UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

LATIN AMERICAN JOURNAL OF APPLIED ENGINEERING

Selección y Evaluación de Microprocesadores para Sistemas Aeronáuticos

Selection and Evaluation of Microprocessors for Aeronautical Systems

Teodoro Álvarez [a,*], **Roberto Herrera** [a], **Jesús Álvarez** [b]
[a]*CITEDI, Instituto Politécnico Nacional, Tijuana, México*
[b]*CIDETEC, Instituto Politécnico Nacional, Ciudad de México, México*
**Corresponding author: talvarez@citedi.mx*

***Abstract*—**This work consists of making known the basis for the selection and evaluation of the microprocessor, as well as its advantages in its particular architecture, and incorporating the DO-178 and DO-254 aeronautics standards. These standards are an integral part of both the verification and implementation of Software and digital hardware used in the aeronautical industry's avionics area.

***Keywords*—**Microprocessors, Architecture, Aeronautical Standards, Avionics.

***Resumen*—**Este trabajo consiste en dar a conocer las bases de la selección y evaluación del microprocesador, así como sus ventajas en su arquitectura particular, además de incorporar los estándares DO-178 y DO-254 de aeronáutica. Estos estándares son parte integral tanto en la verificación, como en las implementaciones de: Software y hardware digital, que se emplean en el área de aviónica de la industria aeronáutica.

***Palabras Claves*—**Microprocesadores, Arquitectura, Estándares Aeronáuticos, Aviónica..

I. INTRODUCCIÓN

CON el fin de lograr la fiabilidad del sistema, la mayoría de los sistemas de aviónica modernos emplean tolerancia de falla, en el diseño con el fin de lograr sus objetivos. Esto es cierto tanto para los sistemas de las aeronaves militares y comerciales, aunque los sistemas militares no obtienen la certificación para sus aeronaves DO-178B / DO-254 (ED-12B/ ED-80), estos son más estrictos [1,2]. (Por lo general los programas militares son compatibles, con estos estándares). Para soportar la tolerancia a fallos, varios diseñadores emplean métodos que incluyen elementos de redundancia en los elementos de cómputo de múltiples trayectos de comunicaciones y otras técnicas [3]. En el sistema de aviónica es característico de incluir arreglos de doble, triple o cuádruple procesadores que forman un conjunto de procesadores que permite ejecutar los mismo programas, que luego se compara el resultado, en una base de tiempo real o una predefinición de sincronización que apunta en la línea de tiempo de cómputo. Cada procesador tiene sus propios sistemas de memoria caché y que son completamente aislado de los otros procesadores (Este módulo, es una tarjeta de circuito impreso individual que contienen el procesador).

En este tipo de sistema con procesadores múltiples, los resultados de los procesadores se compara, si procesadores están de acuerdo con el resultado, entonces se tomo como correcto. Ahora si se produce una discrepancia con un procesador que está en desacuerdo, éste procesador queda fuera de operación del sistema o en otra palabras no se tomara en cuenta para futuros cálculos y luego se adoptan medidas correctivas, esta acción por lo general toma las siguientes opciones: 1) Reiniciar el sistema o 2) Reinicio del procesador, para determinar si el error era un incidente individual (evento) o si aun, en un nivel más básico de hardware o software, si esto continua con el mismo error. Entonces se determina que el error no es un evento único del procesador, en cual el funcionamiento del sistema de la aeronave, continúa operando de forma segura.

Adicional se genera un reporte de información pertinente, que se registra en memoria no volátil para

permitir el mantenimiento posterior, una vez que la aeronave este en tierra.

Las personas certificadas de hardware en DO-254/ED-80 tienen la autorización con experiencia en diseñar y desarrollar con componentes comerciales tales como procesadores que se usan en la aeronáutica [5,6]. También establecen sobre ciclo de vida de las piezas de los procesadores, FPGA, ASIC, etc., en la industria aeronáutica de la aviónica.

II. METODOLOGÍA

El propósito de la evaluación es también ofrecer los hallazgos acerca de los SoC (system-on-chip), con datos comerciales encontrados de manera objetiva que específica y garantice el diseño, identificando con la guía de los documento D80/DO254.

1. La primera actividad de la inspección consiste en la selección de SoC y la IP (Intellectual Property), de manera específica.
2. Metodología para la evaluación de los datos públicos de SoC con los datos públicos que son:
   - Los datos que puede ser accedidos libremente,
   - Los datos que se pueden obtener a través de un acuerdo comercial (licencia).

ED80/DO254 proporciona una guía para la garantía de diseño para el desarrollo de equipos electrónicos en la aviónica, de tal manera que lleva a cabo las funciones previstas en su entorno especificado. Esto garantiza el diseño a desarrollar desde los documentos guía, que son consideraciones especiales en el hardware como una alta seguridad. También se considera en lo adicional que se refieren específicamente a la utilización de hardware desarrollado previamente, con los componentes COTS (Commercial Off-The-Shelf) [9], la experiencia para reparar el equipo y las herramientas.

ED80 / DO 254 adopta un enfoque de diseño basado en los requerimientos de flujo a nivel del sistema hasta un nivel elemental de hardware de acuerdo con el nivel de seguridad de diseño (DAL), que es definido por el análisis de la seguridad del sistema. Para un componente SoC, en el diseño, o al menos una parte del diseño, se realiza por el proveedor de SoC, sobre la base de los requisitos generales del mercado. Entonces por lo tanto, el SoC no necesariamente está alineado con el ED80/DO254, con estas especificaciones.

Se considerará que el uso de un SoC, que habría sido diseñado, de acuerdo con un proceso basado en las especificaciones de los estándares ED80/DO254, no debería constituir un problema en el caso del uso en un sistema crítico de seguridad. De hecho, en este caso, la estrategia de garantía del diseño se puede basar en el proceso de diseño definido.

Para otros SoC, la garantía del diseño debe basarse en métodos alternativos. De hecho, la información que un fabricante SoC que comúnmente se identifica con sus propiedad que incluye: especificaciones detalladas, diseño detallado, códigos fuente, esquemas y dibujos específicos, resultados de la verificación. Todos estos datos normalmente se requieren y se entrega como parte del programa de desarrollo de especificaciones de acuerdo a los procesos ED80/DO254.

En la actualidad, las técnicas alternativas más populares que se utilizan incluyen: la ingeniería inversa, técnica arquitectónica mitigación (ED80/DO254), historial de servicio (ED80/DO254) de proceso, plan de gestión electrónica (ED80/DO254), el procesamiento por procesador, y actividades ED12B/ DO178B. Podría ser útilizar estos métodos alternativos por los siguientes atributos clave identificados dentro de ED80/DO254 y pertinente al SoC:

Por lo tanto, la estrategia consiste en evaluar los datos públicos, encontrar métodos alternativos, por encima de sus características más importantes. A continuación se tiene cuatro pasos principales que se han establecido para cubrir de una manera lógica todas las estrategias identificadas anteriormente:

- Etapa 1: Identificaciones de procesadores y características,
- Etapa2: La tolerancia a fallos y evaluación de características de seguridad,
- Etapa 3: Verificación y evaluación de herramientas de diseño,
- Etapa 4: Evaluación de los SoC.

Para cada etapa, un cuestionario se ha establecido con el fin de hacer frente a todo el SoCs seleccionado con el mismo rigor.

Etapas	/Cuestionario
Las siguientes preguntas se han utilizado como una guía para analizar los datos públicos en contra de los objetivos de la etapa 1.	
1.¿Existe información disponible sobre el diseño, la producción, la validación y verificación de las fases del fabricante SoC? 2.¿Es posible identificar los componentes del núcleo del procesador y determinar sus características? 3.¿Es posible identificar los núcleos de infraestructura y determinar sus características? 4. ¿Son todas las características identificadas internas compatibles con cualquier tipo de seguridad de aplicaciones críticas? 5. ¿Es posible identificar la topología de buses de	

comunicación interna? Son sus características completamente documentados? 6.¿Es posible aislar o desactivar una función específica documentada o núcleo del resto del SoC? 7. Se describe el mecanismo de desactivación / aislamiento? 8.¿Es posible acceder, observar y controlar de forma independiente los diferentes constituyentes del núcleo del procesador y los núcleos de infraestructura? 9. son los datos de las hojas de datos, guías de usuario, notas de aplicación ... completa y coherente con el producto? 10. ¿Son los dispositivos de erratas y soluciones disponibles? 11.¿Puede la fe de erratas dispositivo se consideren poco importantes en cuanto a su impacto en la seguridad?
Las siguientes preguntas se han utilizado como una guía para analizar los datos públicos contra la etapa 2 objetivos:
1.¿Es posible identificar los modos de fallo de los núcleos y los efectos potenciales a nivel SoC? 2.¿Existen mecanismos de seguridad disponibles en el SoC (es decir, la dirección de bus / paridad de datos o la cobertura de ECC, paridad registro interno, monitoreo reloj interno, la memoria de privilegios de acceso interno y externo)? 3.¿Hay alguna parte o función del chip SEU / MBU sensibles y si es así, ¿hay algún mecanismo que permite detectar, prevenir o corregir una SEU / MBU? 4.¿Podemos considerar que la desactivación de las funciones no utilizadas seguro? 5.¿Pueden estos mecanismos de seguridad suficiente para considerar el SoC como de alta disponibilidad o de seguridad? 6.¿El SoC capaz de producir los resultados esperados después de una cantidad determinada de tiempo (tiempo de espera)?
Las siguientes preguntas se han utilizado como una guía para analizar los datos públicos contra la etapa 3 objetivos :
1.¿Hay herramientas disponibles para implementar y verificar el SoC (compilador, constructor, depurador, kit de diseño SoPC (**System on Programmable Chip**))? 2.¿Se puede prescindir de estas herramientas? 3.¿Hay funciones de depuración y de rendimiento implementadas dentro del SoC? 4.¿Podemos confiar en las herramientas y funciones de depuración internas que no introduzca un error en el diseño, o para no fallar en la detección de un error?
Las siguientes preguntas se han utilizado como una guía para analizar los datos públicos contra la etapa 4 objetivos:
1.¿Puede el fabricante de SoC demostrar una trayectoria para la producción de dispositivos SoC de alta calidad? 2.¿Los procedimientos de calidad son establecidos? 3.¿Hay referencias a un proceso de calificación SoC que establecen la fiabilidad SoC? 4.¿Hay datos disponibles de calificación? 5.¿Hay algún registro experiencia de servicio? 6.¿Existe un proceso de control de cambio de diseño? 7.¿Tener que la garantía de que todos los cambios y los problemas son objeto de notificación al cliente? 8.¿Hay una garantía de apoyo y un período garantizado de producción de dispositivos?

La información sobre el diseño, producción, prueba y verificación realizada por el SOC o el proveedor de IP puede considerarse como información registrada y puede requerir acuerdos específicos para el intercambio de datos presentado a la confidencialidad. El acceso a dicha información podría ser útil para completar o consolidar la evaluación de datos pública. El objetivo del cuestionario fue principalmente acceder a la disposición de los proveedores de SoC para cooperar con el mercado aeronáutico y saber qué tipo de información están dispuestos a compartir. Sobre las respuestas, de la evaluación, se observa el compromiso de los proveedores de SoC en el proceso de certificación.

A. Parte Experimental

Selección de microprocesadores SoC.

La inspección de los microprocesadores SoC se centrará en los productos de Freescale. Los microprocesadores de este fabricante se han utilizado en gran parte en los programas de los últimos aviones y están integrados dentro del SoC. Ahora la transferencia de la arquitectura de un procesador simple en el sistema SoC es rentable ya que el sistema operativo que se ejecuta en ambos chips que es compatible.

Por ejemplo la evolución de la tarjeta madre del procesador Core e600, se puede ver en las figura 1,2,3, que esta implementada con dos componentes, en el cual es más fácil la implementación del sistema operativo OS y la certificación de tareas de acuerdo al ED12B/DO178B.

El sistema de la tarjeta madre, que está basada sobre el Procesador de Freescale MPC 74XX (núcleo e600) El puente en amarillo es un diseño personalizado.

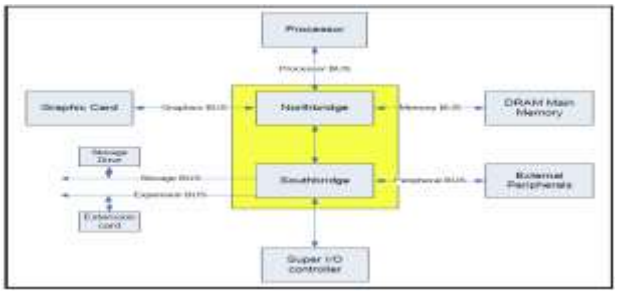

Fig. 1. CPU en la tarjeta madre[8]

Tendencia El nuevo sistema de la tarjeta madre está basada sobre el Procesador de Freescale MPC 86XX (núcleo e600). La funciones del puente están integradas en el MPC 86XX.

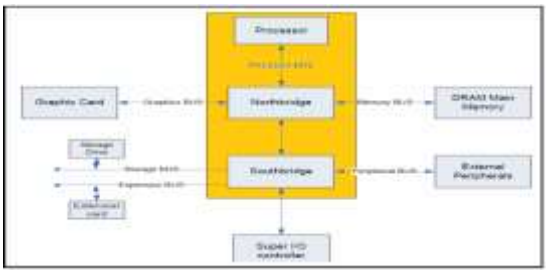

Fig. 2. Evolución del CPU en la tarjeta madre [8]

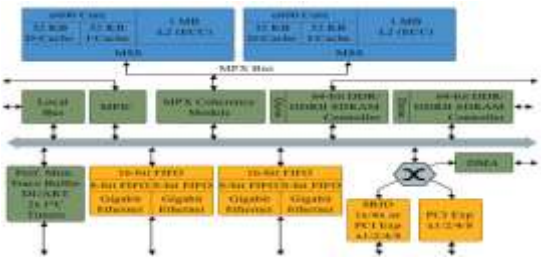

Fig. 3 Freescale MPC 86XX con doble procesador [8]

III. RESULTADOS

Los componentes COTS que nos permite contar con dispositivos comerciales, que cumplen con las normas DO-254, permite reducir los costos de diseño y producción de sistemas aeronáuticos y en particular la aviónica. Es decir, COTS garantizar el suministro y soporte en componente durante al menos la vida útil de la aeronave, así como cumplir con las altos estándares de calidad (DO-254) que garantice la seguridad de operación del viajes de pasajeros y carga de aeronaves. A continuas se tiene resultado de las etapas.

Etapa 1. En general, las características de los principales componentes y mecanismos de los proyectos de investigación que se identifican y se explican en este artículo. Esperando que la información se a suficiente para poner en práctica la IP en una aplicación de seguridad no crítica. Aunque, algunas preocupaciones pueden poner en peligro la información de la IP:

• La acción de registros de software y la programación de puertos de E/S, que permiten desactivar, funciones específicas que no son documentadas,

• Algunos componentes de la IP no se puede acceder directamente y no se pueden evaluar,

• Los errores potenciales y la posible falta de la documentación pueden conducir a una aplicación inadecuada de la IP.

Etapa 2. En la mayoría de los casos, los modos de fallo potenciales no están documentados y sólo se puede suponer a partir del análisis de datos públicos.

Casi todos los componentes pueden tener un impacto crítico en el comportamiento SoPC (System on Programmable Chip) en caso de errores de diseño. La falta de visibilidad interna y conectividad que hace que sea casi imposible, de realizar la identificación de confianza en la fiabilidad IP. En este contexto, el proveedor de IP es esencial su cooperación para obtener datos de diseño IP, así dar algún apoyo para implementar propuesta de soluciones eficientes.

Las IP seleccionados no son iguales en cuanto a la sensibilidad SEU (Single Event Upset). Algunos de ellos no cuentan con funciones sensibles SEU. Algunas otras funciones sensibles no encuentran SEU y no tienen mecanismos de detección ni de corrección. Otros implementan diversos mecanismos para detectar, un SEU y corregir su impacto en sus funciones SEU.

Etapa 3. En la práctica, las herramientas que intervienen en el diseño de un SoPC no deben tener un impacto en la seguridad de la aplicación. Sin embargo, algunos de los proveedores seleccionados de los PLD (Programmable Logic Device), imponen herramientas de diseño específicos. Por lo tanto, al seleccionar una solución SoPC el solicitante debe tener en cuenta los aspectos técnicos, la necesidad de herramientas que pueden conducir, con las normas ED80/DO254 recomendadas o no cumplir.

De la misma manera, ya que los módulos de depuración están sujetos a modos de fallo potenciales, los posibles modos de fallo del módulo de depuración, han de tenerse en cuenta, a la hora de definir las estrategias de verificación de hardware y software.

Etapa 4. Los datos públicos proporcionan alguna información sobre los procesos de calidad y calificación, aplicados a los elementos de silicio, pero no ofrecen visibilidad en los procedimientos de diseño para el proceso de calidad aplicado al proyecto de las IP's. Además, si se proponen diversos medios por los cuales los proveedores de IPs, apoyan e informar a sus clientes, sobre la detección, recolección, de informes y la corrección de errores que no están necesariamente documentados bajo las normas ED80/DO254.

IV. CONCLUSION

El análisis de la información pública para el microprocesador se ha puesto en relieve aplicándole los pasos 1, 2, 3, 4.

Se observo que los objetivos principales del IP del procesador tienen diferentes niveles de complejidad y presentan problemas diversos en cuanto a su uso, bajo una aplicación de seguridad crítica. Los principales problemas identificados fueron:

A falta de visibilidad en el mecanismo de desactivación de las funciones no utilizados,

- La ausencia de datos que permitan una aplicación segura,
- No tener mecanismos de seguridad,
- Una baja sensibilidad en la SEU/MBU (Multiple Bit Upset),
- La poca visibilidad en los procesos de diseño y gestión de datos,
- La escasa visibilidad en la gestión de errores y presentación de informes,
- La falta de experiencia de servicio de registros de las normas,
- Se requiere una herramienta sin restricciones para la configurar principal.

En todo caso, sobre la base de la información pública, el procesador es susceptible de no ser implementado como se requiere en aplicación de seguridad crítica, también se ha identificado -- la aceptación del NIOS II SC cuyo proceso de diseño puede ser realizados--. De hecho, los dispositivos mencionados de Freescale muestran la mayoría de los problemas anteriores. En resumen, se considerará que la aplicación de un SoPC, utiliza la única información publicados que no permite satisfacer la recomendaciones ED80/DO254, esto puede constituir un riesgo para una aplicación de seguridad críticas. En este contexto, dos métodos pueden ser adoptados.

Cuando es posible: el diseñador pueda cambiar el diseño utilizando la IP para diseñar con los estándares ED80/DO254, que se puede complementar con dispositivos (COTS) que cumplan el ciclo de vida del diseño. El otro método consistiría en definir una estrategia de aseguramiento de diseño alternativo para cubrir la ausencia de la información pública y que nos llevaría a:

- Identificar las funciones de IP que sean un riesgo para la seguridad contra los eventos inesperados de la aplicación final,
- Definir el uso de dominio que impacte a la seguridad IP, y que sería limitado,
- Definir los métodos de prevención y revisión en los diferentes niveles para limitar el impacto en las funciones inseguras

V. AGRADECIMIENTOS

El resultado de este trabajo es parte de los apoyos recibidos de la Secretaria de Investigacion y Posgrado del IPN para el proyecto SIP-20160693.

REFERENCIAS

1].- Eurocae ED80/RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware, April 19, 2000.

[2].- Eurocae ED12/RTCA DO-178B, Software Considerations in Airborne Systems and Equipment Certification, December 1, 1992.

[3].- ED79/ARP 4754, Certification consideration for Highly Integrated or complex systems. Nov 1996.

[4].- EASA Certification Memo SW and CEH. Reference: Memo-SWCEH-002 Issue 1 Rev 2 Date: 02/06/2008.

[5].- Microprocessor Evaluations for Safety-Critical Real-Time Applications, Authority for Expenditure No. 43 Phase 1 Report DOT/FAA/AR-06/34, December 2006.

[6].- Microprocessor Evaluations for Safety-Critical Real-Time Applications, Authority for Expenditure No. 43 Phase 2 Report, June 2008.

[7].- European Aviation Safety Agency, Safety implications of the use of system-on chip(SoC) on commercial of the shelf(COTS) devices in airborne critical applications, Research Project EASA.2008/1.

[8].- Freescale.com: Microprocessor http://www.phxmicro.com/Training/Freescale/freescale_Chip/Image%20PQ%20Chips/MPC8641.jpg

[9].- Lt Col Lionel D. Alfrod, Jr., USAF, The problem with aviation COTS, Acquisition Review Quarterly—Summer,1999.

Este estudio fue financiado por los autores. Los autores declaran no tener ningún conflicto de interés.