

Herramienta de configuración para sistemas IMA-SP

YOLANDA VALIENTE, PATRICIA BALBASTRE, JOSÉ ENRIQUE SIMÓ¹

INSTITUTO DE AUTOMÁTICA E INFORMÁTICA INDUSTRIAL (AI2)

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Resumen

En este trabajo se describe la definición, diseño, implementación y prueba del conjunto de herramientas necesarias para realizar las actividades del proceso de desarrollo IMA-SP (Integrated Modular Avionics for SPace). Además, se definirá el modelo de datos, con los archivos asociados, que describen la configuración completa de un sistema con particiones y la evaluación de la viabilidad del sistema; el desarrollo de un prototipo del conjunto de herramientas, que se llamará IMA-SP SDT (System Development Toolkit) y la demostración de la herramienta sobre un caso de estudio.

1.-Introducción

Para hacer frente a la creciente complejidad del software de un satélite, la ESA ha explorado soluciones tecnológicas adoptadas por el dominio aeronáutico para este propósito: la arquitectura IMA Integrated Modular Avionics y los sistemas particionados (TSP).

En [1] se definen las actividades y los roles que intervienen en el proceso de desarrollo de un sistema IMA-SP. Dentro de estas actividades, tenemos: i) Particionado y asignación de recursos y ii) Evaluación de la viabilidad del Sistema.

La actividad de Particionado y asignación de recursos es una de las actividades centrales desde la perspectiva de definir las particiones de un sistema IMA-SP. En esta actividad, se realiza la asignación de componentes de software a nodos físicos teniendo en cuenta: las limitaciones de memoria y tiempo; requisitos de acceso directo a hardware específico; requisitos que afectan a las características del sistema, tales como el intercambio de información entre los componentes.

A lo largo del desarrollo del sistema ha de asegurarse que la asignación de recursos cumple con los requisitos establecidos y las limitaciones del hardware. Esto se puede comprobar mediante, por ejemplo, el análisis estático o mediante simulaciones. Esto incluye comprobar que los requisitos no funcionales del sistema, la planificación tem-

¹ Este artículo ha sido subvencionado por el Ministerio de Economía y Competitividad bajo los proyectos TIN2014- 56158-C4-1-P y TIN2014- 56158-C4-4-P.

poral, el control de fallos o la comunicación se cumplen tanto por la partición como por el hardware seleccionado. La evaluación de la viabilidad del sistema se lleva a cabo por el Integrador del Sistema (SI).

2.-Objetivos

El objetivo general de este artículo es definir , diseñar, implementar y probar el conjunto de herramientas necesarias para desarrollar un sistema IMA-SP. Para ello se definen los siguientes sub-objetivos:

1. Definir un modelo de datos que describa la información que necesita ser capturada para la definición de una partición, asignación de recursos, configuración de la plataforma, etc, es decir, reflejar la configuración completa del sistema con particiones, así como permitir la evaluación de la viabilidad del sistema.
2. Definir un conjunto apropiado de archivos de configuración y formatos de archivo correspondientes para capturar el contenido del modelo de datos, teniendo en cuenta el intercambio de información junto con la confidencialidad según se define en el proceso de desarrollo IMA-SP [1].
3. Desarrollar un prototipo del conjunto de herramientas llamado IMA-SP System Design Toolkit (SDT).
4. Demostrar la viabilidad del prototipo desarrollado con un caso de estudio.

3.-Modelo de datos

El modelo de datos a definir debe incluir la información necesaria para definir los recursos de hardware, los requisitos de la aplicación, la asignación de recursos y la configuración del kernel de particionado (PK). La información que es específica de los contenidos internos de las particiones (por ejemplo, la funcionalidad y la semántica) no está incluida. Los requisitos del modelo de datos son:

- El modelo de datos debe capturar los requisitos de las aplicaciones, como por ejemplo: requisitos temporales, necesidades de memoria o requisitos específicos de hardware.
- El modelo de datos debe capturar las propiedades de la plataforma: procesamiento, memoria, comunicación, temporizadores, recursos compartidos, etc.
- El modelo de datos debe describir la asignación de los recursos físicos a las aplicaciones de partición.
- El modelo de datos debe proporcionar suficiente información para permitir el análisis de planificabilidad de la asignación de recursos dada, así como identificar posibles optimizaciones.
- El modelo de datos debe permitir capturar la configuración del kernel de particionado: planes temporales, tablas de asignación de memoria, canales de comunicación, *health monitoring*, etc.

- El modelo de datos debe permitir la segregación del modelo completo en diferentes ficheros de forma que puedan ser utilizados por diferentes roles en el proceso de desarrollo.
- El modelo de datos debe permitir reusar datos existentes en un nuevo proyecto.
- El modelo de datos debe ser coherente y consistente con una semántica y sintaxis precisa.

Los datos del modelo se organizan de la siguiente forma:

- Modelo de partición. Representa el contrato entre el Proveedor de Aplicación (PA) y el Integrador del Sistema (IS).
 - Propiedades de la partición, tareas, puertos de comunicación, requisitos de memoria.
- Modelo físico. Describe los recursos hardware disponibles para las particiones.
 - Memoria, Procesadores, Interrupciones, periféricos.
- Modelo de sistema IMA-SP. Define la asignación de recursos a las particiones.
 - Asignación de: Memoria, Interrupciones virtuales, recursos hardware, End to end flows (ETEF).
- Modelo de kernel de particionado (PK). Describe el kernel que proporciona el particionado tanto espacial como temporal (TSP).
 - Requisitos de memoria, eventos, acciones y configuración por defecto del Health Monitoring, tanto del sistema como de las particiones;
- Modelo de datos del kernel de particionado. Contiene toda la información necesaria para configurar el PK para un proyecto dado.
 - Tabla del Health Monitoring Table, Scheduling Plan, tabla de conexiones de los puertos, tabla de configuración de la memoria.
- Modelo de datos común. Contiene los tipos básicos que utilizan el resto de modelos.

Las dependencias de cada uno de estos sub-modelos que conforman el modelo de datos total se muestran en la Figura 1.

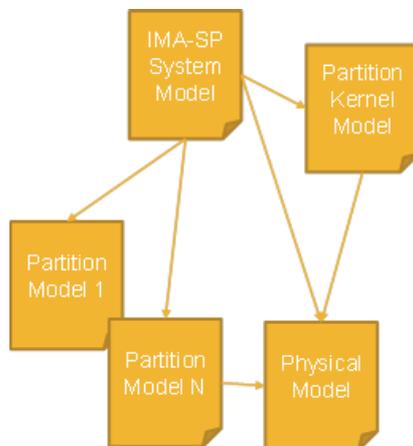


Figura 1 Dependencias del modelo de datos

Para especificar el modelo de datos IMA-SP SDT se utilizará el formato *ecore*, del framework de modelado de Eclipse (EMF, Eclipse Modeling Framework) [2]. Los ficheros del modelo están en formato XML Meta-data Interchange (XMI) [3].

4.-Flujo de trabajo IMA-SP SDT

Junto con el modelo, también se ha definido el flujo de trabajo para especificar cómo las herramientas propuestas se utilizan en el proceso de desarrollo de un sistema IMA-SP para generar el modelo de datos del sistema completo. A continuación se resume este flujo de trabajo en sus principales puntos:

1. El arquitecto del sistema (SA) define el modelo físico y se lo proporciona al Proveedor de Plataforma (PS).
2. El PS define en el modelo de kernel de particionado los siguientes elementos:
 - a. Requisitos de memoria del kernel.
 - b. Eventos y acciones del kernel.
3. El PS define la plataforma para los modelos de partición.
4. El PS realiza una asignación de recursos inicial en el modelo de sistema IMA-SP.
5. El PS proporciona los modelos de datos al SI.
6. El SI define el número de particiones y sus propiedades.

7. El PA o el SI define los puertos, tareas y recursos requeridos por la partición en el modelo de partición.
8. El SI define la tabla del *health monitoring*, la tabla de conexiones de los puertos, la tabla de asignación de recursos y el modelo temporal basado en ETEFs. Esto lo hace en el modelo de sistema IMA-SP y en el modelo de kernel de particionado.
9. El SI realiza un análisis de planificabilidad del modelo de datos completo y almacena la configuración de esta asignación de recursos en el modelo de datos del kernel de particionado en la parte de configuración.
10. El SI genera el fichero de configuración y el modelo redactado. El modelo redactado se utiliza para validar una sola partición. De este modo se elimina del modelo toda la información de otras particiones pero manteniendo la coherencia en el uso de recursos total.

5.-Requisitos de IMA-SP SDT

El modelo de datos descrito en el apartado 3 se ha usado como base para definir los requisitos del conjunto de herramientas IMA-SP SDT que trabaja con este modelo. Las funcionalidades más importantes del IMA-SP SDT son:

- **Asignación de recursos.** Esta parte era un lento proceso manual realizado por el SI que debe encajar las necesidades de recursos de las particiones con el hardware disponible.
- **Análisis de planificabilidad.** En esta fase, debe validarse que la asignación de recursos anterior es realizable, es decir, que los requisitos de cada partición se cumplen con el hardware disponible. Este proceso suele ser automático.
- **Redacción.** El modelo redactado se utiliza para validar una sola partición. De este modo se elimina del modelo toda la información de otras particiones pero manteniendo la coherencia en el uso de recursos total.
- **Configuración de la plataforma.** Con el modelo completo y validado, en esta fase se crea el fichero estático de configuración para el kernel seleccionado.

6.-Diseño de IMA-SP SDT

Con el modelo de datos y los requisitos que debe cumplir el conjunto de herramientas se diseña el IMA-SP SDT.

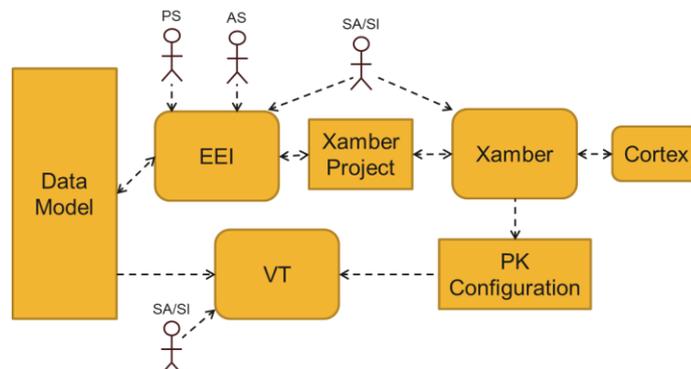


Figura 2 Arquitectura IMA-SP SDT

La arquitectura general se presenta en la Figura 2. El proceso de definición y desarrollo de un sistema IMA-SP implica los siguientes pasos y herramientas:

1. Definición inicial del modelo. Para ello se utiliza la herramienta EEI (Edit. Export and Import). Esta herramienta es un editor de EMF en la cual cada rol introduce la información inicial (definición de recursos hardware en el modelo físico por el SI, definición de requisitos de cada partición por cada PA y definición del kernel de particionado por el PS).
2. En el siguiente paso se realiza la asignación de recursos en función de las necesidades de cada aplicación y del kernel. Esto lo realiza el SI exportando el modelo emf para poder ser importado por la herramienta Xamber. Xamber será la herramienta encargada de realizar de forma automática esta asignación de recursos.
3. Xamber proporciona una representación gráfica del modelo de datos permitiendo ejecutar el planificador para generar el plan temporal y la asignación de memoria.
4. Una vez asignados todos los recursos por Xamber, el modelo de datos está completo. El SI puede entonces importar desde EEI el proyecto de Xamber para así tener el modelo completo en EMF.
5. Al mismo tiempo, el SI puede generar el fichero de configuración del sistema en Xamber. Xamber es capaz de generar este fichero para XtratuM que es el kernel de particionado seleccionado para realizar el caso de uso que validará la bondad de IMA-SP SDT.
6. Para verificar que el fichero de configuración generado se corresponde con el modelo de datos en EMF, la herramienta VT comprueba la coherencia y corrección de ambos.

Estos pasos deben seguirse de forma manual por los distintos actores del proceso de desarrollo. De todas formas, si se salta algún paso, EEI, Xamber y V son capaces de detectar la inconsistencia o falta de datos y avisar sin que se produzcan errores.

7.-Demostrador IMA-SP SDT

El caso de uso para demostrar la bondad y utilidad de las herramientas propuestas fue el Caso de Uso B del proyecto IMA-SP. El sistema está compuesto por 3 particiones:

- Partición de sistema: responsable de la supervisión del sistema y comunicación entre particiones e hipervisor.
- Partición MIRAS: Responsable del manejo de la instrumentación para los experimentos de la misión SMOS (Soil Moisture and Ocean Salinity).
- Partición AOCS: responsable de las aplicaciones de guiado y control del satélite.

El hipervisor utilizado es XtratuM y los requerimientos de hardware son:

- Procesador LEON3.
- Reloj del procesador a 50Mhz.
- 48 MB SDRAM.

Con el conjunto de herramientas IMA-SP SDT se definió el flujo de trabajo y así se configuró la totalidad del sistema siguiendo los siguientes pasos:

1. Definición del modelo físico por el SI con EEI.
2. Definición del modelo de plataforma por el SI con EEI.
3. Definición del modelo de kernel de particionado por el PS con EEI.
4. Definición de los modelos de partición por los AS con EEI.
5. Definición de conexiones de comunicación entre particiones por SI con EEI.
6. Asignación de recursos por el SI con Xamber.
7. Creación del fichero de configuración para XtratuM por el SI con Xamber.
8. Importación del modelo completo por el SI con EEI.

9. Verificación de la corrección y coherencia de modelo y fichero de configuración por el SI con VT.

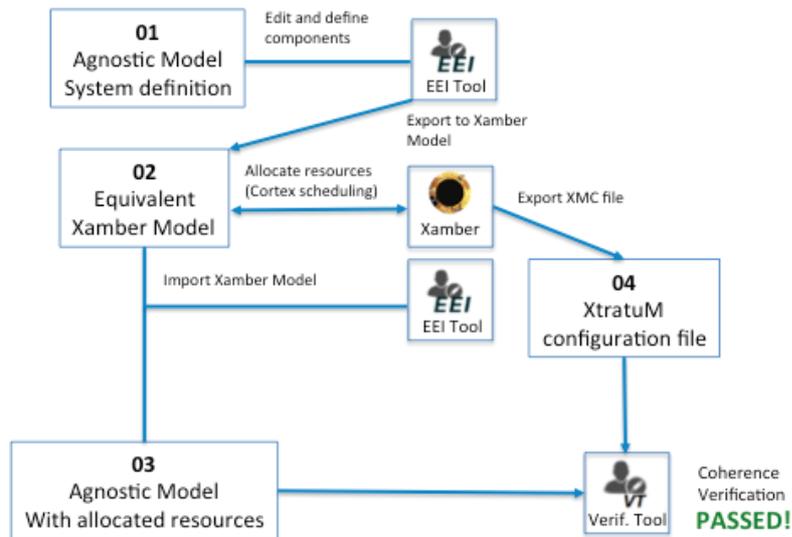


Figura 3 Flujo de trabajo IMA-SP

En la Figura 3 se muestra el flujo de trabajo descrito anteriormente. Los pasos 1 a 5 se corresponden con el recuadro '01 Agnostic Model Definition' realizado con la herramienta EEI. En la Figura 4 se puede ver el aspecto de esta herramienta.

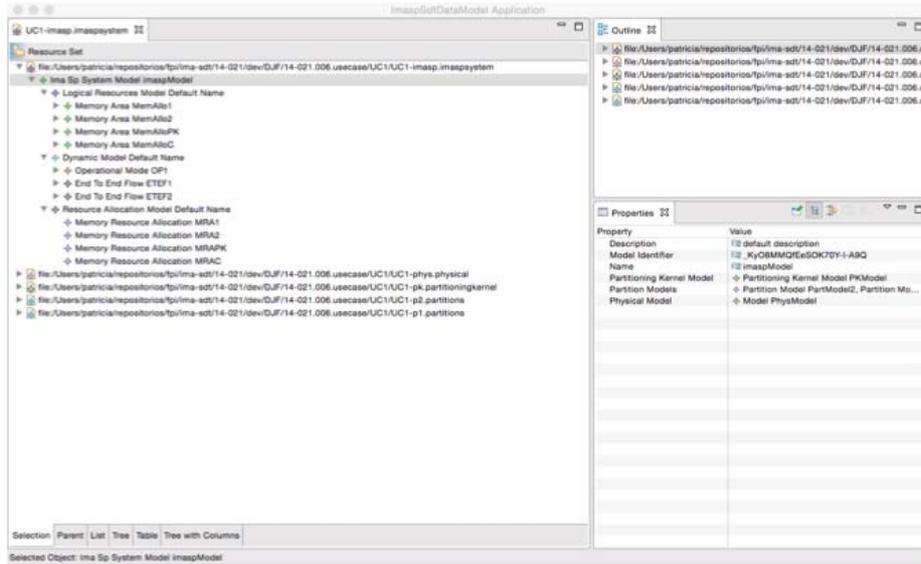


Figura 4 Herramienta EEI

Previo al paso 6, es necesario exportar el modelo de datos al formato de Xamber, por ello el recuadro '02 Equivalent Xamber Model' es la entrada a la herramienta Xamber (Figura 5).

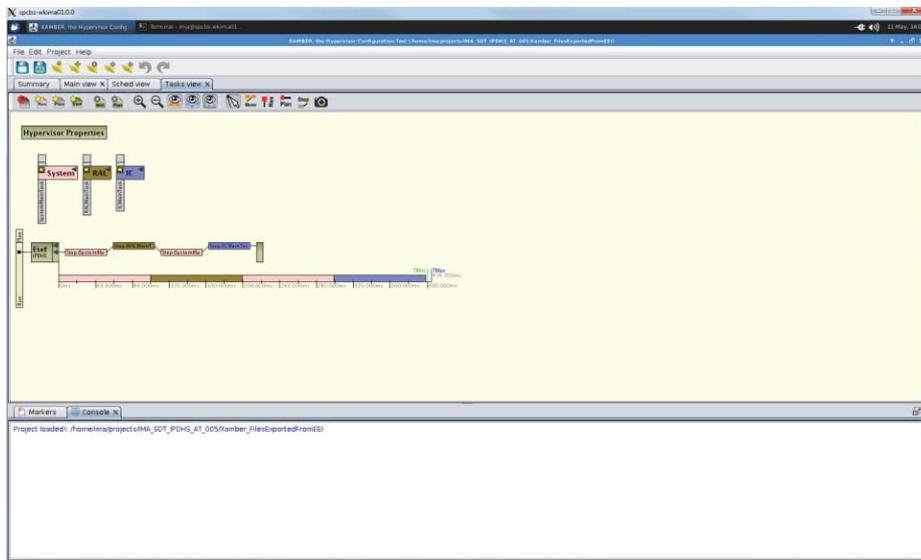


Figura 5 Herramienta Xamber

Una vez asignados todos los recursos se genera, por un lado el fichero de configuración del sistema en formato XMCF y, por otro lado, el modelo de datos de Xamber (con asignación de recursos) se importa desde la herramienta EI. Con el modelo de datos y el fichero XMCF, se comprueba mediante la herramienta VT (Figura 6) si estos dos son coherentes entre sí.



Figura 6 Herramienta VT

8.-Resultados

El resultado de utilizar el conjunto de herramientas desarrollado es la configuración del sistema (fichero XMCF y modelo de datos agnóstico completo). Por motivos de confidencialidad no se puede mostrar el contenido del fichero. Sin la existencia de las herramientas desarrolladas tendría que haberse generado la configuración a mano. Esto es perfectamente posible cuando hay pocas particiones en el caso de la asignación de memoria. Pero cuando hay muchas particiones o en el caso de la asignación de recursos temporales, es imprescindible contar con la ayuda de herramientas que automaticen el proceso, por lo que el conjunto de herramientas IMA-SDT supone un ahorro de tiempo importante en la generación de la configuración del sistema.

9.-Conclusiones y trabajo futuro

En este trabajo se ha descrito la definición, diseño e implementación de un conjunto de herramientas para la configuración de sistemas particionados que siguen la arquitectura IMA-SP. Se ha definido completamente el modelo de datos y se ha organizado siguiendo los roles definidos en el proceso de desarrollo IMA-SP. Con el desarrollo de un caso de estudio se ha demostrado su viabilidad.

Como trabajo futuro se espera ampliar el conjunto de herramientas para soportar la arquitectura multinúcleo, alinear el modelo de datos con la arquitectura OSRA (On-Board Software Reference Architecture) y soportar la configuración de otros kernels de particionado.

Bibliografía

- [1] IMA-SP D08-11 – IMA development process, roles and tools, Issue 2.0, Date 21/01/2013.
- [2] <http://www.eclipse.org/modeling/emf/>
- [3] <http://www.omg.org/spec/XMI/>