XXI Jornada Técnica de AdaSpain

Herramienta basada en modelos para validación y verificación de código autogenerado

Hugo Valente
Miguel Ángel de Miguel

STRAST

UNIVERSIDAD POLITÉCNICA DE MADRID

Dirección General de Investigación e Innovación Tecnológica
CONSEJERÍA DE CIENCIA, UNIVERSIDADES E INNOVACIÓN
Comunidad de Madrid

Motivación

Método tradicional para desarrollar software espacial

- Largo tiempo de desarrollo
- Costes altos
- A la medida que aumenta la complejidad, mayor la probabilidad de introducir errores

POLITÉCNICA

Solución

Generación automática de código para sistemas críticos con tendencias actuales…

- Disminuir tiempo de desarrollo, costes
- Aumentar la calidad del código utilizado

… basada en modelos independientes de la plataforma

- Ver sistemas, no líneas de código
  - Disminuir la complejidad y así la probabilidad de errores
- Independencia de plataforma permite reutilizar código y así disminuir aún más el tiempo de desarrollo y costes

POLITÉCNICA

Tendencias actuales de sistemas espaciales

Funcionalidades

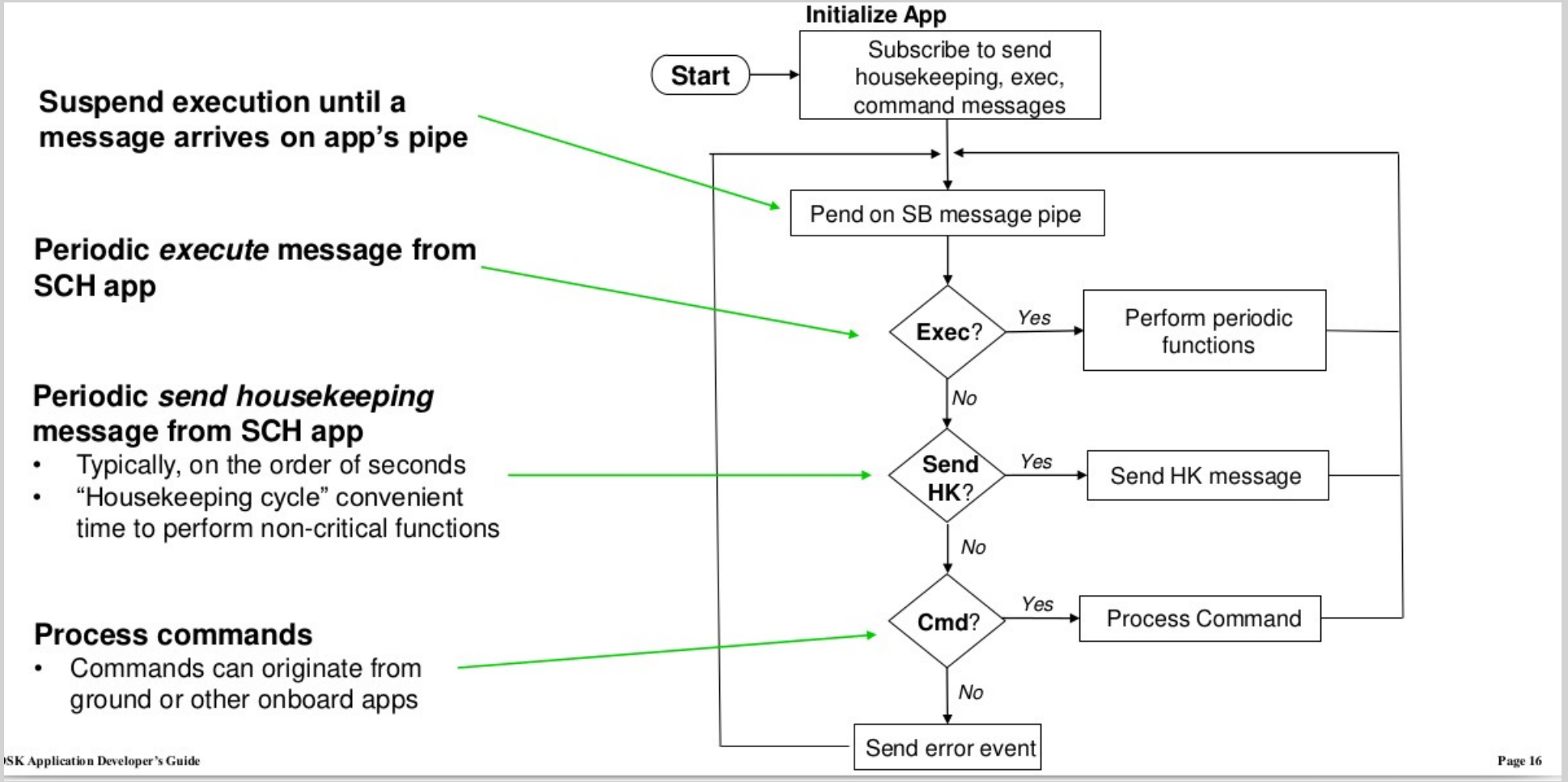
- Comunicación asíncrona N a M
- Eventos
- Gestión de componentes
- Almacén de datos

Framework cFS

- Framework moderna de la NASA aplicada en misiones clase A
- Soporta todas las funcionalidades identificadas
- Arquitectura basada en componentes con abstracción de plataforma que es ideal para representar modelos independientes de la plataforma

POLITÉCNICA

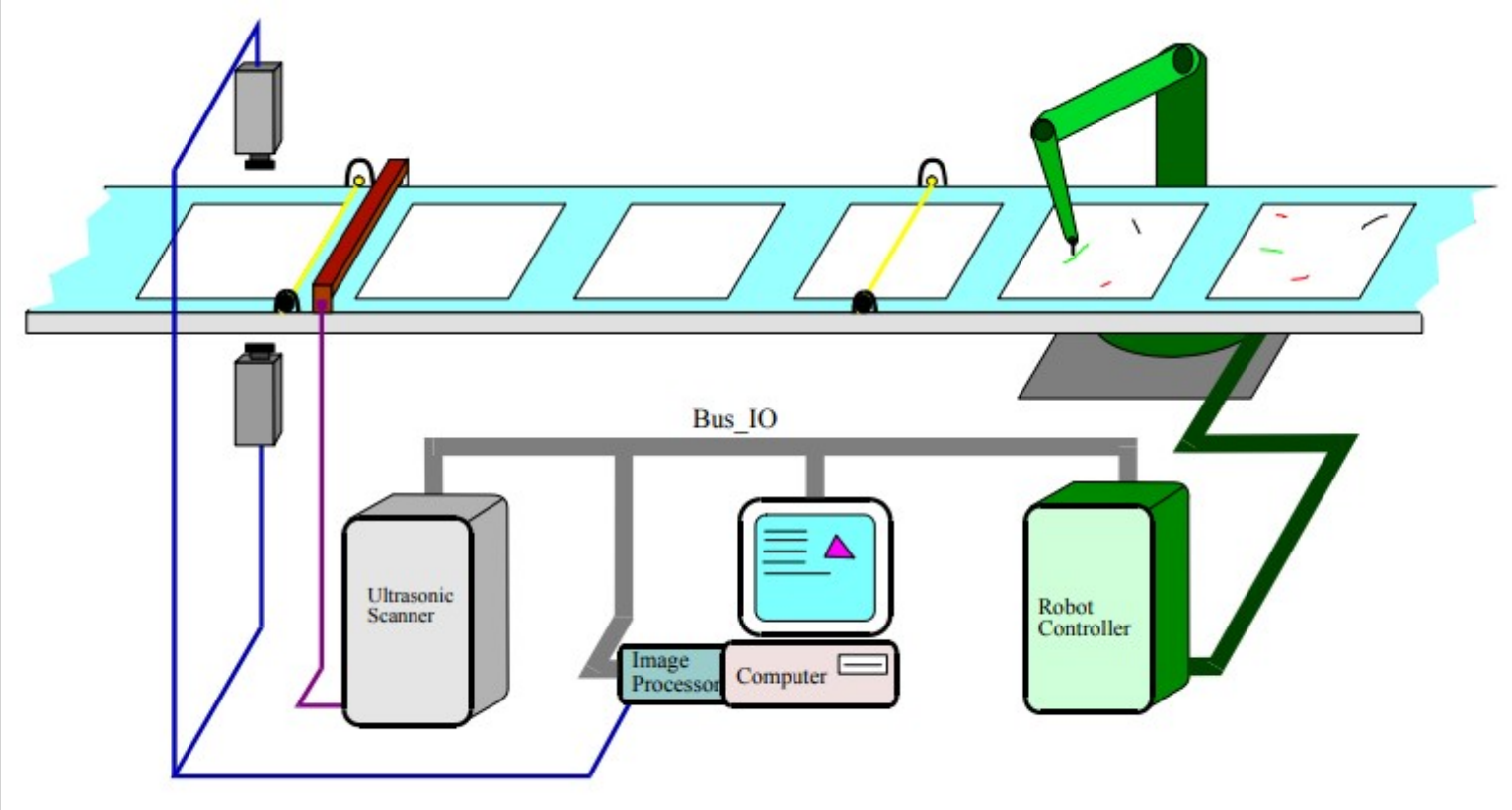
Estructura de aplicación generada



Modelado y generación de código

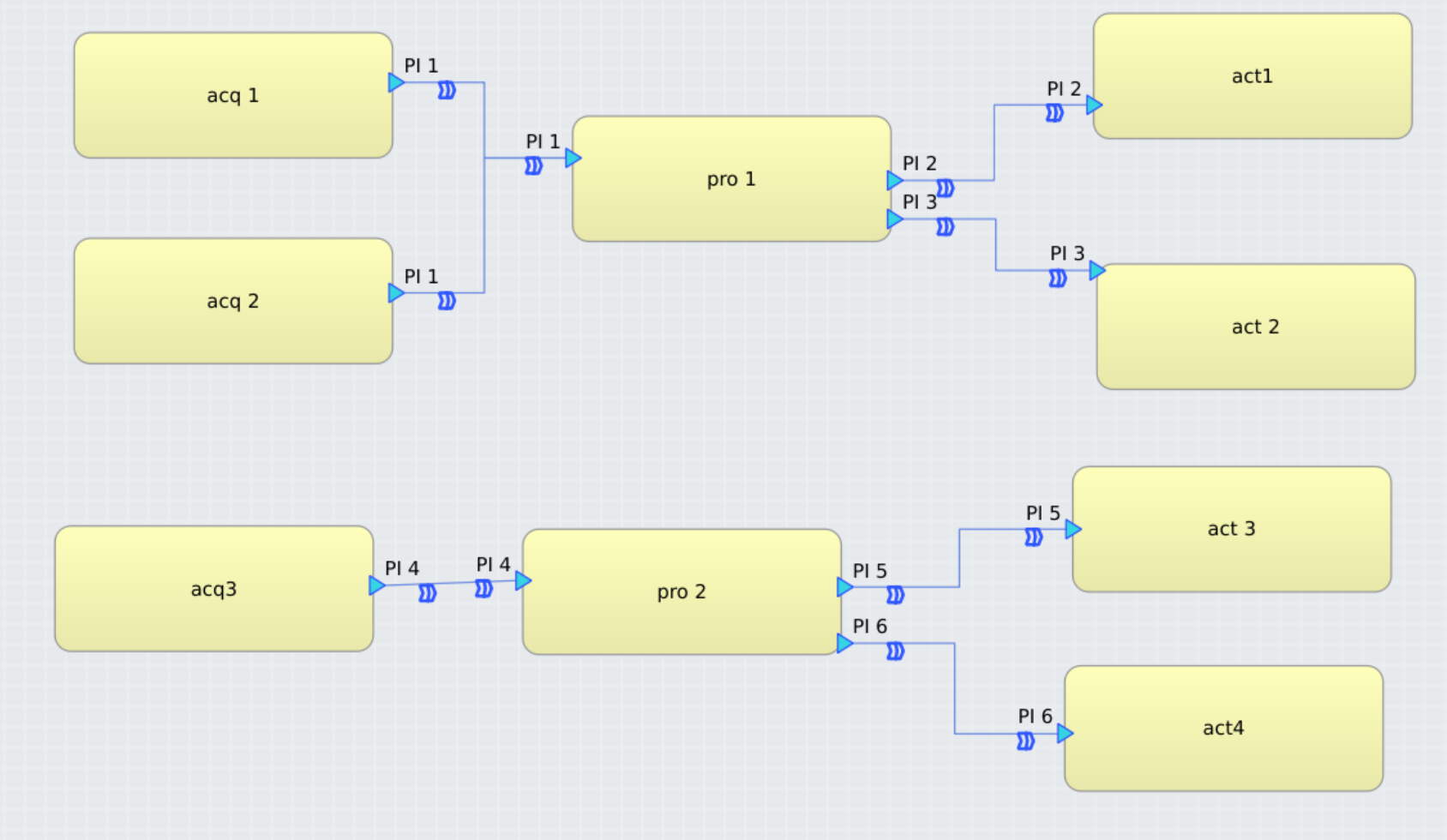
Primer paso: Describir modelos cFS y generar código cFS que puede ser ejecutado en plataformas cFS

Caso de estudio



Ejemplo de MAST. Sistema distribuido 4 procesadores

Resultados generación código



Nr components	9
Nr files	137
Total nr lines	16089
LOC	8063
Comments	4595

Validación y verificación para probar aplicabilidad en sistemas críticos

Garantizar que cumple 3 requisitos:

- Seguridad, protección y calidad del código generado, en línea con estándares industriales
- Análisis dinámico: cobertura del código:
  - Líneas, decisión, funciones
- Cumple requisitos temporales

Seguridad, protección y calidad del código generado

Garantizar que el código generado cumple estándares industriales para sistemas críticos:

- Generar código que cumple la normativa MISRA
  - Análisis estático del código generado para garantizar que no hay violaciones del estándar
    - Evitar errores en tiempo de ejecución
    - Garantizar la calidad del código y mejorar la seguridad de los sistemas

Category	Count
# Advisory violations	0
# Required violations	0
# ERRORS	0
# Total violations	**0**

POLITÉCNICA

Análisis dinámico: cobertura del código

Garantizar que el código generado cumple requisitos de la ESA para sistemas críticos clase A

Code coverage versus Software Classification	A	B	C	D
Source code statement coverage	100%	100%	AM	AM
Source code decision coverage	100%	100%	AM	AM
Source code modified condition and decision coverage	100%	AM	AM	AM
NOTE: "AM" means that the value is agreed and signed off by the Center's Engineering TA and measured.				

POLITÉCNICA

Análisis dinámico: cobertura del código

Directory	Line Coverage	Functions	Branches	Nr of Tests
acq_1_app	**100.0%** (169 / 169)	**100.0%** (13 / 13)	**100.0%** (58 / 58)	165
acq_2_app	**100.0%** (169 / 169)	**100.0%** (13 / 13)	**100.0%** (58 / 58)	165
acq_3_app	**100.0%** (169 / 169)	**100.0%** (13 / 13)	**100.0%** (58 / 58)	165
act_1_app	**100.0%** (158 / 158)	**100.0%** (13 / 13)	**100.0%** (53 / 53)	151
act_2_app	**100.0%** (158 / 158)	**100.0%** (13 / 13)	**100.0%** (53 / 53)	151
act_3_app	**100.0%** (158 / 158)	**100.0%** (13 / 13)	**100.0%** (53 / 53)	151
act_4_app	**100.0%** (158 / 158)	**100.0%** (13 / 13)	**100.0%** (53 / 53)	151
pro_1_app	**100.0%** (216 / 216)	**100.0%** (17 / 17)	**100.0%** (77 / 77)	209
pro_2_app	**100.0%** (216 / 216)	**100.0%** (17 / 17)	**100.0%** (77 / 77)	209
				1517

POLITÉCNICA

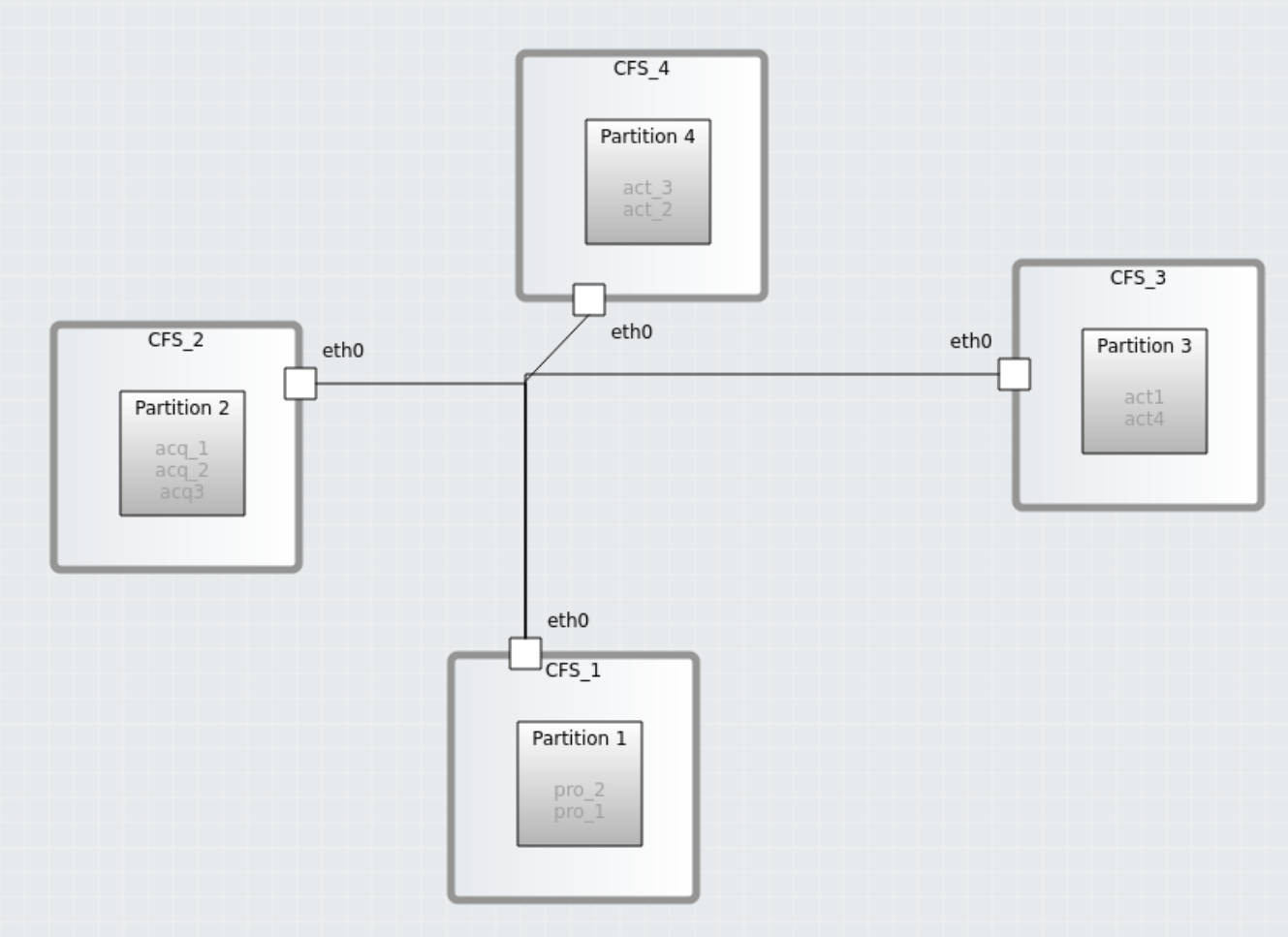
Requisitos temporales

Sistemas de alta criticidad, necesario garantizar que el sistema es planificable, que todas las tareas cumplen sus plazos.

- Integración de herramienta de análisis temporal que soporte análisis de sistemas basados en eventos
  - Integración de Mast de la Universidad de Cantabria en la cadena de herramientas

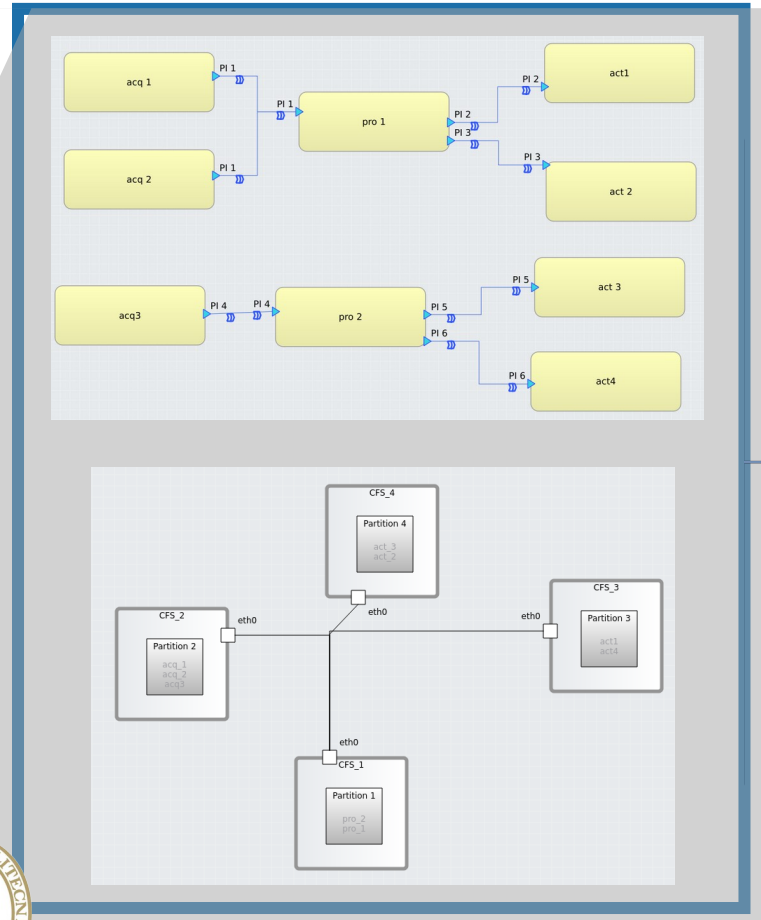
Technique	Single-Processor	Multi-Processor	Simple Transact.	Linear Transact.	Multipath Transact.
Classic Rate Monotonic	☑		☑		
Varying Priorities	☑		☑	☑	
Holistic	☑	☑	☑	☑	☑
Offset Based	☑	☑	☑	☑	

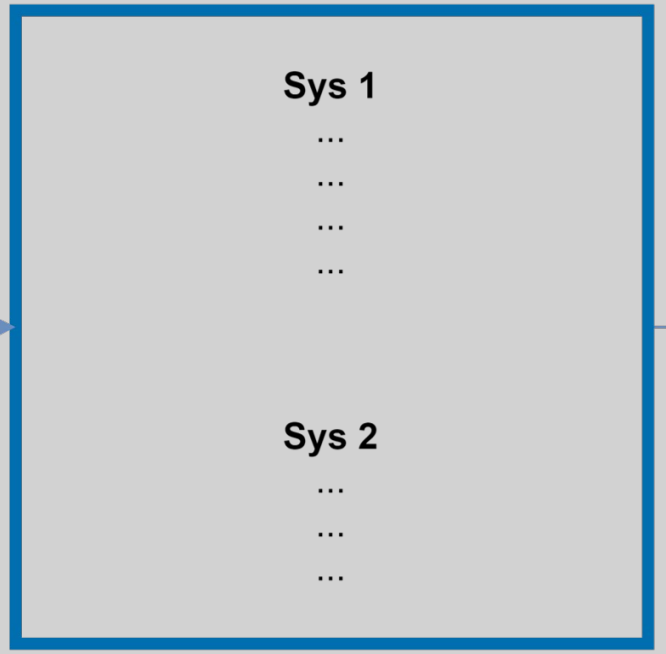
Requisitos temporales



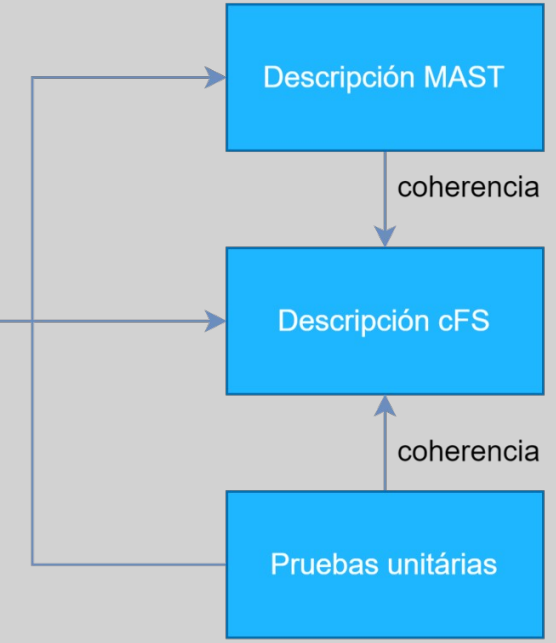
Name	Utilization
eth0	69.50%
partition_1	86.00%
partition_2	84.00%
partition_3	76.00%
partition_4	74.50%

Validación y verificación





Descripción del modelo



POLITÉCNICA

Muchas gracias