

Diseño de una arquitectura tolerante a fallas basada en componentes COTS para vehículos satelitales de nueva generación



Tesista: Arias Emmanuel

Director: Ing. Gustavo Wiman

Universidad Nacional de la Matanza

24 de octubre de 2018



Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
 - Análisis de arquitectura tolerante a fallas
- 6 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 7 Arquitectura propuesta
- 8 Conclusiones

Agenda

1 Motivación

2 Objetivos

- Objetivos del trabajo
- Preguntas de investigación

3 ¿Qué es la tolerancia a fallas?

- Atributos de la fiabilidad
- Falla, Error, Avería

4 Bus CAN

- Definición

• Protocolo CAN

5 Análisis de arquitectura tolerante a fallas

6 CANae

- Introducción
- Capa de aplicación
- CANae Application Layer
- High Application Layer CANae

7 Arquitectura propuesta

8 Conclusiones

Motivación

El desarrollo de proyecto satelitales conlleva costos de importante magnitud. Estos se pueden clasificar en 5 grandes grupo:

- Desarrollo
- Materiales
- Ensamblado, integración y test
- Lanzamiento
- Operaciones

Componentes COTS

- Los componentes COTS suelen tener un costo de compra de hasta 1000 veces menores que los componentes calificados para volar.
- Ayudaría a ahorrar millones de dólares de los proyectos satelitales.
- La tecnología más avanzada de los COTS permite:
 - ▶ Aumentar las prestaciones
 - ▶ Implementar funciones que son imposibles con la tecnología actual
 - ▶ Reducir tiempo de desarrollo
 - ▶ Reducir volumen, masa y consumo de potencia.

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Arquitectura propuesta
- 9 Conclusiones

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Arquitectura propuesta
- 9 Conclusiones

Objetivo del trabajo

El objetivo de este trabajo es investigar y analizar arquitecturas de comunicación de los subsistemas de aviónica tolerante a fallas basada en componentes COTS para vehículos satelitales de nueva generación.

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Conclusiones

Preguntas de investigación

- ¿Es posible la realización de un método de medición del grado de tolerancia a fallas de una arquitectura de aviónica?
- ¿Cuál es la estrategia más indicada de tolerancia a fallas que permita brindar un alto grado de confiabilidad en la utilización de componentes COTS en sistemas críticos?
- ¿Cuál es la arquitectura más indicada que permita desarrollar tolerancia a fallas en sistemas críticos basados en componentes COTS?
- ¿Es factible la utilización de componentes COTS en sistemas espaciales?

Agenda

1 Motivación

2 Objetivos

- Objetivos del trabajo
- Preguntas de investigación

3 ¿Qué es la tolerancia a fallas?

- Atributos de la fiabilidad
- Falla, Error, Avería

4 Bus CAN

- Definición

• Protocolo CAN

5 Análisis de arquitectura tolerante a fallas

6 CANae

- Introducción
- Capa de aplicación
- CANae Application Layer
- High Application Layer CANae

7 Arquitectura propuesta

8 Conclusiones

¿Qué es la tolerancia a fallas?

Ariane 5 - 1996



- Approx. 30 seconds after lift-off the computer within the back-up inertial reference system ... became inoperative. This was caused by an internal variable ... exceeding a limit which existed in the software of this computer.
- Approx. 0.05 seconds later the active inertial reference system, identical to the back-up system in hardware and software, failed for the same reason.^a

^aFlight 501 Failure Report. Prof J. L. Lions

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Conclusiones

Confiabilidad

Es la probabilidad de que un sistema continúe operando correctamente durante un intervalo de tiempo dado. “Es la capacidad del sistema o componente de realizar sus funciones requeridos bajo las condiciones establecidas durante un período de tiempo específico” (IEEE)

$$R(t) = e^{-\lambda t}$$

Disponibilidad

Es la probabilidad de que el sistema esté operando correctamente en un determinado instante de tiempo.

$$A(t) = 1/T \int_0^T A(t) dt$$

Seguridad

Se considera como una extensión de la confiabilidad. Se define como la probabilidad de que el sistema sea capaz de realizar sus funciones correctamente o continuar sus funciones en una manera a prueba de fallas.

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 ● Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Arquitectura propuesta
- 9 Conclusiones

Falla → Error → Avería
Fault → Error → Failure

Agenda

1 Motivación

2 Objetivos

- Objetivos del trabajo
- Preguntas de investigación

3 ¿Qué es la tolerancia a fallas?

- Atributos de la fiabilidad
- Falla, Error, Avería

4 Bus CAN

- Definición

• Protocolo CAN

5 Análisis de arquitectura tolerante a fallas

6 CANae

- Introducción
- Capa de aplicación
- CANae Application Layer
- High Application Layer CANae

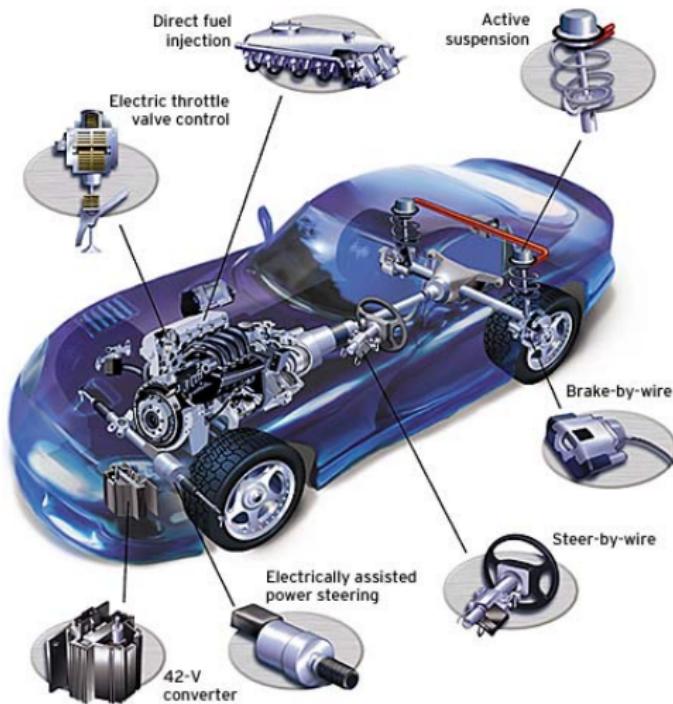
7 Arquitectura propuesta

8 Conclusiones

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Conclusiones

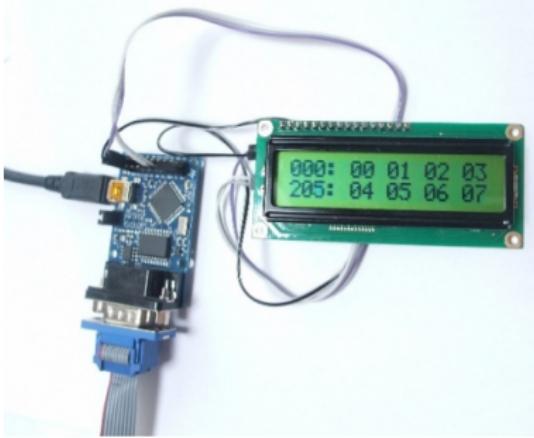
Bus CAN



- Comenzó su desarrollo en 1983
- Estandarizado por la ISO (ISO 11898)
- Nació para ser usada en la industria automotriz
- Conectividad vía bus serial, a través de dos cables.
- **Bajo costo**

¿Por qué CAN Bus?

Test Receive LCD sketch



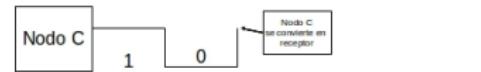
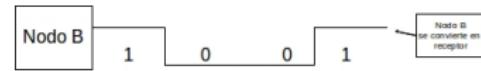
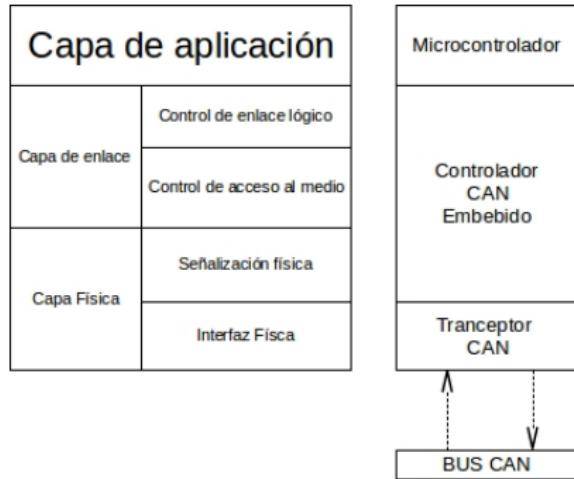
VS.



Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 • Protocolo CAN
- 5 Análisis de arquitectura tolerante a fallas
- 6 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 7 Arquitectura propuesta
- 8 Conclusiones

Protocolo CAN



CAN Estándar



CAN Extendido

Agenda

1 Motivación

2 Objetivos

- Objetivos del trabajo
- Preguntas de investigación

3 ¿Qué es la tolerancia a fallas?

- Atributos de la fiabilidad
- Falla, Error, Avería

4 Bus CAN

- Definición

• Protocolo CAN

5 Análisis de arquitectura tolerante a fallas

6 CANae

- Introducción
- Capa de aplicación
- CANae Application Layer
- High Application Layer CANae

7 Arquitectura propuesta

8 Conclusiones

Se supone una misión:

- Misión de 15 años.
- Sin payload.
- Formados por 6 subsistemas.
- Como mínimo se tomarán 6 nodos en representación de los subsistemas.
- Cada nodo es una computadora con capacidad de procesamiento.
- Cada nodo es un componente COTS.

Se concluye que las topologías que cumplen con los requerimientos y los objetivos de este trabajo de tesis son:

- Árboles binarios
- Redes distribuida
- Arquitectura hypercube

- $R(t)$ de árbol binario

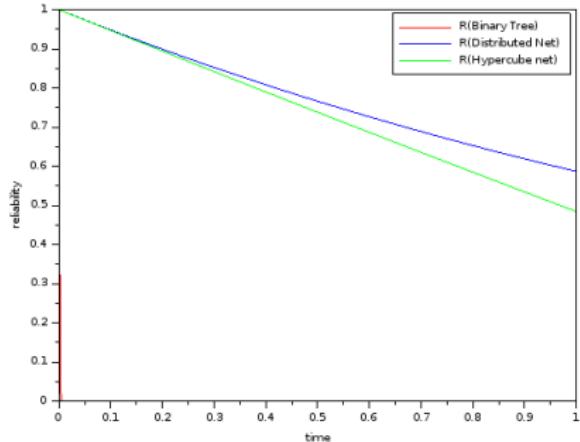
$$R_{sys} = R^{2n+1} \prod_{k=0}^{n-1} [(2^k c + 1) - 2^k]$$

- $R(t)$ de red hypercube

$$R_{sys} = 1 - |N(1 - e^{\lambda t})|$$

- $R(t)$ de red distribuida

$$R_{sys} = \sum_{i=0}^k [(\prod_{v \in S} R(t)) - (\prod_{\#S} R(t)c)]$$



Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
Análisis de arquitectura tolerante a fallas
- 6 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 7 Arquitectura propuesta
- 8 Conclusiones

Agenda

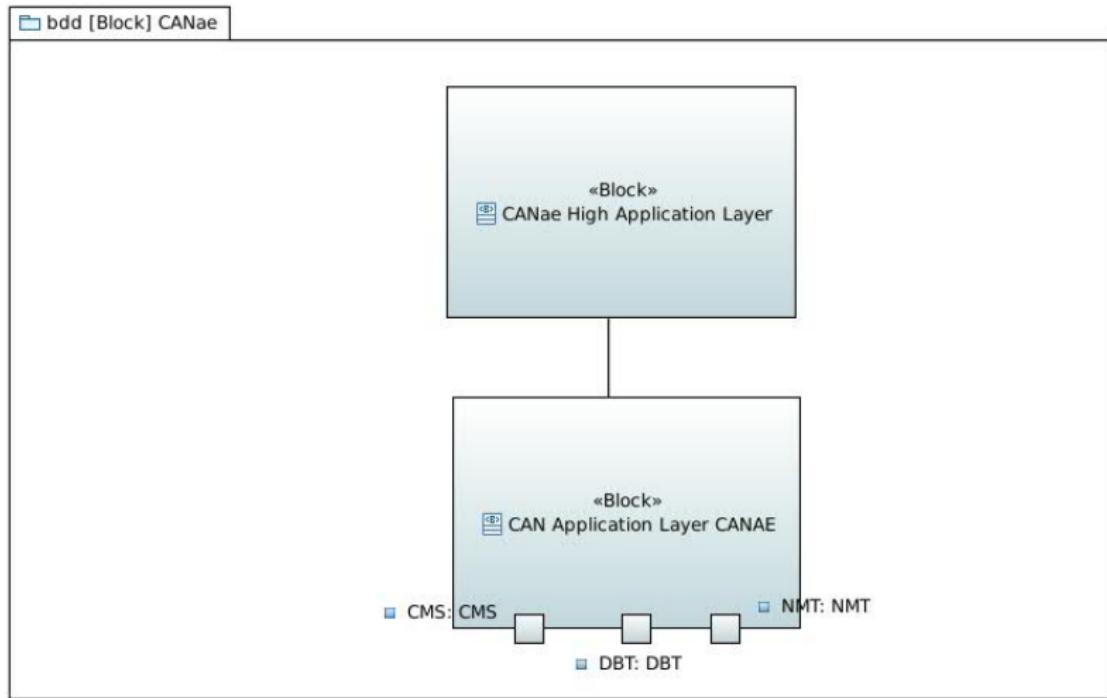
- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Arquitectura propuesta
- 9 Conclusiones

- Surge de la necesidad de desarrollar un protocolo:
 - ▶ Basado en el protocolo CAN
 - ▶ Que actúe en las capas superiores del modelo de OSI
 - ▶ Que permita la distribución de las tareas y el procesamiento llevado a cabo por los nodos
- CANae se divide la capa de aplicaciones en dos:
 - ▶ CANae Application Layer
 - ▶ CANae High Application Layer

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Arquitectura propuesta
- 9 Conclusiones

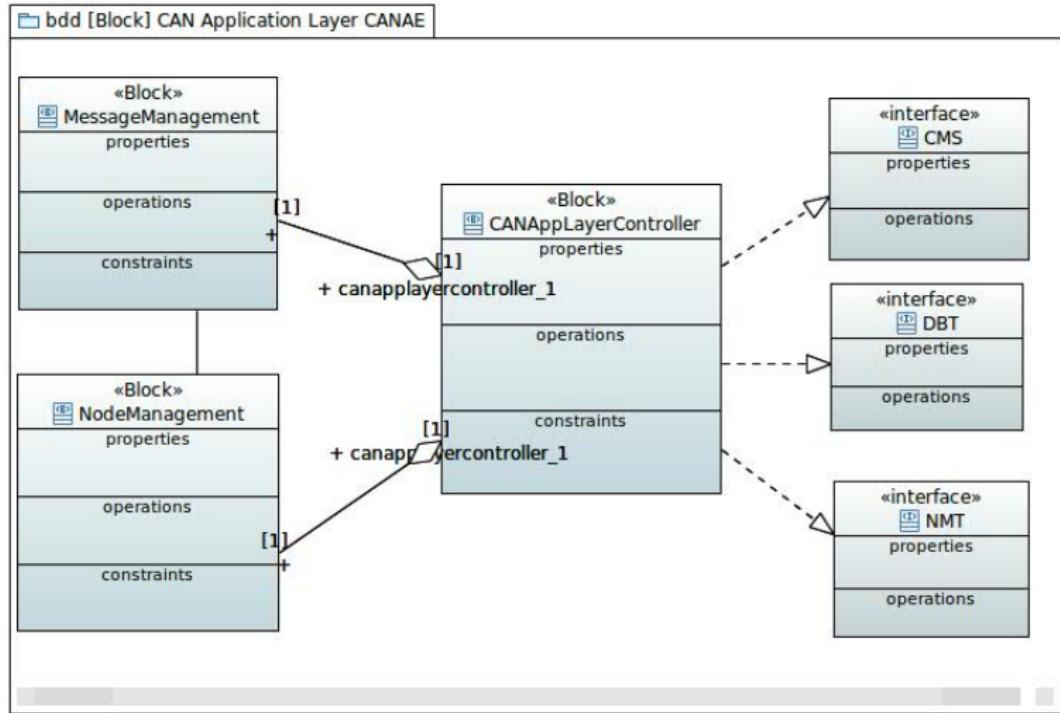
Capa de Aplicación



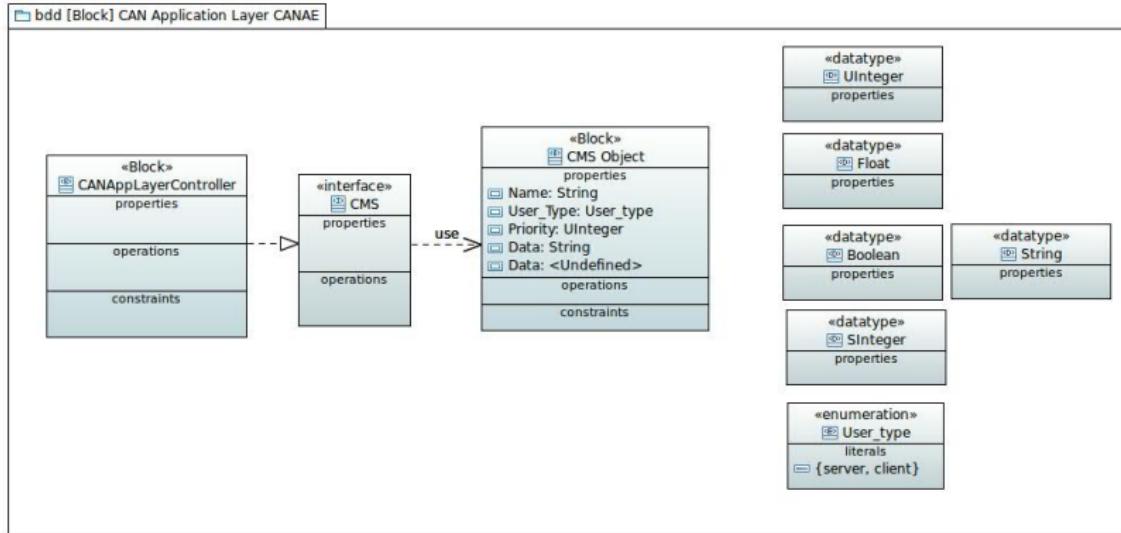
Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Arquitectura propuesta
- 9 Conclusiones

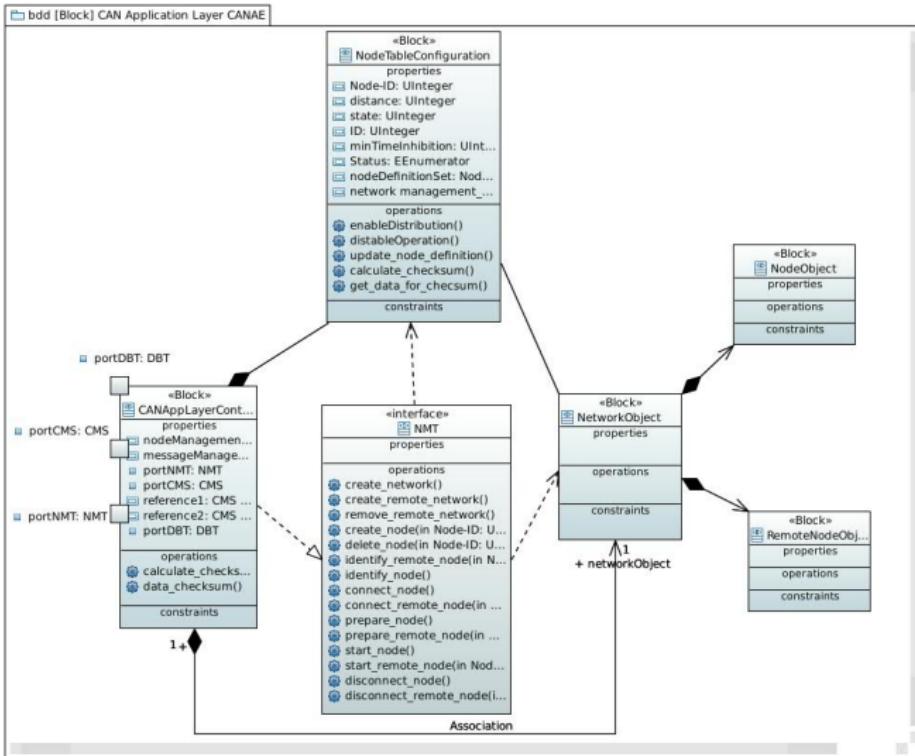
CANae Application Layer



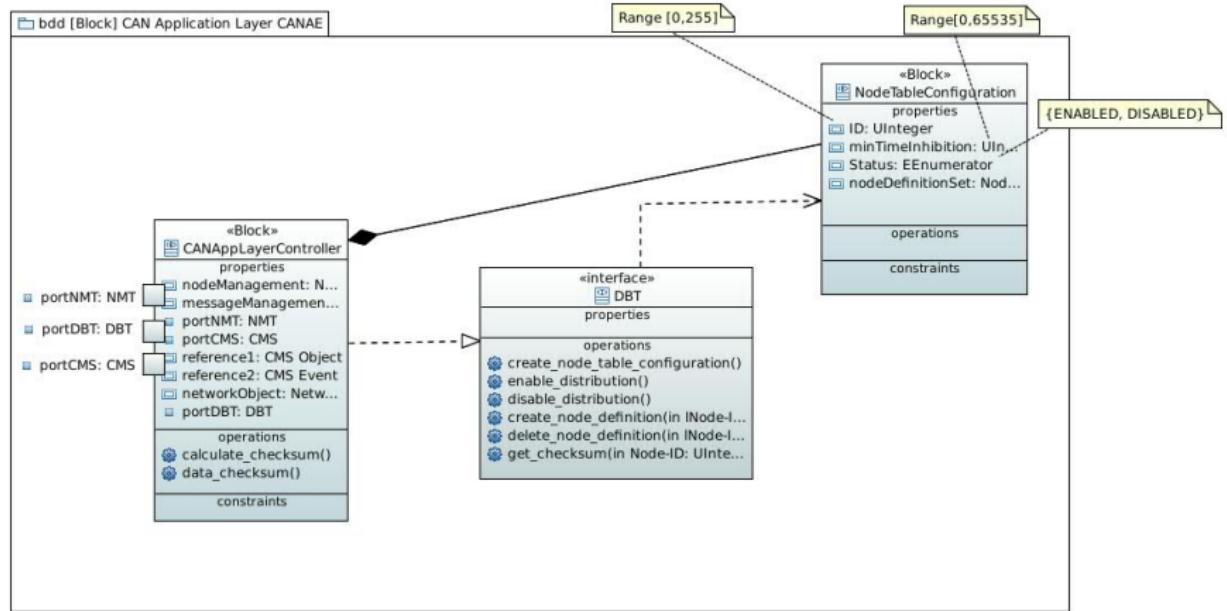
CAN bassed Message Specification (CMS)



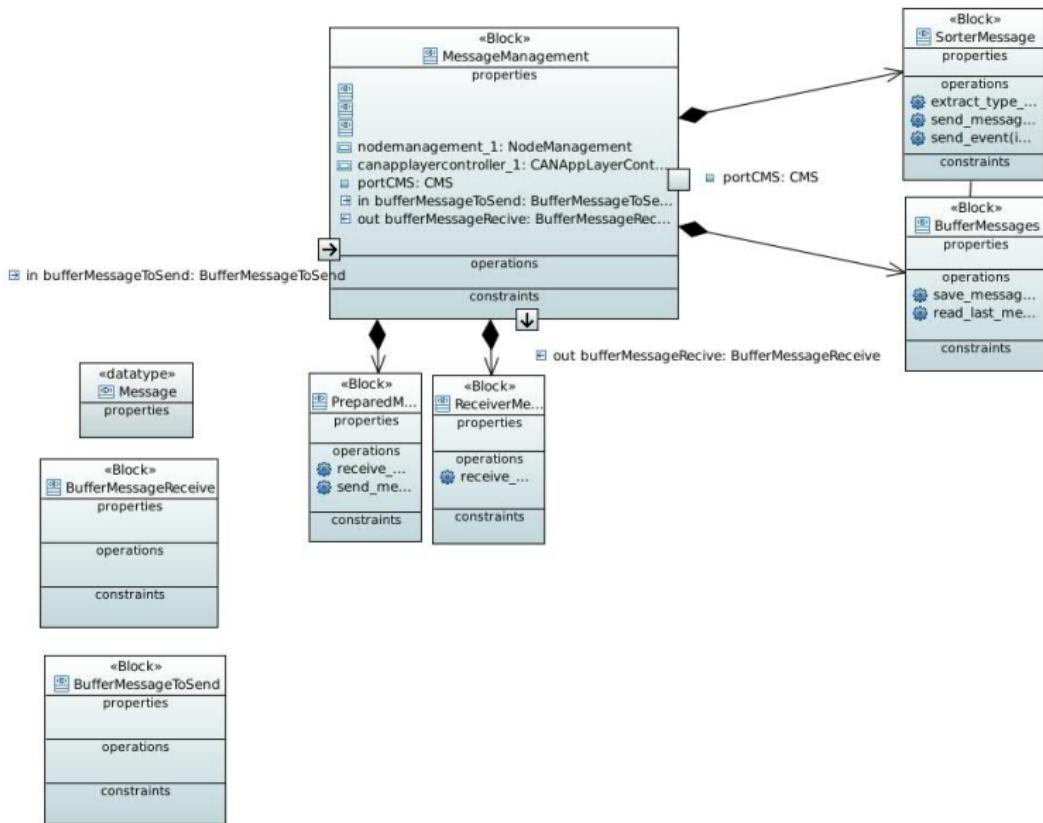
Network Management (NMT)



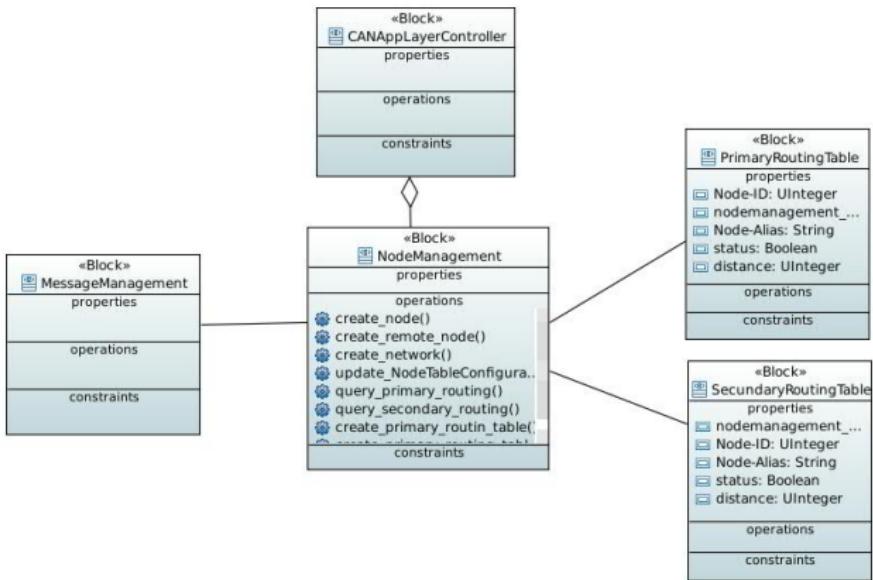
Distributor (DBT)



Gestor de mensajes



Gestor de nodos



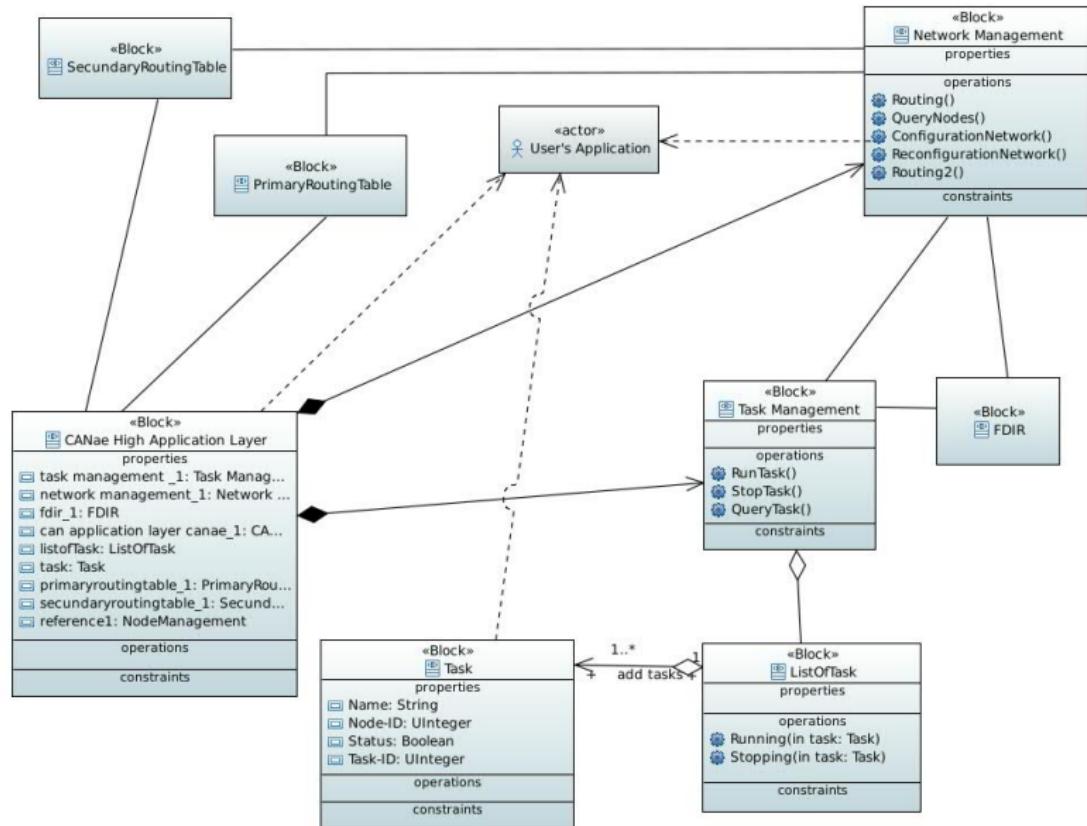
Formato del mensaje

SOF	Priority	Node-ID	RTR	Type of Message	Reserved bit	Data length	Data field	CRC	CRC delimiter	ACK	ACK Delimiter	EOF
1	4	7	1	1	1	0-8	0-64	1	1	1	1	1

Agenda

- 1 Motivación
- 2 Objetivos
 - Objetivos del trabajo
 - Preguntas de investigación
- 3 ¿Qué es la tolerancia a fallas?
 - Atributos de la fiabilidad
 - Falla, Error, Avería
- 4 Bus CAN
 - Definición
- 5 Protocolo CAN
- 6 Análisis de arquitectura tolerante a fallas
- 7 CANae
 - Introducción
 - Capa de aplicación
 - CANae Application Layer
 - High Application Layer CANae
- 8 Arquitectura propuesta
- 9 Conclusiones

High Application Layer CANae



Agenda

1 Motivación

2 Objetivos

- Objetivos del trabajo
- Preguntas de investigación

3 ¿Qué es la tolerancia a fallas?

- Atributos de la fiabilidad
- Falla, Error, Avería

4 Bus CAN

- Definición

• Protocolo CAN

5 Análisis de arquitectura tolerante a fallas

6 CANae

- Introducción
- Capa de aplicación
- CANae Application Layer
- High Application Layer CANae

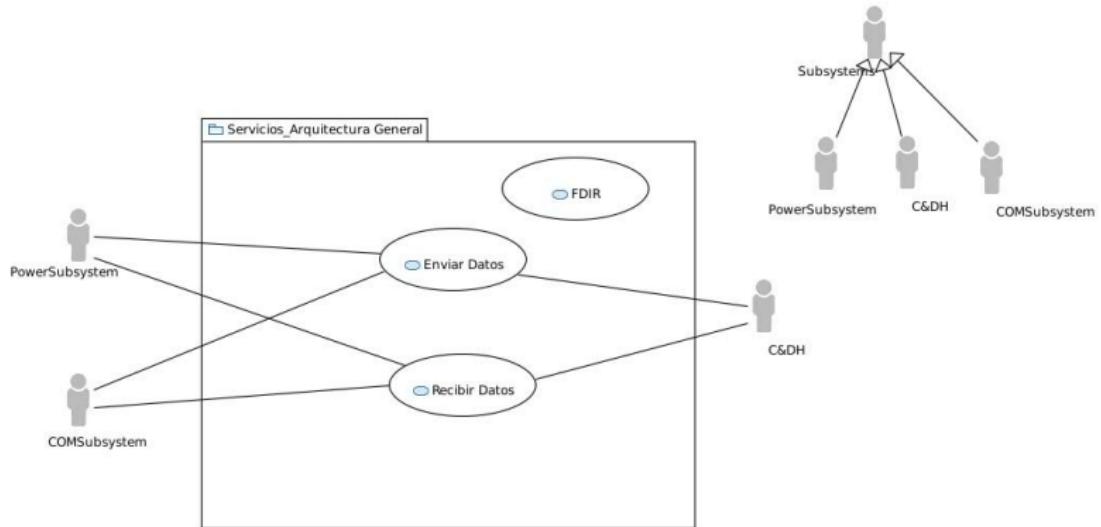
7 Arquitectura propuesta

8 Conclusiones

Arquitectura propuesta

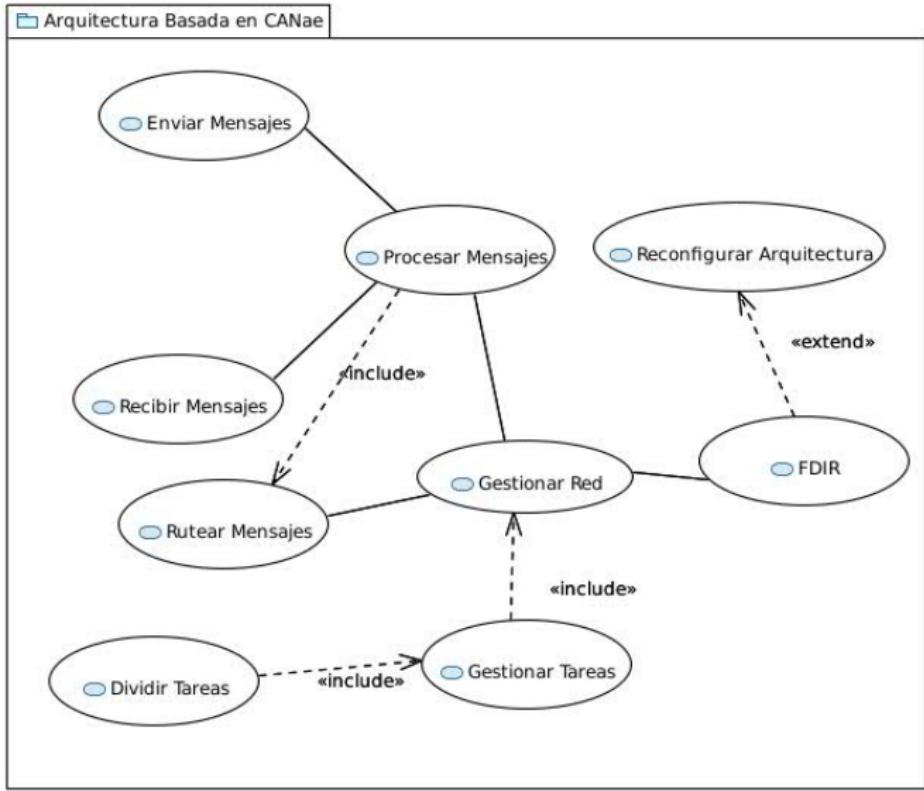
- Se centra en la comunicación de la aviónica de un vehículo espacial.
- Sus componentes primarios son de baja confiabilidad
- Se utiliza el protocolo de comunicación CANae.
- Se propone que la utilización de una filosofía distribuida

Casos de usos





Subsystems

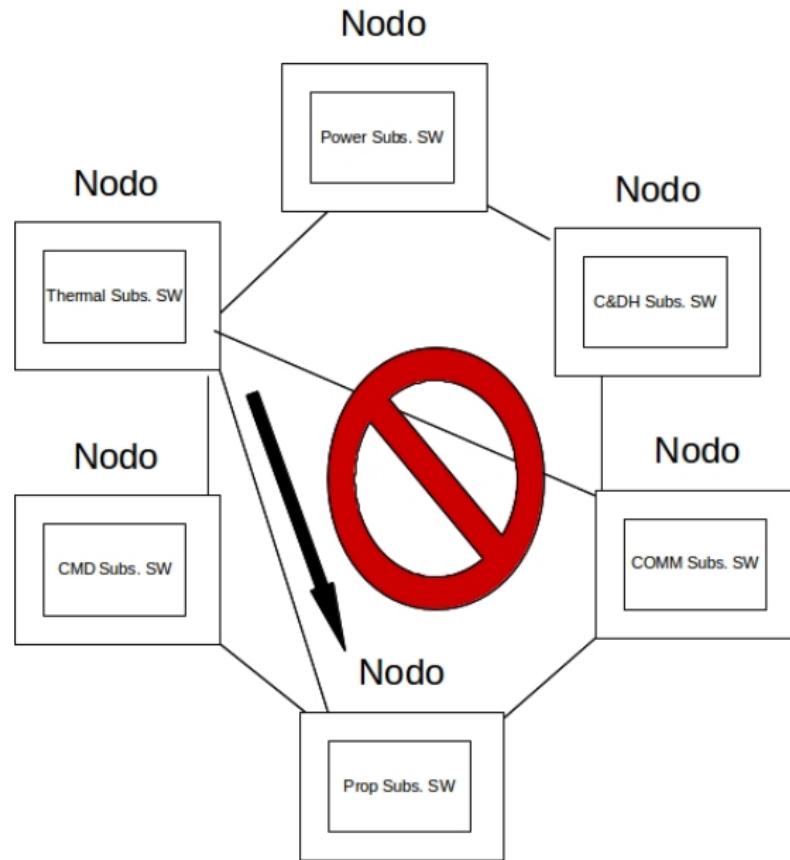


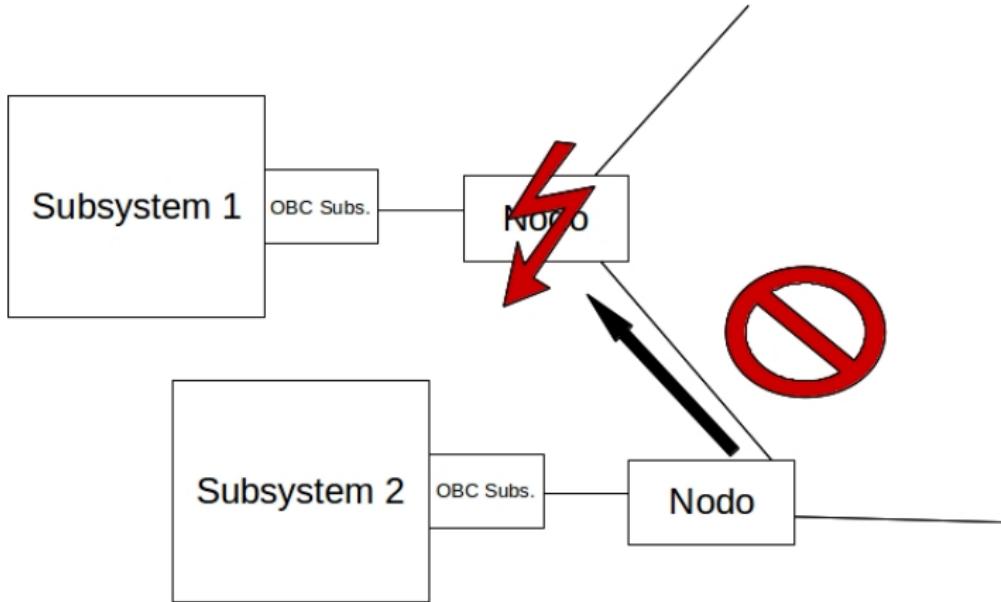
Diseño estructural

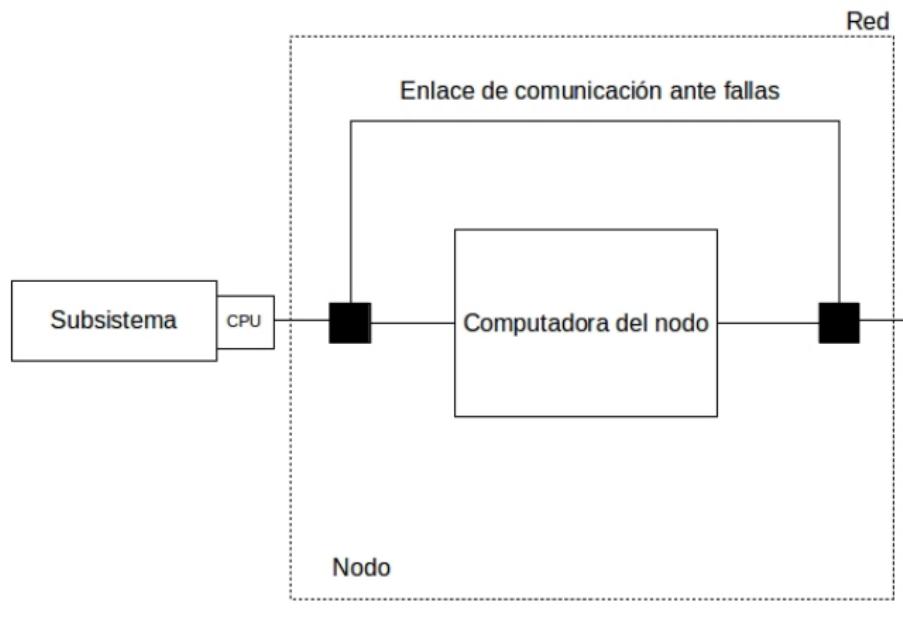
Diseño estructural

- La arquitectura presentada rompe con el diseño tradicional de sistemas espaciales
- La arquitectura permite conectar una cantidad de N nodos ($N < 128$). Sus componentes son COTS.
- La red a bajo nivel, deben trabajar bajo normas preestablecidas por algún protocolo preexistente.
- Surge la necesidad de desarrollar un Bridge Tolerante a fallas.

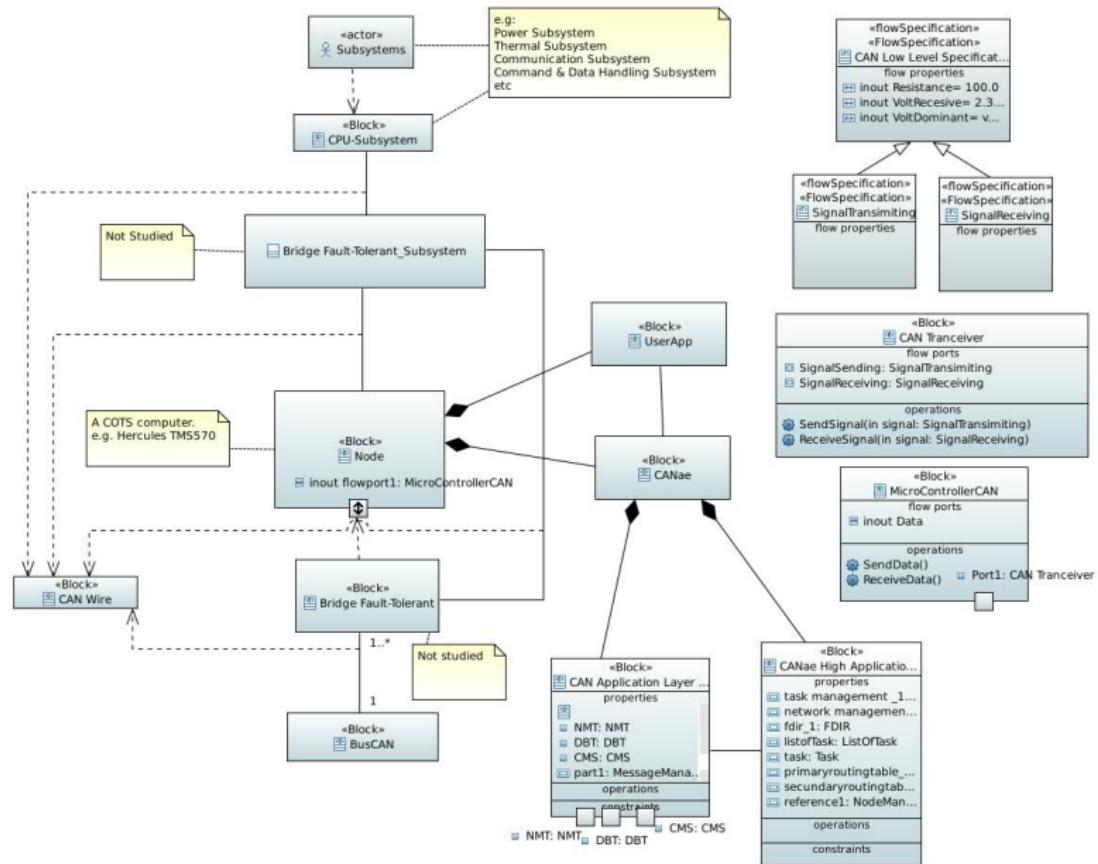
Configuración de conexión



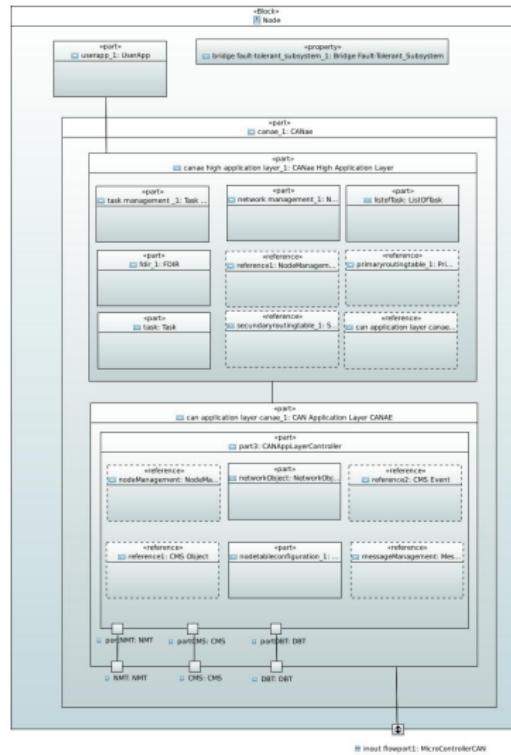




Diseño estructural

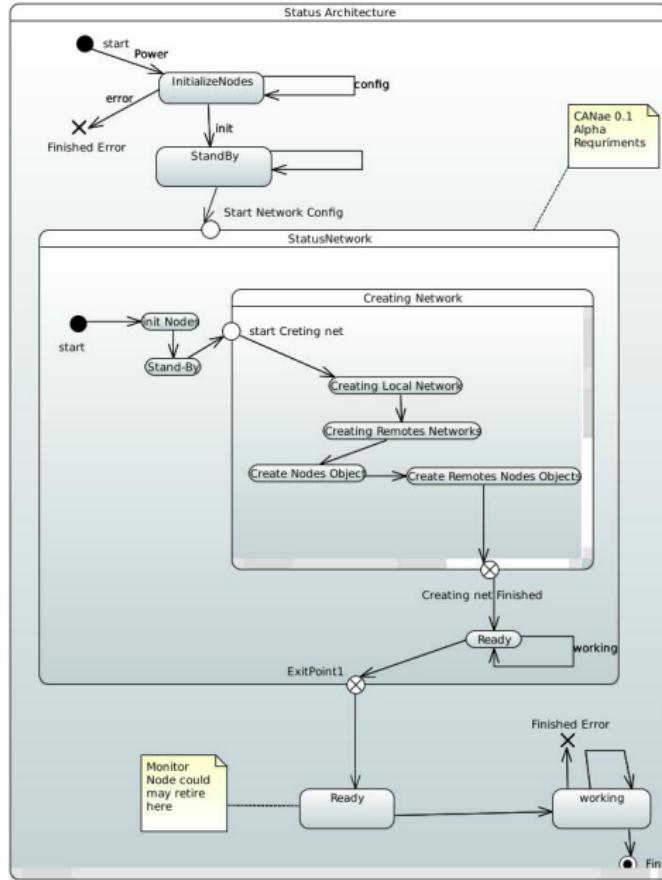


Nodo - Internal Block

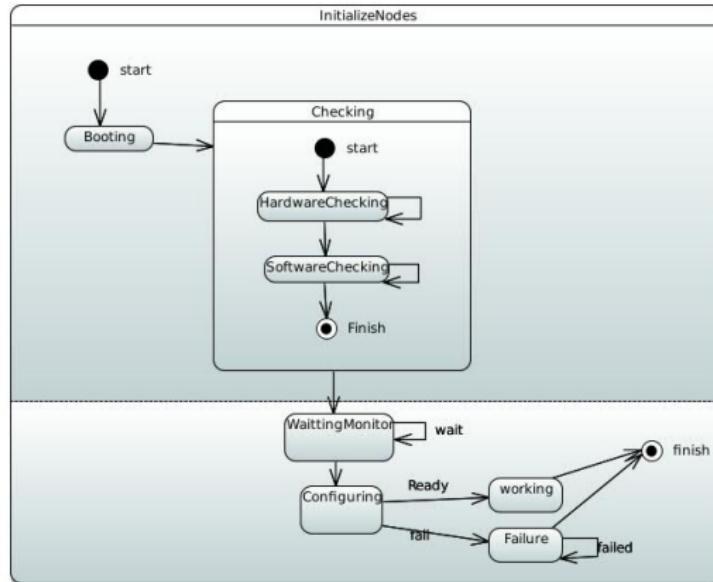


Máquina de estado

Máquina de estado de la arquitectura completa

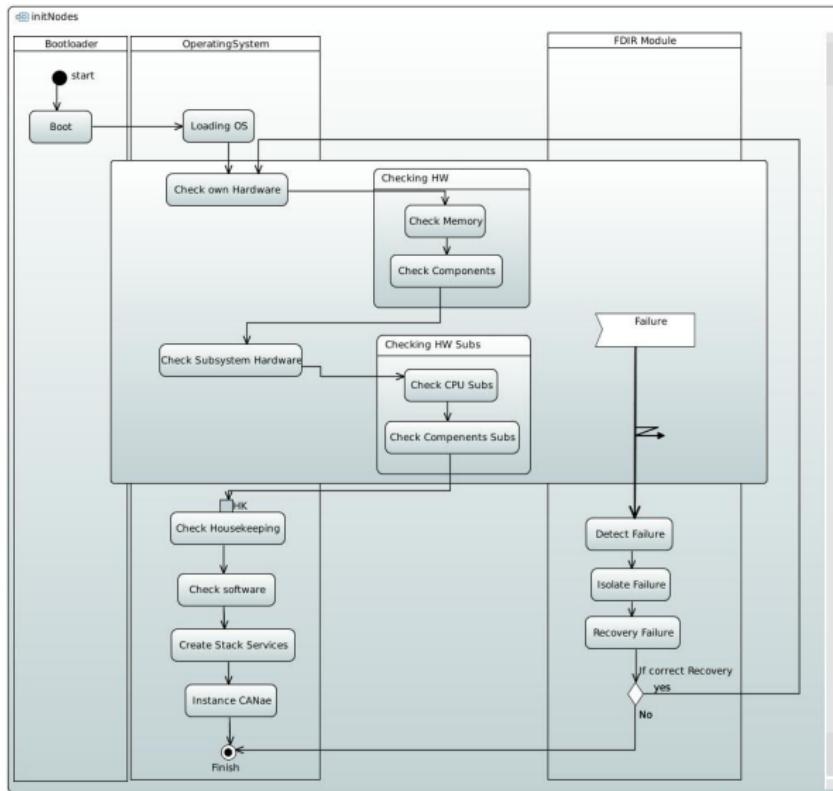


Máquina de estado nodos

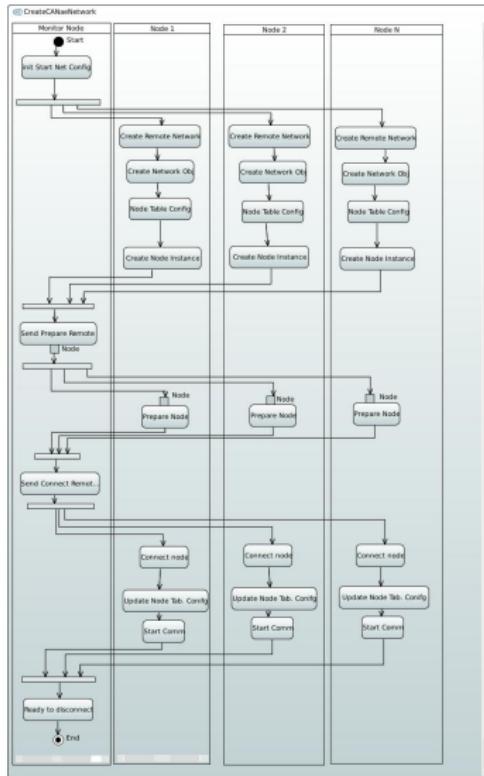


Diagramas de actividades

Inicio de Nodos



Nodo Monitor



Agenda

1 Motivación

2 Objetivos

- Objetivos del trabajo
- Preguntas de investigación

3 ¿Qué es la tolerancia a fallas?

- Atributos de la fiabilidad
- Falla, Error, Avería

4 Bus CAN

- Definición

• Protocolo CAN

5 Análisis de arquitectura tolerante a fallas

6 CANae

- Introducción
- Capa de aplicación
- CANae Application Layer
- High Application Layer CANae

7 Arquitectura propuesta

8 Conclusiones

Conclusiones

Conclusiones

- Es factible la utilización de componentes COTS en sistemas espaciales
- Se demostró que la estrategia más indicada de tolerancia a fallas, para el desarrollo de sistemas espaciales, es una arquitectura basada en redes distribuida
- CANae permite desarrollar tolerancia a fallas en sistemas críticos basados en componentes COTS.

Perspectivas a futuro

- Diseño detallado, desarrollo e implementación del protocolo CANae
- Diseño detallado de la arquitectura propuesta
- Estudio de nuevas técnicas de tolerancia a fallas aplicadas a los diferentes niveles de detalle de las arquitecturas de aviónica.
- Desarrollo de algoritmos de ruteo para la distribución de tareas en redes distribuidas
- Estudio de tecnología Wireless como medio de comunicación alternativo al cableado

Muchas gracias por su atención

Objetivo específico I

- ① Realizar un estudio del estado de la cuestión sobre arquitecturas tolerantes a fallas para sistemas críticos.
- ② Investigar y analizar arquitecturas tolerantes a fallas que aseguren la confiabilidad del sistema y que sean aplicables en la industria satelital.
- ③ Investigar y analizar protocolos de comunicación, para las capas superiores del modelo de OSI (modelo de interconexión de sistemas abiertos - ISO/IEC 7498-1), orientados a la tolerancia a fallas y confiabilidad de los sistemas.
- ④ Investigar una metodología para lograr una medición de la tolerancia a fallas en arquitecturas de aviónica.
- ⑤ Desarrollar un estudio comparativo de arquitecturas tolerantes a fallas con el fin de obtener ventajas y desventajas de cada una de ellas.
- ⑥ Diseñar modelos alternativos de arquitecturas tolerantes a fallas, que tengan un grado de confiabilidad tal, que permita la aplicación de componentes COTS.

Objetivo específico II

- ⑦ Evaluar la confiabilidad de los modelos de arquitecturas.
- ⑧ Proponer el diseño de una nueva arquitectura tolerante a fallas, con un grado de confiabilidad suficiente para la aplicación de componentes COTS en avionicas de vehículos satelitales.
- ⑨ Simular la arquitectura planteada para medir su grado de tolerancia a fallas y performance.

Backup Slides

Fallas != Error != Avería

- **Avería:** ocurre cuando el servicio prestado por el sistema no coincide con las especificaciones del mismo. Existe una consecuencia negativa en el sistema completo. (Failure)
- **Error:** es una parte del estado del sistema que es susceptible de provocar un avería en el sistema. Es una etapa intermedia entre falla y avería. (Error)
- **Falla:** también llamado “bug”. Es la hipótesis de un error. (Fault)

Fallas de modo común vs fallas de causa común

- **Fallas de modo común (CMF):** es una falla que ocurre simultáneamente en dos o más componentes redundantes. CMF son causados por fenómenos que crean dependencias entre unidades redundadas.
- **Fallas de causa común (CCF):** se define como cualquier instancia donde múltiples elementos fallan debido a una causa común

Fallas en el Software

Algunas de las fallas introducidas en el software:

- Especificaciones incorrecta de requerimientos
- Diseño incorrecto
- Errores de programación

Fiabilidad de sistemas

La fiabilidad de un sistema es la capacidad del mismo de entregar a los usuarios un nivel deseado de servicio.

Es una medida de calidad que abarca los conceptos: confiabilidad, disponibilidad, y seguridad.

Es una propiedad global que permite justificar la confianza de los servicios de un sistema

Medios de fiabilidad

- **Evitación de fallas:** técnicas de mejoramiento de la fiabilidad utilizadas durante el desarrollo de SW para reducir el número de fallas.
- **Tolerancia a fallas:** se utiliza como una capa más de protección. FT es la capacidad del sistema a ejecutarse apropiadamente a pesar de la presencia de fallas. FT ocurre en tiempo de ejecución.
- **Eliminación de Fallas:** técnicas utilizadas para mejorar la fiabilidad empleadas durante el proceso de validación y verificación del sistema SW. Se eliminan las fallas que se detectan.
- **Predicción de Fallas:** se aplica mediante la realización de una evaluación del comportamiento del sistema con respecto a la ocurrencia, o la activación de una falla.

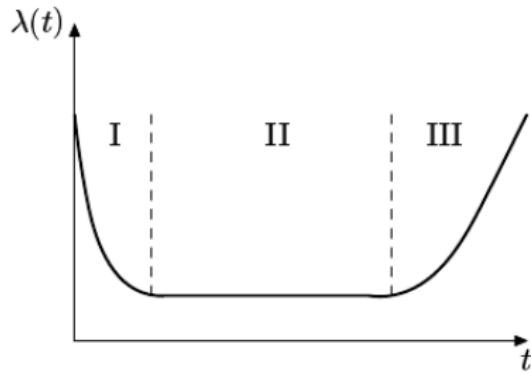
Failure rate

Es el número esperado de fallas por unidad de tiempo. Generalmente, se encuentra a nivel de componente.

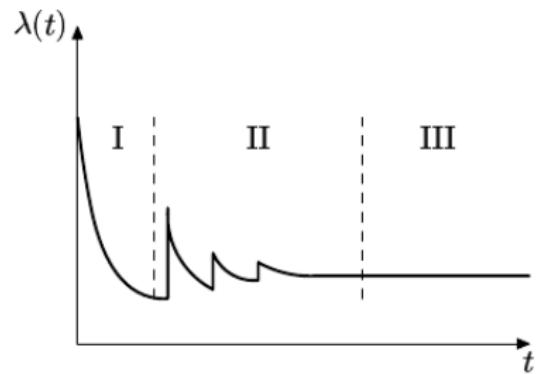
$$\lambda = \sum_{i=1}^n \lambda_n$$

Failure rate

Failure rate de HW vs tiempo



Failure rate de SW vs tiempo



Failure rate

Tiempo medio hasta la falla (MTTF):

$$MTTF = \int_0^{\infty} R(t)dt$$

Tiempo medio de reparación (MTTR):

$$MTTR = 1/\mu$$

Redundancia en el software

- Técnicas single version
- Técnicas multi-version
- Técnicas de detección de fallas
- Técnicas de recuperación de fallas