MODELO DE ANALISIS DE CONFIABILIDAD BASADO EN GESTIÓN DE PROBABILÍSTICA DE RIESGOS

RELIABILITY ANALYSIS MODEL BASED ON PROBABILISTIC RISK ASSESSMENT

AUTOR
Andrea Milena Acevedo Lipes
Ingeniera Electrónica
Magister en Ingeniería
Universidad Industrial de Santander
Facultad de Ingenierías Eléctrica, Electrinica y Telecomunicaciones
andreaacevedo@gmail.com
COLOMBIA

INSTITUCION
Universidad Industrial de Santander - UIS
Universidad Pública
Calle 9 carrera 27
Telefono: 634 4000
webadmin@uis.edu.co
COLOMBIA

Recepción: Junio 8 de 2009

Aceptación: Septiembre 16 de 2009

Temática abarcada por el artículo: Gestión Tecnológica

Tipo de artículo: Reflexión

RESUMEN

La gestión probabilística de riesgos es una herramienta eficaz para la identificación y análisis de los riesgos que pueden afectar el desarrollo exitoso de un proceso. Este análisis, está enmarcado en un sistema de gestión de los eventos identificados que permite documentar y realizar un adecuado seguimiento y control.

PALABRAS CLAVES

Árbol de fallas
diagrama de secuencia de eventos
gestión
riesgos
probabilidad

ABSTRACT

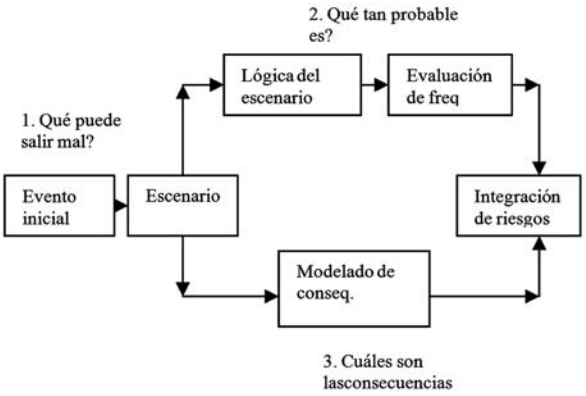
Probabilistic Risk Assessment is a Powerful tool for analisys and identification of risks that can affect a process. This analisys is enclosed in an event management system that allows documenting, tracking and control.

KEYWORDS: Fault tree, event sequence diagram, management, risks, probability.

INTRODUCCIÓN

Se conoce como riesgo, todo evento indeseable que pone en peligro el cumplimiento de los objetivos de un proceso o un proyecto. El riesgo se puede caracterizar contestando las preguntas[1]: 1. Que puede salir mal?, 2. Que tan probable es?, 3. Cuáles son las consecuencias? La respuesta a la primera pregunta es generalmente un conjunto de escenarios de falla. Para responder la segunda pregunta es necesario realizar una evaluación de las probabilidades de ocurrencia de los escenarios de falla, mientras que la tercera pregunta requiere estimar sus consecuencias. En la figura 1 se puede observar como la respuesta a estas preguntas, dan como resultado la descripción del riesgo.

FIGURA 1. Definición de riesgo a través de tres preguntas básicas



Un proceso de análisis de confiabilidad inicia con la identificación de una serie de eventos iniciales(IE) que perturban el sistema(causan un cambio en el estado de operación o en su configuración). Cada evento inicial es analizado para identificar todas las posibles fallas que puedan desembocar en eventos con consecuencias no deseables. Estas consecuencias, así como la probabilidad de ocurrencia de estas fallas, se conocen como escenarios de falla. Finalmente, todos estos escenarios son agrupados para crear el perfil de riesgo del sistema. Este perfil de riesgo es el que se debe gestionar utilizando un método de gestión del riesgo, en este caso, se propone el uso de Continous Risk Management.

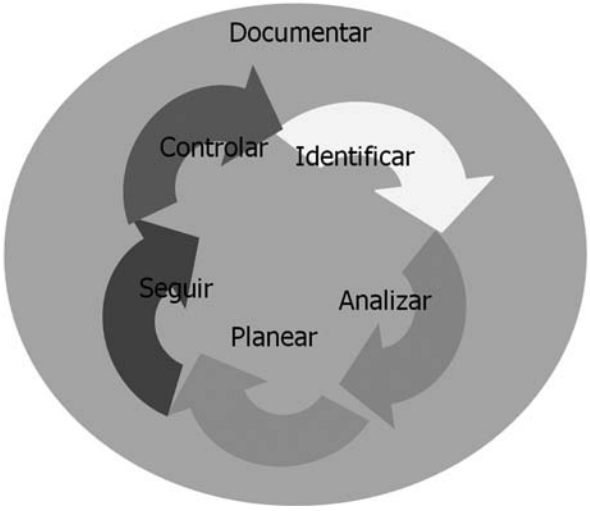
1. GESTIÓN DEL RIESGO CRM (CONTINUOUS RISK MANAGEMENT- CRM)

CRM es una práctica de gestión con procesos, métodos y herramientas para gestionar los riesgos de un proyecto. Provee un enfoque documentado y disciplinado con características como:

- Identifica los aspectos que podrían salir mal (riesgos).
- Determina cuales son los riesgos más críticos.
- Implementa estrategias para tratar estos riesgos.
- Asegura efectividad de las estrategias implementadas.

El ciclo contínuo de CRM se puede observar en la siguiente figura:

FIGURA 2. Proceso de gestión contínua del riesgo



El proceso CRM es iterativo, es decir, su ciclo de vida se repite varias veces durante todo el proyecto. Comienza con la identificación de riesgos y definición de restricciones, los cuales establecerán los criterios de éxito y riesgos no tolerables en el proyecto. El proceso continúa con el análisis de riesgos donde se evalúan sus probabilidades, impactos, severidad, y exposición, clasificándolos en grupos, de acuerdo a sus efectos. Luego, en la etapa de planificación se asignan responsables a los riesgos, el tipo y nivel de tratamiento (prevención, mitigación o contingencia). En la etapa de seguimiento se compila, analiza y organiza los datos de los riesgos. También se reportan los resultados, se verifican y validan las acciones de mitigación. En la etapa de control se analizan los resultados, se definen los procedimientos en cada caso (replanteo, cierre del riesgo, invocar planes de contingencia etc.). Por último

está la etapa de documentación y comunicación donde se comunica al resto del equipo, el estado de los riesgos y se formaliza en un documento. Se debe establecer un sistema de configuración para el control de estos documentos.

Para cada riesgo primario identificado se deben establecer las siguientes características:

1. Descripción del riesgo, incluyendo causas primarias y los factores.
2. Consecuencias primarias.
3. Estimación de la probabilidad ya sea de forma cualitativa o cuantitativa. Esta probabilidad debe contemplar el riesgo absoluto y el riesgo con controles, para estimar el riesgo residual presente. Para realizar estimaciones cuantitativas, generalmente se utilizan enfoques probabilísticos porque permiten tomar gran cantidad de datos y luego utilizarlos para predecir el comportamiento de un sistema.
4. Planes de prevención, mitigación y contingencia.

2. ENFOQUE PROBABILÍSTICO

El enfoque probabilístico es utilizado cuando se necesita tomar decisiones en situaciones complejas de las diferentes etapas en los proyectos. Para tomar estas decisiones es necesario disminuir la incertidumbre de las situaciones presentadas a través de métodos estadísticos que puedan predecir el comportamiento de eventos en los proyectos. La gestión probabilística de riesgos tiene varias etapas bien definidas:

- *Definición de Objetivos*: En esta etapa se definen con claridad los objetivos de la identificación de riesgos y los eventos finales indeseables.

- *Familiarización con el sistema*: Se debe conocer toda la información operacional del sistema, sus manuales, procedimientos, guias etc, e identificar las áreas de impacto y posibles fuentes de riesgo.

- *Identificación de eventos iniciales(IE)*: Identificar los eventos iniciales o eventos disparo de toda la cadena de eventos de falla y que conllevan a estados finales indeseables. Una herramienta para la identificación de eventos iniciales es el Diagrama lógico-DL. El DL es una organización jerárquica que muestra en la parte superior el estado final, siguiendo con las instancias intermedias y en la parte inferior los eventos iniciales. El objetivo del DL no es solo dar soporte a la identificación de los EI, sino también agruparlos de acuerdo al grado de esfuerzo que se debe hacer para mitigar el evento indeseable que generan y a la parte del sistema que afectan. En la Figura 3 se observa un ejemplo de diagrama lógico utilizando como ejemplo un proceso de votación electrónica.. En el nivel 1: Funcionalidades del sistema, se identifican los diferentes subprocesos que se realizan y conforman el gran proceso de votación electrónica. En el nivel 2: se identifican los sistemas que intervienen en los subprocesos y que son críticos para el funcionamiento. De ahí en adelante estos sistemas pueden ser descompuestos en tantos niveles se desee, esto depende del detalle requerido para el análisis. Por último, se llega a los eventos iniciales, los cuales pueden ser agrupados de acuerdo a sus efectos sobre el sistema.

- *Modelado del escenario*: El modelado de cada escenario de falla se realiza a través de lógica inductiva y herramientas probabilísticas llamadas árboles de eventos. Un árbol de eventos empieza con un evento inicial y va evolucionando a través de un grupo de eventos falla llamados eventos pivote hasta alcanzar el estado final. Para esta etapa se utilizan las herramientas gráficas llamadas diagramas de secuencia de eventos(Figura 4) que permiten describir escenarios accidente. Para cuantificación, estos diagramas deben convertirse en árboles de eventos.

- *Modelado de fallas*: cada falla o su complemento, éxito, de un evento pivote en un escenario de fallas es modelado a través de árboles de fallas. Éstos árboles están conformados por las siguientes partes: El evento final, conocido como 'top event' y los eventos intermedios(fallas) que causan el evento final. Estos eventos intermedios están relacionados a través de compuertas lógicas y a su vez están relacionados con los eventos finales(Figuras 5).

- *Recolección de datos, análisis y desarrollo*: Esta etapa se realiza en paralelo con la anterior. Aquí se ensamblan los datos para cuantificar los escenarios de falla y sus causas. Entre los datos a recopilar están: rata de fallas, tiempo de reparación, probabilidades de evento iniciales, probabilidades de fallas de la estructura del proceso, probabilidades de error humano y causas de fallas comunes, así como límites y distribuciones de incertidumbre.

FIGURA 3. Estructura general de un diagrama lógico

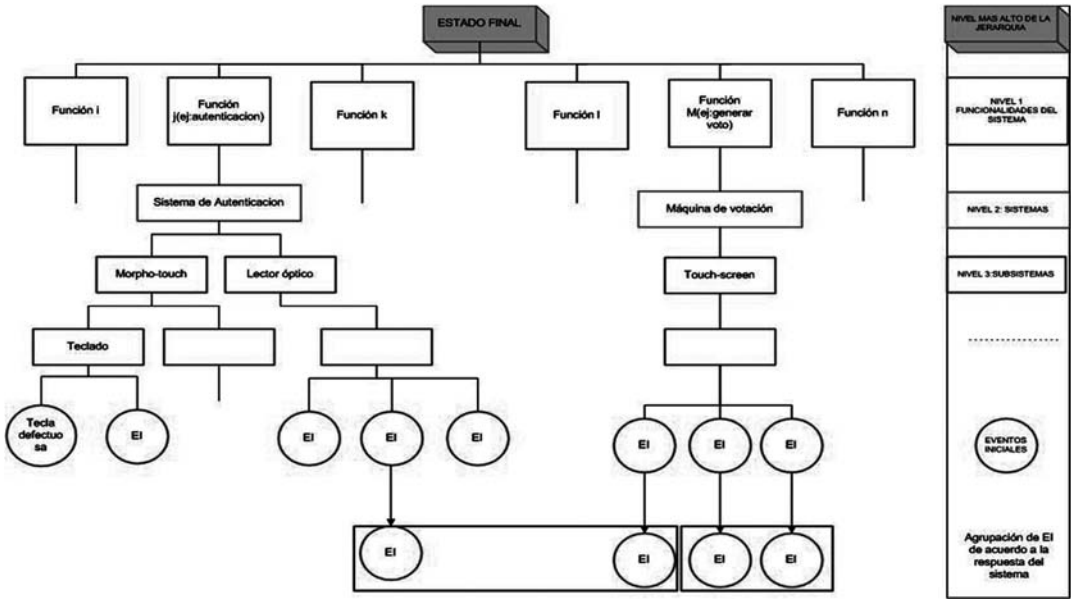


FIGURA 4. Estructura general de un diagrama de secuencia de eventos

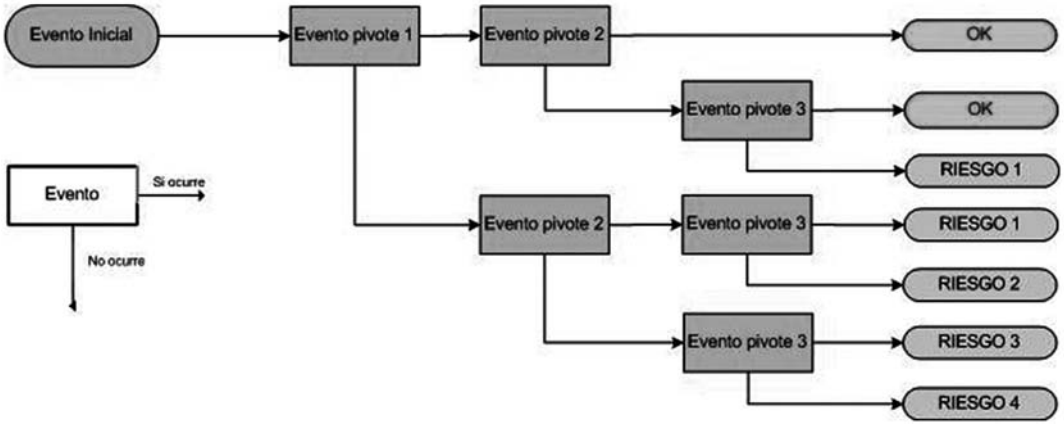
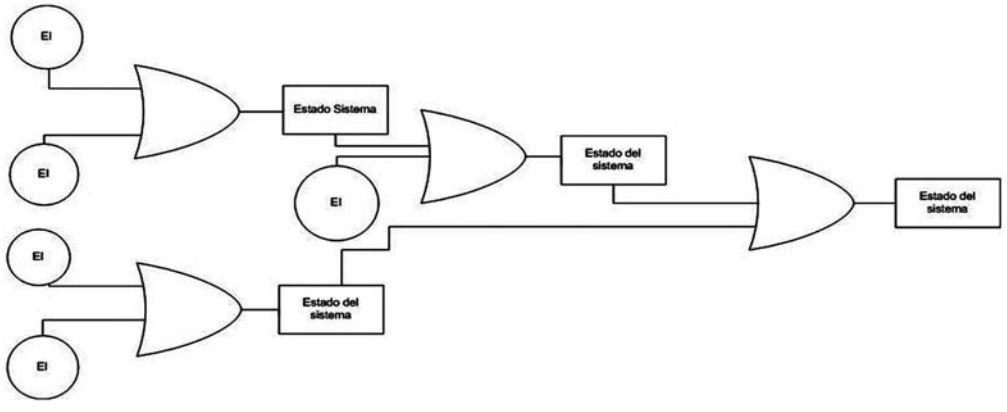


FIGURA 5. Modelo general de un árbol de fallas(Compuertas OR)



- *Cuantificación e Integración*: La frecuencia de ocurrencia de cada estado final en el árbol de eventos es el producto de la frecuencia de los eventos iniciales y las probabilidades condicionales de los eventos pivote a lo largo del escenario. Los escenarios se agrupan de acuerdo a su estado final y su consecuencia. En las figuras 6 y 7 se observa cómo se relacionan los datos a través de las compuertas AND y OR y las ecuaciones que los representan.

- *Análisis de Incertidumbre*: Estos análisis se realizan para evaluar el grado de conocimiento y confianza en los análisis numéricos resultantes. En esta etapa se pueden implementar las simulaciones Montecarlo.

- *Análisis de sensibilidad*: Este análisis se realiza para identificar grandes cambios a variaciones pequeñas en la entrada a los procesos.

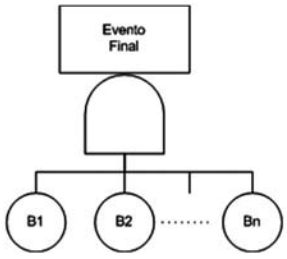
- *Jerarquización*: Es importante al final del proceso para clasificar las causas más importantes del os eventos de falla.

Debe aclararse que antes de iniciar este tipo de análisis debe establecerse completamente el enfoque para que los resultados brinden respuestas a casos específicos previamente identificados.

El método de gestión probabilística de riesgos se utiliza cuando es necesario tomar decisiones en situaciones complejas porque da las pautas principales para la asignación de presupuesto en un proceso. Un diagrama de flujo del típico proceso se observa en la figura 8. La característica esencial de este método probabilístico es que permite mapear una realidad bastante compleja y representarla a través de relaciones lógicas, que a su vez, permiten la creación de algoritmos computacionales para su análisis.

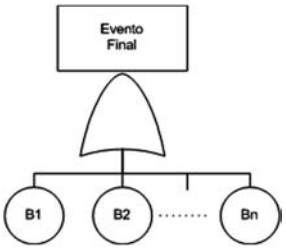
El análisis posteriores, se aplicará en modelo descrito en este articulo, a procesos de votación electrónica, como parte del proyecto de investigación sobre los riesgos de nivel estratégico, táctico, operativos y técnicos que este proceso puede presentar.

FIGURA 6. Compuerta AND



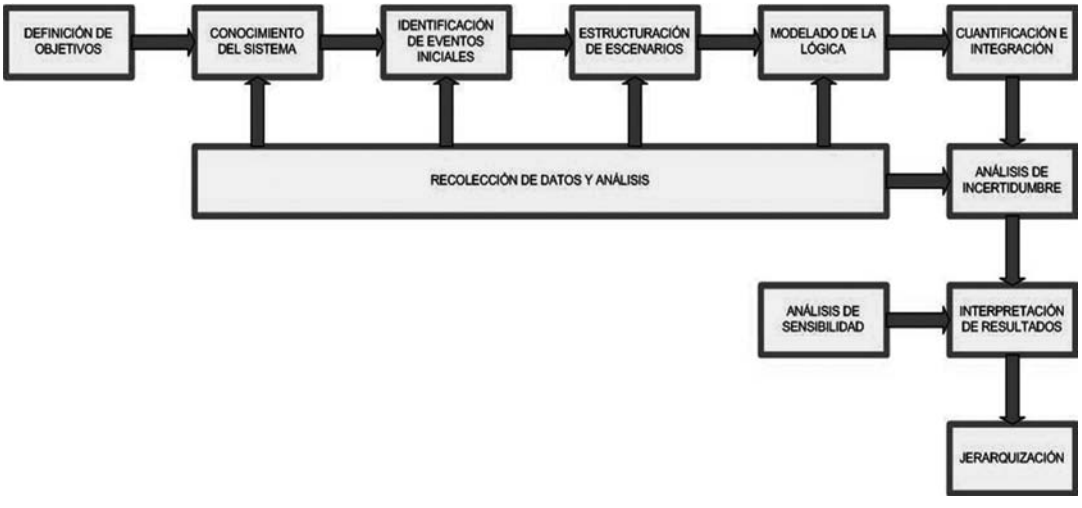
$$Q_s = P_r\{B_1 \cup B_2 \cup \ldots . \cup B_n\} \quad \text{Ec 1.}$$

FIGURA 7. Compuerta OR



$$Q_s = P_r\{B_1 \cap B_2 \cap \ldots . \cap B_n\} \quad \text{Ec 2.}$$

FIGURA 8. Diagrama de flujo del enfoque probabilístico



3. REFERENCIAS

[1] Stamatelatos, Michael, et al. "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners". Oficce of Safety and Mission Assurance, Nasa Headquarters. Manual de procedimientos. Washington D.C. Agosto de 2002.

[2] Kumamoto,Hiromitsu. Henley, Ernest. "Probabilistic Risk Assessment and Management for Engineers and Scientists". Second Edition. ISBN 0-7803-6017-6. IEEE Reliability Society. IEEE PRESS. New York, EE.UU. 1996.

[3] W.E. Vesely, F.F. Goldberg, N. H. Roberts, D.F. Haasl. "Fault Tree Handbook". U.S Nuclear Regulatory Commission. Nureg-0492. Washington D.C. 1992.

[4] BS ISO/IEC 27001:2005. Information Technology-Security Techniques-Information Security Management Systems-Requirements. British Standars. Versión Electrónica. 18 de Octubre de 2005.

[5] "Systems Security Engineering Capability Maturity Model". SSE-CMM. Versión 3.0. Carnegie Mellon University. Junio 15 de 2003. http://www.sei.cmu.edu/

[6] CobIT 4.1. IT Governance Institute. ISBN 1-933282-72-2. United States. 2007. www.isaca.org

[7] CobIT Mapping:Mapping of ITIL with CObIT 4.0. IT Governance Institute. ISBN 1-933284-77-3. United States. 2007. www.isaca.org

[8] Enterprise Risk Management Integrated Framework. Committee of Sponsoring Organizations of the Treadway Commission-COSO. 2004. www.isaca.org

[9] Association of Insurance and Risk Managers(AIRMIC), ALARM(National Forum for Risk Management in the Public Sector) and Institute of Risk Management(IRM). A risk Management Standard. Londres, 2002.

[10] AS/NZ 4360:2004. Risk Management systems Standard. Australia and New Zealand. 2004

[11] Williams, Graham. "Management of Risks(M_o_R):The facts v1.0 Office of Government Commerce. U.k 2007."

[12] ISO/TMB WG on Risk Management-Guideliness on Principles and Implementation of Risk Management. June 2007

[13] Yang. Guangbing. "Life Cycle Reliability Engineering" John Wiley and Sons. Inc. 2007.