Análisis de estructuras para la norma en ISO 13849-1 con base en un comportamiento estocástico usando cadenas de Markov

Mauricio Holguín Londoño[1]
Diego Fernando Muñoz Torres[2]
Álvaro Ángel Orozco Gutiérrez[3]

RESUMEN

Con el propósito de mejorar la calidad en la producción industrial, así como reducir los impactos ambientales y los accidentes industriales, la rama de la ingeniería de mantenimiento se ha enfocado en desarrollar técnicas, metodologías y normas pertinentes que permitan atacar estos puntos críticos en la automatización industrial. La norma EN ISO 13849-1 es un ejemplo de protocolo por seguir para asegurar la reducción de los impactos negativos en cuanto a seguridad. En este trabajo se presenta una metodología que permite emplear la norma EN ISO 13849-1 de una manera cuantitativa mediante la aplicación de teoría de la probabilidad. Para ello se recurre a las cadenas de Markov, las cuales describen de manera eficaz la evolución de la degradación de los sistemas industriales al calcular el nivel de seguridad de un sistema de forma cuantitativa, lo que permite una descripción numérica de las estructuras de seguridad, además de ponderar la respuesta del sistema de seguridad mediante la inclusión de la tradicional forma cualitativa.

Palabras clave: cadenas de Markov, nivel integral de seguridad, norma EN ISO 13849-1, sistema integrado de seguridad.

[1] PhD (C). Ingeniero electricista. Magíster en Ingeniería Eléctrica, Universidad Tecnológica de Pereira, Colombia. Profesor de tiempo completo, Facultad de Ingenierías, Programa de Ingeniería Eléctrica, Universidad Tecnológica de Pereira. Estudiante de Doctorado en Ingenierías, área de Automática, Colombia. Correo electrónico: mau.hol@utp.edu.co

[2] Ingeniero electricista, Universidad Tecnológica de Pereira, Colombia. Estudiante de Maestría en Ingeniería Eléctrica, área de Automática, Universidad Tecnológica de Pereira, Colombia. Correo electrónico:diegomtor@hotmail.com

[3] PhD. Ingeniero electricista, Universidad Tecnológica de Pereira, Colombia. Abogado, Universidad Libre de Pereira, Colombia. Magíster en Ingeniería Eléctrica, área de Control e instrumentación, Universidad Tecnológica de Pereira. Doctor en Bioingeniería, Universidad Politécnica de Valencia, España. Profesor titular, Facultad de Ingenierías, programa de Ingeniería Eléctrica, Universidad Tecnológica de Pereira, Colombia. Correo electrónico: aaog@utp.edu.co

Fecha de recepción: 20 de febrero de 2013 • Fecha de aprobación: 29 de abril de 2013

Cómo citar el artículo: Holguín Londoño, M.; Muñoz Torres, D. F y Orozco Gutiérrez, A. A. (2013). Análisis de estructuras para la norma en ISO 13849-1 con base en un comportamiento estocástico usando cadenas de Markov. *Épsilon* (20), 237-264.

Structure Analysis for the ISO 13849-1 Standard Based on a Stochastic Behavior Using Markov Chains

ABSTRACT

In order to improve quality in industrial production, reduce environmental impacts and industrial accidents, maintenance engineering has focused on developing techniques, methodologies and standards to approach these critical issues in industrial automation. The EN ISO 13849-1 standard is a protocol to be followed in order to ensure the decrease of negative impacts in safety. This article presents a methodology that allows using the EN ISO 13849-1 standard in a quantitative way by applying the probability theory. This is established by using Markov chains, which effectively describe the evolution of the degradation of industrial systems by making a quantitative calculation of the safety level of a system in order to present a numeric description of the safety structures and weigh the response of the safety system by including the traditional qualitative method.

Keywords: Markov chains, safety integrity level, EN ISO 13849-1 standard, safety integrated system.

Análise de estruturas para a norma em ISO 13849-1 com base em um comportamento estocástico usando cadeias de Markov

RESUMO

Com o propósito de melhorar a qualidade na produção industrial, assim como reduzir os impactos ambientais e os acidentes industriais, o ramo da engenharia de manutenção tem se enfocado em desenvolver técnicas, metodologias e normas pertinentes que permitam atacar estes pontos críticos na automatização industrial. A norma em ISO 13849-1 é um exemplo de protocolo a seguir para garantir a redução dos impactos negativos em quanto à segurança. Neste trabalho se apresenta uma metodologia que permite empregar a norma em ISO 13849-1 de uma maneira Quantitativa através da aplicação de teoria da probabilidade. Para isso se recorre às cadeias de Markov, as quais descrevem de maneira eficaz a evolução da degradação dos sistemas industriais ao calcular o nível de segurança de um sistema de forma quantitativa, o que permite uma descrição numérica das estruturas de segurança, além de ponderar a resposta do sistema de segurança através da inclusão da tradicional forma qualitativa.

Palavras chave: cadeias de Markov, nível integral de segurança, norma em ISO 13849-1, sistema integrado de segurança.

Introducción

La evaluación de los riesgos es vital para el desarrollo y la optimización de la seguridad en los componentes de un sistema industrial. A partir de la correcta documentación de estas medidas es posible evaluar el desarrollo y el proceso de minimización de los riesgos. Este proceso se realiza con un adecuado manejo de la normatividad vigente, su aplicación a los procesos industriales y teniendo presente el propósito de reducir las tasas de fallas y accidentes por mal uso de maquinaria, como se menciona en la Directiva de Máquinas 2006/42/CE (2010).

Durante años se implementó el estándar EN 954-1 como una norma clave para garantizar, justificar y respaldar la seguridad y fiabilidad de los sistemas de mando en máquinas. Debido a los constantes avances tecnológicos y a la exigencia de las empresas por disminuir sus accidentes y sus tasas de falla, se notó que esta norma tenía una gran deficiencia al ser cualitativa, lo que provocaba un gran margen de error ante fallos peligrosos. Por lo anterior, se pasó a exigir un nivel cuantitativo, que abarque más parámetros que afectan la seguridad y el rendimiento del sistema, entre los cuales están los desgastes frecuentes, los fallos de causa común, la gravedad de la lesión, etc., como se menciona en Pilz Automation Technology (2012). El estándar EN ISO 13849-1 entra en escena desde el año 2006, rige desde el 31 de diciembre de 2011 y deja obsoleta la EN 954.1 llevando a las empresas a cambiar los procesos de evaluación de riesgos y obtención de niveles de seguridad para las máquinas, ABB Jokab Safety (2011).

Se tiene el interés técnico en establecer la vida útil de determinado componente industrial, sea este una unidad funcional, un equipo o un sistema. Para obtener la estimación de riesgos es necesario tener en cuenta cierto tipo de consideraciones como son la gravedad de la lesión, la frecuencia con que se presenta y las probabilidades de ocurrencia y de evitar o limitar el daño, para lo cual es necesaria alguna herramienta que realice dicho proceso, como lo describe Ecay (2007).

El alto número de accidentes que se producen en los procesos industriales puede ser causado por el poco conocimiento e implementación de la normativa pasada sobre la seguridad de las máquinas. Al aplicar la normativa presente y los modelos predictivos, como es el caso de las cadenas de Markov, es posible obtener un sistema seguro predecible a fallas, con el cual se pueda garantizar mayor confiabilidad y seguridad para los trabajadores, como mencionan Castellano y Sánchez (2013).

El estudio basado en teoremas probabilísticos de cadenas de Markov permite obtener una herramienta telescópica con la cual se podría predecir una serie de posibles daños en la máquina basándose en eventos ocurridos con anterioridad y de esta manera saber en qué nivel de seguridad se encuentra un sistema (Hildebrandt, 2007). En este tipo de sistemas seguros lo que generalmente se busca es que en caso de falla el sistema se dirija a un estado seguro donde se pueda controlar sin necesidad de sacarlo de operación y no permitir fallas peligrosas en las cuales el sistema interrumpe su funcionamiento y queda imposibilitado para cubrir las demandas del proceso.

Materiales y métodos

Sistema integrado de seguridad

Un sistema integrado de seguridad (SIS) es un sistema designado para implementar las funciones de seguridad requeridas y necesarias a fin de lograr o mantener un estado seguro en algunos equipos, y se utiliza con frecuencia para reducir los procesos peligrosos en plantas de producción. Para cada proceso se realiza una función de seguridad que se diseña a fin de detectar una situación de riesgo y, automáticamente, tomar las medidas necesarias para prevenir o mitigar dicho suceso peligroso. Estas funciones están implementadas por las funciones instrumentadas de seguridad (SIF), compuestas por múltiples subfunciones en una única, y donde cada una recoge y analiza información de los sensores para determinar si se produce una condición peligrosa y, en consecuencia, generar una secuencia de parada y llevar el proceso a un estado seguro.

El SIS está conformado por una instrumentación o controladores instalados con la finalidad de prevenir o reducir el riesgo y llevar el proceso a un estado seguro en presencia de una demanda de seguridad. Sus principales componentes son los siguientes (figura 1):

- Detectores (o sensores).
- Solucionador de la lógica (por ejemplo, PLC).
- Actuadores (por ejemplo, válvulas, pistones).

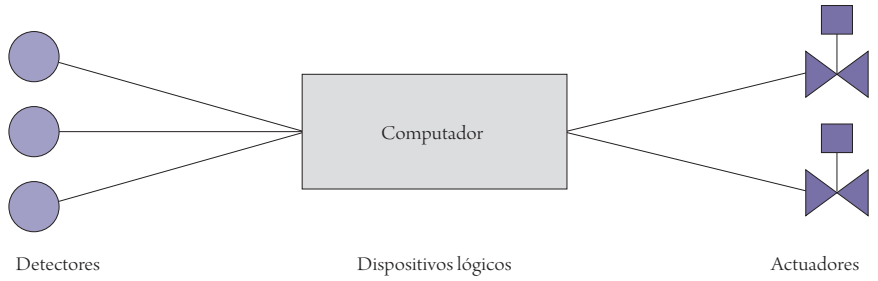

Figura 1. **Elementos que componen un SIS**

Función de seguridad

Las funciones de seguridad (FS) tienen por objetivo mantener los equipos que vigilan en un estado de seguridad con respecto a peligros específicos. Cuando se presentan fallas en dichas funciones de seguridad el resultado es un aumento inmediato de los riesgos al utilizar algún equipo, y se llega a una condición peligrosa donde alguna persona puede quedar expuesta y protegida solo por su capacidad de reconocer y evitar un riesgo. Es obligación del diseñador evitar que dichas condiciones de peligro se presenten. Las funciones de seguridad no son ejecutadas por un solo dispositivo, para llevarlas a cabo se debe contar con algún tipo de módulo de entrada mediante el cual se envía un comando a un dispositivo lógico, este a su vez inhabilita los actuadores con los cuales se pretende disminuir el peligro. El sistema de seguridad debe estar diseñado con un nivel de integridad acorde con los riesgos de la máquina, de tal forma que los riesgos más altos requieren niveles de integridad mayores. Los sistemas de seguridad se pueden clasificar por niveles de rendimiento, por su capacidad de asegurar la función de seguridad o por su nivel de integridad de seguridad funcional.

Norma EN ISO 13849-1

La norma EN ISO 13849-1:2006 (Seguridad de las máquinas. Partes del sistema de mando relativas a seguridad. Parte 1: Principios generales para el diseño) ha sido preparada con el fin de guiar los procesos de diseño y evaluación de los sistemas de mando. Esta norma se complementa con la IEC BS EN 62061:2005, aunque esta última está referida sobre todo a sistemas de mando eléctricos, electrónicos y electrónicos programables, mientras que la EN ISO 13849-1 abarca todo tipo de tecnologías.

La EN ISO 13849-1 evalúa las funciones de seguridad existentes a partir de los niveles de rendimiento (PL) según categorías. Cubre cualquier componente seguro en sistemas de control (SRP/CS) y todo tipo de máquina, independientemente de la tecnología y forma energética de que se trate (eléctrica, hidráulica, neumática, mecánica, etc.).

Procedimiento según la norma EN ISO 13849-1

Los pasos que se deben seguir en la norma EN ISO 13849-1 son:

1. Identificación y requisitos de las funciones de seguridad (SF).

2. Determinación del PL requerido (PLr).

3. Diseño e identificación de las partes del sistema de mando relativas a seguridad.

4. Determinación del PL de las partes del sistema de mando relativas a seguridad.

    - Aspectos cuantificables (categoría, tiempo medio hasta fallo peligroso, cobertura del diagnóstico, fallos de causa común).

    - Aspectos no cuantificables.

5. Verificación PL ≥ PLr.

6. Validación.

Nivel de rendimiento requerido (PLr)

El PLr determina el nivel de prestación requerido, es decir, la cantidad de reducción de riesgo que posee cada parte del sistema de mando relativa a la seguridad. Se presenta un árbol de selección (figura 2) donde:

- S, F y P son los parámetros de decisión utilizados para la evaluación del PLr.

    S = Gravedad de la lesión.

F = Frecuencia / tiempo exposición al peligro.

P = Posibilidad de evitar o limitar el peligro.

- Existen cinco niveles directos para determinar el PLr (de la "a" a la "e") a la salida del árbol.

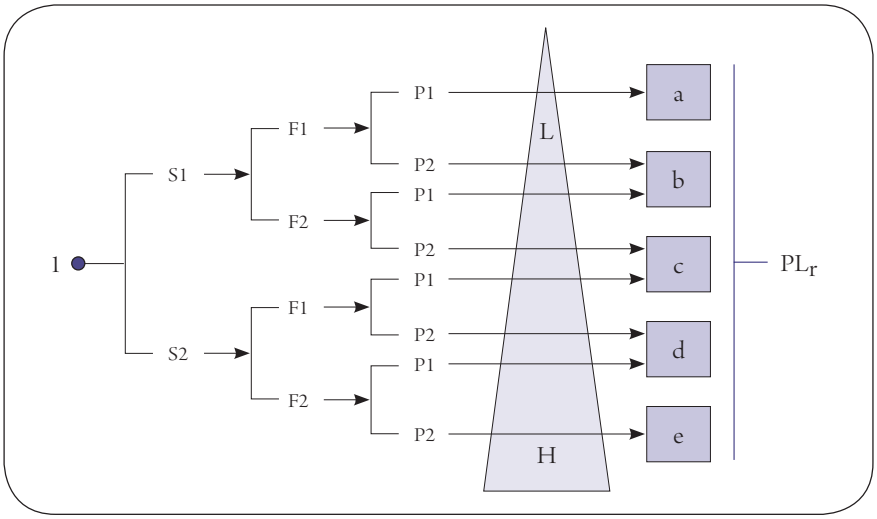

Figura 2. **Selección de riesgo y determinación del PLr según la norma EN ISO 13849-1**

Diseño de las partes del sistema de mando relativas a la seguridad (SRP/CS)

El diseño de las SRP/CS puede contener cualquier tipo de tecnologías disponibles, ya sean separadas o combinadas, pudiendo a su vez implementar alguna función operativa. Las funciones del sistema de mando pueden estar formadas por varias funciones de seguridad que a su vez pueden compartir las partes del sistema de mando de seguridad correspondientes. En la figura 3 se muestra una representación esquemática, donde i_{ab} e i_{bc} son los medios de interconexión (eléctricos, ópticos, etc.), 1 es el evento de iniciación (interrupción de cortina, pulsación botón parada, etc.), y 2 es el evento actuador en máquina (frenos del motor, cierre de válvulas, etc.).

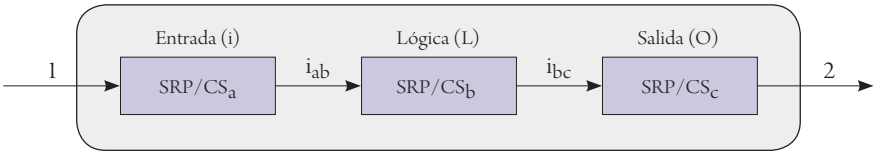

Figura 3. **Representación de las partes de un sistema de mando**

Determinación del PL

El PL se define como la capacidad de una parte relacionada con la seguridad del sistema de mando de una máquina para ejecutar la función de seguridad y mitigar el riesgo deseado. El PL se divide en niveles desde la *a* hasta la *e*, donde *a* representa un nivel de confiabilidad bajo y *e* representa el nivel más alto. Se debe realizar una estimación del nivel de PL para cada una de las partes del sistema de mando relativas a la seguridad o cada combinación de estas partes que formen una función de seguridad. Los aspectos cuantificables para la determinación del PL y que influyen en las partes del sistema de mando relativas a la seguridad, son:

- La estructura del sistema (categoría): determina el nivel de confiabilidad requerido.
- MTTFd (tiempo medio hasta fallo peligroso) del conjunto: valor que cuantifica la confiabilidad de los componentes.
- Cobertura del diagnóstico (DC): da una idea de la confiabilidad gracias al diagnóstico.
- Medidas contra los fallos de causa común (CCF): representa la inmunidad del sistema a fallos que afectan a más de un canal.

Categorías designadas por la norma EN ISO 13849-1

Las partes del sistema de mando relativas a la seguridad deben estar relacionadas con una o varias de cinco categorías. Dichas categorías son parámetros utilizados para la obtención de un PL específico con base en las consideraciones de diseño. La determinación de estas categorías depende de: la reducción del riesgo por

obtener mediante la función de seguridad, el nivel de prestación requerido (PLr), la tecnología utilizada, la posibilidad de evitar uno o varios defectos, el tiempo medio hasta fallo peligroso (MTTFd), la cobertura de diagnóstico (DC) y los fallos de causa común (CCF) en el caso de las categorías 2, 3 y 4. A continuación se describen las categorías.

Categoría B

Las partes deben ser diseñadas, construidas, seleccionadas, montadas y combinadas de acuerdo con las normas pertinentes y usando los principios de seguridad básicos para la aplicación considerada, de manera que puedan resistir las solicitudes de funcionamiento, la influencia externa y de los materiales procesados. Es una estructura monocanal donde no existe cobertura de diagnóstico (DCavg = 0), el MTTFd debe ser medio o bajo para cada canal y no se exigen medidas para los fallos de causa común. El máximo PL alcanzable es PL = b (figura 4).

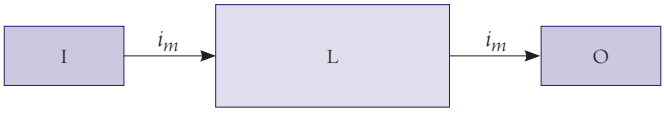

Figura 4. **Arquitectura designada en categoría B**

Categoría 1

Además de los requisitos de la categoría B, debe ser diseñada y construida usando componentes de eficacia probada en seguridad y con principios que demuestren pertinencia y fiabilidad para aplicaciones relativas a seguridad. Al ser estructura monocanal no tiene en cuenta fallos por causa común y la cobertura de diagnóstico no es relevante (DCavg = 0). Es necesario un MTTFd alto para cada canal, por lo que la pérdida de seguridad es menos probable (figura 5).

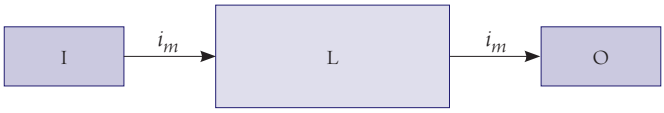

Figura 5. **Arquitectura designada en categoría 1**

Categoría 2

Además de los requisitos de la categoría B, debe ser diseñada y construida utilizando componentes y principios de eficacia probada en seguridad. Solo se deben tener en cuenta los bloques de canal funcional para el cálculo del MTTFd y del DCavg. La cobertura de diagnóstico de todo el SRP/CS debe ser baja, el MTTFd debe ser entre bajo a alto, dependiendo del nivel de prestaciones requerido, y se deben aplicar medidas contra los CCF. El máximo nivel es PL = d. Posee equipos de chequeo (TE) con la papel principal de comprobar la función de seguridad.

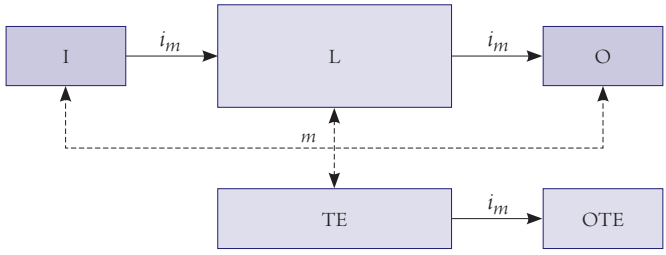

Figura 6. **Arquitectura designada en categoría 2**

En la figura 6, *m* es la supervisión, TE es el equipo de chequeo y OTE la salida de TE; la línea discontinua representa detección de defectos razonablemente factibles.

Categoría 3

Además de los requisitos de la categoría B, debe ser diseñada y construida utilizando componentes y principios de eficacia probada en seguridad. Por ser doble canal, un solo defecto en cualquiera de las partes no conduce a la pérdida de la función de seguridad. La acumulación de defectos no detectados puede entrañar una salida imprevista y una situación peligrosa en la máquina. La cobertura de diagnóstico (DCavg) debe ser baja para todas las partes del sistema de mando relativas a la seguridad, el MTTFd puede ser alto, medio o bajo dependiendo del PLr, y es necesario aplicar medidas contra los fallos por causa común (figura 7).

Categoría 4

Además de los requisitos de la categoría B, debe ser diseñada y construida utilizando componentes y principios de eficacia probada en seguridad. Las partes

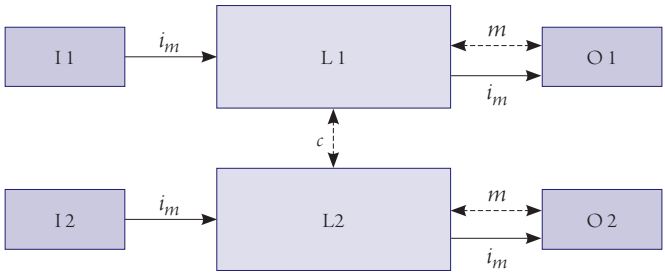

Figura 7. **Arquitectura designada en categoría 3**

deben ser diseñadas de tal forma que un solo defecto en cualquiera de estas no ocasione la pérdida de la función de seguridad. Se debe detectar dicho defecto al instante de producirse o antes de la siguiente solicitud de la función de seguridad; si la detección no se presenta, la acumulación de los defectos no deberá conducir a la pérdida de la función de seguridad. Se exige una cobertura de diagnóstico alta para el conjunto de todas las partes del SRP/CS, un MTTFd alto en cada uno de los canales, además de poseer y aplicar medidas contra los CCF (figura 8). La línea discontinua en la supervisión representa una cobertura de diagnóstico mayor que la designada en la categoría 3.

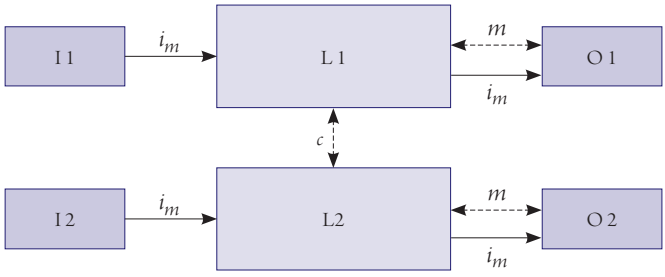

Figura 8. **Arquitectura designada en categoría 4**

Tiempo medio hasta fallo peligroso (MTTFd)

El MTTFd representa el valor en años del tiempo medio hasta un fallo peligroso de cada canal de alguno de los componentes del sistema de mando relativos a la seguridad. Se clasifica en tres niveles, como se muestra en la tabla 1. El valor está entre 3 y 100 años para el canal completo.

Tabla 1. **Descripción de calidad mediante rangos de MTTFd**

Descripción de la calidad	Rango de valores de MTTFd
Baja	3 años ≤ MTTFd ≤ 10 años
Media	10 años ≤ MTTFd ≤ 30 años
Alta	30 años ≤ MTTFd ≤ 100 años

No se consideran MTTFd menores de 3 años ya que esto significaría que, tras un año, el 30 % de los sistemas en el mercado deberían ser sustituidos. Al considerar el MTTFd se asume una distribución exponencial del fallo coincidente, es decir, después de la secuencia del MTTFd, el 63 % de todas las unidades han fallado y la probabilidad de supervivencia es de solo el 37 %.

Verificación PL ≥ PLr (requerido)

Se deben satisfacer los niveles de prestaciones requeridos (PLr) para cada función de seguridad individual. El PL de las diferentes partes del sistema de mando referente a la seguridad debe ser superior o igual al nivel requerido obtenido mediante árbol de selección.

Nivel integral de seguridad (SIL)

El término SIL representa un nivel de tolerancia hacia los fallos, o el riesgo que debe ser reducido o cubierto. Los niveles SIL aplicables en el sector de las maquinarias son numerados entre el 1 y el 3, siendo el SIL 3 el más alto. Existen riesgos mayores que no pueden contenerse dentro de las anteriores categorías, los cuales ocurren dentro de sectores como la industria de procesos y las plantas nucleares, por esta razón la norma IEC 61508 incluye la categoría SIL 4. La estimación de este riesgo es un proceso iterativo para verificar el cumplimiento de todos los requisitos necesarios.

Cadenas de Markov (CM)

Las cadenas de Markov son un tipo especial de proceso estocástico discreto en el que la probabilidad de que ocurra un evento depende del evento inmediatamente anterior, como dicen Zapata (2011), Torres (1996) y Lawyer (1995). Las cadenas de este tipo recuerdan el último evento, lo cual condiciona las posibilidades

de los eventos futuros. Una CM posee un conjunto de estados $S = \{S_1, S_2, \ldots S_r\}$, el proceso se inicia en uno de estos estados y se mueve sucesivamente de uno a otro. Cada movimiento se llama un paso, si la cadena se encuentra en el estado S_i, a continuación se mueve en un paso a S_j con probabilidad P_{ij} y esta probabilidad no depende de los estados de la cadena antes de la situación actual.

Una CM representa un sistema que varía su estado a lo largo del tiempo, siendo cada cambio una transición del sistema. Dichos cambios no están predeterminados, aunque sí lo está la probabilidad del próximo estado en función de los estados anteriores, la cual es constante a lo largo del tiempo. Una CM es una secuencia X_1, X_2, X_3, ... de variables aleatorias cuyo rango se denomina espacio de estado. El valor de X_n es el estado del proceso en el tiempo n. Si la distribución de probabilidad condicional de X_{n+1} en estados pasados es una función de X_n, entonces:

$$P(X_{n+1} = x_{n+1} \mid X_n = x_n, X_{n-1} = x_{n-1}, \ldots, X_1 = x_1) = P(X_{n+1} = x_{n+1} \mid X_n = x_n) \qquad (1)$$

Modelado para la seguridad

La seguridad es la probabilidad de que un sistema funcione o falle de modo seguro. Se modela con una cadena de Markov definiendo dos estados de fallo: el fallo seguro (FS) y el fallo inseguro (FI). La figura 9 muestra el modelo con tasa de avería λ y cobertura de detección de fallos C. Los fallos seguros son aquellos detectables por los autodiagnósticos de la cobertura y los inseguros son los no detectables. La seguridad del sistema en un instante de tiempo, S(t), es la probabilidad de tener el sistema funcionando (estado O) o en un fallo seguro (FS) como mencionan Mechri, Simon, Ben Othman y Benrejeb (2011).

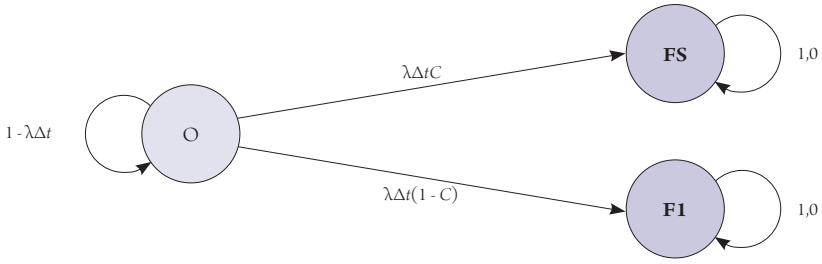

Figura 9. **Diagrama del modelo para la seguridad mediante cadenas de Markov**

$$S(t) = P_0(t) + P_{FS}(t) \tag{2}$$

Donde se tiene el siguiente sistema de acuerdo con la matriz de transiciones:

$$\begin{bmatrix} P_0(t+\Delta t) \\ P_{FS}(t+\Delta t) \\ P_{FI}(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-\lambda\Delta t & 0 & 0 \\ \lambda\Delta tC & 1 & 0 \\ \lambda\Delta t(1-C) & 0 & 1 \end{bmatrix} \begin{bmatrix} P_0(t) \\ P_{FS}(t) \\ P_{FI}(t) \end{bmatrix} \tag{3}$$

Y las ecuaciones del proceso extraídas de estas matrices son:

$$P_0(t+\Delta t) = (1-\lambda\Delta t)P_0(t) \tag{4}$$

$$P_{FS}(t+\Delta t) = (\lambda\Delta tC)P_0(t) + P_{FS}(t) \tag{5}$$

$$P_{FI}(t+\Delta t) = \lambda\Delta t(1-C)P_0(t) + P_{FI}(t) \tag{6}$$

Por tanto, la seguridad del sistema, S(t), es directamente dependiente de la cobertura de detección de fallos.

Modelado para la disponibilidad

La disponibilidad es la probabilidad de que un sistema se pueda utilizar para realizar sus funciones en un instante *t*. Conociendo el MTTF (tiempo medio hasta fallo igual a $\frac{1}{\lambda}$), el MTBF (tiempo medio entre fallos) y el MTTR (tiempo medio para reparación igual a $\frac{1}{\mu}$), y con N fallos durante el tiempo de vida (figura 10), entonces se define la disponibilidad de estado constante (DEC) como:

$$DEC = \frac{MTTF}{MTBF} = \frac{N(MTTF)}{N(MTTF)+N(MTTR)} = \frac{MTTF}{MTTF+MTTR} = \frac{\mu}{\mu+\lambda} \tag{7}$$

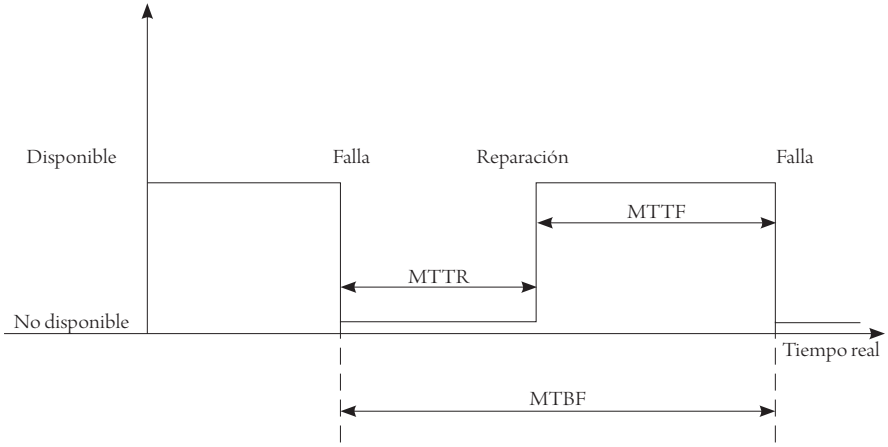

Figura 10. **Diagrama de MTTF, MTTR y MTBF**

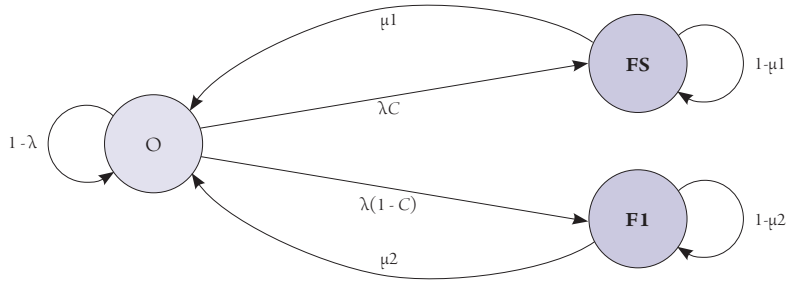

Figura 11. **Modelo para la disponibilidad mediante cadenas de Markov**

Este modelo es completamente asimilable con el modelo para la seguridad en el cual el sistema se repara como mencionan Castellano y Sánchez (2013). Para este caso se tiene el siguiente sistema de acuerdo con la matriz de transiciones:

$$\begin{bmatrix} P_0(t+\Delta t) \\ P_{FS}(t+\Delta t) \\ P_{FI}(t+\Delta t) \end{bmatrix} = \begin{bmatrix} 1-\lambda\Delta t & \mu_1 & \mu_2 \\ \lambda\Delta t C & 1-\mu_1 & 0 \\ \lambda\Delta t(1-C) & 0 & 1-\mu_2 \end{bmatrix} \begin{bmatrix} P_0(t) \\ P_{FS}(t) \\ P_{FI}(t) \end{bmatrix} \quad (8)$$

Las ecuaciones del proceso extraídas de estas matrices son:

$$P_0(t+\Delta t) = (1-\lambda\Delta t)P_0(t) + \mu_1 P_{FS}(t) + \mu_2 P_{FI}(t) \quad (9)$$

$$P_{FS}(t+\Delta t) = (\lambda\Delta t C)P_0(t) + (1-\mu_1)P_{FS}(t) \quad (10)$$

$$P_{FI}(t+\Delta t) = \lambda\Delta t(1-C)P_0(t) + (1-\mu_2)P_{FI}(t) \quad (11)$$

La disponibilidad del sistema, D(t), es:

$$D(t) = P_0(t) + P_{FS}(t) \quad (12)$$

Resultados

Análisis de arquitecturas mediante cadenas de Markov

Teniendo en cuenta los requisitos de cada una de las arquitecturas disponibles en la norma EN ISO 13849-1 se plantean modelos de Markov como cadenas de disponibilidad mediante las cuales se puede observar el funcionamiento de cada una de las arquitecturas y las categorías que se presentan. Los modelos de Markov serán planteados con valores para estados de falla detectada (FD), falla no detectada (FU), funcionamiento normal o adecuado (OK) (figura 11). Las transiciones en cada modelo de Markov representan las probabilidades de falla de algún dispositivo (λ) y las probabilidades de que el dispositivo se recupere de la falla, como mencionan Ecay (2007) y Hildebrandt (2007). En la reparación interviene el tiempo medio de reparación y el intervalo de prueba de diagnóstico (T2). Se tiene presente que algunas arquitecturas reconocen los fallos por causa común, los cuales serán tratados como fallos que no pueden ser detectados, con probabilidad β. Se debe tener en cuenta que las matrices que se presentan a continuación se expresan en su forma transpuesta.

Modelo de Markov para las categorías B Y 1

Para estos dos tipos de categorías se deben tener en cuenta los requisitos de la tabla 2.

En este modelo de Markov los fallos son no detectados, por consiguiente es necesario que se aplique el factor T2 de pruebas de diagnóstico (figura 12).

Tabla 2. **Requisitos para los modelos de Markov de las categorías B y 1**

Modelo para la categoría B	Modelo para la categoría 1
• DCavg: no exige (igual a 0)	• DCavg: no exige (igual a 0)
• MTTFd: medio o bajo para cada canal	• MTTFd: alto para cada canal
• CCF: no relevante	• CCF: no relevante

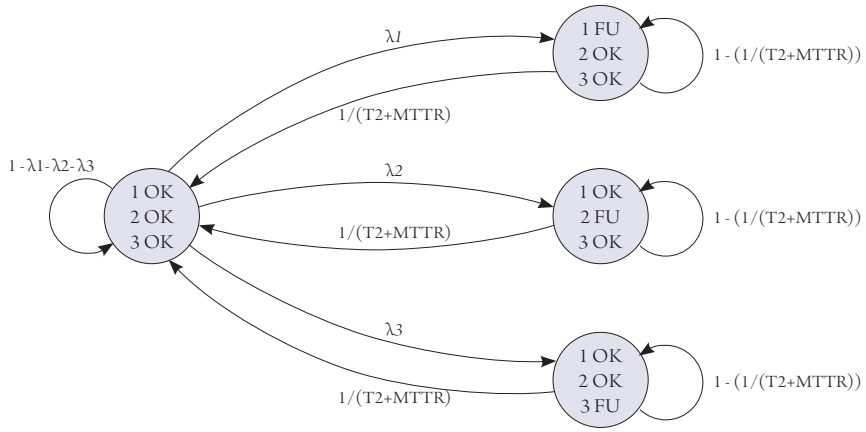

Figura 12. **Modelo de Markov para las categorías B y 1**

La cadena está compuesta por cuatro estados, donde el primero se compone de los tres elementos que funcionan de manera adecuada (OK). Los tres elementos que se tienen son: entrada, lógica y salida. A los demás estados es posible llegar cuando se presenta un fallo en alguno de los elementos. Si se presenta una falla se marca un nuevo estado con un fallo no detectado (FU) con probabilidad representada por la tasa de fallo de cada uno de los elementos. Al ser un modelo de disponibilidad, el valor de μ puede verse expresado por 1/MTTR. Al MTTF es necesario sumarle T2 debido a que es un fallo no detectado. Las transiciones que salen y entran al mismo estado expresan la probabilidad que tiene el sistema de permanecer en ese estado, y teniendo presente que el máximo es del 100 %, se obtienen las probabilidades salientes de restar de dicho 100 %. Con el modelo anterior se puede obtener la siguiente matriz de transiciones:

$$\begin{bmatrix} 1-\lambda 1-\lambda 2-\lambda 3 & \lambda 1 & \lambda 2 & \lambda 3 \\ \frac{1}{T2+MTTR} & 1-\frac{1}{T2+MTTR} & 0 & 0 \\ \frac{1}{T2+MTTR} & 0 & 1-\frac{1}{T2+MTTR} & 0 \\ \frac{1}{T2+MTTR} & 0 & 0 & 1-\frac{1}{T2+MTTR} \end{bmatrix} \quad (13)$$

Modelo de Markov para la categoría 2

Para esta categoría se deben tener en cuenta los siguientes requisitos:

- DCavg: bajo.
- MTTFd: medio, alto o bajo, dependiendo del PLr.
- CCF: relevante.

En este modelo (figura 13) solo se tienen en cuenta los canales funcionales y no los de comprobación; además, al tener los canales de comprobación los fallos que se presentan son detectados y, por consiguiente, no se hace necesaria la aplicación de las pruebas de diagnóstico; estas pruebas únicamente se utilizan para los fallos por causa común, ya que no es posible detectarlos. La cadena de Markov está compuesta por cinco estados, similares al modelo de las categorías B y 1, con la diferencia de que se presenta un estado extra, el cuál es el estado de fallos por causa común. Para llegar al estado FCC es necesario pasar por la transición β, la cual representa la probabilidad que existe de tener un fallo por causa común en todo el sistema. Las transiciones entre el estado de no falla y los estados de falla están expresados por dos probabilidades: la probabilidad de que dicho elemento falle (λ) y la probabilidad de que no se presente un fallo por causa común (1 – β), las cuales se multiplican a fin de obtener la probabilidad total que existe para que se pase de un estado bueno a uno de falla.

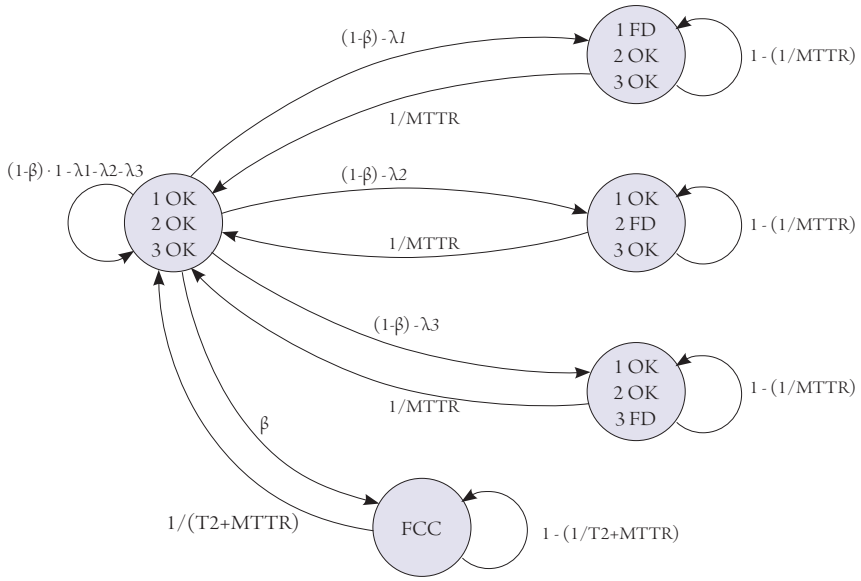

Figura 13. **Modelo de Markov para la categoría 2**

La matriz de transiciones para el modelo anterior es:

$$\begin{bmatrix} (1-\beta)(1-\lambda 1-\lambda 2-\lambda 3) & (1-\beta)\lambda 1 & (1-\beta)\lambda 2 & (1-\beta)\lambda 3 & \beta \\ \frac{1}{MTTR} & 1-\frac{1}{MTTR} & 0 & 0 & 0 \\ \frac{1}{MTTR} & 0 & 1-\frac{1}{MTTR} & 0 & 0 \\ \frac{1}{MTTR} & 0 & 0 & 1-\frac{1}{MTTR} & 0 \\ \frac{1}{T2+MTTR} & 0 & 0 & 0 & 1-\frac{1}{T2+MTTR} \end{bmatrix} \quad (14)$$

Modelo de Markov para las categorías 3 y 4

Para estos dos tipos de categorías se deben tener en cuenta los requisitos de la tabla 3.

Tabla 3. **Requisitos para los modelos de Markov de las categorías 3 y 4**

Modelo para la categoría 3	Modelo para la categoría 4
• DCavg: bajo	• DCavg: alto para todas las partes
• MTTFd: alto o medio, según el PLr	• MTTFd: alto
• CCF: relevante y necesario	• CCF: relevante y necesario

Esta cadena de Markov modela doble canal y se debe tener en cuenta que es necesario tener 2 fallas para perder la función de seguridad diseñada. El modelo se muestra en la figura 14, las equivalencias para los símbolos usados se indican en la tabla 4.

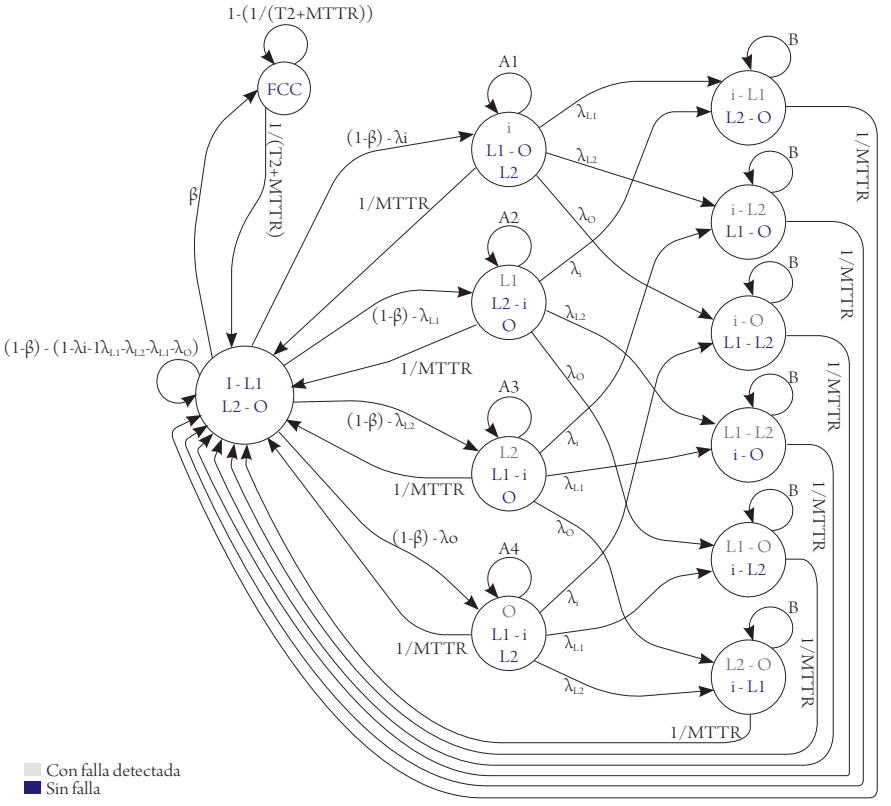

Figura 14. **Modelo de Markov para las categorías 3 y 4**

Tabla 4. **Equivalencias de símbolos para la figura 14**

Símbolo	Equivalencia
A0	(1-β)(1-λi - λL1 - λL2 - λo)
A1	1-(1/MTTR)- λ L1 - λ L2 - λo
A2	1-(1/MTTR)- λi - λ L2 - λo
A3	1-(1/MTTR)- λi - λ L1 - λo
A4	1-(1/MTTR)- λi - λL1 - λL2
B	1- (1/MTTR)

En la figura 14, con color gris se muestran las fallas detectadas en todo el sistema, con excepción de las fallas por causas comunes, las cuales siempre serán no detectadas. En cada estado se encuentran cuatro partes del sistema: dos componentes de lógica que operan por separado y el conjunto de componentes de entrada y salida. La cadena en general consta de doce estados, de los cuales se pueden destacar cuatro conjuntos: el primero es un estado de funcionamiento correcto del sistema donde se tienen todos los elementos trabajando; el segundo es el estado de falla por causa común; el tercer grupo está conformado por cuatro estados en los cuales se tienen fallas en un único elemento, pero al ser de categoría tres o cuatro el sistema conserva su función de seguridad permitiendo que opere con normalidad; el cuarto grupo está conformado por seis estados en los cuales después de un fallo se presenta otro, haciendo que automáticamente se pierda la función de seguridad lo que obliga a que el sistema tenga que ser reparado y así volver al estado inicial. En caso de que se tengan dos elementos en falla se puede tomar un mayor tiempo de reparación debido a que se pueden reparar los dos a la vez en forma paralela. En este caso también es necesario tener en cuenta que para las primeras transiciones, es decir, entre el estado donde el funcionamiento es correcto y los estados donde se presenta un solo fallo se debe aplicar el factor $(1 - \beta)$ que influye en la probabilidad de que se presente un fallo en un único elemento del sistema. Como el sistema no fluye de estado a estado de manera permanente, también es necesario tener en cuenta las probabilidades de que este permanezca en un mismo estado, esto se representa mediante las transiciones que salen y entran de un estado. La matriz de transiciones de esta cadena se muestra a continuación:

$$\begin{bmatrix}
A0 & (1-\beta)\lambda i & (1-\beta)\lambda L1 & (1-\beta)\lambda L2 & (1-\beta)\lambda_0 & 0 & 0 & 0 & 0 & 0 & 0 & \beta \\
\frac{1}{MTTR} & A1 & 0 & 0 & 0 & \lambda L1 & \lambda L2 & \lambda_0 & 0 & 0 & 0 & 0 \\
\frac{1}{MTTR} & 0 & A2 & 0 & 0 & \lambda i & 0 & 0 & \lambda L2 & \lambda_0 & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & A3 & 0 & 0 & \lambda i & 0 & \lambda L1 & 0 & \lambda_0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & A4 & 0 & 0 & \lambda i & 0 & \lambda L1 & \lambda L2 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & B & 0 & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & B & 0 & 0 & 0 & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & B & 0 & 0 & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & B & 0 & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & B & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & B & 0 \\
\frac{1}{T2+MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\frac{1}{T2+MTTR}
\end{bmatrix} \quad (15)$$

Ejemplo de aplicación

Se aplica la metodología a un sistema de parada de emergencia para un motor trifásico que presenta una avería potencialmente peligrosa. El sistema está diseñado con dispositivos de seguridad y consta de dos pulsadores de parada, dos PLC de seguridad que controlan las entradas y las salidas del sistema y, por último, dos relés de seguridad que se encargan de la desconexión total del motor (figura 15).

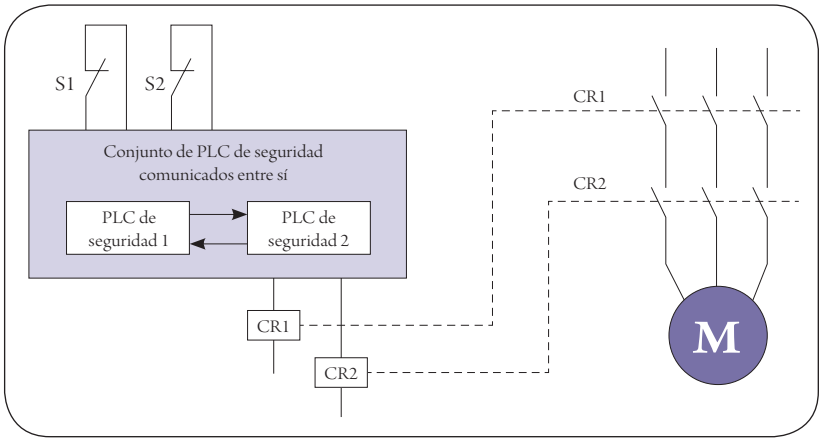

Figura 15. **Esquema de paro de emergencia de un motor trifásico**

Procedimiento para la solución según la norma EN ISO 13849-1

La categoría para el sistema es 3. Se inicia encontrando el PLr mediante el respectivo árbol de selección, con las siguientes condiciones:

- Importancia de los daños (S): un nivel S2 donde se puede ocasionar una lesión grave (irreversible) y hasta la muerte en caso de que no se pueda detener.
- Frecuencia o tiempo de exposición (F): se tiene F2 debido a la larga exposición, ya que es una máquina usada a diario.
- Probabilidad de evitar el peligro o al menos minimizar los daños (P): es P1 ya que es posible evitar el riesgo en ciertas condiciones.

El árbol resultante se muestra en la figura 16, donde PLr = d.

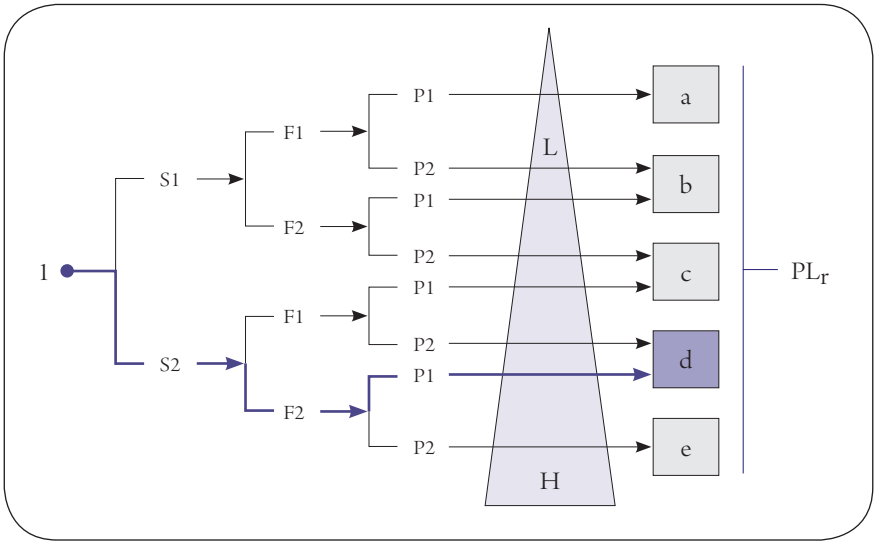

Figura 16. **PLr del paro de emergencia de una maquina trifásica**

Lo siguiente es verificar los datos de reparación y las tasas de fallos del sistema; para el presente ejemplo se emplean los datos de la tabla 5.

Tabla 5. **Datos de MTTR y tasas de fallos para ejemplo**

Elemento por considerar	MTTR [horas]	λ [fallas/hora]
Pulsadores S1 y S2	32	$1{,}60 \times 10^{-10}$
PLC1 y PLC2	160	$2{,}00 \times 10^{-9}$
Contactores CR1 y CR2	95	$1{,}35 \times 10^{-8}$
Fallos por causa común	200	

El valor T2 de intervalos de diagnóstico para FCC es de 24 horas para identificar los fallos por causa común:

Separación/Segregación = 15 puntos

Diversidad = 20 puntos

Diseño/Aplicación/Experiencia = 20 puntos

Competencia/Formación = 5 puntos

Ambiental = 25 puntos

Otras influencias = 10 puntos

Con estas puntuaciones se obtiene un total de 95 puntos y se tiene un factor de falla por causa común de $\beta = 0{,}1\ \%$. Para la cobertura de diagnóstico se tiene: 99 % en la entrada, 90 % en la lógica, 90 % en la salida. De los tres anteriores se elige el más bajo, debido a que corresponde al peor caso, y $90\ \% \leq DC < 99\ \%$. El PFH_d se puede obtener para la categoría 3-4 a partir de la cadena de Markov de la figura 17.

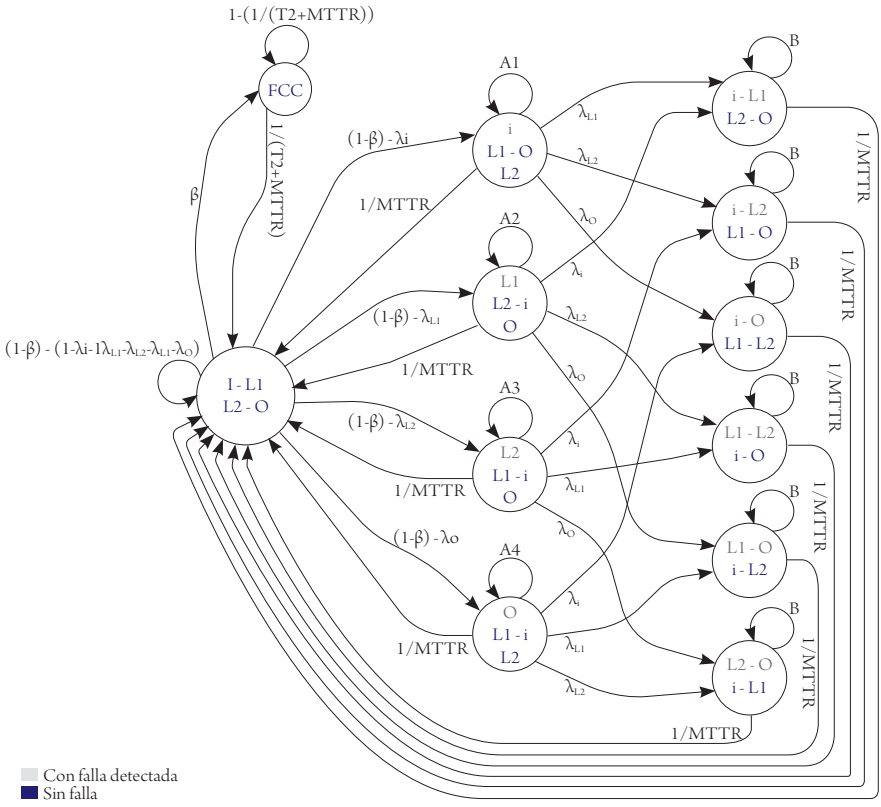

Figura 17. **Cadena de Markov para el ejemplo**

$$PFH_d = (1-\beta) * \left[\lambda_i * \left(\frac{1}{MTTR} \right)_i + \lambda_{L1} * \left(\frac{1}{MTTR} \right)_{L1} + \lambda_{L2} * \left(\frac{1}{MTTR} \right) + \lambda_0 * \left(\frac{1}{MTTR} \right) + \beta * \left(\frac{1}{T_2 + MTTR} \right)_\beta \right] = 4,4645 \times 10^{-6} \; Fallos / Hora \quad (16)$$

El valor del MTTFd para todo el sistema, transformado a años y luego categorizado, es de 25,9658 años. En la figura 18 se determina el PL de todo el sistema, donde PL=d. Esta parte del ejercicio se apoya en el anexo K de la norma, con la intención de tener un valor exacto.

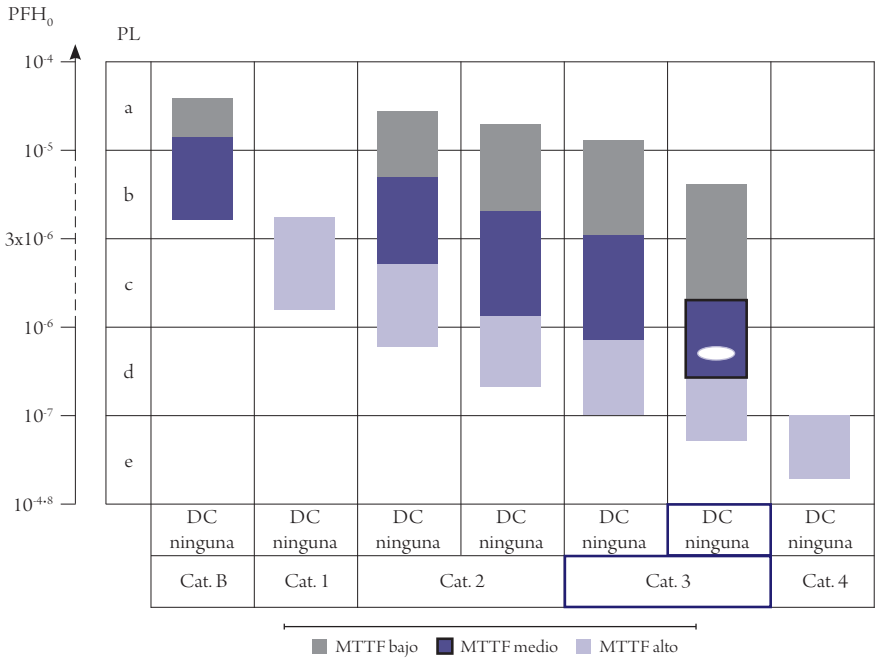

Figura 18. **Obtención del PL del ejemplo**

Por último, solo queda verificar que PL ≥ PLr. Entonces se tiene que d ≥ d.

Se puede concluir que el sistema está protegido bajo una categoría de PL = d. Con esto se puede proceder a la validación de la función de seguridad, la cual deberá ser realizada por personal diferente a los encargados del diseño de dicha función para garantizar la imparcialidad.

Conclusiones

Los requerimientos especificados por la norma EN ISO 13849-1 indican las pautas que se deben seguir con el fin de abarcar parámetros de diseño en la seguridad funcional, y los cuales se determinan por categorías y subsistemas según los elementos y las configuraciones de mando relativas a seguridad implementadas.

Se determinaron indicadores de la norma EN ISO 13849-1 que cubren una serie de parámetros cuantitativos y cualitativos, estos se implementan con base en la

necesidad de la industria de contar con parámetros accesibles, tales como la tasa media de fallo y las probabilidades de falla de cada uno de los elementos que conforman un sistema de mando.

Es posible construir cadenas de Markov con base en modelos para la disponibilidad que describen las arquitecturas y categorías en la norma EN ISO 13849-1. Estos modelos se basan exclusivamente en conceptos cualitativos y cuantitativos. Se resalta que no todos los modelos, las categorías o los subsistemas reconocen los fallos de causa común, o fallos no detectados. Además, cada categoría y subsistema maneja sus propios requerimientos.

Es posible plantear un procedimiento general para la obtención de un modelo de Markov definiendo grupos de estados según el sistema opere correctamente, tenga un fallo de causa común, tenga la falla de un único elemento o se pierda la función de seguridad. Este procedimiento se aplica de manera puntual con el ejemplo de paro de emergencia en un motor trifásico.

Referencias

ABB Jokab Safety (2011). *Seguridad en sistemas de control según la norma EN ISO 13849-1*. Barcelona: Asea Brown Boveri S.A., Low Voltage Products.

BS EN 62061:2005 (2005). *Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems*.

Castellano, R. y Sánchez, M. (2013). Modelos de Markov: análisis de reparaciones imperfectas en sistemas de control para seguridad. *Mecánica Computacional*, XXII.

Directiva de Máquinas 2006/42/CE (2010). *Seguridad y fiabilidad de los sistemas de mando de máquinas e instalaciones automatizada* [Norma EN ISO 13849-1].

Ecay, H. (2007). *e-PIC Ingeniería de la Confiabilidad Industrial*. Buenos Aires: Universidad Austral.

Hildebrandt, A. (2007). *Calculating the "Probability of Failure on Demand" (PFD) of complex structures by means of Markov Models*. Pepperl+Fuchs.

Interempresas (2012). *Nuevas normativas de seguridad EN 62061 y EN ISO 13849-1*. Recuperado de: http://www.interempresas.net/MetalMecanica/Articulos/21049-Nuevas-Normativas-de-Seguridad-EN-62061-y-EN-ISO-13849-1.html.

ISO 13849-1:2006 (2006). *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design*. ISO 13849-1:2006/Cor 1:2009.

Lawyer, G. F. (1995). *Introduction to Stochastic Processes*. New York: Chapman and Hall.

Mechri, W., Simon, CH., Ben Othman, K. y Benrejeb, M. (2011). *Uncertainty evaluation of Safety Instrumented Systems by using Markov chains*. Milano: International Federation of Automatic Control IFAC World congress.

Pilz Automation Technology (2012). *De la EN 954-1 a la EN ISO 13849-1*. Recuperado de: http://eshop.pilz.com/company/news/sub/services/articles/05066/ index.es.jsp.

Torres, A. (1996). *Probabilidad, variables aleatorias, confiabilidad y procesos estocásticos en ingeniería eléctrica*. Bogotá: Universidad de los Andes.

Zapata, C. J. (2011). *Procesos estocásticos, confiabilidad de sistemas eléctricos*. Pereira: Universidad Tecnológica de Pereira.