plataforma de medida).
- Un osciloscopio digital que permite capturar las señales de un circuito integrado (*Infiniium 9000 Series*).
- Un analizador lógico de bajo precio y portátil que permite generar y adquirir señales del circuito integrado de manera cómoda (*Digital Discovery*).
- Una fuente de alimentación lo suficientemente modular para alimentar el circuito.
- Un ordenador con sus drivers y programas correspondientes.

A continuación, pasamos a describir detalladamente cada uno de los equipos del laboratorio.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

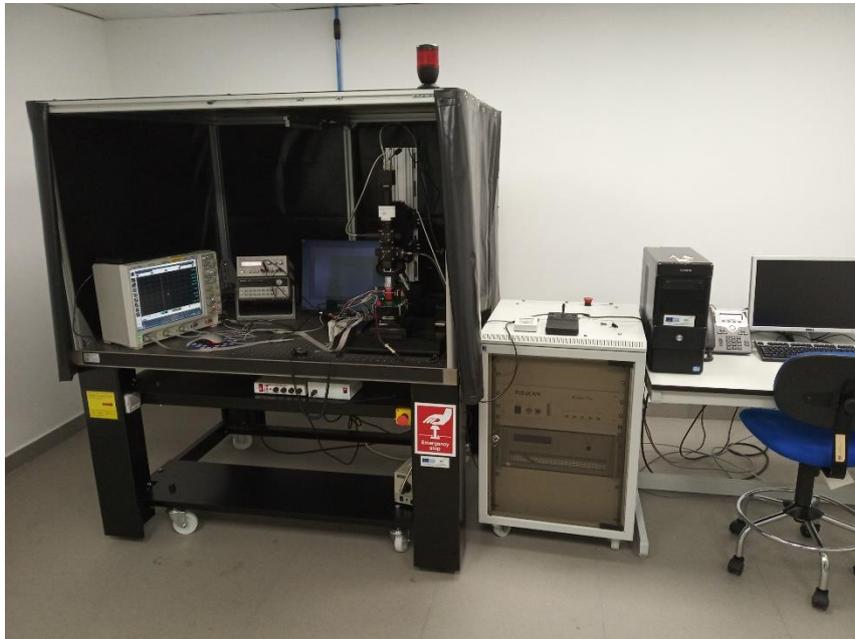


Figura 7: Visión general del sistema Láser

2.2 Módulo *PulSys*

El módulo *PulSys* es el sistema que permite el desplazamiento del haz del láser sobre la superficie del circuito. Es uno de los componentes principales del láser y se compone de:

- Microscopio.
- Monitor.
- Plataforma motorizada de desplazamiento. *ZRANGE200*.
- Dial de rotación en el ángulo theta.
- Diales de modificación de la inclinación.
- Ejes de movimiento.
- Otros equipos como fuente de alimentación o marcadores de desplazamiento.

La mayoría de las características y usos sobre los equipos de este laboratorio se encuentra en el manual de usuario de laser pulsado [18].

2.2.1 Microscopio

El microscopio está compuesto por:

- Un soporte mecánico.
- Cabezal óptico.
- Plataforma del eje Z.
- Plataforma del eje X e Y.

El diseño de la cabeza óptica esta optimizado para la visualización de dispositivos de silicio. También esta optimizado para pulsos de alta energía y para eliminar ruido de longitud de onda de 1064 nm. La cabeza óptica tiene tres lentes de diferentes aumentos, cuyas características se muestran en la Tabla 1.

Aumento	X5	X20	X100
<i>Distancia focal (mm)</i>	36.1	22.2	10
<i>Apertura numérica</i>	0.16	0.35	0.7
<i>Profundidad de campo (μm)</i>	10.7	2.2	0.7

Tabla 1: Características de las lentes

También tiene una cámara nGaAs C10633-23 que visualiza la imagen del circuito en un monitor (Figura 8).

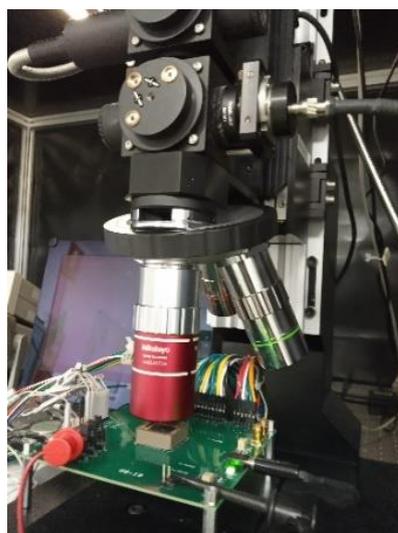


Figura 8: Microscopio

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		
			Página 16 de 72

2.2.2 Monitor

El equipo del láser dispone de un monitor LCD (Figura 9) para la observación directa del dispositivo bajo test (en sus siglas DUT) a través de la cámara anteriormente mencionada. Además, también hay disponible unos marcadores ajustables en pantalla para la nivelación de la plataforma en los ejes X e Y, señalización del spot del láser en el DUT, etc.

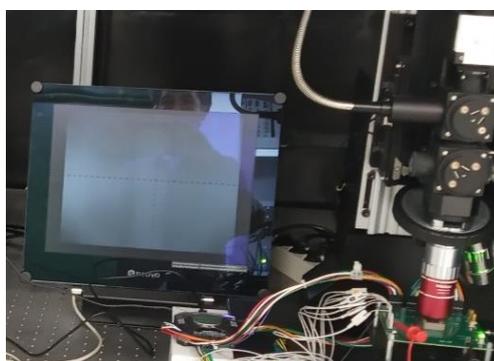


Figura 9: Monitor

2.2.3 Eje Z

El movimiento del circuito en el eje Z (Figura 10 y Figura 11) está compuesto por 3 componentes. Uno encargado del eje, colocado debajo del circuito, un controlador que se conecta al ordenador y el mando para controlarlo de forma manual.

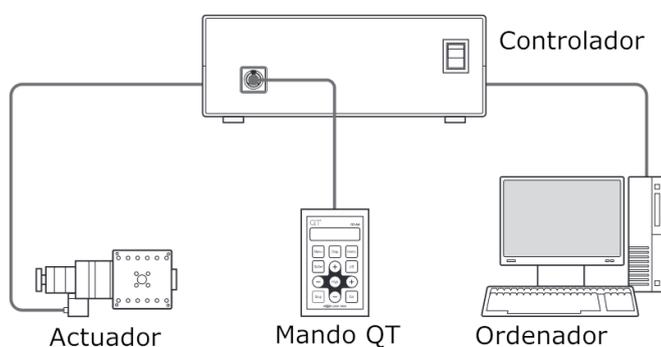


Figura 10: Ejemplo del sistema de control del eje Z

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		
			Página 17 de 72

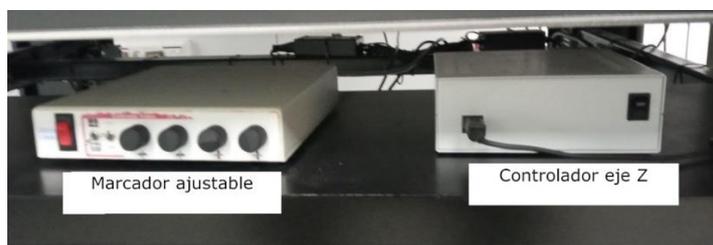


Figura 11: Marcador ajustable y controlador

2.2.4 Plataforma motorizada de desplazamiento ZRANGE200

El microscopio tiene la opción de modificar su altura hasta 20 cm (Figura 12). Si un objeto no se pudiera colocar bajo la lente, habría que aflojar los tornillos de ajuste, visibles en la Figura 12 y subir todo el conjunto con la máxima precaución para no dañar ningún componente ni modificar su configuración.

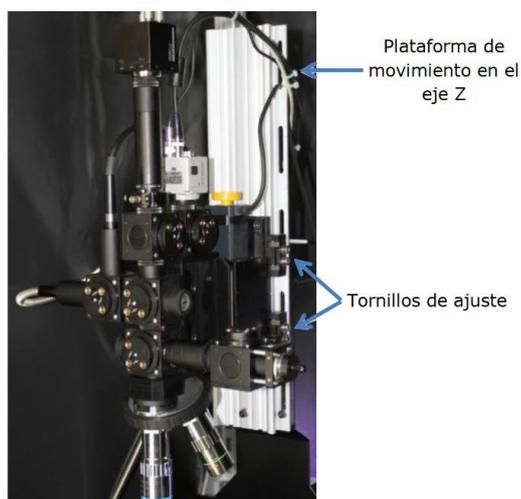


Figura 12: Ajuste de la cabeza en el eje Z

2.3 Módulo PulsBox

El módulo PulsBox es el encargado de generar la energía del láser y en él se ajusta las configuraciones como la potencia, el modo del disparo o *trigger*, etc.

El módulo *PulsBox* está compuesto por dos partes, la fuente del láser y el control del láser. Sus características más importantes se muestran en la Tabla 2.

Longitud de onda	1064 nm
Duración del pulso	30 ps
Energía máxima del pulso	50 nj
Potencia máxima del pulso	1.67 KW
Potencia máxima media	0.5 W
Rango de frecuencia	Hasta 20 MHz
Resolución de la energía	0.0025 %
Dimensiones	Rack de 19"
Polarización	Lineal
Salida de fibra óptica	Modo único

Tabla 2: Características PulsBox

2.3.1 Control del laser

El panel frontal está compuesto por 4 secciones (Figura 13):

- 1) Botón On/Off (*POWER*).
- 2) Bloqueo del láser (*Laser Enable*).
- 3) LEDs de estado.
- 4) Entradas y salidas de señales por conector *BNC*.
- *Boton On/Off*



Figura 13: Panel frontal PULSCAN

El botón On/Off es el primer paso para encender el módulo *PulsBox*. Hay que esperar unos 10 minutos para desactivar el bloqueo del láser después de pulsar el botón. El tiempo se indica en una pantalla a la izquierda superior de la fuente del láser.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 19 de 72

- *Bloqueo del láser*

El bloqueo del láser permite activar y desactivar el láser de forma manual. Se tiene que girar después de los 10 minutos de encenderse y si la llave está bloqueada no se puede disparar el láser por software. Por tanto, sirve a modo de bloqueo de seguridad.

- *Leds de estado*

La columna de leds permite ver tanto la configuración del láser como su estado o si hay errores.

Los diferentes leds son:

- Config: Encendido cuando la configuración está cargada.
- Boot: Encendido después de la inicialización de los elementos de control del láser.
- L0: Encendido cuando la fuente del láser tiene alimentación.
- L1: Encendido durante el tiempo de calentamiento del láser.
- L2: Encendido cuando el láser está listo.
- L3: Encendido cuando el láser está activado.
- M0, M1, M2: Códigos del modo de trigger. Las distintas combinaciones de estos LEDs se recogen en la Tabla 3.
- Trig: Encendido cuando la señal en la entrada “Trig In” está a nivel alto.
- Gate: Encendido cuando la señal en la entrada “Gate In” está a nivel alto.
- E0, E1, E2: Códigos de error (reservado para mantenimiento).
- Interlock: Encendido cuando el bloqueo del láser está activado.
- R0, R1, R2: Reservado.
- Pulse: Encendido durante la emisión de un pulso (no visible para pulsos de picosegundos).
- Ethernet status: Encendido cuando hay comunicación Ethernet.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 20 de 72

Nombre	Trig In	Gate In	Int Clk	Continuos
M0	On	Off	Off	On
M1	Off	On	Off	On
M2	Off	Off	On	On

Tabla 3: Diferentes combinaciones del M0, M1, M2 para los modos trigger

- Entradas y salidas BNC

En el panel frontal se encuentran disponibles cinco entradas/salidas por conectores BNC. La descripción de estas señales se muestra en la Tabla 4.

Nombre I/O	Voltaje mínimo	Voltaje máximo	Descripción
Laser Clk (salida)	2.2V	2.7V	Tren de pulsos a 10 MHz en fase con el oscilador del láser
Trig In (entrada)	2.2V	2.7V	Señal trigger de entrada
Gate In (entrada)	2.2V	2.7V	Señal de entrada. Si no está conectada, la señal está en alto (pull-up)
Synch Out (salida)	0V	3.3V	Lectura de la ventana de selección del pulso
Pulse Out (salida)	0V	3.3V	Lectura de la salida del pulso (señal analógica)

Tabla 4: Entradas y salidas del módulo PulsBox

2.3.2 Fuente del laser

La fuente del láser tiene una pantalla LCD (Figura 14) en la parte superior izquierda donde se va a indicar toda la información del estado. Por ejemplo, el tiempo de espera de calentamiento del láser y dos leds a la derecha donde se indica si el láser está habilitado.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 21 de 72



Figura 14: Fuente del laser

2.4 Analizador Lógico

Digital Discovery (Figura 15) es un equipo compacto y portátil que combina la función de analizador lógico y generador de patrones el cual usamos para introducir patrones en el circuito y analizar las salidas de éste. Se conecta al circuito usando cables simples por sus entradas, sus salidas y conectándolo al ordenador vía USB.

Para poder usarlo hay que instalar en el ordenador el driver gratuito *WaveForms*. Con el driver también se pueden crear formas de ondas, lectura de las señales y controlar las salidas a tiempo real con su interfaz. En nuestro caso controlamos el dispositivo mediante un programa *Python*. El programa genera patrones y luego usamos su librería para programar por *Python* la lectura del archivo .txt que genera las formas de onda que se representan en *WaveForms* y se la introducimos al *Digital Discovery*. La forma de hacer esto está explicado en la documentación del dispositivo a la que se puede acceder a través de la página principal de *Digilent* indicado en la bibliografía [19].

Una vez conectado el *Digital Discovery* por USB la mayoría de los errores que se suelen producir se deben a que el programa tiene la dirección incorrecta del aparato porque haya habido una interrupción del programa o se ha conectado el equipo después de abrir el programa. Estos problemas se solucionan cerrando el programa, desconectando y volviendo a conectar de nuevo el *Digital Discovery* y volver a abrir el programa. Si aparece una luz azul es que el *Discovery* está en modo espera, que es el estado necesario para generar un patrón.

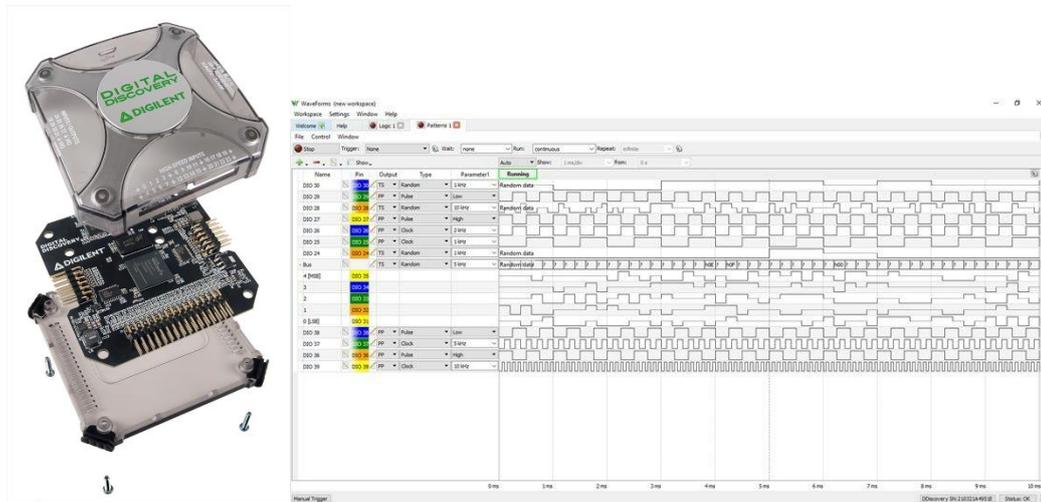


Figura 15: Digital Discovery y Waveform

2.5 Osciloscopio Digital

Un osciloscopio es un instrumento electrónico dedicado a la representación gráfica de una señal electrónica que varía en el tiempo. Comúnmente se representan los valores en una gráfica donde el eje X está dedicada al tiempo y el eje Y está dedicada normalmente a la tensión.

En el laboratorio se ha usado un osciloscopio *Infiniium* 9000 Series que combina la función de osciloscopio, analizador analógico y analizador de protocolos. En nuestro caso utilizamos la función del osciloscopio, conectando las principales señales del circuito integrado (máximo de 16) y configurando la señal de disparo (flanco de subida) del osciloscopio con la señal de carga de datos al circuito. Así es posible ver todas las señales cada vez que se introducen nuevos datos al circuito [20].

2.6 Fuente alimentación

Se necesita una fuente de alimentación para polarizar los circuitos que se coloquen en el banco del laboratorio. En nuestro caso se tiene una placa de prueba que contiene un circuito que se alimenta con 5V. La placa lleva a su vez

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

un regulador de alimentación que proporciona alimentación de 2.5V y 1.2V que son las que necesita el circuito integrado [21].

Como fuente de alimentación se ha usado un modelo *HP Model E3630A* (Figura 16), que tiene una triple salida de tensión. A 20V otra a -20V y la del centro a 0V y soporta una corriente de 0,5A nominales. Se puede usar la salida de $\pm 20V$ para generar 40V y 0,5A nominales. También tiene una salida de 6V con una intensidad nominal de 2.5A y todas las salidas tiene protección de sobrecarga y cortocircuito [21]. Gráficamente, sus elementos se detallan en la Figura 16.

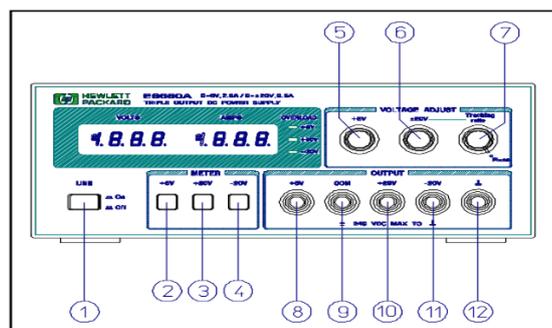


Figura 16 : Parte frontal de la fuente de alimentación

- 1.- Botón de encendido
- 2.- Botón medida salida de 6V
- 3.- Botón medida salida de 20V
- 4.- Botón medida -20V
- 5.-Ruleta de las salidas de 6V
- 6.- Ruleta de la salida de 20V
- 7.- Tracking ratio
- 8.- Salida de 6V
- 9.- Salida COM
- 10.- Salida de 20V
- 11.- Salida de -20V
- 12.- Entrada a tierra

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 24 de 72

2.7 Preparación del láser pulsado

A continuación, se van a detallar todos los pasos a seguir para configurar el test o ensayo del circuito, pero los pasos después de iniciar el ordenador se detallarán en el Capítulo 4 dedicado al código. Los pasos van a ser:

- 1) Activar la regleta trasera de alimentación general.
- 2) Activar regleta delantera para el monitor, fuente de alimentación eje Z y fuente de la luz infrarroja.
- 3) Alimentar el circuito, encender el osciloscopio, conectar el analizador lógico *Digital Discovery*.
- 4) Encender el módulo *PulsBox*.
- 5) Encender el PC y sus programas correspondientes.
- 6) Colocar en posición inicial el puntero del láser.
- 7) Activar el modo pruebas en el láser.

2.7.1 Activar la regleta trasera

Antes de comenzar con el encendido del sistema láser, hay que asegurarse de que todas las conexiones eléctricas estén operativas y que todas las regletas del laboratorio están conectadas y encendidas. Como observación se puede decir que la regleta que está justo detrás de la mesa anti-vibración, como se puede apreciar en la (Figura 17), suele estar desactivada para evitar que los ventiladores del módulo *PulsBox* queden encendidos.

Cuando se finalice la jornada de trabajo con el láser hay que asegurarse que esta misma regleta quede desactivada nuevamente.

			
	Memoria	Documento 1	
Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 25 de 72



Figura 17: Regleta trasera

2.7.2 Activar regleta delantera, encender los instrumentos

Una vez encendida la regleta trasera. Se comprueba que las conexiones de la regleta delantera están debidamente conectadas, se activa y se encienden los marcadores del monitor, el eje Z y la fuente infrarroja (Figura 18). La regleta está sobre la mesa anti vibración detrás de la pantalla.

En este momento se puede encender la pantalla y ver en el monitor donde está colocado el eje del láser y controlar el eje Z. pero no se puede controlar el eje X, Y hasta que se encienda el PC.



Figura 18 : Parte de debajo de la mesa

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 26 de 72

Ahora hay que polarizar el circuito. Para ello con el cable de alimentación desconectado se comprueba que la tensión de la fuente de alimentación son 5V entre la salida de +20V y tierra de la fuente. Se apaga, se conecta la fuente al circuito en las entradas de +20V y tierra y se comprueba que la intensidad suministrada se sitúa alrededor de 0.02A una vez encendida de nuevo la fuente. Una vez hecho esto se puede conectar el analizador Digital Discovery por el USB y encender el osciloscopio el cual tarda unos minutos.

Finalmente se enciende el módulo *PulsBox* dando al botón (Figura 19) (*On/Off power enable*) y se conecta el cable del *trigger*. Hay que coger las gafas de seguridad y darles a los interruptores de las luces antes de girar las llaves por motivo de seguridad ya que en este momento los módulos están listos para disparar un haz de láser pulsado. No se puede girar la llave hasta que no pase unos 10 min. Ya que este es el tiempo en el que tarda el módulo *PulsBox* en activarse (Figura 20). También es recomendable tapar un poco con la cortina de la cabina del circuito como protección.

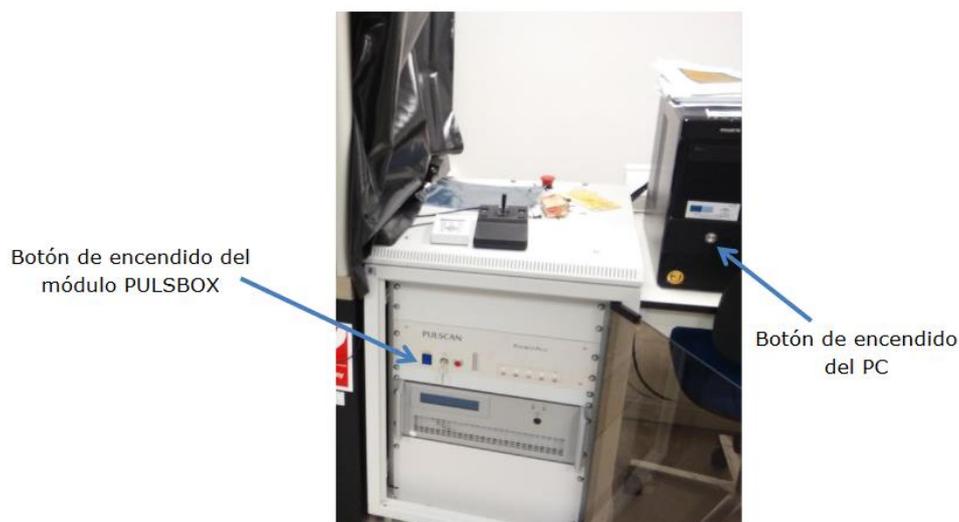


Figura 19: Módulo PulsBox y PC

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 27 de 72

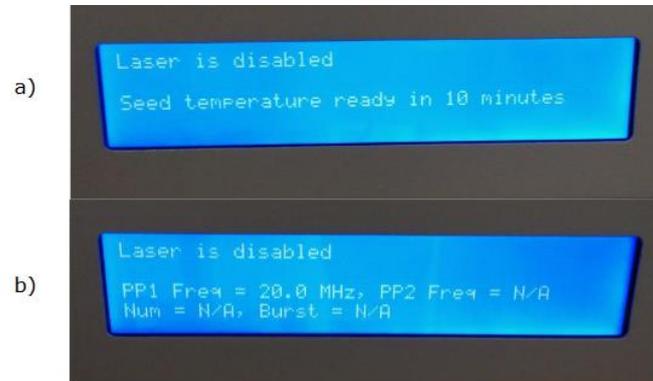


Figura 20: Pantalla de información PulsBox a) preparación b) modulo listo

A continuación, es posible una vez encendido el PC y todos sus programas, comenzar con el ensayo. Este paso se indica en el Capítulo 4 sobre el código.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 28 de 72

3 Descripción del circuito integrado

El circuito integrado o ASIC utilizado como vehículo de test y usado en los ensayos está tiene en su interior tres bloques cada uno de los cuales incluye diseños de diferentes circuitos. Los principales diseños son cifradores de flujo Trivium, algunos de ellos con lógica adicional para permitir pruebas de contramedidas y de introducción de fallos además de algunos bloques de comunicación criptográfica.

Para la realización de este TFG no ha sido necesario el conocimiento completo del funcionamiento del circuito Trivium, ya que solo se van a usar ciertos flip-flops de su registro de estado para comprobar el efecto de un haz del láser sobre ellos y cómo afecta al contenido almacenado en ellos el uso de diferentes energías de incidencia y el bombardeo en diferentes posiciones. Tampoco es necesario el conocimiento del funcionamiento completo del circuito integrado, aunque es aconsejable una pequeña explicación sobre el funcionamiento del cifrador de flujo Trivium.

El cifrador Trivium es un cifrador de flujo basado en un registro de desplazamiento de 288 bits con realimentaciones en ciertos bits y que se puede dividir en tres registros de desplazamiento de diferente longitud (con 288 bits en total). El circuito es capaz de generar usando 80 bits de una clave y un vector de inicialización también de 80 bits, hasta 2^{64} bits a la salida del circuito.. El proceso de inicialización requiere de 1152 ciclos de reloj antes de poder sacar una trama de datos encriptada [22].

También en el ASIC hay versiones para salidas multibit del cifrador Trivium, que permiten sacar varios bits en paralelo y versiones optimizadas del cifrador de flujo Trivium para consumo de baja potencia.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 29 de 72

3.1 Arquitectura del circuito de prueba

Para los ensayos con el láser en este el TFG se han usado flip-flops que pertenecen a unos cifradores Trivium implementados en el ASIC que llevan además un registro de desplazamiento paralelo-serie asociado a su registro de estado serie de 288 bits que permite leer el contenido del registro y enviarla vía serie a la salida del circuito integrado, siendo posible por tanto leer y escribir estos registros y por consiguiente también sus flip-flops, véase la Figura 21.

En los ensayos llevados a cabo se carga el registro de estado con valores lógicos de ceros y unos y a continuación se activa el láser pulsado para intentar producir en uno o varios flip-flops un cambio de valor (error). Después se comparan las salidas en el instante posterior del disparo para comprobar si ha habido cambio (se tiene hasta 288 flip-flops en cada registro del cifrador Trivium y se conocen sus posiciones en el ASIC). El proceso completo consiste en cargar en el circuito integrado la clave y el vector de inicialización que se va a utilizar en el Trivium (en este circuito esta carga se realiza de forma serie), pasarle al Trivium esta clave y este vector de inicialización (esto se hace de forma paralela) y una vez realizado el bombardeo con el láser cargar el registro de estado en el registro paralelo serie y sacar los datos al exterior de forma serie.

Para automatizar el proceso se ha usado la señal de carga de los flip-flops del registro paralelo-serie como señal de disparo del láser. Después del disparo se lee este registro y se compara con los resultados anteriores para buscar patrones de fallos.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

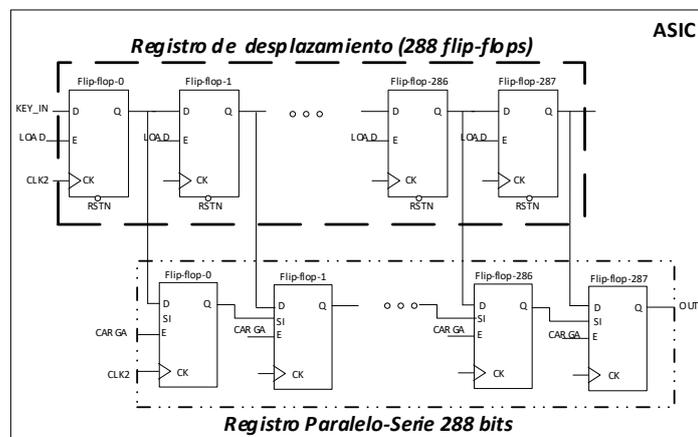


Figura 21: Registro de desplazamiento y carga paralelo

3.2 Generación de patrones y adquisición de datos

Para introducir los patrones en el registro de desplazamiento del ASIC se utiliza el analizador *Digital Discovery* (descrito en el Capítulo 2) el cual trae un programa gratuito llamado *WaveForm* (Figura 22) que permite crear patrones y cargarlos en el analizador.

La primera acción que se debe hacer es generar un patrón con la aplicación *WaveForm*. Después se comprueba el funcionamiento del circuito con ese patrón capturando los datos en la salida, visualizándolos con la propia aplicación *WaveForm* y también se exporta a un archivo de texto (.txt). La interfaz finalmente tendrá que leer este archivo y procesarlo adecuadamente para coordinarlo con la generación del pulso del láser, el movimiento del sistema laser y la lectura de los datos del ASIC.

El código para interpretar los archivos de texto, ejecutar el patrón e indicar los pines que se van a utilizar ya estaba realizado con anterioridad con indicaciones de todas las funciones necesarias y como utilizarlas [15]. En esta nueva versión se han añadido los ficheros y algunas optimizaciones en el código para que el programa tuviera más funciones y poder realizar los ensayos en menor tiempo.

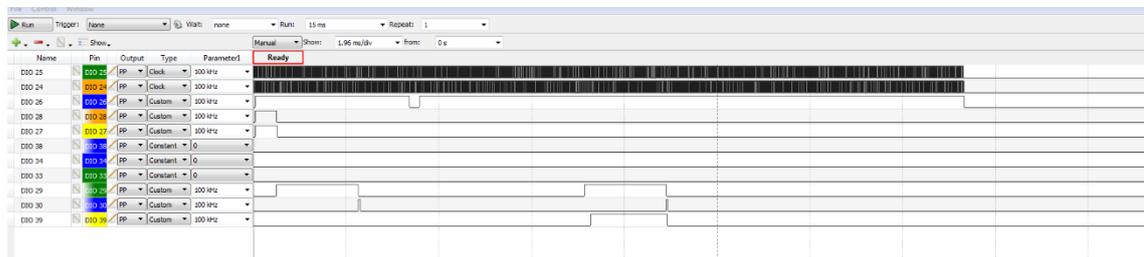


Figura 22: Patrón creado en WaveForm

Para generar un patrón lo primero que hay que tener en cuenta es que en el circuito a utilizar como banco de pruebas existen dos relojes. El reloj principal *CLK*, que se usa para todas las operaciones del circuito y el reloj secundario *CLK2* que se usa para leer y escribir datos serie, por tanto, si no se quiere introducir ningún dato se puede dejar *CLK2* como un valor constante.

En primer lugar, hay que diseñar un patrón con un pulso de *RESET* (es una entrada activa en nivel bajo, por tanto, el pulso es un '0' y después de un tiempo determinado se cambia a '1' para inicializar los bits del registro e indicar la configuración para que se active los módulos que contienen el registro de desplazamiento y registro paralelo-serie.

Después hay que activar la señal de habilitación del desplazamiento de los datos, *LOAD* tanto ciclos de reloj *CLK2* como datos se quiera introducir. En nuestros casos necesitamos introducir 172 bits para cargar la clave, el vector de inicialización y algunos otros bits de activación de los diferentes relojes de los circuitos Trivium, por tanto, se deja la señal *LOAD* en '1' durante 172 ciclos de reloj.

Con esta operación se consigue cargar en el registro de estado los 160 bits pertenecientes a la clave y al vector de inicialización. Los restantes bits hasta completar los 288 bits están prefijados a valores lógicos de 0's y 1's. Por último, se activa un ciclo de reloj la señal de cargar para almacenar este valor en el registro paralelo-serie y si el láser se encuentra operativo activarlo, véase Figura 23.

Para agilizar el ensayo cuando se quiere realizar otro disparo se le vuelve a introducir un valor lógico '0' en la señal *RESET* para inicializar los módulos y se vuelve a hacer de nuevo los pasos anteriores. Véase figura 23.

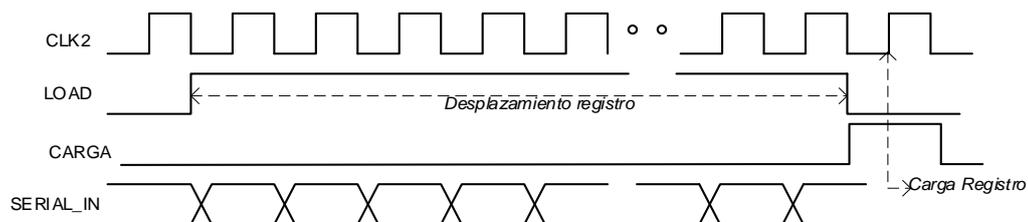


Figura 23: Cronograma de patrones de entrada

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 33 de 72

4 Descripción de la interfaz del programa

4.1 Introducción

La interfaz está programada en *Python* y se ha usado la librería de *PyQt5* para hacer la interfaz gráfica [16], ya que se estaba trabajando con este lenguaje y esta librería en los anteriores proyectos.

La gran ventaja de esta librería es que además de ser sencilla tiene bastante documentación tanto en su página principal como por otros usuarios que hacen resúmenes del uso de dicha librería. Sin embargo, su gran defecto es el mal funcionamiento cuando se usa para sistemas que sean externos al ordenador o PC, por ejemplo, en nuestro caso con la conexión del pulso laser y el equipo *Digital Discovery*., Parece que no se gestiona bien cuando se hace procesos externos y las ventanas se quedan ‘congeladas’. Por ello hay que tener un poco de cuidado y limita algunas funciones como, por ejemplo, no es viable que informe a tiempo real los fallos que hay en un test ya que puede producir problemas en la ventana.

Para los ensayos es necesario hacer incidir el haz de láser pulsado en una zona determinada del circuito integrado que contenga flip-flops para poder analizar su respuesta. . Se selecciona el registro de estado del cifrador de flujo Trivium y su registro paralelo asociado como banco de pruebas. Con este objetivo el programa primero recoge los datos sin usar el láser para obtener las salidas correctas del registro y luego hace incidir el láser pulsado en unos puntos indicados por sus coordenadas (X, Y) donde se tiene un flip-flop o varios. Después se recoge los datos y se compara con la salida correcta. Si se detecta alguna diferencia, se guarda la posición de las coordenadas donde se ha producido esta discrepancia o fallo, el tipo de fallo según su valor anterior e incluso es capaz de calcular solo con la salida, el flip-flop donde se ha producido el error. Finalmente muestra los fallos en una gráfica para que sea más visual para el usuario.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 34 de 72

En este TFG la nueva interfaz desarrollada permite hacer una ruta de puntos personalizada, eligiendo punto por punto el camino que va a seguir el láser o usando comandos que le permite diseñar con más agilidad la ruta. Se ha partido de un código realizado con anterioridad [17] el cual ha sido mejorado, simplificado y optimizado como en apartados posteriores se indica.

4.1.1 Iniciación del programa

Para ejecutar los ensayos se necesitan tres aplicaciones. El navegador para entrar en los ajustes del *PulsBox*, la consola del *PulSys* para comprobar que todo esté conectado (*PULSYS_Server_Controller*) (Figura 24) y encendido en el momento de realizar un ensayo (antes de usar esta interfaz se introducía los comandos directamente al laser) y un compilador *Python* (*JetBrains*) donde va a estar la aplicación de escritorio del láser. Mientras se está diseñando el programa y no se transforme en un ejecutable se inicia desde el compilador.

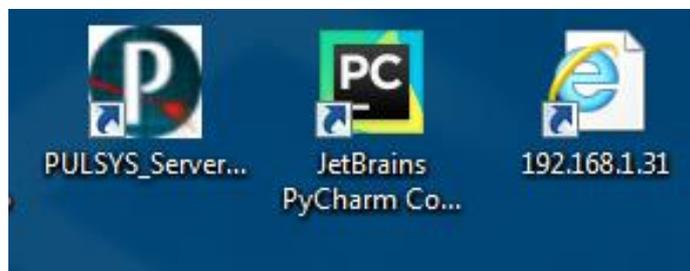
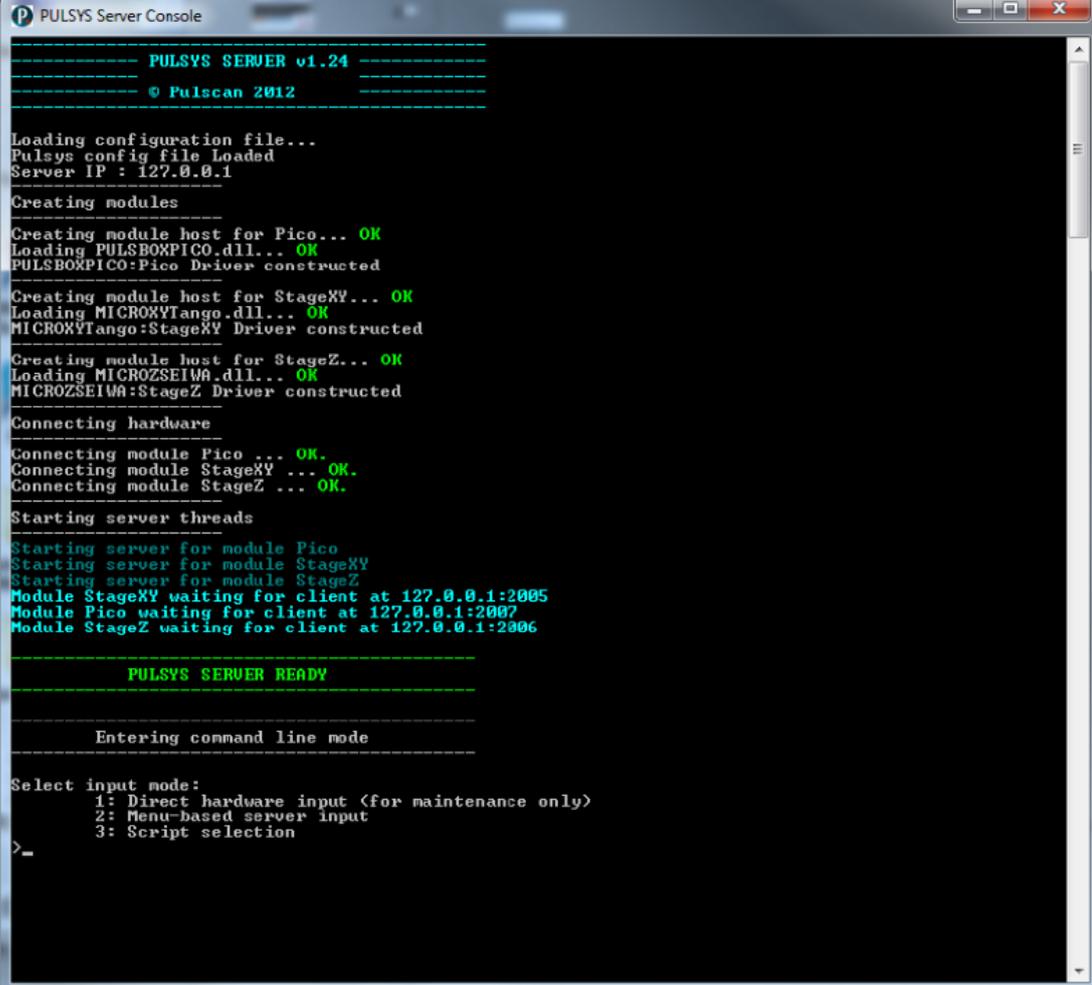


Figura 24: Programas de escritorio

Primero para comprobar que todos los sistemas están preparados se abre la ventana de comandos (Figura 25). Esto permite modificar los parámetros de posición X, Y, Z, potencia del láser, tipo de disparo del láser, retraso, etc., pero no se va a entrar en detalle ya que esto lo va a hacer la aplicación de escritorio. La ventana de comando permite ver todos los procesos que está realizando el láser a tiempo real.

			
	Memoria	Documento 1	
Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 35 de 72



```

PULSYS Server Console
-----
PULSYS SERVER v1.24
-----
© Pulscan 2012
-----
Loading configuration file...
Pulsys config file Loaded
Server IP : 127.0.0.1

Creating modules
-----
Creating module host for Pico... OK
Loading PULSBOXPICO.dll... OK
PULSBOXPICO:Pico Driver constructed

Creating module host for StageXY... OK
Loading MICROXYTango.dll... OK
MICROXYTango:StageXY Driver constructed

Creating module host for StageZ... OK
Loading MICROZSEIWA.dll... OK
MICROZSEIWA:StageZ Driver constructed

Connecting hardware
-----
Connecting module Pico ... OK.
Connecting module StageXY ... OK.
Connecting module StageZ ... OK.

Starting server threads
-----
Starting server for module Pico
Starting server for module StageXY
Starting server for module StageZ
Module StageXY waiting for client at 127.0.0.1:2005
Module Pico waiting for client at 127.0.0.1:2007
Module StageZ waiting for client at 127.0.0.1:2006

-----
PULSYS SERVER READY
-----

Entering command line mode
-----

Select input mode:
  1: Direct hardware input (for maintenance only)
  2: Menu-based server input
  3: Script selection
>_

```

Figura 25: Consola de PulSys

Luego hay que desactivar la sincronización del disparo, *Trig In*. Para ello se entra en el navegador y se introduce la dirección **192.168.1.31** (Figura 26).

Se accede a la interfaz gráfica del módulo *PulsBox Pico* y se desmarca la opción **Synchronize Trig In**. Finalmente se pulsa **apply all**.

También en esta ventana se puede apagar o encender el láser, útil cuando se interrumpe un experimento y se quiere apagar el láser de forma manual. Se puede modificar su retraso o *delay* y el modo de disparo o *trigger*.

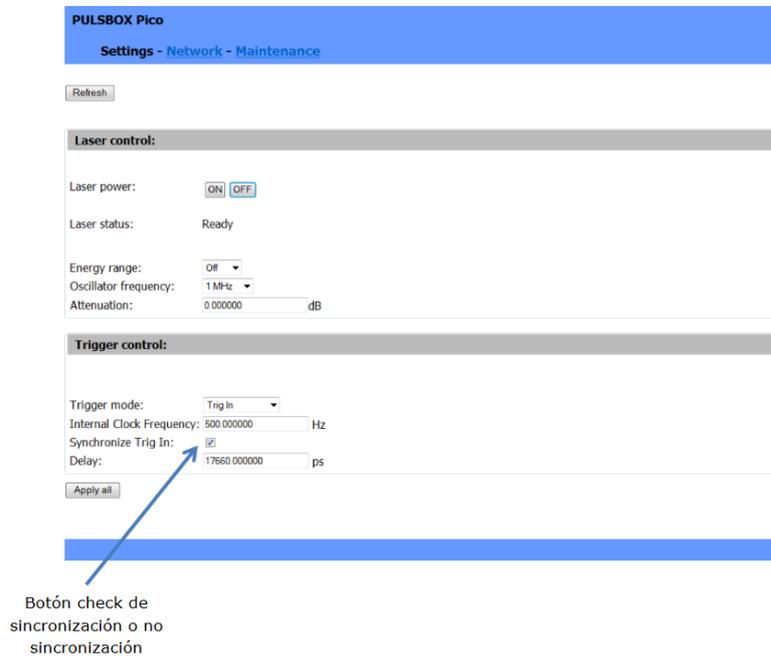


Figura 26: Interfaz gráfica del módulo pico

Finalmente hay que abrir el compilador y ejecutar el programa, seleccionar si se quiere entrar en el modo “Prueba” (pulsar *p* en la consola) o en el modo “Normal” (pulsar *n* en la consola), véase interfaz del programa Apartado 4.4.

El modo “Prueba” se utiliza para probar el funcionamiento del ASIC y preparar el cabezal del láser haciéndole un recorrido alrededor del chip. En el funcionamiento normal aparecer una ventana con tres pestañas Test Funcional, Introducción Fallos y, Bombardeo Manual, véase Figura 27. Cuando se esté dispuesto a hacer ensayos se selecciona la tercera pestaña la cual se corresponde con la nueva interfaz.

			
	Memoria	Documento 1	
Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 37 de 72



Figura 27: Nueva interfaz

4.1.2 Colocar en la posición inicial el puntero laser

Ahora que todos los sistemas están listos hay que colocar el puntero del láser en una posición de referencia. El programa cuando inicia un experimento guarda la primera posición y la usa como referencia para hacer sus movimientos y vuelve a ésta después de un experimento. Nosotros como punto de referencia usamos la esquina superior derecha de la U que esta dibujada en el circuito (Figura 28).

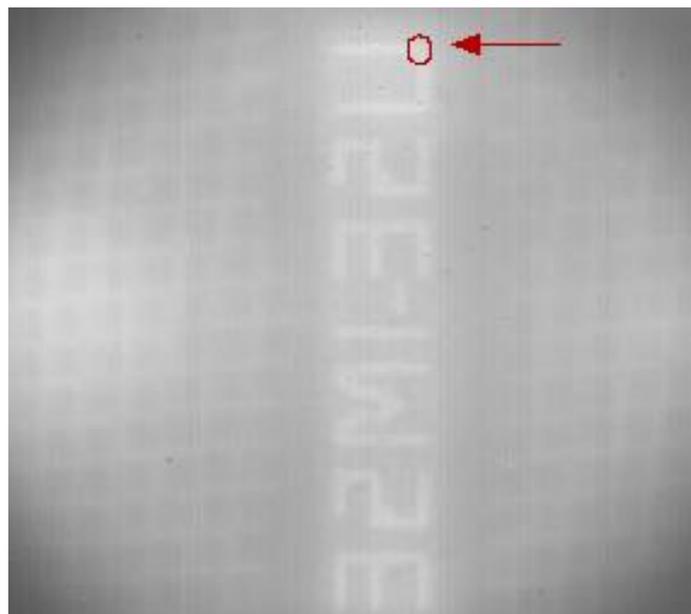


Figura 28: Texto dibujado en el circuito

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 38 de 72

Para Mover el puntero láser se usa dos controladores. Uno de color blanco el cual con los pulsadores +/- de la derecha e izquierda se puede controlar el eje Z y otro de color negro que puede controlar el eje X, Y con el *joystick* (Figura 29).



Figura 29: Controlador eje Z y controlador eje X, Y

4.2 Desarrollo de las aplicaciones de programa.

Gran parte del desarrollo del programa viene de unas funciones anteriores de antiguos alumnos. En este caso lo que se ha hecho es estudiar estas funciones previas, resumirlas y optimizarlas. Como el antiguo programa estaba muy estrechamente enlazado con su respectiva interfaz y no había funciones sencillas para programar de forma rápida algunas funciones nuevas, se optó por crear un nuevo fichero en *Python* que llamaba a las anteriores funciones, además se creó una pequeña base de datos para guardar información de varios experimentos consecutivos.

4.2.1 Ventana de inicio y ventana de ejecución

Esta es la primera ventana la cual aparece cuando se selecciona el modo manual y luego se selecciona bombardeo personalizado. Es donde se genera las rutas del cabezal del láser y da una vista general del diseño del ensayo (Figura 30).

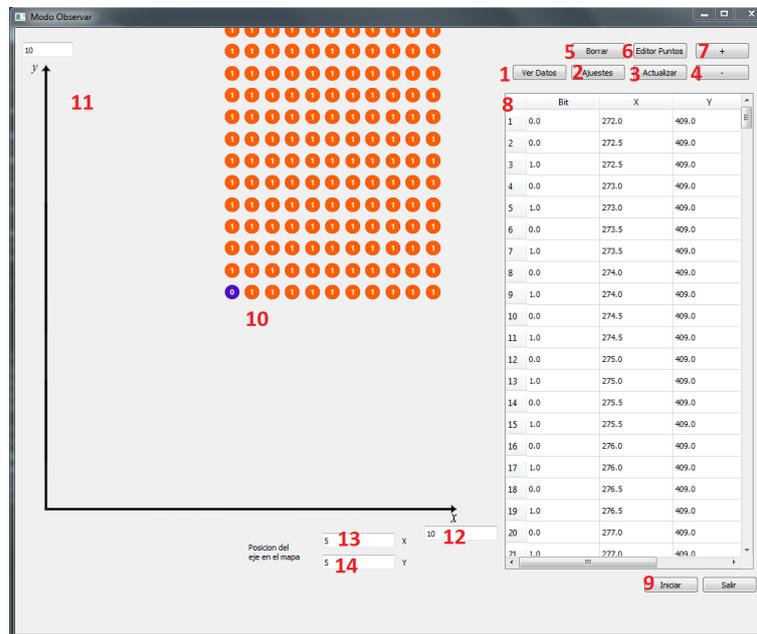


Figura 30: Ventana inicio ruta

En la ventana del programa se puede ver tanto numéricamente en la tabla (8) como gráficamente (10) la ruta de puntos creada.

En los huecos (11) y (12) se elige los tamaños del eje en micras. Por ejemplo, ahora tanto el eje X como el eje Y tienen un tamaño de 20 micras.

Los huecos a la derecha de posición del eje en el mapa (13) y (14) indica la posición del primer punto de la tabla en el mapa de la interfaz. Tomando de referencia el cruce del eje X e Y abajo a la izquierda. Ahora el punto que esta primero en la tabla (bit: 1 | X: 1 | Y: 5) está en el mapa en la posición (5,5).

El botón de borrar (5) hace que toda la tabla se borre sus valores menos el primero que no tiene que ser borrado porque produce error en el programa.

El botón ajustes (2) abre la ventana de ajustes del láser y el analizador lógico.

El botón editor de puntos (6) abre una ventana que se explica en el siguiente apartado que permite crear rutas de forma rápida.

El botón actualizar dibuja los puntos de la tabla (8) en el mapa (10) y es necesario darle antes de pulsar iniciar si quieres guardar la ruta.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

El botón + (7) y – (4) sirven para añadir o quitar una fila de la tabla y así añadir nuevos puntos de forma manual.

Una vez todo configurado y actualizado si se le da a iniciar (9) iniciará el ensayo y se abrirá una nueva ventana (Figura 31) donde informa que operación está realizando, por donde se está incidiendo el láser y si se produce algún fallo en el flip-flop (zona de texto donde hay números consecutivos del 0 al 19).



Figura 31: Ventana ejecución

Una vez terminado el ensayo esta ventana se cierra y aparece de nuevo la siguiente ventana (Figura 32) donde se resume cuáles han sido los puntos donde se ha provocado errores. El valor lógico que tenía antes de producirse el fallo [$0 \rightarrow 1$ | $1 = 1 \rightarrow 0$], el registro que ha fallado y la posición del fallo.

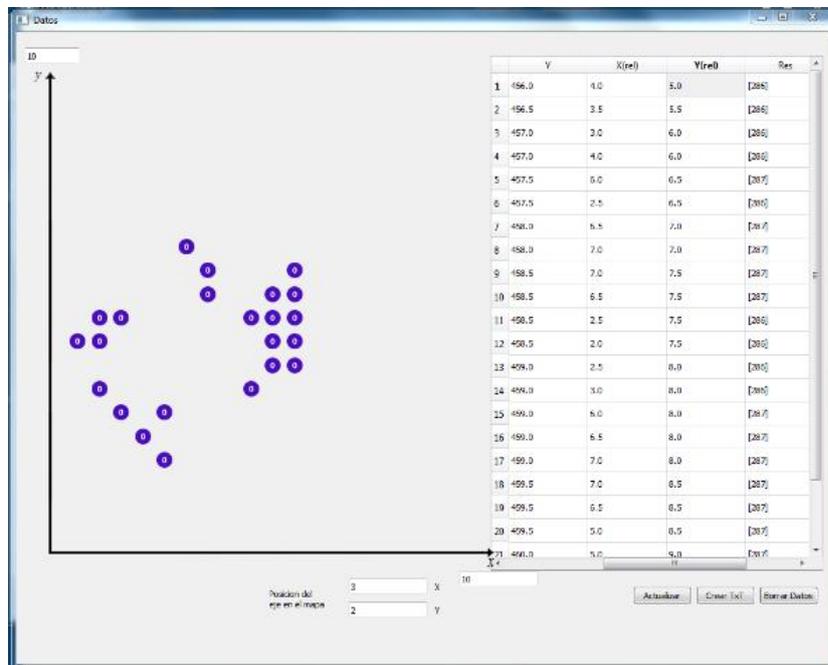


Figura 32: Ventana Datos

En la parte inferior de la tabla se encuentra 3 botones:

- Crear TxT: Crea un fichero de texto .txt en una carpeta del programa llama TXT donde se escribe todos los datos de la tabla para copiarlo directamente en un Excel u otro tipo de archivo de base de datos.
- Borrar Datos: borra todo el dato de la tabla.
- Actualizar: Dibuja sobre los ejes los fallos que están escritos en la tabla para ver de forma gráfica.

A este menú también se puede acceder en cualquier momento con el botón Ver datos (1) de la ventana da inicio y ver los datos que tiene guardado el programa de anteriores experimentos.

4.2.2 Creación de ruta de puntos

Esta ventana se puede abrir en paralelo con la ventana inicial con el botón editor de puntos (6)(Figura 33). Se usa para agilizar el proceso de crear rutas de ensayo ya que permite crear líneas y S solo colando sus parámetros mas importantes.

			
	Memoria	Documento 1	
Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 42 de 72

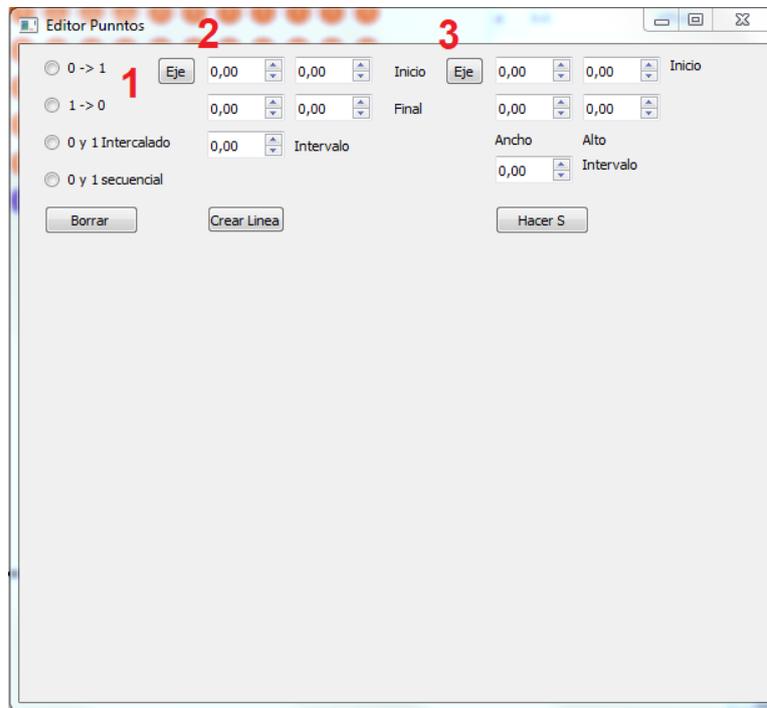


Figura 33: Ventana crear rutas

Por ahora solo se puede crear dos tipos de rutas: líneas y con forma de S, pero se puede combinar estas para hacer rutas más complejas. El apartado (1) indica que valor lógico o estado se quiere que esté el registro cuando se vaya a realizar la ruta.

0 → 1: Todos los registros a 0 lógico.

1 → 0: Todos los registros a 1 lógico .

0 y 1 intercalado: Primero dispara en un punto con registros a 0 luego repite el disparo, pero con registros a 1 y después pasa al siguiente punto.

0 y 1 secuencial: primero hace la ruta con los registros a 0 y luego vuelve a hacer la misma ruta, pero con los registros a 1.

A la derecha (2) está un apartado que permite crear líneas siendo los primeros recuadros la posición del inicio de la línea y el apartado de abajo el final de la línea. El último apartado (Intervalo) es la separación entre los puntos a lo largo de la línea.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 43 de 72

El botón eje sirve para que el programa te coloque automáticamente el último punto del ensayo que tienes en la lista de la ventana inicial. Si no tienes ningún punto te coloca el Eje (La fila 0 de la tabla 8).

El siguiente apartado (2) sirve para crear una ruta con forma de serpiente siendo los dos primeros apartados el punto inicial y los dos de abajo el ancho y alto de la S. El botón de eje hace lo mismo que el anterior, pero en el apartado (2) y el intervalo también hace lo mismo.

Cuando pulsas los botones crear Línea y crear S si los datos están bien asignados creará la ruta correspondiente. Se le puede dar varias veces a estos botones para crear varias veces la misma ruta y así hacer varios experimentos seguidos.

4.2.3 Ajustes del laser

Esta ventana es la encargada de almacenar todos los ajustes del láser tales como: el tipo de circuito o la energía que suministra el láser en cada disparo (Figura 34).

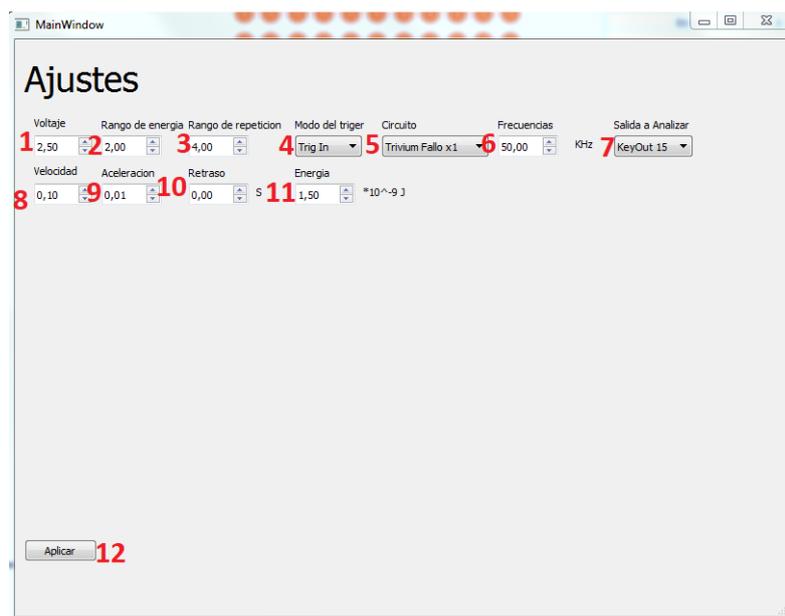


Figura 34: Ventana ajustes

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 44 de 72

Si en la ventana inicial se pulsa ajustes (2) se abre esta ventana en paralelo y el botón aplicar (12) aplica los ajustes y cierra la ventana. Los apartados son:

- Voltaje (1): Indica el Voltaje (V) que se le aplica al circuito.
- Rango de energía (2): Selecciona el rango de energía.
 - rango: 0 -> Min, 1 -> Low, 2 -> High [24].
- Rango de repetición (3): Permite seleccionar la tasa de repetición en frecuencia de la salida de laser [24].
 - tasa: 1 -> 1 MHz, 2 -> 2 MHz, 3 -> 5 MHz, 4 -> 10 MHz, 5 -> 20
- Modo del trigger (4): Lo normal es que sea pulsado, pero se le puede colocar continuo o en frecuencia a un reloj interno.
- Circuito (5): Para indicar el tipo de circuito integrado que se quiere analizar.
- Frecuencia (6): Divisor de frecuencia por el que el *Digilent* va a leer y enviar al ordenador.
- Salida a analizar (7): Es la salida del circuito por donde se van a leer los datos.
- Velocidad (8): Velocidad a la que va el láser (mm/s).
- Aceleración (9): Aceleración a la que va el láser (m/s²).
- Retraso (10): Tiempo que espera el láser una vez dada la señal para ejecutar un disparo (s).
- Energía (11): Energía que se aplica el láser pulsado en cada disparo *10⁻⁹ J.

4.3 Modo Prueba

Al iniciar el programa se pregunta en la consola el modo en el que el usuario quiere comenzar, modo Programa (P) o modo Manual (M). Si se pulsa M o m, no se abrirá ninguna ventana y se preguntará por un número. Cada número es una acción independiente que está programada para hacer pequeñas acciones simples. Está indicada en el script prueba y la clase funciones manuales. Este modo no está preparado para un usuario habitual sino para programar, hacer

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 45 de 72

mantenimiento, ver código de ejemplo o para empezar a programar funciones y no tener que tratar con la interfaz.

Las funciones se pueden clasificar por:

- 1-5: Funciones de movimiento del láser.
- 6-10: Funciones de configuración del láser, pero sin disparar excepto la 10 que si dispara y hay que tener la precaución necesaria.
- 11-18: Funciones de la base de datos y el analizador lógico.
- 19-23: Funciones más complejas en la que se dispara el láser y se comprueba algún fallo o se manipula la base de datos.

Si se va a hacer algún disparo (la función 10 y las que estas entre la 19-23) con el modo prueba siempre hay que tener las gafas puestas, las luces de seguridad activadas y cerrar la escotilla del microscopio por seguridad y para no dañar ningún componente.

4.3.1. Funciones generales (Bombardeo_manual)

Este fichero tiene todas las funciones básicas y la pequeña base de datos que va a ser necesario para todos los procesos. Cada apartado es una clase del fichero y a continuación se hace una explicare resumidamente que hace cada función y variable pública.

4.3.1.1 Base de datos

Nombre	Función	Variables entradas
GuardarUltimo	Guarda las cuatro variables para usarse luego	k15, k14, k13, k12

Tabla 5: variables base de datos

Es una clase que contiene la función que guardar en vectores los valores tanto los sin errores como los que se ha experimentado. Lo más importante es la función *GuardarUltimo* que la declara cada vez que se hace un disparo del láser, Tabla 5

			
	Memoria	Documento 1	
Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 46 de 72

4.3.1.2 Función manual

Esta clase es la que contiene todas las funciones básicas del programa. Se van llamando en las clases posteriores y así solo hay que asegurar que estas funciones estén bien implementadas Tabla 6 y Tabla 7.

Nombre	Función	Tipo
K15, k14, k13, k12	VARIABLES que se guardan	list
SalidasCerosCorrecta	Salida del circuito correcta con '0' lógico	Vector
SalidasUnoCorrecto	Salida del circuito correcta con '1' lógico	Vector
PosicionFalloX	Vector de posición de fallos respecto el eje X	Vector
PosiciónFalloY	Vector de posición de fallos respecto el eje Y	Vector
RegistrosFallos	Vector de los diferentes tipo de registros que han fallado	Vector

Tabla 6: Función manual

Nombre	Función	Variables de entrada
Calentamiento	Recorre un cuadrado un numero X de veces a una velocidad	x, y, Hi, Le, Veces, Velocidad <ul style="list-style-type: none"> (x/y): Posicion de la esquina inferior izquierda del cuadrado (float) Hi: Altura del cuadrado (micras)(float) Le: Anchura del cuadrado (float) Veces: Número de veces que realiza el movimiento (int) Velocidad Velocidad a la que realiza el movimiento (float)
ConectarMaquina	Conecta el módulo pico y abre el brazo.	aceleracion, velocidad <ul style="list-style-type: none"> Aceleración: Aceleración inicial del cabezal(float) Velocidad: Velocidad inicial del cabezal (float)
PreparandoBombardeo	Prepara el láser para el ensayo e introduce las configuraciones.	EnergyRange, RepetitionRate, TriggerMode, EnergyElec <ul style="list-style-type: none"> EnergyRange: Selecciona el rango de energía. <ul style="list-style-type: none"> rango: 0 -> Min, rango: 1 -> Low, rango: 2 -> High [24]. RepetitionRate: Permite seleccionar la tasa de repetición en frecuencia de la salida de laser [24]. Tasa:

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 47 de 72

Preparando Bombardeo		<ul style="list-style-type: none"> ▪ 1 -> 1 MHz, ▪ 2 -> 2 MHz, ▪ 3 -> 5 MHz, ▪ 4 -> 10 MHz, ▪ 5 -> 20 MHz. • TriggerMode: Elige la respuesta del láser cuando se activa <ul style="list-style-type: none"> ▪ 1 -> Trig In, ▪ 2 -> Gate In, ▪ 3 -> Int Clk, ▪ 4 -> Continuous • EnergyElec: La energía que proporcionada el láser cuando se activa. El valor se multiplica por 10^{-9} j
Apagar laser	Desconectar laser y quita la conexión con el pc	
Cargar Analizador	Enciende el analizador lógico.	<p>circuito,f_clk</p> <ul style="list-style-type: none"> • Circuito: Numero entero que se introduce según el circuito. <ul style="list-style-type: none"> ▪ 1: Trivium fallo 0 y 1. ▪ 2: Trivium fallo de baja potencia 0 y 1. ▪ 3: Trivium fallo x2 0 y 1. ▪ 4: Trivium fallo x2 de baja potencia 0 y 1. ▪ 5: Trivium fallo x8 0 y 1, 6-> Trivium fallo x8 de baja potencia 0 y 1. ▪ 6: Trivium fallo x16 0 y 1, 7-> Trivium fallo x16 de baja potencia 0 y 1. • F_clk: Frecuencia a la que se divide el reloj del analizador lógico.
Cargar Funcion	Carga los valores de entrada en un formato .txt diseñado en <i>WaveForm</i>	<p>dir,circuito,f_clk</p> <ul style="list-style-type: none"> • Dir: Localización del archivo TxT. • Circuito: Numero entero que se introduce según el circuito. <ul style="list-style-type: none"> ▪ 1: Trivium fallo 0 y 1. ▪ 2: Trivium fallo de baja potencia 0 y 1. ▪ 3: Trivium fallo x2 0 y 1. ▪ 4: Trivium fallo x2 de baja potencia 0 y 1.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 48 de 72

CargarFuncion		<ul style="list-style-type: none"> ▪ 5: Trivium fallo x8 0 y 1, 6-> Trivium fallo x8 de baja potencia 0 y 1. ▪ 6: Trivium fallo x16 0 y 1, 7-> Trivium fallo x16 de baja potencia 0 y 1. • F_clk: Frecuencia a la que se divide el reloj del analizador lógico.
GuardarEnBaseDeDatos	Guarda la última salida del circuito	<p>índice, Salida.</p> <ul style="list-style-type: none"> • Índice: introducir "Ceros" cuando es una salida correcta con 0 lógico y "Uno" cuando es de 1 lógico • Salida: Salida que se quiere guardar ("K12","K13","K14","K15").
Comparar	<p>Compara dos vectores de datos y devuelve si son distintas o iguales. Si son distintas devuelve el registro donde estaría el error. El error se calcula porque se conoce la frecuencia del analizador lógico de digilent. Se sabe que son 6 veces más rápida que el circuito por tanto si se encuentra 6 bit de diferencia entre la salida correcta y la incorrecta sabemos que es un fallo. El calculo del registro se hace calculando la posición del primer bit que falla, se divide entre 6 y se le suma</p>	dato1, dato2
IniciarBomba	Combina las funciones anteriores para encender el láser pulsado y conectar el analizador lógico y se prepara para hacer una prueba.	<p>velocidad, Aceleracion, energiaRange, RepetitionRate, TriggerMode, EnergyElec, QueSeAnaliza, clk, circuito, Salida, MenuGuardado</p> <ul style="list-style-type: none"> • Velocidad: Velocidad inicial (float) • Aceleración: Aceleración inicial (float) • energiaRange: Selecciona el rango de energía. • rango: 0 -> Min, • 1 → Low, • 2 → High [24]. • RepetitionRate: Permite seleccionar la tasa de repetición en frecuencia de la salida de laser [24].

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 49 de 72

<p>IniciarBomba</p>		<ul style="list-style-type: none"> • tasa: 1 → 1 MHz, • 2 → 2 MHz, • 3 → 5 MHz, • 4 → 10 MHz, • 5 → 20. • TriggerMode: Elige la respuesta del láser cuando se activa. • 1 → Trig In, • 2 → Gate In, • 3 → Int Clk, • 4 → Continuous. • EnergyElec: Energía que da el láser cuando se activa. El valor se multiplica por 10^{-9} j máximo 50×10^{-9} J • QueSeAnaliza: Se debe introducir 0,1,2 • 0-> Se guarda salida sin fallos de 0 lógico. • 1-> se guarda salidas sin fallos de 1 lógico. • 2-> se guarda salidas sin fallos de 0 y de 1 lógico. • Clk: Frecuencia a la que se divide el reloj del analizador lógico para leer los datos. • Circuito: Es un numero entero que se introduce según el circuito [17] <ul style="list-style-type: none"> ▪ 1: Trivium fallo 0 y 1. ▪ 2: Trivium fallo de baja potencia 0 y 1. ▪ 3: Trivium fallo x2 0 y 1. ▪ 4: Trivium fallo x2 de baja potencia 0 y 1. ▪ 5: Trivium fallo x8 0 y 1, 6-> Trivium fallo x8 de baja potencia 0 y 1. ▪ 6: Trivium fallo x16 0 y 1, 7-> Trivium fallo x16 de baja potencia 0 y 1. • Salida: Salida la cual se quiere analizar. ("K12", "K13", "K14", "K15") • MenuGuardado: Fichero del menu Si no se usa el menú hay que borrar todas las referencias dentro de
----------------------------	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		esta función de la variable MenuGuardado.
Disparar	Realiza un disparo en un lugar concreto	<p>Cargar, X, Y, energía, clk, circuito</p> <ul style="list-style-type: none"> • Cargar: elegir "0" para introducir 0 lógico, elegir. "1" para introducir 1 lógico. • X, Y: Posición x y donde se quiere disparar. • Energía: Energía con la que dispara el laser. • Clk: Frecuencia a la que se divide el reloj del analizador lógico para leer los datos • Circuito: Tipo de circuito [17] <ul style="list-style-type: none"> ▪ 1: Trivium fallo 0 y 1. ▪ 2: Trivium fallo de baja potencia 0 y 1. ▪ 3: Trivium fallo x2 0 y 1. ▪ 4: Trivium fallo x2 de baja potencia 0 y 1 ▪ 5: Trivium fallo x8 0 y 1, 5-> Trivium fallo x8 de baja potencia 0 y 1. ▪ 6: Trivium fallo x16 0 y 1, 7-> Trivium fallo x16 de baja potencia 0 y 1.

Tabla 7: Tablas función manual

4.3.1.3 Automatización

Esta es una clase que está muy relacionada con la interfaz nueva y solo tiene una función, Tabla 8.

Nombre	Función	Variable salida
RecabarDatos	Recaba todos los datos introducidos en la interfaz. Comprueba los errores si los hay y ejecuta una prueba según este indicada en la interfaz	

Tabla 8: Automatización

	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

4.3.2. Código de la interfaz gráfica (Bombardeo_personalizado)

El fichero *menú_bombardeo_manual* realiza la programación de todas las ventanas de la nueva interfaz.

Para programar la interfaz se usa una librería de *Python* llamada *PyQt5* [16]. que tiene una aplicación para diseñar interfaz llamada *PyQt5_design*. La ventaja de esta aplicación es que no necesitas programar código para crear ventanas sencillas y luego en *Python* con la función *Uic.loadUI(dirección_de_la_ventana_en_el_ordenador, class_donde_se_quiere_asociar)*. El problema que se encontró es que para poder programar una interfaz para dibujar objetos y que actualice la posición de estos objetos no se podía usar la aplicación. Por tanto, tuve que programar todo manualmente (Figura 35).

Para ello lo primero que hay que hacer es crear unas clases por cada ventana que se va a utilizar (*MiVentana*, *VentanaDatos*, *VentanaAjustes*, *VentanaEditorPuntos*) y hay que indicar por código que esa clase va a tener la función de ventana. Que jerarquía va tener tamaño, nombre, color, etc... Luego si se tiene guardada la clase en otro script se puede usar la función *show()* para enseñar por pantalla la ventana nueva.

```

14 > class MiVentana(QMainWindow):
15
16     class VentanaDatos(QMainWindow):
17         def __init__(self, MiMenu):
18             super(VentanaDatos, self).__init__()
19             self.setGeometry(100, 100, 300, 200)
20             self.setWindowTitle("Datos")
21             self.posx = []
22             self.posy = []
23             self.registro = []
24             self.bits = []
25             self.tabla = QTableWidgetItem(self)
26             self.tabla.setColumnCount(6)
27             self.tabla.setGeometry(QRect(60, 30, 421, 60))
28             self.Main = MiMenu
29
30             self.BorrarBoton = QtGui.QPushButton(self)
31             self.BorrarBoton.setGeometry(QRect(100, 10, 75, 25))
32             self.BorrarBoton.setText("Borrar Datos")
33             self.BorrarBoton.clicked.connect(self.BorrarDatos)
34
35             self.TxtBoton = QtGui.QPushButton(self)
36             self.TxtBoton.setGeometry(QRect(100, 10, 75, 25))
37             self.TxtBoton.setText("Crear Txt")
38             self.TxtBoton.clicked.connect(self.CrearTxt)
39

```

Figura 35: Código inicio ventana

Lo segundo que hay que hacer es crear todos los elementos estáticos que tiene la interfaz. Para programar de una forma ordenada se propone la creación de estos objetos en una función que se llama en el *Init* de la clase (*_init_* en *Python*, es una función que siempre se ejecuta cuando se declara una clase por primera vez). Por ejemplo, en la clase *mi ventana* el cual es la clase de la ventana

			
	Memoria	Documento 1	
Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 52 de 72

principal tiene una función llamada *CrearObjetosInit(self)* donde se crea todos los elementos estáticos y luego al final de la función *init* la llama.

Para crear un objeto *PyQt5* tiene en su librería una serie de clases que tienen diferentes funciones. Para aclararlo se usa las clases *QLabel* para poner texto en una posición de la ventana o imágenes. Se le pasa la dirección de un archivo .png. Para crearla solo haría falta guardar en una variable *QLabel* que hará referencia a lo que queremos crear, indicar tamaño y pasar la dirección del .png si es una imagen o pasar un texto he indicar tamaño y fuente del texto. Así se haría con todos los objetos individualmente (Figura 36).

```
def CrearObjetosInit(self):
    self.EjeX = QLabel(self) ← Declarar la clase
    self.EjeX.setGeometry(QRect(40, 660, 565, 70)) ← Indicar tamaño
    self.EjeX.setScaledContents(True)
    self.EjeX.setPixmap(QPixmap("C:\Program Files\App_laser\Dibujos\Lado.png")) ← Mandar direccion del .png
```

Figura 36: Código de la barra del Eje x

Y finalmente hay que crear los objetos dinámicos, que serían los puntos de la interfaz. El problema de estos objetos es que se desconoce cuántos de estos se van a tener que crear y en qué posición van a terminar. Para solucionarlo se crea una clase específica para este objeto llamada *Punto(self)*. De tal forma que se puede crear tantas clases *Punto(self)* como se quiera y dentro de esta clase se tendría guardada las variables de posición y la localización de los archivos .png que haría referencia al dibujo del punto con un 1 (Figura 37) o el punto con un 0 (Figura 38).



Figura 37: Punto con cambio 0->1



Figura 38: Punto con cambio 1->0

Luego dentro de esta clases se crean tres funciones llamadas *CrearPunto(self,Ventana,Bit)*, *BorrarPunto(self)*, *Localizar(self,x,y,maxx,maxy)*. *CrearPunto* (Figura 39) que se utilizan para indicar a que ventana corresponde esta clase y que foto se quiere usar 1/0.

	<p style="text-align: center;">Memoria Documento 1</p>		
	<p style="text-align: center;">Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.</p>		

Localizar se usa para mover la foto desde un punto a otro de la ventana sin tener que borrar y volver a crear

BorrarPunto sirve para borrar el punto y liberar el espacio en memoria. Al final esta clase se llamaba tantas veces como puntos sean necesarios en una de las ventanas anteriores y se almacenaba en un vector para tenerlas localizadas.

```

class punto(QMainWindow):
>     def CrearPunto(self,Ventana,bit): ...
>
>     def BorrarPunto(self): ...
>     """def Mover(self,x,y,maxx,maxy): ...
>     def Localizar(self,x,y,maxx,maxy): ...

```

Figura 39: Clase punto

Como se ha indicado antes todas estas funciones se pueden buscar en la librería de *PyQt5* [16] o mirar el programa de *Qt Designer* que trae ejemplo de programación de estos objetos (Figura 40).

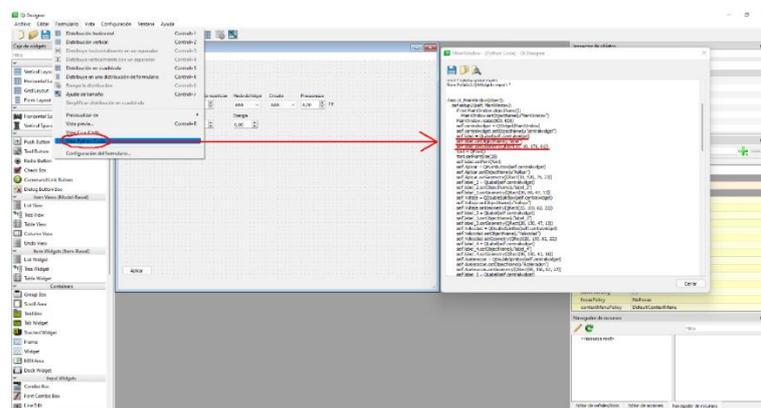


Figura 40: Códigos ejemplo Qt Design

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 54 de 72

5 Resultados experimentales

Para poder acceder al interior del circuito integrado con el láser se han realizado una serie de pasos que incluyen la apertura de un pequeño orificio en el encapsulado del ASIC del tamaño del dado de silicio que ocupa el circuito y el posterior pulido de la parte trasera del ASIC algunos cientos de micras para permitir que el láser pueda llegar a incidir en los componentes físicos internos del circuito. La parte frontal o superior del circuito no es válida para poder incidir con el haz del láser pues existen numerosas capas de metal de conexionado antes de llegar a la estructura física del flip-flop, ver Figura 41.

También hay que tener en cuenta como están distribuidos físicamente los diferentes flip-flops en el circuito integrado, para ello hay que tener en cuenta que el circuito esta girado unos 90° . Por tanto, hay que contar que todos los flip-flops están girado unos 180° en referencia al eje X y 90° en referencia al eje Z.

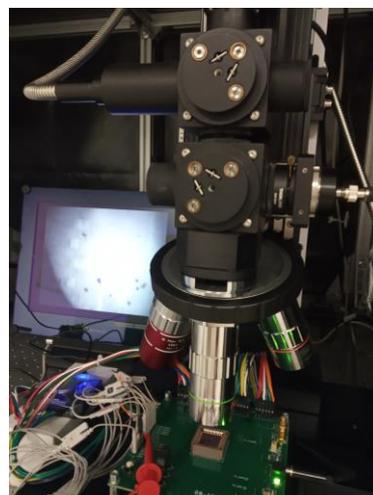
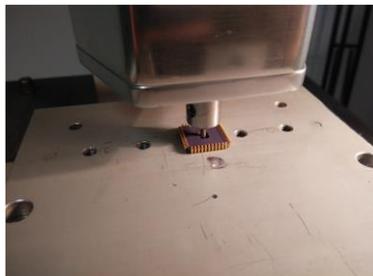


Figura 41: Apertura orificio en el circuito ASIC y placa de prototipado

Cada flip-flop se le ha puesto un nombre según su posición, creándose cuatro grupos de flip-flops y se ha analizado cada grupo individualmente. A continuación, en la Figura 42 puede verse la vista *abstract* (vista en la librería de celdas de la *foundry* con las conexiones de entrada-salida y el metal de más bajo nivel).

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		

- R90: Es el flip-flop de referencia tiene la VDD a la izquierda y la GND a la derecha y tiene la salida Q arriba a la izquierda y la entrada D abajo. CP es la entrada de reloj y CDN la entrada de reset asíncrono.
- R270: Es un flip-flop girado 180° sobre el eje Z tomando como posición inicial un R90
- MY90: Es un flip-flop girado 180° sobre el eje Y
- MX90: Es un flip-flop girado 180° sobre el eje Z

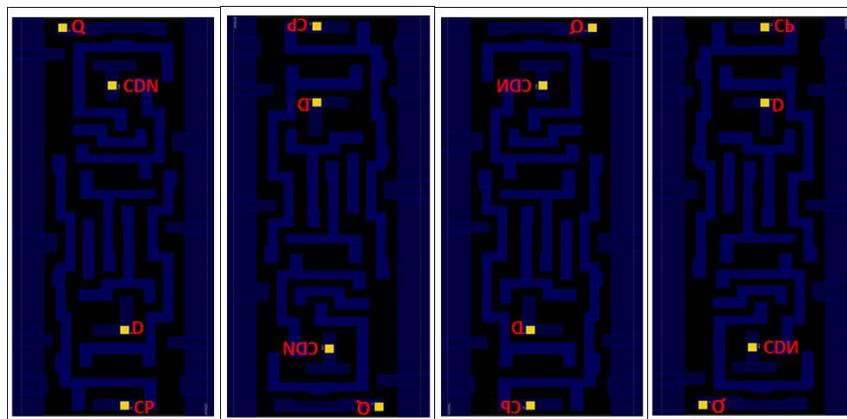


Figura 42: R90 R270 MY90 MX90

5.1 Ensayos preliminares

Las primeras pruebas se realizan conociendo la posición exacta del flip-flop y su valor lógico interno almacenado. Se analiza la salida del flip-flop elegido ante la exposición de un haz láser con diferentes energías desde 1.5 nJ hasta 0.3 nJ cuando se le carga con un '0' o un '1' lógico. El ensayo consiste en colocar el cabezal del láser en la esquina inferior izquierda del flip-flop. Esta se conoce porque previamente se tenía calculado las posiciones de los flip-flop con el *layout* del ASIC y después se hace una sucesión de disparos separado 0.5 micrómetros de distancia formando una figura de serpiente o S.

Los flip-flop miden 3x6 micrómetros (Figura 43), datos facilitados por la *foundry* de la tecnología, en este caso 90 nm, por tanto, se tiene que hacer 72 disparos por flip-flop. Si en alguna circunstancia hay dos flip-flop que están cerca se

				
	Memoria	Documento 1		
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 56 de 72

ensaya con los dos flip-flop a la vez aumentando o el ancho o el alto del área donde se hace el desplazamiento en S

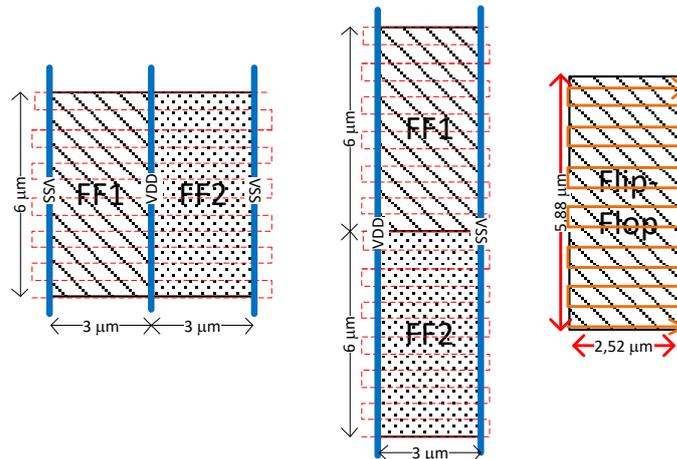


Figura 43: Recorrido flip-flop

Uno de los problemas que tiene este método es que en algunas ocasiones no se encuentra fallos y tenemos que probar con otro flip-flop. No se sabe con claridad el motivo, puede ser porque no está lo suficientemente bien pulido la capa la superficie posterior del ASIC o es la precisión de la posición del láser en el eje X-Y es insuficiente o que hacía falta hacerle más pruebas ya que se observa que si a un flip-flop se le hace las suficientes pruebas en algún momento sale los errores esperados.

El objetivo de estos ensayos es buscar patrones de fallo(cambio de valor lógico del flip-flop $0 \rightarrow 1$ o $1 \rightarrow 0$). Por ahora se ha encontrado 2 tipos de patrones: El primero se basa en que es más fácil encontrar fallos en transiciones de $0 \rightarrow 1$ (para resumir le vamos a llamar a esta transición “Unos”) que fallos de transición de $1 \rightarrow 0$ (para resumir le vamos a llamar “Ceros”) a una energía en torno a 0.7 nJ y 0.5 nJ. Por tanto, se deduce que en energía bajas se puede llegar a tener una probabilidad mayor de fallos de un tipo con la misma cantidad de ensayos tanto en ensayos de Unos como en ensayos de Ceros.

El segundo se basa en que los fallos se producen en unas zonas concretas más cercana o más alejada de los raíles de alimentación.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 57 de 72

De todos estos ensayos se plantea un procedimiento más complejo que resuelve varios de los problemas anteriores y es una de las razones por la que es necesario un nuevo programa para optimizar la interfaz, para que sea más cómodo para el usuario a la hora de diseñar rutas e introducir ajustes y el código para automatizar algunos procesos.

Con el objetivo de localizar flip-flops usando solo la generación de fallos y poder discriminar también áreas donde no se encuentren fallos relevantes se hace una ruta más amplia (suele hacerse un cuadrado de 8x10 micrómetros) desde un punto alejado de la esquina inferior izquierda del flip-flop y con una energía más alta de lo habitual, pero que no rompa el flip-flop (1.5 nJ). Este valor se elige porque en anteriores ensayos se ha comprobado que con una energía de 3 nJ se podía romper un flip-flop.

Con ello se consigue no depender de la calibración de la máquina pues a estos niveles de energía el fallo siempre ocurre y permite también a veces encontrar áreas no prevista para investigarlas pues aparecen errores.

Para el diseño de la ruta se utiliza la ventana de la Figura 44 que ya se detalló en el Capítulo 4.

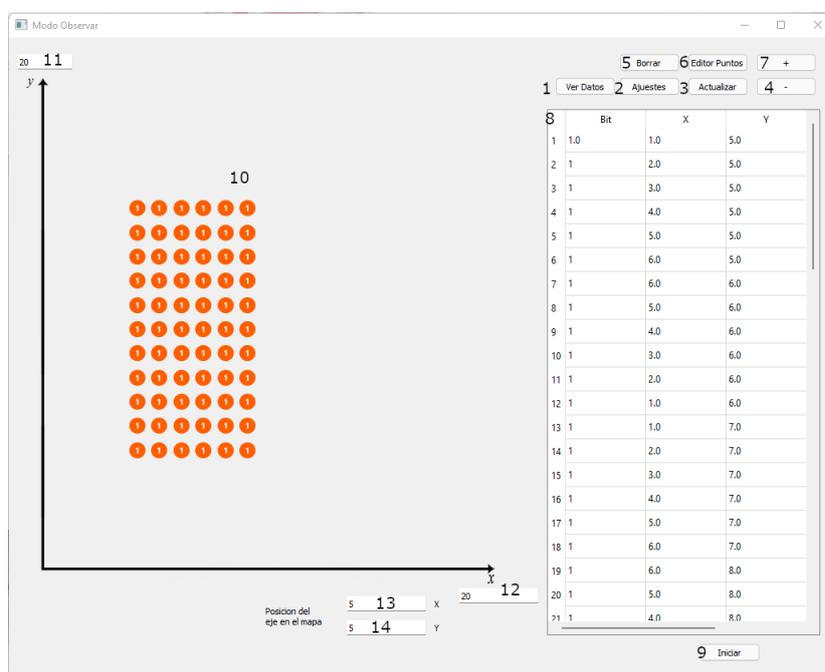


Figura 44: Ventana inicio

El flip-flop en cuestión puede ser localizado en el área seleccionada al generarse fallos de Ceros y Unos.

Se encuentra que casi todos los fallos de un flip-flop, tanto si son Ceros como si son Unos se sitúan en la mitad superior del flip-flop. Por tanto, es posible encontrar una zona de 4x3 micrómetros en el que ensayar (no es una zona de 3x3 porque en mi experiencia al hacer ensayos siempre se ha dejado un micrómetro de margen en el eje X). Como las zonas más relevantes son más pequeñas nos permite pasar de hacer una S en un área de 3x6 micrómetros a hacerlas en un área de 4x3 micrómetros de media pasando de hacer 72 disparos a 48 disparos. Esta diferencia al realizar varias pruebas seguidas reducía considerablemente el tiempo de ensayo.

Después una vez localizado una zona con alta probabilidad de fallo, se pueden hacer dos ensayos. Se puede empezar a hacer ensayos desde energía bajas hasta energía altas (0.3 a 0.7 nJ) hasta encontrar fallos, apuntarlos y sacar conclusiones, esto nos sirve para comprobar si son más probable colocar Unos o colocar Ceros.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 59 de 72

Se puede empezar desde una energía alta hasta una más baja (1 a 0.5 nJ), esto lo usamos para observar si existen zonas donde suele frecuentar más los Unos o los Ceros.

5.2 Resultados

A continuación, se describen los resultados con los dos tipos de ensayos realizados.

5.2.1 Análisis de las áreas de exposición

Para analizar las áreas más probables de exposición del láser se usa después de hacer el primer paso una energía entre 0.7 y 0.5 nJ. Primero se comprueba la posición del flip-flop con 1,5 nJ, luego se cota la zona con 1 nJ y finalmente se hace 10 o más ensayos a 0.7 nJ o 0.5 nJ. Esta prueba se repitió por cada tipo de flip-flop.

La gráfica representa el número de fallos de los flip-flop del mismo tipo habiendo tomado como referencia la esquina inferior izquierda de los diferentes flip-flop, esta esquina es el punto (0,0) de la gráfica.

Es bastante habitual al hacer varios test que en una misma zona se registre varios de los mismos fallos, por tanto, para realizar la gráfica con mayor claridad se ha usado un sistema de transparencia para su representación. Cuando más transparente este el círculo significa que es menos habitual que se registre un fallo en esa posición y cuando más opaco significa que es más probable. Siempre respetando que se ha analizado el mismo número de flip-flops de cada tipo (3 flip-flops por tipo) y el mismo ensayo (10 ensayos de 0→1 y 10 ensayos de 1→0). Por tanto, cada gráfica de la Tabla 9 representa una muestra de 60 ensayos repartidos en tres flip-flops y 2 tipos de ensayos.

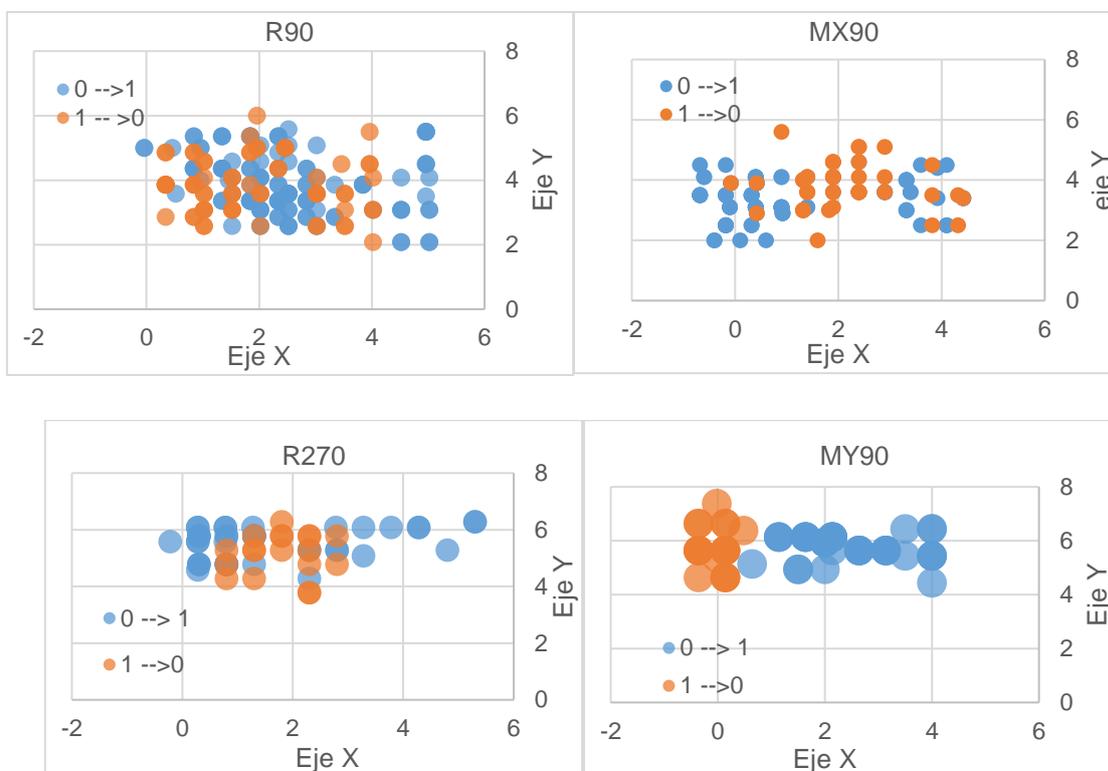


Tabla 9: Análisis por zona

Unas de las conclusiones más directa de este ensayo es que los flip-flop donde la VDD está la izquierda y la GND a la derecha (R90 y MY90) tienen los Unos más a la derecha (cerca de GND) y los Ceros a la izquierda (más cerca de VDD) y en los otros dos (R270 y MX90), los Unos estarían a la izquierda y los Ceros a la derecha, pero como estos tipos de flip-flop al girarse también giran GND y VDD seguirían conservando la relación de los Ceros y Unos con GND y VDD. Por tanto, se podría sacar una relación entre estas dos variables para sacar los datos de un flip-flop.

El problema que tiene esta relación es que antes de hacer algún experimento habría que localizar los carriles de alimentación de los flip-flop y el resultado no se vería de forma directa porque está en función de las referencias de los raíles de alimentación, además existen algunas posiciones registradas que están en valores negativos respecto el eje X o son mayores de 3 micrómetros (esta sería la anchura máxima de un flip-flop en nuestra tecnología) que no se ha encontrado

su significado o si se debe a un error de la herramientas de medida.

5.2.2 Análisis a baja energía

Para analizar esta hipótesis se comprueba la posición del flip-flop con una energía de 1.5 nJ y se selecciona una zona donde se encuentra un flip-flop. Se hace ensayos a 0.5 nJ y registrándose el número de fallos. Por tiempo solo se analizaron 3 tipos de flip-flops MY90, R270 y R90.

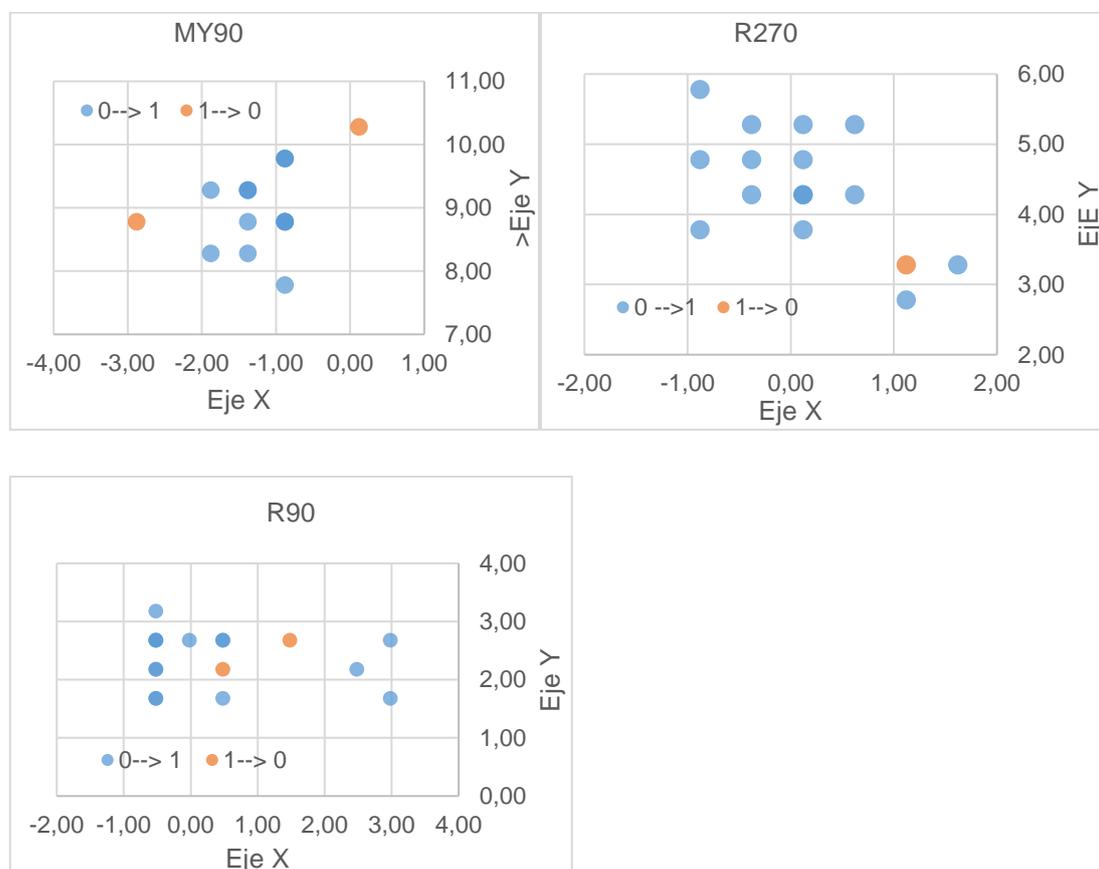


Tabla 10: Análisis de los flip-flops a baja energía

Las tres graficas de la Tabla 10 tienen algo en común. En los tres flip-flop hay una relación 21 Unos contra 2 Ceros (MY90: 21 Unos /2 Ceros, R270 20 Unos/1 Ceros, R90 23 Unos /2 Ceros). Esto vendría a decir que a energía bajas es más fácil introducir fallos de Unos respecto fallos de Ceros y se vería de una forma bastante clara. El problema de este método es que habría que descubrir antes de usarlo cual es la energía donde se produce esta relación, la cual depende de

la tecnología. Pero se puede averiguar si antes se hace varios ensayos probando desde energía más baja hasta la más alta y analizando los resultados.

5.3 Ensayo con flip-flop de solo lectura

Para probar estas deducciones se decide hacer un test con flip-flop los cuales son solo de lectura, con el objetivo de intentar deducir el valor que tiene almacenado.

Primero se le hace un ensayo a 1.5 nJ a dos flip-flop. El primero contiene un '0' y el segundo contiene un '1', véase la Tabla 11.

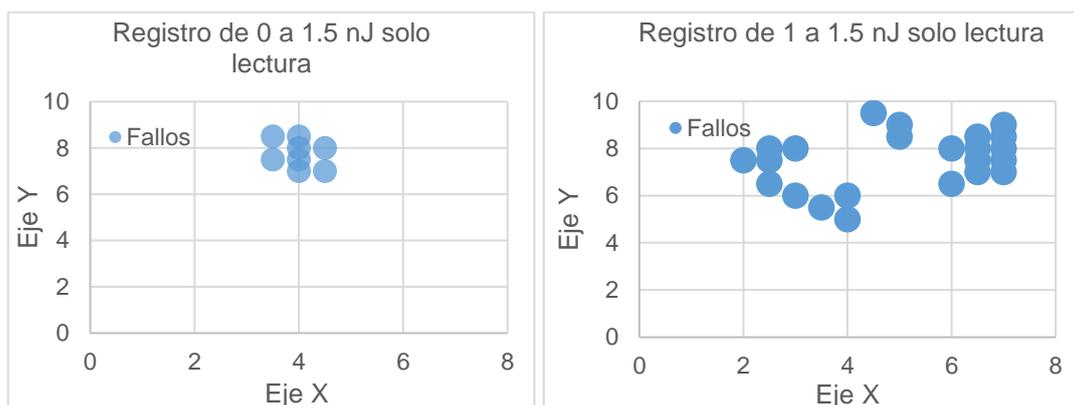


Tabla 11: Análisis de los flip-flops de lectura

En el primer caso solo se encuentra una zona que damos a entender que es donde está un flip-flop. En el segundo caso se encuentra has tres zonas distintas. Analizando las salidas del circuito y observando que bit cambia respecto a una salida sin fallos, gracias a esto podemos deducir que la zona de la izquierda y la del centro (la que solo tiene tres fallos) son fallos del mismo flip-flop y la zona de la derecha es la de uno distinto, porque hay dos flip-flop que están cerca.

Ahora se realiza un ensayo analizando la misma área, pero bajando a la energía a 0.5 nJ, Tabla 12.

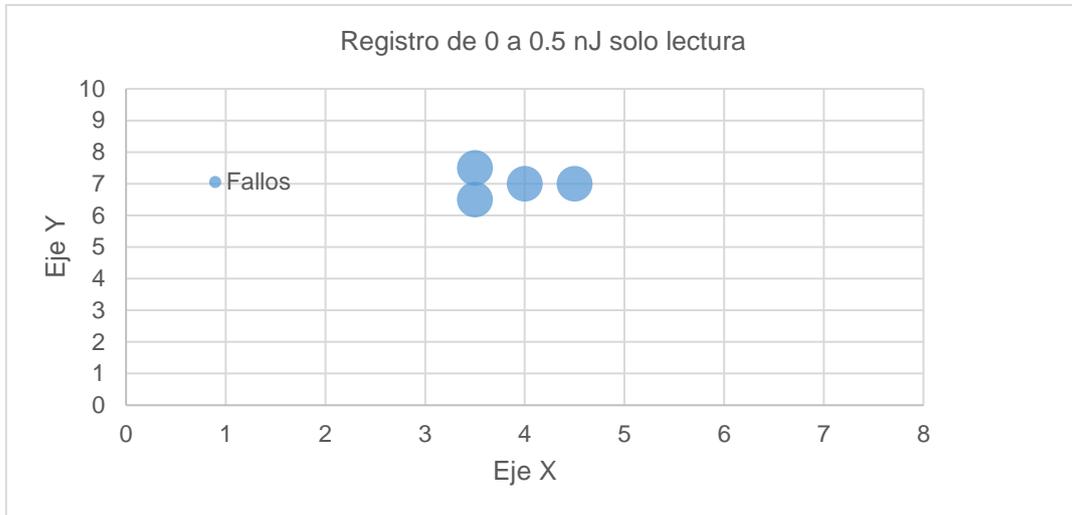


Tabla 12: Análisis flip-flop baja energía

En el primer caso se encuentra 4 fallos y en el segundo caso no se encuentra ningún fallo. Por tanto como se dice en el apartado anterior es más fácil producir un cambio del valor lógico interno del flip-flop de $0 \rightarrow 1$ que de $1 \rightarrow 0$ en una relación de 21 respecto 1 fallo. Esto confirma que en el primer caso se tiene un valor de '0' lógico almacenado y en el segundo caso los dos flip-flop tienen un '1' lógico.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 64 de 72

6. Conclusión

Como se ha indicado en este Trabajo de Final de Grado, el láser pulsado es un tipo de ensayo que puede llegar a dar cierta información sobre un ASIC. Esta información se puede utilizar para analizar las vulnerabilidades de un circuito o para obtener información secreta como puede ser las claves de un circuito de encriptación.

Se ha detectado también que nuestro equipo tiene ciertas imprecisiones en el movimiento de desplazamiento de cabezal del láser, se ha detectado en algunas medidas que el cabezal de laser se desplaza algunas micras entre ensayos o que algunos de los circuitos integrados presentaban algunas imperfecciones en el pulido que dificultaban las medidas. Por estos motivos se diseñó un método para los ensayos que tardaba más tiempo en dar los resultados, pero daba los resultados más precisos y se eliminaba algunos errores que podían dar las muestras.

Una vez realizado los ensayos se demuestra que se puede llegar conocer la posición de un flip-flop y su valor lógico almacenado por dos métodos distintos. Tanto porque hay una cierta diferencia en la posición de los errores en los Ceros como en los errores de los Unos como que los errores de los Unos son más frecuentes a baja energía. Pero los dos métodos a pesar de ser diferentes se pueden usar de forma simultanea para asegurar los resultados de los ensayos.

Por esto en algunos circuitos que puedan estar en entornos afectados por láser o radiación necesitarían algún tipo de protección o como mínimo que se conozca cuáles son sus vulnerabilidades y la repercusión de que ocurra algún fallo en uno de sus registros. Para aumentar la seguridad a día de hoy se han realizados otros ensayos tales como poner un sensor de corriente inducida, reiniciar el circuito cuando se detecta alguna anomalía [12] o crear simulaciones del circuito en entornos hostiles o ante un efecto de un láser pulsado para analizar sus vulnerabilidades e intentar mitigarlas [10][13][14].

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 65 de 72

6 Bibliografía

- [1] S. P. Skorobogatov and R. J. Anderson, "Optical fault induction attacks," in 4th International Workshop on Cryptographic Hardware and Embedded Systems, ser. CHES '02. London, UK, UK: Springer-Verlag, 2002, pp. 2–12.
- [2] R. A. C. Viera, P. Maurine, J. -M. Dutertre and R. Possamai Bastos, "Simulation and Experimental Demonstration of the Importance of IR-Drops During Laser Fault Injection," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 6, pp. 1231-1244, June 2020, doi: 10.1109/TCAD.2019.2928972.
- [3] J. -M. Dutertre et al., "Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model," 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2018, pp. 1-6, doi: 10.1109/FDTC.2018.00009.
- [4] F. Courbon, J. J. A. Fournier, P. Loubet-Moundi and A. Tria, "Combining Image Processing and Laser Fault Injections for Characterizing a Hardware AES," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 6, pp. 928-936, June 2015, doi: 10.1109/TCAD.2015.2391773.
- [5] R. A. C. Viera, P. Maurine, J. -M. Dutertre and R. P. Bastos, "Importance of IR drops on the modeling of laser-induced transient faults," 2017 14th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), 2017, pp. 1-4, doi: 10.1109/SMACD.2017.7981593.
- [6] J. -M. Dutertre et al., "Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model," 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2018, pp. 1-6, doi: 10.1109/FDTC.2018.00009.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 66 de 72

[7] J. -M. Dutertre et al., "Laser Fault Injection at the CMOS 28 nm Technology Node: an Analysis of the Fault Model," 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), 2018, pp. 1-6, doi: 10.1109/FDTC.2018.00009.

[8] H. Shindou *1 , A. Maru 1 , T. Ebihara1 , A. Makihara2 , S. Kuboyama 1 and T. Tamura, "Investigation of the SEE sensitivity of 90nm DICE based Flip-Flops, using pulsed-laser testing methodology", 2013 Proceedings of 10th international workshop on radiation effects on semiconductor devices for space applications (JAXA-SP--12-008E). Japan Aerospace Exploration Agency, Chofu, Tokyo (Japan) (2013).

[9] C. Roscian, A. Sarafianos, J. Dutertre and A. Tria, "Fault Model Analysis of Laser-Induced Faults in SRAM Memory Cells," 2013 Workshop on Fault Diagnosis and Tolerance in Cryptography, 2013, pp. 89-98, doi: 10.1109/FDTC.2013.17.

[10] R. A. C. Viera, P. Maurine, J. -M. Dutertre and R. Possamai Bastos, "Simulation and Experimental Demonstration of the Importance of IR-Drops During Laser Fault Injection," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 6, pp. 1231-1244, June 2020, doi: 10.1109/TCAD.2019.2928972.

[11] Sung-Ming Yen and M. Joye, "Checking before output may not be enough against fault-based cryptanalysis," in IEEE Transactions on Computers, vol. 49, no. 9, pp. 967-970, Sept. 2000, doi: 10.1109/12.869328.

[12] K. Matsuda et al., "A 286 F2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack on Cryptographic Processor," in IEEE Journal of Solid-State Circuits, vol. 53, no. 11, pp. 3174-3182, Nov. 2018, doi: 10.1109/JSSC.2018.2869142.

			
	Memoria	Documento 1	
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.		Página 67 de 72

[13] López Calle, Isabel (2011) Emulación de los efectos de la radiación ionizante en dispositivos analógicos mediante láser pulsado de femtosegundo sintonizable. [Tesis].

[14] D. H. Habing, "The Use of Lasers to Simulate Radiation-Induced Transients in Semiconductor Devices and Circuits," in IEEE Transactions on Nuclear Science, vol. 12, no. 5, pp. 91-100, Oct. 1965, doi: 10.1109/TNS.1965.4323904.

[15] Fernando López Orellana, "Control de un analizador lógico y de un sistema láser para la inserción de fallos y el test de circuitos integrados", TFG, Universidad de Sevilla, Departamento de Tecnología Electrónica, Sevilla, España, Junio 2021.

[16] PyQT5, 2022, Qt Documentation, [Accedido el 07-06-2021]. [Online]. Available: <https://doc.qt.io/qt-6/classes.html>.

[17] Fernando López Orellana, "Control de un analizador lógico y de un sistema láser para la inserción de fallos y el test [TFG].

[18] Rodrigo Gómez, "Laser pulsado, manual de usuario", IMSE, Sevilla, Documento tecnico, 2018.

[19] Catalog No. Documentacion Digital Discovery, Digilent, Pullman, Washington, Estados Unidos.

[20] Catalog No. 54904-97006 ,Infiniium 9000^a Series Oscilloscope, Agilent Technologies, Santa Clara, California, Estados Unidos.

[21] Catalog No. Manual de Hp Model 3630^a, Hp, Palo Alto, California, Estados Unidos.

[22] Rodrigo Gómez, " Pulsysrad.pyd", IMSEC, Sevilla, Fichero de código, 2018.

				
	Memoria	Documento 1		
	Estudio de la inserción de fallos en un flip-flop de un circuito integrado con láser pulsado.			Página 68 de 72