Estudio de la confiabilidad de arquitecturas tolerantes a fallas basada en componentes COTS para aviónicas de vehículos espaciales

Arias Emmanuel
emmanuelarias30@gmail.com
Universidad Nacional de La Matanza
CONAE - UFS
Ruta C 45, km8,5
Falda de Cañete, Córdoba, Argentina

Gustavo Wiman
guswiman@invap.com.ar
INVAP
Av. Cmte. Luis Piedrabuena 4950, (R8403CPV)
S.C. de Bariloche, Río Negro, Argentina

RESUMEN

El desarrollo de proyectos satelitales conlleva costos de importante magnitud. Uno de ellos es el costo debido a los componentes y materiales que se utilizan para la fabricación de vehículos espaciales. En los últimos años, se han incrementado los esfuerzos en el estudio e investigación, a nivel mundial de los llamados *componentes COTS* (Commercial Off-The-Shelf) o de estantería, que ayudarían a disminuir los costos significativamente. Esto para la industria espacial argentina es de suma importancia. Para lograr una correcta aplicación de estos componentes, es necesario desarrollar técnicas, estrategias y arquitecturas que aseguren que la probabilidad de fallas catastróficas y de degradación, sean compatibles con la misión que se está planteando. En este trabajo se comparan tres tipos de topologías diferentes: 1) árbol binario, 2) red distribuida y, 3) redes hypercube, que será utilizada en futuros trabajos para el desarrollo de una arquitectura tolerante a fallas basada en componentes COTS. Para ello, en primer lugar, se estudió cada una de estas topologías y se planteron modelos que permitieron medir su grado de confiabilidad. En segundo lugar se realizó un estudio del impacto negativo de la falla de uno o más nodos en las diferentes arquitecturas. Finalmente se llevó a cabo una comparativa, haciendo uso de los modelos desarrollados en el primer punto, para determinar qué topología es la más conveniente para el desarrollo de aviónica satelital utilizando componentes COTS y que a su vez sea tolerante a fallas.

1.- INTRODUCION

El desarrollo de proyectos satelitales conlleva costos de importante magnitud. De estos, el más importante es el proceso de planificación, análisis, diseño e implementación del mismo, y sobre todo el de los componentes y materiales que se suelen utilizar para la fabricación de satélites. El elevado costo de estos componentes se debe a que son de uso exclusivo para la actividad espacial, es decir que están calificados para volar. Además de sus precios elevados, estos componentes calificados para uso espacial, comúnmente, son tecnologías obsoletas, con una baja capacidad de procesamiento, en comparación de los componentes contemporáneos, lo que limita en gran medida el procesamiento y desarrollo de vehículos espaciales.

En los últimos años, a nivel mundial se ha incrementado la necesidad de disminuir los costos de construcción de misiones satelitales, y en igual medida, aumentaron los esfuerzos y el tiempo en investigaciones y estudio referentes a los componentes denominados COTS (Commercial Off-The-Shelf), o también conocidos como de estantería. Los componentes COTS suelen tener un costo hasta 1000 veces menores que los componentes calificados para volar, por lo tanto la aplicación de estos componentes permitiría reducir costos y ahorrar millones de dolares del proyecto, además se podrían incrementar las

prestaciones satelitales mediante la utilización de estos componentes con tecnología más avanzada que la de aquellos habilitados para volar.

La habilitación de los componentes COTS en aplicaciones espaciales requiere que la probabilidad de fallas catastróficas y de degradación, causadas por el ambiente espacial, sea compatible con las características de la misión, y se deben diseñar arquitecturas que, mediante el uso de redundancias, permitan que el sistema sea tolerante a las fallas inducidas, en sus componentes, por el ambiente espacial. Por lo tanto, la aplicación de estos componentes no es directa, ya que al no estar calificados para volar, se necesita llevar a cabo una serie de técnicas para lograr hacer frente esa "desventaja", para asegurarnos que no fallarán durante la misión. Por tal motivo, no se podría pensar en utilizar arquitecturas "tradicionales" en el desarrollo de vehículos basados en componentes COTS.

Otras de las ventajas de estos componentes COTS es que no están sujetos a las restricciones de importación/exportación (como ITAR) que se aplican a los componentes aptos para aplicaciones militares ni tienen los largos plazos de entrega asociados a los componentes que se producen en pequeña escala y con procesos especiales.

El objetivo de este trabajo es el de evaluar la aplicación de componentes COTS en el desarrollo de aviónicas para satélites de nueva generación. La utilización de estos componentes es de especial interés para INVAP, ya que esto permitiría reducir considerablemente costos, masa, volumen y consumo de potencia de la electrónica de sus satélites al mismo tiempo que permitiría aumentar sus prestaciones. El empleo de estos componentes mejoraría la competitividad de los productos satelitales argentinos en el mercado global.

Así, en este trabajo nos centramos en el estudio de diferentes topologías de arquitecturas que nos aseguren una mayor tolerancia a fallas a nivel de sistema, de modo tal que, si se llegase a producir alguna falla en una de las computadoras (nodo) que forman parte de la arquitectura, esta puede reconfigurarse y continuar funcionando normalmente sin degradación de la perfomance, aún en la presencia de falla.

2.- METODOLOGIA

Luego de una búsqueda bibliográfica de diferentes topologías utilizadas en arquitecturas tolerantes a fallas se identificaron a priori 3 topologías a ser estudiadas: 1) árboles binarios; 2) redes distribuidas; y 3) redes de tipo hypercube.

3.- DESARROLLO

A continuación se muestra el estudio de las tres topologías mencionadas anteriormente.

3.1-Árboles binarios

La arquitectura de árboles binarios es aplicable en el desarrollo de sistemas de computadoras jerárquicas, y sobre todo en computadoras de alta perfomance [1]. Un árbol binario está compuesto por nodos y enlaces (links). En esta estructura, existe un nodo que es el central dónde se desprenden dos nodos hijos, estos se encuentran enlazados al nodo padre. Recursivamente se van generando dos nuevos hijos, por cada uno de los nodos.

Si bien las arquitecturas de árbol binario, son aplicadas en la construcción de circuitos VLSI, asumimos que pueden ser llevadas a arquitecturas de aviónica. En [1] se identifican dos tipos de esquemas posibles de esta topología:

1. Esquemas con Back up.
2. Esquemas con degradación de perfomance.

Por simplicidad, se trabajó con esquemas con Back Up. En [1] se demuestra que un esquema con Back Up tiene mayor confiabilidad que sin estos. La confiabilidad de estas arquitecturas fueron estudiadas en profundidad por [1] [2] y [3].

Un árbol binario está conformado por

$$2^n - 1 \quad (1)$$

nodos, donde n es la cantidad de niveles del árbol. La confiabilidad de cada nodo se puede calcular del siguiente modo:

$$R = e^{-\lambda t} \quad (2)$$

siendo λ la tasa de falla. De (1) y (2) se obtiene que la confiabilidad de todo el árbol binario es:

$$R_{nr} = R^{2^n - 1} \quad (3)$$

[1] incluye en sus cálculos un factor c, el cual es la probabilidad condicional de que se realice una recuperación exitosa, luego de que una falla se haya detectado. Resumiendo, la confiabilidad de todo el sistema incluyendo un nodo back up por cada nivel se obtiene de la siguiente manera:

$$R_{sys} = R^{2n+1} \prod_{k=0}^{n-1} \left[(2^k c + 1) - 2^k cR \right] \quad (4)$$

Esta arquitectura solo puede tolerar una falla singular por cada nivel del árbol, o varias fallas que se den en diferentes niveles. Para mayor tolerancia se deben agregar más redundancias [1].

3.2-Redes distribuidas

La principal característica de una red distribuida es que no cuenta con un nodo central. Esto puede resultar beneficioso a la hora del desarrollo de sistemas satelitales, ya que las tareas de procesamiento se distribuyen en los nodos de la red y no quedan centrados en una sola computadora.

Una red distribuida es tolerante a fallas si se pueden formar subredes [4]. Esto significa que la red debe mantenerse activa y conectada, con diferentes topologías e interconexiones, de modo tal que, permita tolerar posibles fallas producidas en algunos nodos y mantener la perfomance [4].

Para asegurar la tolerancia a fallas en este tipo de redes es necesario el desarrollo de algoritmos de ruteo: *algoritmo primario* y *algoritmo alternativo* . En [5] se exponen 2 tipos de ruteo. Estas arquitecturas necesitan la aplicación de algoritmos de diagnóstico distribuido de fallas, que son basados en los algoritmos de ruteo, lo cual se encuentra fuera de los objetivos de este trabajo.

Calcular su confiabilidad no es una tarea trivial, como en el caso explicado en la sección anterior (2.1- Árboles binarios). Una red G está conformada por V nodos, cada uno con su probabilidad de operación P, y una función π de asignación de esas probabilidad a los nodos. Esta red tiene una cantidad de subconjunto de nodos S, que mantienen operativa la red. Su tolerancia a fallas puede ser calculada de la siguiente manera [4]:

$$FT(G; \vec{P}; \pi) = \sum_{S \in \Theta} Pr(S) = \sum_{S \in \Theta} \prod_{v \in S} P\pi(v) \prod_{v \notin S} (1 - P\pi(v)) \quad (5)$$

dónde Θ representa a todas las subredes.

3.3-Redes hypercube

Hypercube es una técnica utilizada para conectar múltiples procesadores. Esta topología tiene propiedades de tolerancia a fallas de un componente, ya que si esto se produce, no se transmite a todo el sistema [6]. Otra ventaja que presenta esta topología es la disponibilidad de enlaces entre cualquier par de nodos [7]. Un hypercube n-dimensional tiene

$$2^n \quad (6)$$

nodos y

$$n 2^{n-1} \quad (7)$$

enlaces. Los nodos están conectados a n nodos vecinos a través de n enlaces [6]. Estas relaciones pueden ser representadas en forma de matrices de proximidad [7]. En [7] se muestra una manera sencilla de calcular la confiabilidad de sistemas de este tipo. La probabilidad de falla de la red (p_n) depende de la probabilidad de falla de cada uno de los nodos (p_v), suponiendo que todos los nodos tiene la misma probabilidad de falla la confiabilidad del sistema sería:

$$R(N) = 1 - (N\, p_v) \quad (8)$$

3.4- Estudio de confiabilidad

Para realizar el estudio de confiabilidad de estas topologías, se pensó en una misión de aproximadamente 15 años, ignorando la carga útil, y poniendo énfasis en la plataforma satelital (objetivo de este trabajo). Esta misión cuenta con 6 subsistemas, basados en los ejemplos de [8], los cuales a partir de este momento serán considerados nodos de la red. Los nodos se suponen computadoras (componentes COTS),

con capacidad de procesamiento suficiente para cada subsistema. Estos nodos tienen un cierto grado de confiabilidad, relativamente menor que componentes calificados para volar. Se supone que el sistema sólo puede fallar una vez, por lo tanto la tasa de fallas de cada nodo será de

$$\lambda = 1/15 \quad (9)$$

En primer lugar planteamos un árbol binario de 4 niveles con Back Ups basada en la arquitectura de [1] (Figura 1) con 15 nodos. Esta, fue modificada para satisfacer nuestras necesidades.

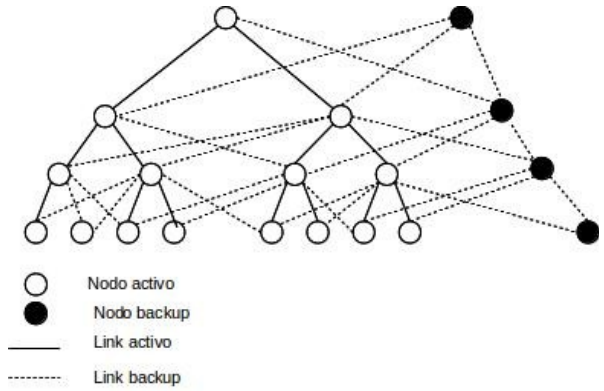

Figura 1: árbol binario (basado en [1]).

Aplicando la fórmula (4), con un factor c = 1, se obtiene la gráfica de la Figura 2.

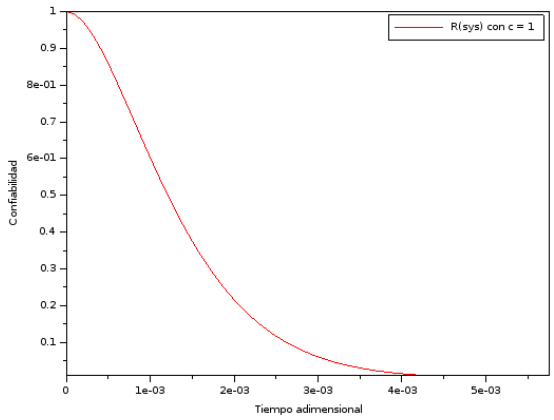

Figura 2: Cálculo confiabilidad de árbol binario.

Para el estudio de la red distribuida diseñamos la topología que se observa en la Figura 3. Está conformada por 8 nodos, siguiendo la metodología de diseño de [5] (los 6 nodos que representan los subsistemas de la misión y 2 de redundancias).

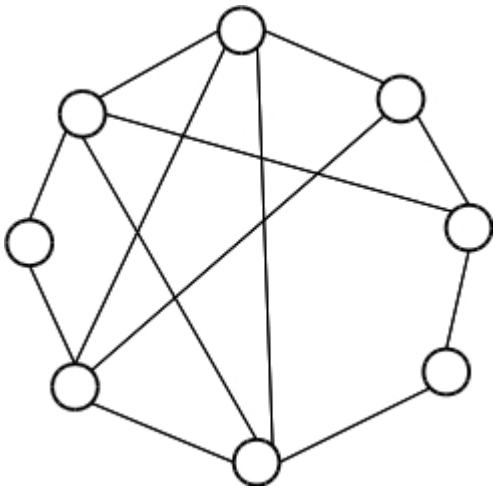

Figura 3: Topología diseñada para su estudio preliminar.

Esta es una topología de n = 8 nodos. Existen cuatro nodos de grado 4, dos nodos de grado 3 y dos nodos de grado 2. Se identificó que pueden fallar hasta cuatro nodos. Para mantener una coherencia con los cálculos de confiabilidad, se modificó la fórmula utilizada en [4]. La confiabilidad del sistema completo con todos los nodos funcionales se calcula aplicando:

$$R_{sys} = \prod_{v \in S} e^{-\lambda \cdot t} \quad (10)$$

Cuando existen nodos que fallan se aplica:

$$R_{sys} = \sum_{i=0}^{k} ((\prod_{v \in S} R(t)) - (\prod_{v \notin S} (1 - R(t)c))) \quad (11)$$

Siendo R(t) la confiabilidad del nodo. La curva de confiabilidad para la red diseñada (Figura 3) se muestra en la Figura 4.

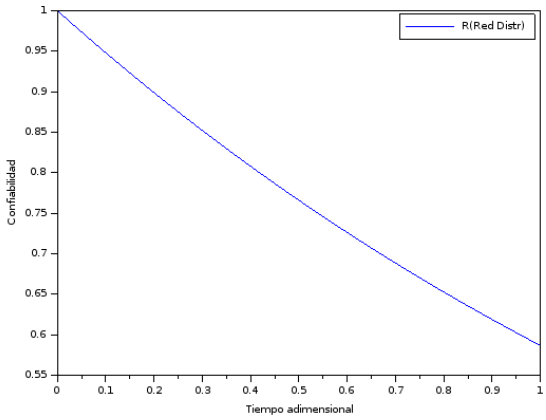

Figura 4: confiabilidad de una red distribuida de 8 nodos

Suponiendo que 4 nodos han fallado (requerimiento de fallas máxima de nodos, que fue planteado en este trabajo), se puede observar en la Figura 5 (en color rojo y línea discontinua) la degradación de la confiabilidad a través del tiempo.

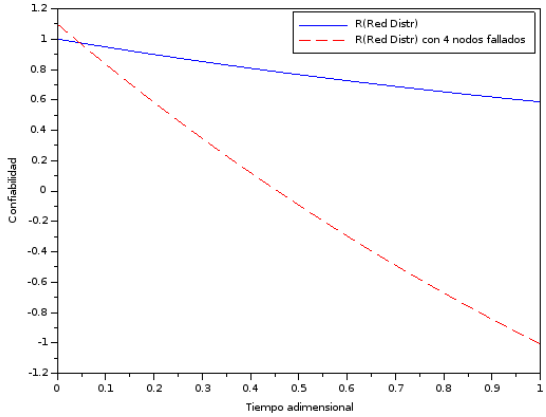

Figura 5: Confiabilidad de red distribuida de 8 nodos en los cuales han fallado 4 nodos.

Por último, para calcular la confiabilidad de una red hypercube seguimos la fórmula (8), haciendo leves modificaciones para lograr que esta se acople al trabajo que venimos desarrollando. Entonces la confiabilidad se la calculó de la siguiente manera:

$$R_{sys} = 1 - [N(1 - e^{-\lambda t})] \quad (12)$$

Para un cubo de 3 dimensiones, el cual está compuesto por 8 nodos y 12 enlaces, tal como se muestra en la Figura 6. La confiabilidad de esa topología se la muestra en la Figura 7.

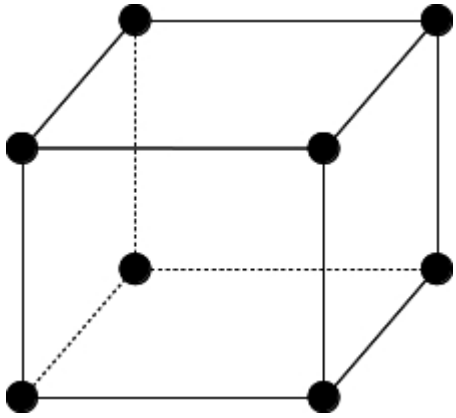

Figura 6: topología Hypercube típica de 3 dimensiones.

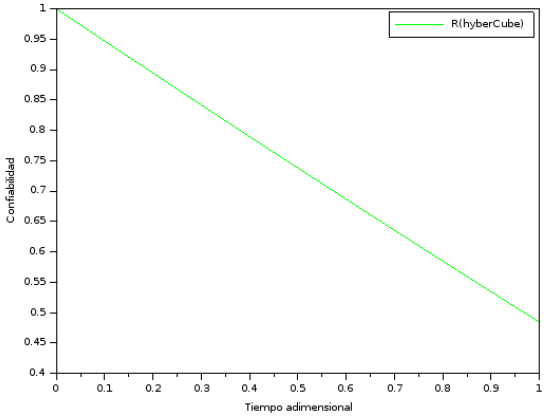

Figura 7: Confiabilidad de una red hypercube.

3.4 Comparativa

Una vez desarrollado el estudio y la unificación de lo métodos de cálculos de confiabilidad de las diferentes topologías propuestas, resulta sencilla su comparación.

Conceptualmente, luego del análisis en profundidad del estado del arte sobre la temática, logramos identificar que la mejor opción como topología, arquitectura y como filosofía de desarrollo son las redes distribuidas.

Los árboles binarios, podrían resultar una buena opción debido a la sencillez en el desarrollo de este tipo de topologías, pero existe un riesgo mayor. La falla del nodo raíz y de su redundancia, aún siendo un árbol binario

distribuido, pondría en peligro la misión. Otro punto negativo que se puede mencionar es la gran cantidad de enlaces que se necesitan para mantener conectada la red.

La red distribuida cuenta con la capacidad de distribuir el trabajo en todos sus nodos. Si en un nodo se produce una falla irrecuperable, la red puede continuar funcionando sin verse afectada por la ausencia de dicho nodo. Esto demanda un procesamiento computacional extra, y la necesidad de algoritmos de ruteo extras. Agregando, este tipo de topologías exigen una gran cantidad de enlaces.

Por último, las topologías hypercube resultan teóricamente tentadoras, exigen menor cantidad de enlaces, y pueden tolerar la falla de una gran cantidad de nodos (hasta el 50% de los nodos). Su complejidad aumenta en gran medida, cuando se desarrollan arquitecturas de más dimensiones. En contraposición esta decisión aumenta su confiabilidad.

En el presente trabajo se comparó la confiabilidad de las diferentes topologías. Se asumió que la distribución de la confiabilidad es exponencial, con una tasa de falla fija de 1/15, y se estudió su evolución en un rango de tiempo adimensional entre 0 y 1, para acotar el problema. El resultado de esta comparación se puede observar en la Figura 8 y en la Tabla 1.

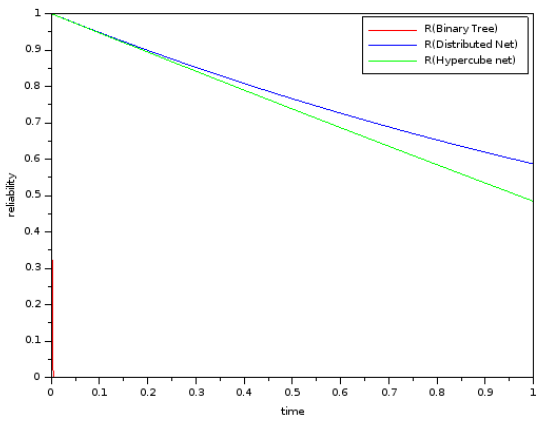

Figura 8: comparación de la confiabilidad de las topologías estudiadas.

Tabla 1: Comparativa de las topologías de red.

	Topologies Networks		
T	Tree Net	Distr Net	Hyper Net
0	1	1	1
0,001	0,803766	0,999947	0,999947
0,002	0,64604	0,999893	0,999893
0,003	0,519265	0,99984	0,99984
0,004	0,417368	0,999787	0,999787
0,005	0,335466	0,999733	0,999733
...	...	...	...
0,995	0	0,948317	0,947109
0,996	0	0,948266	0,947056
0,997	0	0,948216	0,947003
0,998	0	0,948165	0,94695
0,999	0	0,948115	0,946897

3.5 Arquitectura final

La arquitectura final propuesta se plantea en la Figura 9. En esta se puede observar que cada subsistema (térmico, power, telemetría, etc.) tiene su propia CPU controladora. Estas CPU se deben conectar a los nodos.

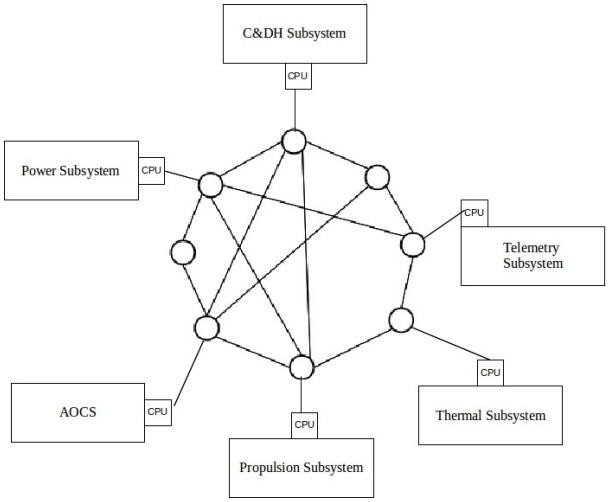

Figura 9: Arquitectura final propuesta.

De este modelo surge como requerimiento principal, que cada nodo debe estar compuesto por una computadora (componente COTS) que es la encargada de realizar el procesamiento de las tareas, y en paralelo debe existir un puente de comunicación entre la red y la CPU del subsistema. De este modo se hace frente a las posibles fallas de la computadora del nodo (Figura 10).

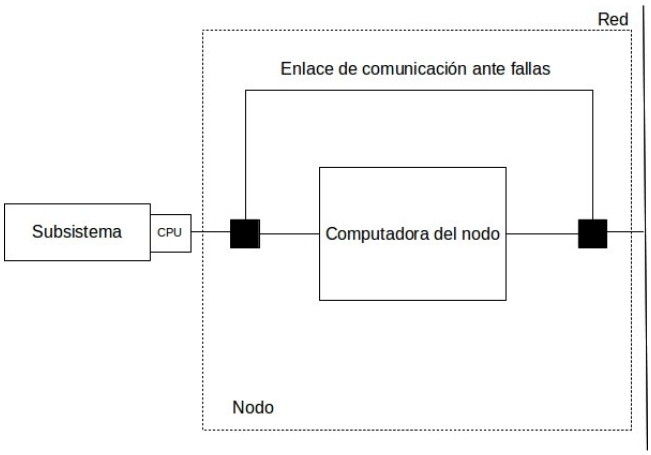

Figura 10: Propuesta de comunicación entre el nodo y los subsistemas.

4.- CONCLUSIONES

Teniendo en cuenta los resultados presentados en este trabajo, la topología de intercomunicación que presenta un alto grado de confiabilidad es la que responde a una filosofía de **red distribuida** (bajo las condiciones presentadas en el presente). Por lo tanto nosotros recomendamos que al momento de desarrollar arquitecturas de satélites con componentes COTS, y para mantener un alto grado de tolerancia a fallas, suponiendo que la ocurrencia de fallas de estos tiene una distribución exponencial, y aceptando el riesgo inherentes a los componentes COTS (por el lado de HW), la topología más segura a utilizar para la intercomunicación de los diferentes subsistemas es la **red distribuida**, siguiendo la metodología de desarrollo de [5].

En el presente trabajo no se analizó la tecnología de los enlaces de comunicación. En futuros estudios se abocará sobre la aplicabilidad, tanto de tecnología wireless como wired, en la arquitectura propuesta.

REFERENCIAS

[1] C. S. Raghavendra, AVIvizienis A., y M. D. Ercegovac. **Fault tolerance in binary tree architectures.** IEEE Transactions on Computers, (6):568–572, 1984.

[2] Adit D. Singh y Hee Y. Youn. **A modular fault-tolerant binary tree architecture with short links**. IEEE Transactions on Computers, 1991.

[3] John P. Hayes. **A graph model for fault-tolerant computer systems.** IEEE Transactions on Computers, 1976.

[4] Constantine Stivaros. **A measure of fault-tolerance for distributed networks.** Computing and Information, 1992. Proceedings. ICCI ’92., Fourth International Conference on, páginas 426–429, 1992.

[5] Dhiraj K. Pradhan y Sudhakar M. Reddy. A. **A Fault-Tolerant Communication Architecture for Distributed Systems.** IEEE Transactions on Computers, C-31(9):863–870, Sept 1982. ISSN 0018-9340.

[6] Yuh-Rong. Leu y Sy-Yen. Kuo. **A fault-tolerant tree communication scheme for hypercube systems.** IEEE Transactions on Computers, 45(6):641–650, 1996.

[7] Mostafa Abd-El-Barr, Fayez Gebali. **Reliability analysis and fault tolerance for hypercube multi-computer networks.** Information Sciences, Volume 276, 20 August 2014, Pages 295-318.

[8] Peter Fortescue, John Stark, y Graham Swinerd. **Space Systems Engineering**. Wiley, West Sussex, England, 3 edition, 2003. ISBN 0171619515.