Sumario

La relevancia que la electrónica adquiere en la seguridad de los productos ha crecido inexorablemente, puesto que cada vez ésta copa una mayor influencia en la funcionalidad de los mismos. Pero, por supuesto, este hecho viene acompañado de una necesidad constante de mayores prestaciones para cumplir con los requerimientos funcionales, al tiempo que se mantienen los costes y el consumo en unos niveles reducidos. En este escenario, la industria está realizando esfuerzos para proveer una tecnología que cumpla con todas las especificaciones de potencia, consumo y precio, a costa de un incremento en la vulnerabilidad a múltiples tipos de fallos conocidos o la introducción de nuevos.

Para ofrecer una solución a los fallos nuevos y crecientes en los sistemas, los diseñadores han recurrido a técnicas tradicionalmente asociadas a sistemas críticos para la seguridad, que ofrecen en general resultados sub-óptimos. De hecho, las arquitecturas empotradas modernas ofrecen la posibilidad de optimizar las propiedades de confiabilidad al habilitar la interacción de los niveles de hardware, firmware y software en el proceso. No obstante, ese punto no está resulto todavía. Se necesitan avances en todos los niveles en la mencionada dirección para poder alcanzar los objetivos de una tolerancia a fallos flexible, robusta, resiliente y a bajo coste. El trabajo presentado aquí se centra en el nivel de hardware, con la consideración de fondo de una potencial integración en una estrategia holística.

Los esfuerzos de esta tesis se han centrado en los siguientes aspectos: (i) la introducción de modelos de fallo adicionales requeridos para la representación adecuada de efectos físicos surgentes en las tecnologías de manufactura actuales, (ii) la provisión de herramientas y métodos para la inyección eficiente de los modelos propuestos y de los clásicos, (iii) el análisis del método óptimo para estudiar la robustez de sistemas mediante el uso de inyección de fallos extensiva, y la posterior correlación con capas de más alto nivel en un esfuerzo por recortar el tiempo y coste de desarrollo, (iv) la provisión de nuevos métodos de detección para cubrir los retos planteados por los modelos de fallo propuestos, (v) la propuesta de estrategias de mitigación enfocadas hacia el tratamiento de dichos escenarios de amenaza

y (vi) la introducción de una metodología automatizada de despliegue de diversos mecanismos de tolerancia a fallos de forma robusta y sistemática.

Los resultados de la presente tesis constituyen un conjunto de herramientas y métodos para ayudar al diseñador de sistemas críticos en su tarea de desarrollo de diseños robustos, validados y en tiempo adaptados a su aplicación.