Título del Proyecto: Certificación de la Confiabilidad de Sistemas que utilizan COTS mediante BBN

Autoría: Dr. Ing. José Luis Roca, Ing. Ricardo Oscar Juliá, Ing. Ariel Serra

Descriptores: COTS (commercial off-the-shelf), BBN (Belief Bayesian Nets), Confiabilidad, Software

Resumen:

Las mejores practicas indican que certificar un sistema implementado con COTS (commercial off-the-shelf) como componentes de software es problemático y debe ser llevado en forma totalmente independiente. Esta investigación tiende a explorar métodos de certificación de sistemas implementados con COTS utilizando redes de probabilidad bayesianas (BBN). De esta forma se pretende que mediante esta metodología se podría resolver un problema que afecta una de las más amplias áreas de incerteza acerca de la confiabilidad de sistemas implementados con componentes de software comerciales. En este aspecto cabe hacer notar que las principales contribuciones a la Confiabilidad de estos sistemas vienen dadas por la Calidad, Impacto y Utilización (Quality, Impact, Usability) de dichos componentes de software. Cada uno de estos aspectos da origen a otros tantos que se abren en una configuración arbolada. Por otro lado y es una realidad la construcción de sistemas en los que la seguridad (safety) es un parámetro de suma importancia, como sistemas de uso espacial, militar o nuclear (safety-critical systems) esta tendiendo a ser llevada a cabo utilizando COTS. El objetivo de este proyecto es el estudio y análisis de las diversas técnicas utilizadas para el análisis de la confiabilidad de sistemas basados en componentes de software comerciales denominados comúnmente COTS (Commercial-off-the-shelf). Modelizar el sistema vía una red de probabilidad Bayesiana (BBN) utilizando el conocimiento a priori de los componentes intervinientes juntamente con los registros históricos del comportamiento de dichos componentes del lado proveedor. Luego mediante la utilización de los datos recolectados durante el proceso de certificación realizar la actualización correspondiente de la BBN propuesta como modelo. Finalmente es posible obtener la confiabilidad del sistema bajo análisis.

### *1. Sistemas que utilizan COTS.*

En general en los sistemas de uso comercial es ampliamente aceptado el uso de COTS. La preocupación llega cuando se trata de sistemas en los que la confiabilidad es de principal interés debido a su utilización en el campo espacial, nuclear o militar. Es entonces necesario certificar que los COTS a utilizar reúnan las condiciones de confiabilidad y seguridad adecuadas. La idea es construir una BBN basada en el conocimiento a priori de los COTS y de los registros de los proveedores de los mismos en cuanto a su funcionamiento. Luego es posible alimentar la BBN con los datos provenientes del proceso de certificación para así finalmente obtener la confiabilidad de todo el sistema. La propuesta es utilizar para la certificación de la confiabilidad una BBN orientada a objetos (OOBBN). En la Fig.1 se observa la OOBBN propuesta.

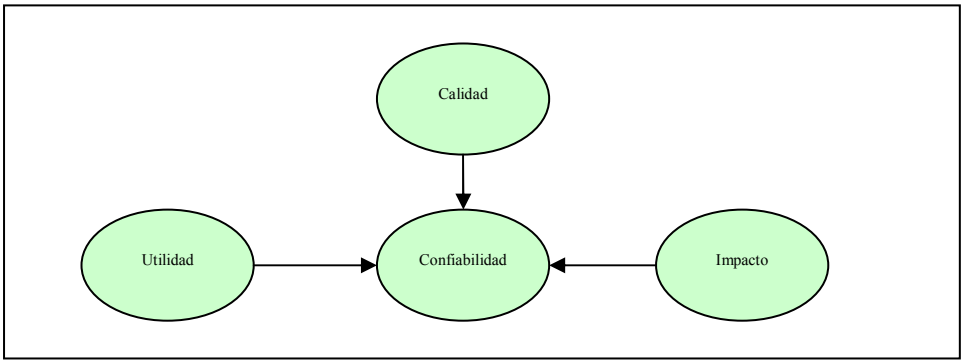


Fig.1 – OOBBN de Certificación

Entonces cada subred BBN aparece enlazada con la OOBBN vía nodos de las subred BBN. Utilidad, calidad e impacto son las mayores contribuciones a la confiabilidad de un sistema basado en COTS. Se investigaran las distintas subredes BBN de modo de analizar que elementos contribuyen a cada una de las diferentes entradas de le OOBBN.

### *2. Sobre la Utilidad.*

En la Fig. 2 se observa la BBN propuesta.

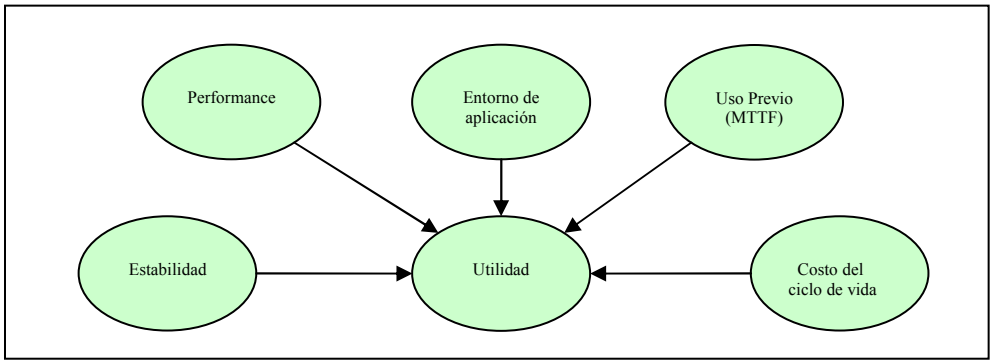


Fig.2 – Subred BBN Utilidad

### *3. Sobre la Calidad.*

En la Fig. 3 se observa la BBN propuesta.

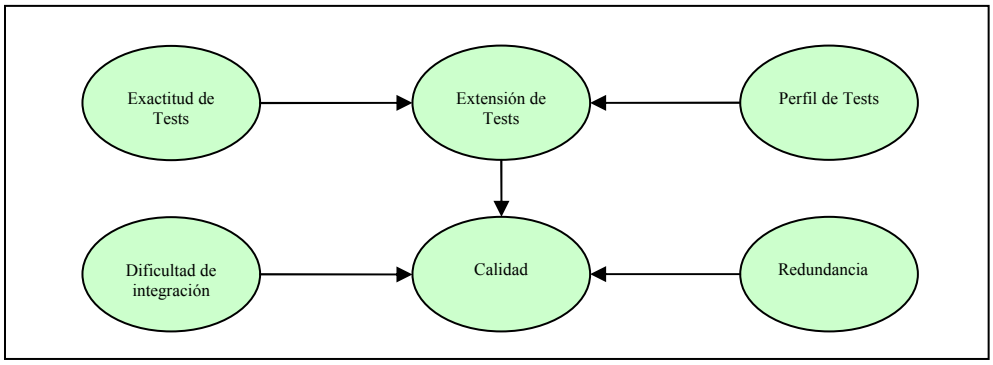


Fig.3 – Subred BBN Calidad

### *4. Sobre el Impacto.*

En la Fig.4 se observa la BBN propuesta.

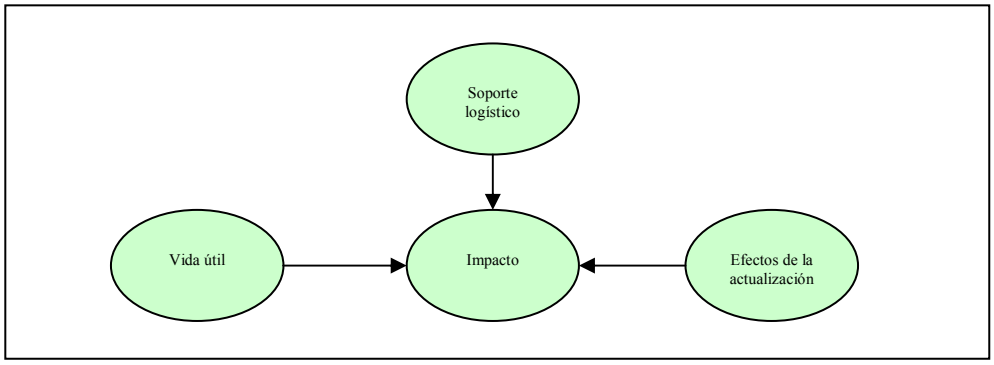


Fig.4 – Subred BBN Impacto

Los principales nodos de la red OOBBN han sido establecidos, con lo que las etapas 1 a 4 se han concluido. Tres serian los pasos que seguirían a continuación: poblar los nodos de la red con probabilidades, recolectar evidencia durante el proceso de certificación y posteriormente corriendo el programa sobre la red propuesta, actualizar las probabilidades de los diferentes nodos, propagando la evidencia causalmente.

### *4. Aplicación.*

Se procede a continuación a armar las redes propuestas en el entorno del programa NETICA. En principio se utilizara el modelo propuesto construyendo las tablas correspondientes a los nodos de decisión. Estos nodos son aquellos donde confluyen varios nodos individuales cuyas probabilidades se asignan a priori, a saber: Nodo Confiabilidad: OOBBN de Certificación, Nodo Utilidad: Subred BBN Utilidad, Nodo Extensión de Tests: Subred BBN Calidad, Nodo Calidad: Subred BBN Calidad, Nodo Impacto: Subred BBN Impacto. En la red propuesta cada nodo posee dos estados. De la misma forma se procede al

llenado de las probabilidades en los demás nodos, designando los valores de corte. La primer red de Certificación se muestra en la Fig.5

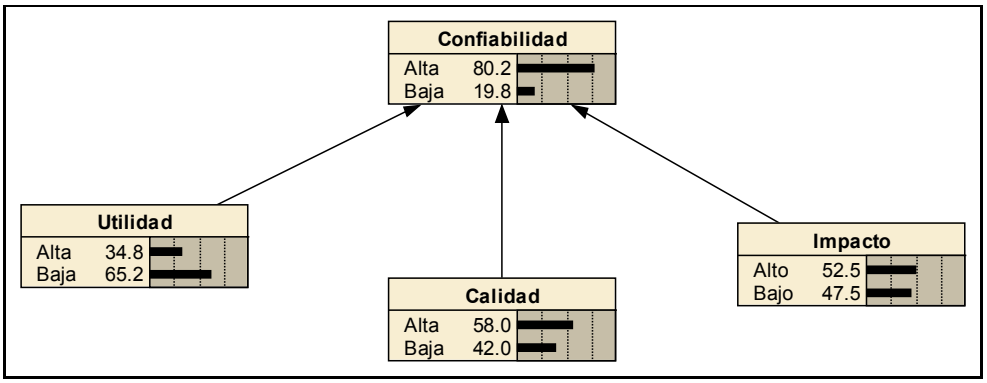


Fig.5 – BBN de Certificación

La red correspondiente al nodo Utilidad se muestra en la Fig. 6

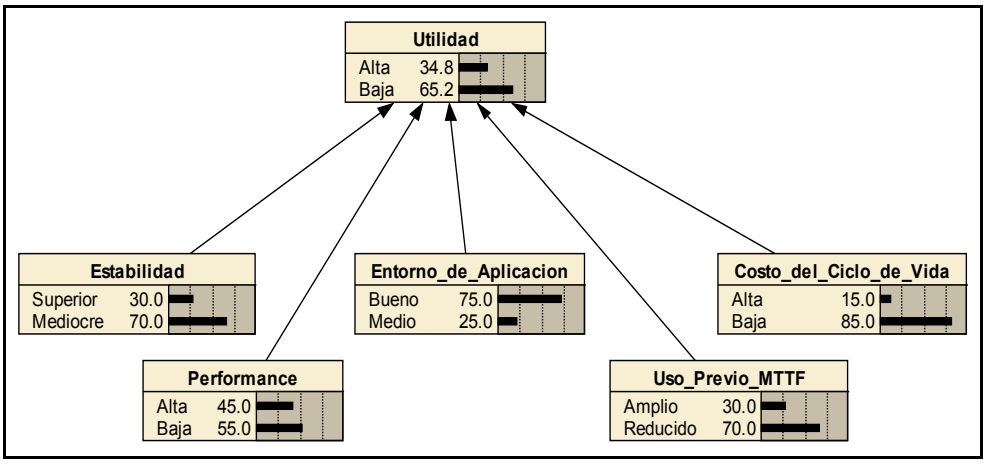


Fig.6 – Subred BBN Utilidad

La red correspondiente al nodo Calidad se muestra en la Fig.7

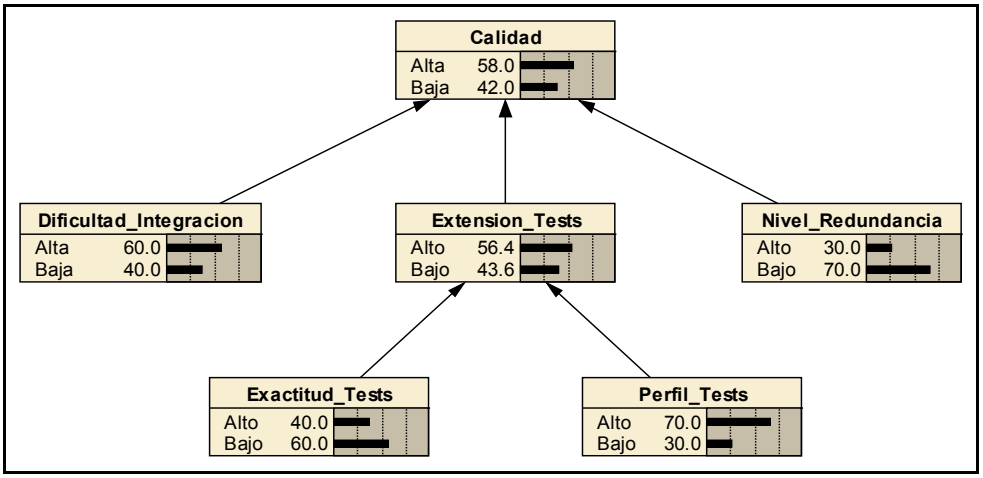


Fig.7 – Subred BBN Calidad

Por ultimo, en la Fig.8 se muestra la red correspondiente al nodo Impacto.

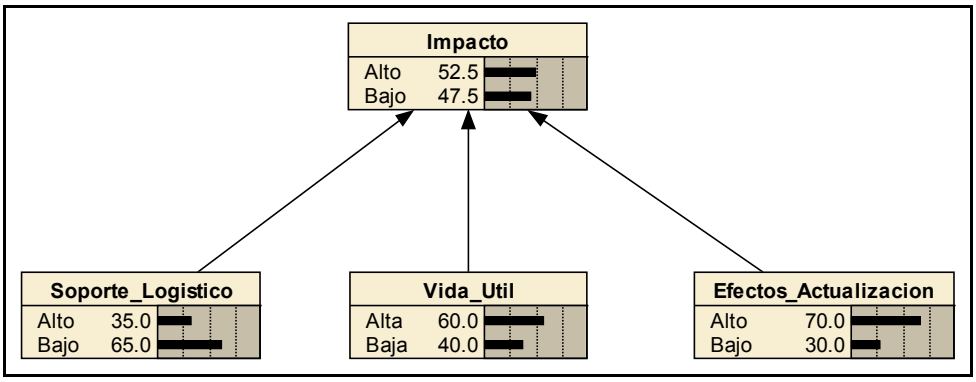


Fig.8 – Subred BBN Impacto

El segundo paso consiste en coleccionar evidencia dentro del proceso de certificación, en lo que respecta a las probabilidades asociadas a los nodos base de las redes. Luego con esa evidencia actualizar dichas probabilidades, de modo de que esos valores se propaguen por la red modificando los valores finales asociados a los diversos nodos de decisión de la red hasta el nodo final de Certificación de Confiabilidad del COTS. Para el ejemplo aplicativo se tomo un COTS correspondiente a una aplicación sobre un sistema operativo en tiempo real QNX utilizado en un sistema de sensado remoto como se observa en la Fig.9. En este caso solo se recolecto evidencia sobre el nodo correspondiente a Utilidad, de modo que la evidencia sobre cada uno de los componentes se modifico como se observa en la tabla de la Fig. 10.

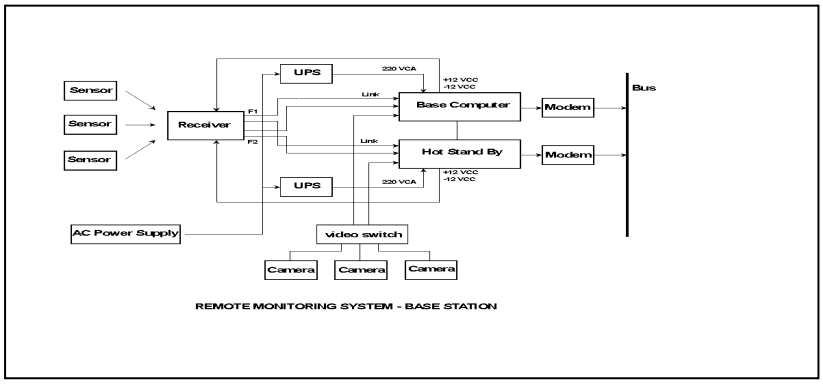


Fig.9 – Sistema QNX

| | | | |
|---|---|---|---|
| Estabilidad | Superior | 30 | 45 |
| | Mediocre | 70 | 55 |
| Performance | Alto | 45 | 80 |
| | Baja | 55 | 20 |
| Costo del Ciclo de Vida | Alto | 15 | 40 |
| | Bajo | 85 | 60 |
| Uso Previo (MTTF) | Amplio | 30 | 10 |
| | Reducido | 70 | 90 |
| Entorno de Aplicación | Bueno | 75 | 45 |
| | Medio | 25 | 55 |

Fig.10 – Evidencia Recolectada

En la misma tabla se observa la evidencia recolectada en la segunda línea de cada nodo. Así la Estabilidad paso de tener el corte de 30-70 % a 45-55%. Asimismo la Performance de 45-55 % a 80-20%, el Costo del Ciclo de Vida de 15-85% a 40-60%, el Uso Previo (MTTF) de 30-70% a 10-90% y el Entorno de Aplicación finalmente de 75-25% a 45-55%. Con esta evidencia la subred BBN Utilidad cambio a la de la Fig.11, donde se muestran los nuevos valores, fruto de la evidencia recolectada durante la certificación.

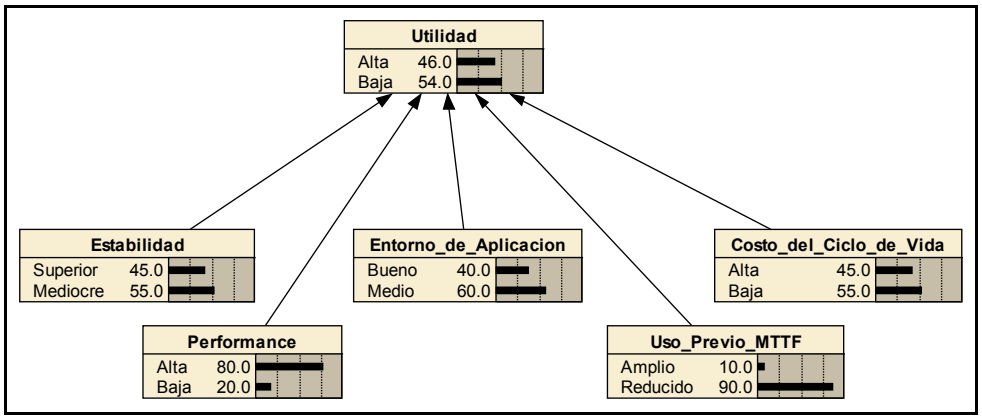


Fig.11 – Subred BBN Utilidad / Evidencia

Todos los demás parámetros permanecen sensiblemente constantes excepto la Utilidad. La evidencia se traslada a lo largo de la red completa afectado el nodo Confiabilidad. En la Fig.12 se observa los nuevos valores una vez compilada la red completa.

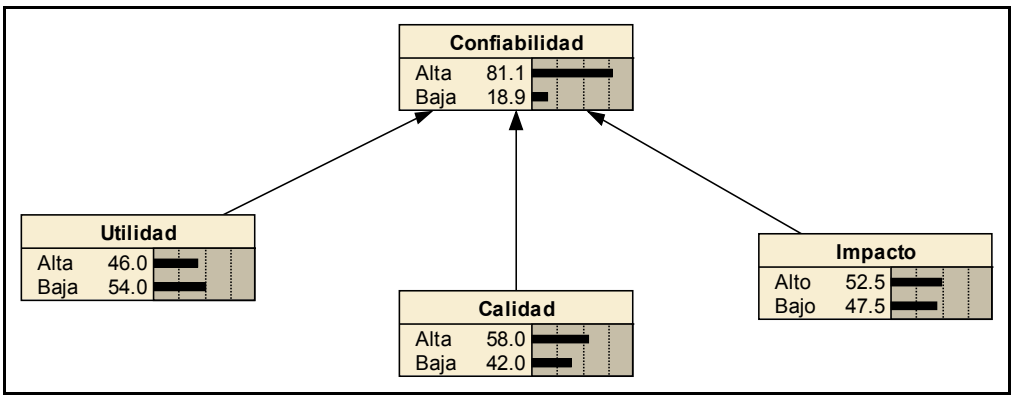


Fig.12 – BBN de Certificación / Evidencia

La Confiabilidad Certificada para el mismo punto de corte paso de 80,2-19,8% a 81,1-18,9%. En este caso la cualidad Estabilidad gano extremadamente poco en lo que Confiabilidad se refiere para el mismo punto de corte. Una nueva alimentación de evidencia durante procesos posteriores de certificación proveerán información que, utilizada de la misma manera, mejorara la estimación emergente de la presente metodología, inclusive contando con más de dos estados por nodo.