4.1 Información general

4.1.1 Definición  
A diferencia de las otras propiedades analizadas en este informe, la comunidad fiabilidad ha sido  
capaz de llegar a un consenso sobre la terminología. Esta acordada terminología está codificado por Laprie  
[Laprie 92]. Un proyecto revision1 posterior forma la base de gran parte de esta sección.

4.1.1.1 IFIP WG10.4 definición [Laprie 92]

Formalidad es propiedad de un sistema informático que dependencia puede ser justificadamente colocado en el servicio de entrega. Confiabilidad tiene varios atributos, incluyendo

• disponibilidad: preparación para el uso

• confiabilidad, continuidad del servicio

• seguridad — no ocurrencia, de consecuencias catastróficas para el medio ambiente

• confidencialidad — no ocurrencia, de divulgación no autorizada de la información

• integridad — no ocurrencia, de alteración indebida de información

• mantenimiento — aptitud para someterse a las reparaciones y evolución

Observe que los tres últimos atributos corresponden a las áreas de seguridad y se discute en otras secciones de este informe. En [Laprie 92] se agrupan la confidencialidad e integridad bajo la rúbrica "medidas de seguridad." En un proyecto más adelante [Laprie 94] los dos aspectos de la seguridad son llamados como anteriormente.

4.1.2 taxonomía

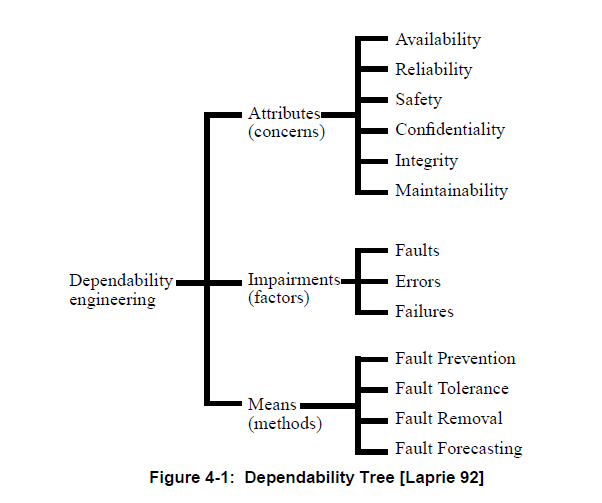
Figura 4-1 muestra un árbol de confiabilidad. Además de los atributos de confiabilidad, muestra los medios para lograr la confiabilidad y los impedimentos para lograr confiabilidad.

4.2 las preocupaciones

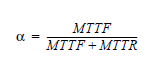
Las preocupaciones de confiabilidad son los parámetros mediante el cual la fiabilidad de un sistema son juzgado. Una visión del mundo centrada en la confiabilidad subsume los atributos habituales de confiabilidad, disponibilidad, seguridad y seguridad (confidencialidad e integridad). Dependiendo de la aplicación particular de interés, se acentúan diferentes atributos.

4.2.1 disponibilidad

La disponibilidad de un sistema es una medida de su preparación para el uso. La disponibilidad es siempre un preocupación al considerar la confiabilidad del sistema, aunque en diferentes grados, dependiendo de acerca de la petición.



La disponibilidad se mide como el límite de la probabilidad de que el sistema está funcionando correctamente a tiempo t, t tiende a infinito. Este es el estado estacionario la disponibilidad del sistema. Puede ser calculado [Trivedi 82] como:



Donde MTTF es el tiempo promedio de falla, y MTTR es el tiempo promedio de reparación.

4.2.2 confiabilidad

La fiabilidad de un sistema es una medida de la capacidad de un sistema para seguir operando en el tiempo. Dependiendo del sistema, fiabilidad a largo plazo no puede ser un motivo de preocupación. Por ejemplo, considerar un sistema de auto-tierra. El requisito de la disponibilidad de este sistema es alto — debe ser disponible

Cuando se le solicite al aterrizar el avión. Por otro lado, el requisito de fiabilidad es algo baja en que no tiene que permanecer operacional durante largos períodos de tiempo.

La fiabilidad de un sistema se mide normalmente como su tiempo promedio de falla (MTTF), la esperada

vida del sistema.

4.2.3 Capacidad de mantenimiento  
El mantenimiento de un sistema es su capacidad para someterse a la reparación y la evolución. Es menos precisa medida que las dos preocupaciones anteriores. MTTR es una medida cuantitativa de la capacidad de mantenimiento, pero no cuenta toda la historia. Por ejemplo, la filosofía de reparación debe tenerse en cuenta. Algunos sistemas son mantenidos por el usuario, otros por el fabricante. Algunos son mantenida por ambos (por ejemplo, la máquina diagnostica un fallo en la placa, envía un mensaje a la  
fabricante que envía una tarjeta de repuesto para el usuario con instrucciones de instalación.) No  
es un costo vs. MTTR trade-off que entra en juego. Por ejemplo, diagnósticos integrados pueden reducir el tiempo medio de reparación en el posible coste de la memoria extra, tiempo de ejecución, o el tiempo de desarrollo.

4.2.4 Seguridad  
Desde un punto de vista de la fiabilidad, la seguridad se define como la ausencia de consecuencia catastróficas en el medio ambiente lo define como la ausencia de accidentes y la pérdida. Esto conduce a una medida binaria de seguridad: un sistema es segura no es seguro. Seguridad se trata por separado en el presente informe.

4.2.5 Confidencialidad  
La confidencialidad es la no ocurrencia de la divulgación no autorizada de información. Se trató  
por separado, en la sección "Seguridad" de este informe (véase la sección 5 en la página 25) 0.4

4.2.6 integridad

La integridad es la no ocurrencia, de la alteración indebida de información. Junto con confidencialidad, este tema es tratado por separado en la sección 5 en la página 25.

4.3 impedimentos a la confiabilidad

Las debilitaciones de confiabilidad incluyen la falla, error y fracaso propiedades del hardware y software de los cuales el sistema está formado, como se muestra en la figura 4.1

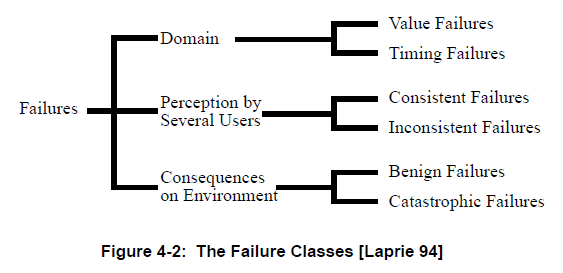
4.3.1 fallas

Como se ha dicho anteriormente, un sistema de falla cuando su comportamiento difiere de lo que pretendía.

Tenga en cuenta que definimos fracaso con respecto a la intención y no con respecto a la especificación. If la intención del comportamiento del sistema termina difieren de la especificación del comportamiento tienen una falla de especificación.

Hay muchas maneras en que un sistema puede fallar. Como se muestra en la figura 4-2, el llamado

"modos de falla" de un sistema pueden agruparse libremente en tres categorías; fallas de dominio, percepción de los usuarios y las consecuencias sobre el medio ambiente.



Fallas de dominio incluyen tanto valor fracasos y fallas de sincronización. Se produce un error de valor cuando se calcula un valor incorrecto, uno incompatible con la correcta ejecución del sistema. Sincronización fracasos ocurren cuando el sistema ofrece su servicio demasiado pronto o demasiado tarde.

Una forma extrema de una falta de sincronización es el fracaso vacilante — el sistema ya no ofrece ninguna servicio al usuario. Es difícil distinguir un fracaso muy tarde de sincronización de un fracaso vacilante. A sistema cuyos fallos pueden hacerse para ser sólo frenar fallas se llama un sistema fail-stop [Schlichting 83]. La asunción de fail-parada puede conducir a simplificaciones en el diseño del sistema confiable.

Otro caso especial del fracaso vacilante que conducen a la simplificación es uno en el cual un sistema fallido ya no genera ninguna salida. Esto se denomina un sistema fail-silencioso.

Hay dos tipos de errores de percepción. Un fracaso puede ser coherente o incoherente.

En el caso de una falla consistente, todos los usuarios del sistema tienen la misma percepción de un fracaso. En el caso de un fallo inconsistente, algunos usuarios del sistema pueden tener percepciones del fracaso que se diferencian unos de otros. Este tipo de fallas es llamado fracasos bizantinos [Lamport 82] y son las fallas más difíciles de detectar.

Finalmente, podemos calificamos fracasos por sus consecuencias sobre el medio ambiente. Aunque extremadamente difícil de medir, fallas pueden clasificarse en la gama benigna a catastrófica. Un sistema de que sólo puede fallar de manera benigna se denomina prueba de fallos.

4.3.2 errores

Es un estado del sistema que es capaz de conducir a un fracaso si no se corrige un error. O no se a conducir a un fracaso es una función de tres factores principales:

1. la redundancia (ya sea diseñado en o inherente) en el sistema

2. la actividad del sistema (el error puede desaparecer antes de que cause daños)

3. lo que el usuario considere un comportamiento aceptable. Por ejemplo, en la transmisión de datos existe la noción de "tasa de error aceptable"

4.3.3 fallas

Una falla es la causa de un error adjudicada o hipotética. Como se muestra en la figura 4-3, que pueden clasificarse en cinco ejes principales: causa fenomenológica, la naturaleza, la fase de creación, sistema límite y persistencia.

