MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES ESPAÑA
INSTITUTO NACIONAL DE SEGURIDAD E HIGIENE EN EL TRABAJO

NTP 328: Análisis de riesgos mediante el árbol de sucesos

Arbre d'êvenements pour l'analyse des risques
Event tree risk analysis

Redactor:

Manuel Bestratén Belloví
Ingeniero Industrial

CENTRO NACIONAL DE CONDICIONES DE TRABAJO

El árbol de sucesos es una sencilla técnica de análisis cualitativo y cuantitativo de riesgos que permite estudiar procesos secuenciales de hipotéticos accidentes a partir de sucesos iniciales indeseados, verificando así la efectividad de las medidas preventivas existentes.

Introducción

Existen diversas técnicas para el desarrollo de estudios de seguridad que aplican sistemas de árboles para considerar las cadenas causales de acontecimientos que llegan finalmente a materializarse en accidentes.

Es importante su distinción ya que sus finalidades y aplicaciones son bien diferentes.

El "árbol causal" es una técnica ya tratada en la anterior Nota Técnica de Prevención 274.91 que permite, a partir de un accidente real ya sucedido, investigar sobre las circunstancias desencadenantes que han confluido en el mismo a fin de determinar sus causas primarias.

Como cada accidente es único, el árbol causal también reproducirá con fidelidad tan solo lo que sucedió y no lo que pudiera haber acontecido adicionalmente.

Muy diferente sucede con la técnica denominada "árbol de fallos y errores" tiene como objetivo reproducir todas las vías posibles que puedan conducir a un acontecimiento final antes de que éste suceda.

Ante un determinado y posible accidente (normalmente grave) que puede ser generado por una multiplicidad de causas y circunstancias adversas, trata de conocer todas las posibles vías desencadenantes, identificando los fallos básicos y originarios.

La probabilidad de materialización de tales fallos también deberá ser averiguada, para poder estimar cuál es la del acontecimiento final en cuestión. Es, como vemos, una técnica inductiva de tipo cualitativo y cuantitativo, más compleja que la anterior, debido a que incorpora el análisis probabilístico.

El "árbol de sucesos", objetivo de este documento, es una técnica de algún modo complementaria al "árbol de fallos y errores". Esta técnica del árbol de sucesos, desarrolla un diagrama gráfico secuencial a partir de sucesos "iniciadores" o desencadenantes de incidencia significativa y, por supuesto indeseados, para averiguar todo lo que puede acontecer y, en especial, comprobar si las medidas preventivas existentes o previstas son suficientes para limitar o minimizar los efectos negativos. Evidentemente tal suficiencia vendrá determinada por el correspondiente análisis probabilístico que esta técnica también acomete.

El "árbol de sucesos" ha tenido su origen y más amplia aplicación en las industrias nuclear, aeronaútica y química.

Descripción del método

El proceso de desarrollo general de los árboles de sucesos consta de las siguientes etapas:

Cuadro 1: Etapas en el desarrollo de los árboles de sucesos

1. Etapa previa, familiarización con la planta.
2. Identificación de sucesos iniciales de interés.
3. Definición de circunstancias adversas y funciones de seguridad previstas para el control de sucesos.
4. Construcción de los árboles de sucesos con inclusión de todas las posibles respuestas del sistema.
5. Clasificación de las respuestas indeseadas en categorías de similares consecuencias.
6. Estimación de la probabilidad de cada secuencia del árbol de sucesos.
7. Cuantificación de las respuestas indeseadas.
8. Verificación de todas las respuestas del sistema.

Etapa previa, familiarización con la planta

Es imprescindible, antes de iniciar un estudio de este tipo, haber agotado el análisis preliminar de riesgos que permita conocer y controlar la diversidad de situaciones anómalas que puedan acontecer en una instalación, ya sea tanto por factores internos como externos a la misma.

Un estudio documental con la recogida de experiencias sobre instalaciones similares será, junto al análisis histórico de incidentes-accidentes acaecidos, una buena base de partida a ser discutida y analizada conjuntamente por los mandos y trabajadores implicados en el funcionamiento del proceso y por quienes deban conducir la aplicación de esta técnica analítica. Esta es una metodología que requiere ser aplicada en un marco participativo a través de grupos de trabajo establecidos, que conozcan los diferentes aspectos que determinan el funcionamiento correcto o incorrecto de una instalación. Cuanto más compleja sea ésta, mayor deberá ser el soporte documental y la preparación previa del equipo de trabajo.

Identificación de sucesos iniciales de interés

Tras los análisis preliminares de familiarización con la planta es necesario elaborar una lista de sucesos iniciadores lo más completa posible, de acuerdo al alcance del análisis. Dicha lista inicial surgirá principalmente de:

- Los sucesos iniciadores ocurridos en otras plantas.
- La comparación con otros análisis previos realizados.
- El análisis preliminar de sistemas.

Los sucesos iniciadores corresponden a fallos que, de producirse, requieren la respuesta de lo que se denominan sistemas "frontales" de seguridad, para evitar efectos negativos de importancia. Cabe distinguir los sucesos iniciadores propiamente dichos, de otros sucesos que son consecuencia de los primeros, especialmente en esta fase de identificación en la que será imprescindible efectuar también, por necesidad de simplificación, un agrupamiento de sucesos iniciadores de acuerdo a las funciones de seguridad que deben realizarse o a la combinación de respuestas de sistemas.

Definición de las circunstancias adversas y de las funciones de seguridad para el control de sucesos

Una **función de seguridad** es una respuesta activa de previsión o dispositivo, o bien una barrera, capaz de interrumpir la secuencia de un suceso inicial a una consecuencia peligrosa.

Las funciones de seguridad pueden ser de muchos tipos, la mayoría de ellas se caracterizan por su respuesta ante fallos o éxitos de demandas. Algunos ejemplos son:

- Sistemas automáticos de seguridad.
- Alarmas de aviso y la consiguiente respuesta de los operarios.
- Barreras o sistemas de contención para limitar los efectos de un accidente.

Hay que considerar también aquellas circunstancias que puedan tener un papel adverso en el desarrollo secuencial de sucesos. Así por ejemplo, en un derrame de sustancia inflamable:

- Ignición o no ignición de la fuga.
- Explosión o deflagración.
- Líquido derramado en interior de cubeto de retención o no.
- Durante el día o en la noche.
- Condiciones meteorológicas.

Dentro de las funciones de seguridad cabe diferenciar las que son generadas por los sistemas "frontales", que son los sistemas primarios de respuesta ante los sucesos iniciadores, de las que son generadas por los sistemas "soporte" o "redundantes", que son los que deben actuar, ya sea para garantizar la eficacia de los anteriores o bien cuando se produce un fallo de respuesta de éstos. Habrá casos en que será conveniente considerar, en el desarrollo del árbol, todas las funciones de seguridad incluidos los sistemas "soporte". En otros casos no será necesario, siempre que en la respuesta del sistema "frontal" del que dependa se indique la probabilidad real de fallo en el que estaría integrada la fiabilidad de respuesta del conjunto de ambos sistemas.

Tanto las circunstancias potencialmente adversas como las funciones de seguridad previstas han de ser definidas de forma

simplificada siguiendo la secuencia lógica de acontecimiento o intervención en el proceso concatenado de sucesos y consecuencias, y designadas normalmente por letras correlativas del abecedario.

La mayoría de circunstancias y funciones de seguridad son consideradas normalmente de respuesta binaria. Las situaciones intermedias en función de los diferentes rangos de respuesta suelen ser traducidas también a la doble opción. Por ejemplo, una válvula de seguridad que deba abrirse para liberar una sobrepresión en un recipiente, tendrá en el análisis una doble opción: abrirse o no abrirse. La situación de abertura parcial se considerará normalmente como no abertura, ya que las consecuencias desde el punto de vista de la seguridad posiblemente le sean más próximas. A pesar de ello cabría la posibilidad de considerar, si fuera necesario, más de dos situaciones de respuesta de las funciones de seguridad, a costa de complicar el árbol, al ser necesario discernir las probabilidades de acontecimiento de cada una de las opciones, y más aún si en función de éstas debieran intervenir los sistemas "soporte" de seguridad.

El analista debe ser cuidadoso en detallar de forma cronológica, según el orden de intervención, todas las funciones de seguridad previstas. Las circunstancias adversas por su parte aparecerán en el árbol tantas veces como sea necesario, y siempre que puedan afectar a las funciones de seguridad, según lo que pueda ir sucediendo en el tiempo.

Las intervenciones humanas que representan funciones clave de respuesta de seguridad ante fallos deben ser incorporadas en los momentos oportunos.

Construcción de los árboles de sucesos

La representación gráfica del árbol se realiza siguiendo la progresión cronológica de sucesos previsibles, a partir del suceso iniciador considerado, en principio, de interés. Convencionalmente se construye el diagrama de izquierda a derecha.

En línea de cabecera horizontal se indican las diferentes funciones de seguridad y circunstancias a considerar en el orden cronológico esperado, las cuales corresponderán en el desarrollo del árbol con los nudos en los que la respuesta afirmativa se traduce en una línea vertical ascendente y la negativa en una línea descendente, para proseguir luego horizontalmente a cada uno de los sucesivos nudos. Solamente los nudos que afecten materialmente a las consecuencias deberían ser mostrados explícitamente en el árbol de sucesos. Algunas ramas pueden ser más desarrolladas que otras, según necesidades. Las secuencias finales del árbol recogerán las diferentes situaciones de éxito o fracaso.

A fin de facilitar la interpretación de las diferentes vías secuenciales de éxitos y fallos hasta alcanzar los sucesos finales, es conveniente denominara cada función de seguridad con letras correlativas del abecedario, con el mismo orden de actuación esperado. Cuando una función de seguridad actúe favorablemente se representará por ejemplo con la letra B, y cuando falle por B. Así podremos identificar fácilmente las diferentes combinaciones de fallos y éxitos de las funciones de seguridad previstas en el sistema en estudio.

Cabe destacar que el árbol, además de representar el papel que desempeñan las funciones de seguridad y lo favorables o desfavorables que puedan ser las consecuencias finales de cada suceso iniciador, habría de mostrar también los diversos tipos de desenlaces negativos que puedan surgir. Así por ejemplo, una fuga de gas inflamable, podría originar diversas consecuencias finales adversas como: explosión BLEVE, deflagración de nube no confinada, bola de fuego, dispersión segura. Todas ellas habrían en principio de ser reflejadas en el árbol.

Clasificación de las respuestas indeseadas en categorías de similares consecuencias

Uno de los objetivos del árbol es identificar aquellas consecuencias negativas de significativa importancia que puedan acontecer. En tal sentido, y por necesidades de simplificación, aquellos efectos de escasa relevancia no habrían de ser desarrollados en las sucesivas etapas del análisis.

Ante las consecuencias significativas es necesario detenerse en el acontecimiento mismo y estudiar la posible incidencia de factores meteorológicos o ambientales y que no hubieran quedado reflejados en el primer desarrollo del árbol de sucesos, para incorporarlos si cabe.

Muchas consecuencias desarrolladas a través de las diferentes ramas del árbol serán similares (por ejemplo, una explosión puede ser la consecuencia de diversos sucesos en los que estén implicados sustancias inflamables o explosivas). Por ello las respuestas finales indeseadas deben ser clasificadas de acuerdo al tipo de modelo de consecuencias que debe ser estudiado para completar el análisis.

Estimación de la probabilidad de cada secuencia del árbol de sucesos

A cada una de las secuencias del árbol le corresponde una determinada probabilidad de acontecimiento. Consecuentemente la suma de las probabilidades de cada nudo ante las diferentes alternativas valdrá 1,0. Ello será válido tanto para respuesta binaria como múltiple.

Las fuentes de datos de probabilidades pueden ser diversas: registros históricos de incidentes-accidentes, datos de la instalación y de proceso, datos de productos químicos, datos medioambientales y meteorológicos, datos de fiabilidad de componentes, datos de fiabilidad humana y, como no, la opinión de los expertos. Puede ser necesario en algunos casos utilizar la técnica del árbol de fallos para estimar algunas probabilidades, especialmente en sistemas de seguridad que encierren cierta complejidad en conocer su capacidad de respuesta.

En algunos casos, ya sea porque no se disponga de datos precisos o porque es suficiente disponer sólo de una cuantificación orientativa, los datos probabilísticos a emplear tendrán un valor aproximado. Pero en todo caso es imprescindible disponer siempre de tal información. El mayor o menor rigor en el dato de probabilidad estará en función de la gravedad de las consecuencias resultantes.

Cuantificación de las respuestas indeseadas

La frecuencia de cada una de las posibles consecuencias podrá ser determinada por el producto de la frecuencia del suceso inicial y de cada una de las probabilidades de los sucesos intermedios.

Como comprobación, la suma de todas las frecuencias de las diferentes consecuencias, tanto las favorables como las desfavorables, debe coincidir con la frecuencia del suceso inicial. El tratamiento sería más complejo si hubiera dependencia entre los diferentes sucesos o hubiera situaciones de parcial éxito o fracaso.

Si lo que nos interesa es determinar la probabilidad conjunta de consecuencias negativas, al margen de su individualizada importancia, deberemos efectuar la adición de frecuencias de todas estas. Ello tendrá sentido normalmente cuando la magnitud de las consecuencias negativas sea similar.

Por motivos de simplificación y cuando se pretenden valores orientativos en el cálculo de la probabilidad de cada acontecimiento final indeseado, se multiplican exclusivamente las probabilidades de fallo de las diferentes secuencias, despreciando las probabilidades de éxito.

Verificación de todas las respuestas del sistema

Debido a la limitación de datos disponibles o a incorrecciones en la aplicación del método en el proceso estudiado, al haberse omitido importantes ramas del árbol, pueden alcanzarse resultados del árbol incorrectos.

Para evitarlo es fundamental cubrir adecuadamente esta etapa final de verificación de resultados, aplicando el sentido común y contrastando con datos históricos. Si ello es realizado por alguien, conocedor del proceso analizado pero independiente del grupo de trabajo, mucho mejor.

Ejercicios

Ejercicio 1: Árbol de sucesos para un suceso inicial de pérdida de agua de refrigeración en proceso químico exotérmico

Se trata de estudiar las condiciones de seguridad de un reactor químico que dispone de los siguientes sistemas de control térmico frente a procesos exotérmicos:

Un indicador de temperatura visual en el área de trabajo, un indicador de temperatura con alarma al alcanzarse la temperatura T, y finalmente un indicador de la temperatura máxima T_2 asociado a un sistema automático de cierre de la válvula de entrada de materias primas al reactor.

Por motivos de simplificación se han integrado en el árbol algunas funciones de seguridad en una sola. Así, la función B "Detección y actuación del operario" integra tres funciones de seguridad: que el indicador de temperatura funcione correctamente, que el operario visualice en el momento oportuno la lectura y finalmente que el operario actúe correctamente, tras observar que aquella es superior a la normalmente esperada.

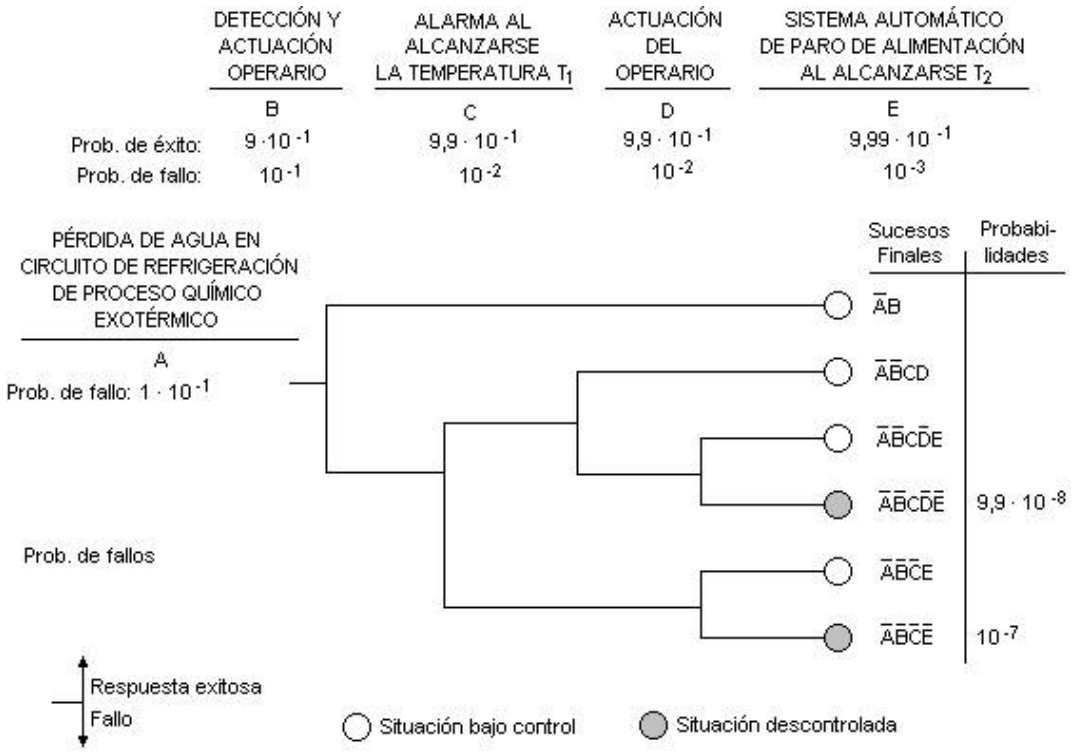
Por tanto, cuando se indica que tal función tiene una probabilidad de fallo de 10^{-1} (muy alta) se entiende que esta representa la adición de las correspondientes probabilidades de los susodichos posibles fallos, ya que con cualquiera de ellos en último término el operario no actuaría, ya sea porque no se entera de lo que acontece o porque omite hacerlo.

Téngase en cuenta que cuando un acontecimiento final requiere la conjunción o simultaneidad de varios fallos, su probabilidad resultante es igual al producto de las probabilidades de cada uno de tales fallos.

En cambio, cuando un acontecimiento indeseado puede tener lugar de varias formas diferentes, su probabilidad de materialización es igual a la suma de las probabilidades de cada una de ellas. Por ello, como fase final del árbol de sucesos, al determinar la probabilidad de una situación descontrolada debemos sumar las probabilidades de cada una de las situaciones finales indeseadas.

La resolución de este ejercicio se indica en el cuadro.

Cuadro 2: Ejercicio 1: árbol de sucesos para un suceso inicial de pérdida de agua de refrigeración en proceso químico exotérmico



Probabilidad de acontecimiento indeseado $\bar{A}\bar{B}\,C\,\bar{D}\bar{E}$ (fallo A, fallo de B, respuesta favorable C, fallo de D y fallo de E):

$P(\bar{A}\bar{B}\,C\,\bar{D}\,E) = 1.10^{-1} \times 10^{-1} \times 9,9.10^{-1} \times 10^{-2} \times 10^{-3} = 9,9.10^{-8}$

Probabilidad del acontecimiento indeseado $\bar{A}\bar{B}\bar{C}\bar{E}$:

$P(\bar{A}\bar{B}\bar{C}\bar{E}) = 1.10^{-1} \times 10^{-1} \times 10^{-2} \times 10^{-3} = 10^{-7}$

Probabilidad de reacción descontrolada = $\bar{A}\bar{B}\,C\,\bar{D}\bar{E} + \bar{A}\bar{B}\bar{C}\bar{E}$

$P = 9,9.10^{-8} + 10^{-7} = 2.10^{-7}$

Se trata de una posibilidad remota, por lo que los sistemas de seguridad existentes se considerarían suficientes.

Ejercicio 2: Árbol de sucesos para un suceso inicial de fallo de control térmico en túnel de secado

Un secadero por aire caliente utilizado para el secado de piezas impregnadas de disolvente dispone de un sistema de ventilación forzado que aspira aire del exterior calentándolo mediante resistencias eléctricas protegidas, y lo expulsa al exterior, salvo una parte que por razones de aprovechamiento energético se recircula en el secadero.

Existe un control de temperatura del aire de impulsión asociado al funcionamiento del ventilador. Por características de diseño solamente, en caso de fallar tal control térmico, puede formarse atmósfera inflamable.

Para evitar que se pueda formar atmósfera inflamable en el interior del secadero, se ha instalado un explosímetro de medición continua con dos unidades de lectura independientes, conectado con la válvula de regulación de la recirculación del aire, de tal forma que cuando se supera el 30% del límite inferior de inflamabilidad, se cierra automáticamente mediante servosistema dicha válvula. La segunda unidad de lectura debería dar señal acústica perceptible, al alcanzarse el límite inferior de inflamabilidad, a fín de avisar para situar el sistema en condiciones de seguridad. Un fallo en el funcionamiento del explosímetro provocaría el paro de las dos unidades de lectura.

1. Representar el árbol de sucesos tras el fallo del control térmico (probabilidad de fallo 2.10^{-2}).
2. Determinar cada una de las probabilidades de las diferentes consecuencias indeseadas a partir de las siguientes probabilidades de fallo obtenidas de bancos de datos del suministrador de equipos y de la experiencia. Determinar la probabilidad de tener una atmósfera inflamable en el secadero.

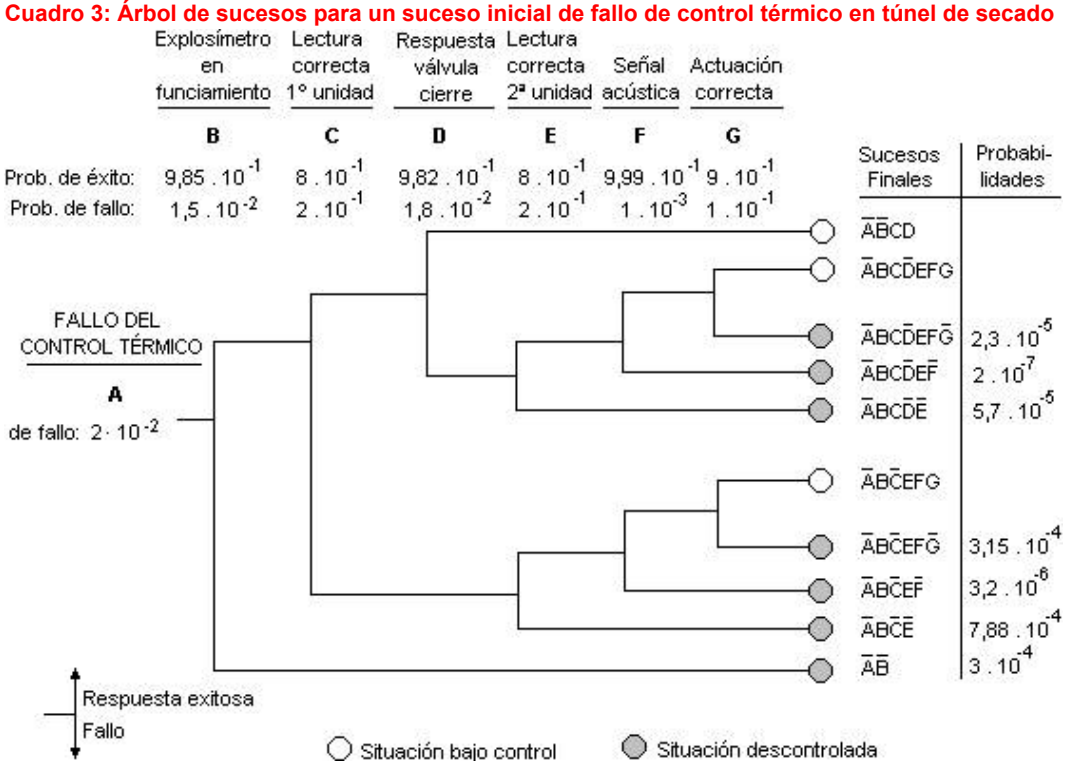
Fallo de funcionamiento del explosímetro	$1.5 \cdot 10^{-2}$
Fallo de lectura del explosímetro	$2.0 \cdot 10^{-1}$
Fallo del sistema de accionamiento de la válvula de regulación de la recirculación	$1.8 \cdot 10^{-2}$

Fallo del sistema de alarma	$1.0 \cdot 10^{-3}$
Fallo por actuación incorrecta tras alarma	$1.0 \cdot 10^{-1}$

3. A la vista de los resultado del apartado anterior, ¿qué medida preventiva prioritaria recomendaría para mejorar la seguridad del sistema?

La resolución de este ejercicio se indica en el cuadro 3.

Cuadro 3: Árbol de sucesos para un suceso inicial de fallo de control térmico en túnel de secado



Probabilidades de acontecimientos indeseados, igual al producto de probabilidades de cada uno de los sucesos confluyentes:

$\bar{A}B\bar{C}\bar{D}EF\bar{G}$	$2{,}3 \cdot 10^{-5}$
$\bar{A}B\bar{C}\bar{D}\bar{E}F$	$2 \cdot 10^{-7}$
$\bar{A}B\bar{C}\bar{D}\bar{E}$	$5{,}7 \cdot 10^{-5}$
$\bar{A}B\bar{C}EF\bar{G}$	$3{,}15 \cdot 10^{-4}$
$\bar{A}B\bar{C}E\bar{F}$	$3{,}2 \cdot 10^{-6}$
$\bar{A}B\bar{C}\bar{E}$	$7{,}88 \cdot 10^{-4}$
$\bar{A}\bar{B}$	$3 \cdot 10^{-4}$

Probabilidad de formación de atmósfera inflamable en el secadero:

P = ΣProbabilidades de acontecimientos indeseados

P =$1{,}48.10^{-3}$

En los resultados obtenidos podemos observar que el explosímetro es el factor predominante en la determinación de las probabilidades de las situaciones de riesgo, ya que el fallo de este instrumento nos produce directamente el acontecimiento indeseado. con una probabilidad digna de consideración (10^{-4}).

Sería conveniente instalar un segundo explosímetro de medición continua con dos unidades de lectura, este segundo explosímetro deberá ser totalmente independiente del primero, con el fin de evitar fallos en los dos por causa común.

Bibliografía

(1) AMERICAN INSTITUTE OF CHEMICAL ENGINERS
Guidelines for Hazard Evaluation Procedure
New York. 1985

(2) LEES, FRANK P.
Loss Prevention in the Process Industrias
London. 1980

(3) AMERICAN INSTITUTE OF CHEMICAL ENGINERS
Guidelines for Chemical Process Quantitative
Risk Analysis. New York. 1.989.