

Índice

CAPITULO 1 – INTRODUCCIÓN	1
1.1 Fundamentos y Motivación	1
1.2. Objetivos	2
1.3. Desarrollo	3
CAPITULO 2 – CONCEPTOS BÁSICOS	5
2.1. Confiabilidad	5
2.1.1. Atributos	5
2.1.2 Impedimentos	6
2.1.2.1. Fallos	6
2.1.2.2. Errores	7
2.1.2.3. Averías	8
2.1.3. Medios	9
2.2. Tolerancia a Fallos en Sistemas Físicos	10
2.2.1. Detección de errores	10
2.2.1.1. Códigos de detección de errores	10
2.2.1.2. Detección de errores mediante estrategias de almacenamiento ...	13
2.2.1.3. Estrategias de comprobación periódicas	14
2.2.1.4. Estrategias funcionales	15
2.2.2. Procesamiento de errores	15
2.2.2.1. Técnicas de recuperación de errores	16
2.2.2.2. Compensación	16
2.3. Validación de Sistemas Tolerantes a Fallos	16
2.3.1. Eliminación de fallos	17
2.3.2. Predicción de fallos	18
2.4. Tolerancia a Fallos en Sistemas Distribuidos	18
2.4.1. Comportamiento funcional	19
2.4.2. Hipótesis de fallos	19
2.4.3. Modos de avería	20
2.4.3.1. Averías con parada y reintegración	20
2.4.3.2. Averías bizantinas	20
2.4.3.3. Averías SOS	21
2.4.3.4. Suplantación de otra identidad	22
2.4.3.5. Transmisiones espurias	22
2.4.3.6. Pérdida de conexión	22
2.4.4. Consistencia	23
2.4.4.1. Sincronización de la base de tiempos	23
2.4.4.2. Consenso	23
2.4.4.3. Grupos de comunicación	24

2.4.5. Técnicas para alcanzar la tolerancia a fallos	24
2.4.5.1. Recuperación distribuida	25
2.4.5.2. Replicación	25
2.5. La Tolerancia a Fallos y la Validación Experimental	25
2.6. Resumen y Conclusiones del Capítulo	27
CAPITULO 3 – TÉCNICAS DE INYECCIÓN DE FALLOS	29
3.1. Fallos Físicos: Causas y Modelos	29
3.1.1. Causas de los fallos físicos en circuitos integrados	30
3.1.1.1. Efectos de la radiación en los semiconductores	30
3.1.1.2. Efectos de la radiación en memorias SRAM	33
3.1.1.3. Efectos de la radiación en la lógica combinacional	35
3.1.1.4. Efectos debidos al deterioro, desgaste o condiciones ambientales	36
3.1.1.5. Efectos debidos al deterioro de las soldaduras	38
3.1.2. Modelos de fallos	38
3.1.2.1. Fallos intermitentes y permanentes	39
3.1.2.2. Fallos transitorios	41
3.1.3. Fallos físicos y técnicas de inyección	42
3.2. Descripción de la Inyección de Fallos	42
3.2.1. Fallos	42
3.2.2. Activación	43
3.2.3. Resultados	44
3.2.4. Medidas	44
3.3. Técnicas de Inyección de Fallos	44
3.3.1. Propiedades de las técnicas de Inyección de Fallos	45
3.3.2. Inyección física de Fallos o Implementada por Hardware HWIFI	48
3.3.2.1. Inyección física de fallos a nivel de pin	48
3.3.2.2. Interferencias electromagnéticas EMI	50
3.3.2.3. Inyección mediante radiación de partículas	51
3.3.2.4. Inyección mediante radiación láser	52
3.3.3. Otras técnicas de inyección	53
3.3.3.1. Inyección mediante cadenas de exploración	53
3.3.4. Inyección de Fallos Implementada por Software SWIFI	54
3.3.4.1. División práctica de las herramientas SWIFI	54
3.3.4.2. Algunos ejemplos de herramientas SWIFI	56
3.3.4.3. Otras herramientas compatibles con SWIFI	59
3.3.5. Inyección de Fallos basada en técnicas de simulación de modelos	60
3.3.5.1. Nivel eléctrico	60
3.3.5.2. Nivel lógico	61
3.3.5.3. Nivel RTL	61
3.3.5.4. Nivel de sistema	61
3.3.5.5. Inyección de fallos basada en VHDL	63
3.3.5.6. Emulación de fallos con FPGA	64
3.4. Comparación de las Técnicas de Inyección de Fallos	64
3.5. Resumen y Conclusiones del Capítulo	69

CAPITULO 4 – LA ARQUITECTURA TTA 71

4.1. Sistemas Guiados por Cable 71

4.2. División de Arquitecturas en Sistemas Distribuidos 73

4.3. Conceptos Básicos de la Arquitectura TTA 75

 4.3.1. Estructura 76

 4.3.2. El sistema de comunicaciones 78

4.4. Protocolos de comunicación basados en TTA 80

 4.4.1. Comparación entre diferentes protocolos de comunicaciones 82

 4.4.2. El controlador de comunicaciones TTP/C 84

 4.4.2.1. La unidad de control del protocolo (PCU) 85

 4.4.2.2. La interfaz de comunicaciones (CNI) 86

 4.4.2.3. El descriptor de mensajes (MEDL) 87

 4.4.2.4. El guardián del bus (BG) 87

4.5. Representatividad de los Fallos a Nivel de pin en el TTP/C 88

 4.5.1. Efecto de la inyección de fallos sobre un pin de entrada-salida 89

 4.5.1.1. Generación de un pulso inexistente 89

 4.5.1.2. Eliminación de un pulso existente 90

 4.5.1.3. Variación de los márgenes temporales del pulso 91

 4.5.2. Impacto de los fallos sobre las barreras de contención 91

 4.5.2.1. Validación de la fiabilidad del guardián del bus local 91

 4.5.2.2. Evaluación de la interfaz de comunicaciones 93

4.6. Resumen y Conclusiones del Capítulo 94

CAPITULO 5 – AFIT – LA HERRAMIENTA DE INYECCIÓN 97

5.1. Evolución de la Herramienta de Inyección de Fallos 97

 5.1.1. Descripción modular de la herramienta 97

 5.1.1.1. Módulo de sincronización y disparo 97

 5.1.1.2. Módulo de temporización 98

 5.1.1.3. Módulo de activación 99

 5.1.1.4. Módulo de lectura de eventos 100

 5.1.1.5. Módulo de potencia 100

 5.1.2. Mejoras realizadas en AFIT 101

 5.1.2.1. Nuevo módulo de temporización 101

 5.1.2.2. Nuevo módulo de potencia 102

 5.1.2.3. Terminadores para las puntas de inyección de alta velocidad 103

5.2. Adaptación a Sistemas Distribuidos 104

 5.2.1. Procesos implicados en la inyección de fallos 105

 5.2.2. Un Monitor para sistemas distribuidos 106

5.3. Resumen y Conclusiones del Capítulo 109

CAPITULO 6 – VALIDACIÓN DEL PROTOCOLO DE COMUNICACIONES **112**

6.1. Introducción	112
6.2. Servicios del Protocolo	113
6.2.1. Capa física	114
6.2.2. Capa de enlace de datos	114
6.2.3. Capa de servicios del protocolo	115
6.2.3.1. Arranque y reintegración	115
6.2.3.2. Algoritmo de sincronización	116
6.2.3.3. Servicio de pertenencia	116
6.2.3.4. Reconocimiento implícito	116
6.2.3.5. Gestión de errores	117
6.2.3.6. Algoritmo de vida	118
6.2.4. Capa de tolerancia a fallos	118
6.3. Comportamiento del Protocolo TTP ante Averías	119
6.3.1. Averías con parada y reintegración	119
6.3.1.1. Parada durante una transmisión ya iniciada	120
6.3.1.2. Reintegración del nodo	122
6.3.2. Transmisiones espurias y averías SOS	123
6.3.2.1. Transmisiones espurias sobre un canal	124
6.3.2.2. Transmisiones espurias conexas	125
6.3.2.3. Observación de averías SOS en el dominio del tiempo	125
6.3.2.4. Averías SOS observadas con otras técnicas de inyección	133
6.3.2.5. Observación de averías SOS en el dominio del valor	134
6.3.2.6. Reflexión sobre las estrategias NGU	135
6.3.3. Pérdidas de Conexión	135
6.4. Resumen y Conclusiones del Capítulo	137

CAPITULO 7 – MEJORA DE LA COBERTURA DE DETECCIÓN **141**

7.1. Errores de Diseño e Implementación	141
7.2. Errores Simples y Múltiples Derivados de Fallos Físicos	143
7.2.1. Errores no detectados	143
7.2.1.1. Errores unidireccionales sobre datos derivados de fallos simples	144
7.2.1.2. Errores aleatorios múltiples derivados de fallos simples	145
7.2.1.3. Errores derivados de fallos múltiples	147
7.2.2. Erres detectados vs. errores no detectados	148
7.2.2.1. Eliminación de pulsos en las señales de control	148
7.2.2.2. Variación de pulsos existentes y generación de pulsos inexistentes	148
7.3. Evaluación de los Resultados	152
7.4. Propuesta para la Mejora de la Cobertura de Detección	155
7.4.1. Código de detección cíclico redundante	155
7.4.2. Códigos de detección verticales	157
7.4.2.1. CRC con polinomio generador de grado 3	158

7.4.2.2. U_n : Detección de errores unidireccionales	159
7.4.2.3. U_n y R_{α} : Detección de errores unidireccionales y aleatorios múltiples	161
7.4.2.4. Alternancia entre diferentes códigos de detección	164
7.5. Resumen y Conclusiones del Capítulo	166
CAPITULO 8 – CONCLUSIONES Y TRABAJO FUTURO	169
8.1. Conclusiones	170
8.1.2. Técnicas de inyección de fallos	170
8.1.3. La arquitectura TTA	171
8.1.4. Inyección de fallos en sistemas distribuidos	171
8.1.5. Validación del protocolo de comunicaciones	172
8.1.6. Mejoras en la cobertura de detección de errores	173
8.2. Resultados de la Investigación	174
8.2.1. Publicaciones relacionadas con la investigación	175
8.2.2. Otras publicaciones relacionadas con Inyección de Fallos	175
8.2.3. Publicaciones relacionadas con la divulgación del proyecto FIT.....	175
8.3. Trabajo Futuro	176
BIBLIOGRAFÍA	177