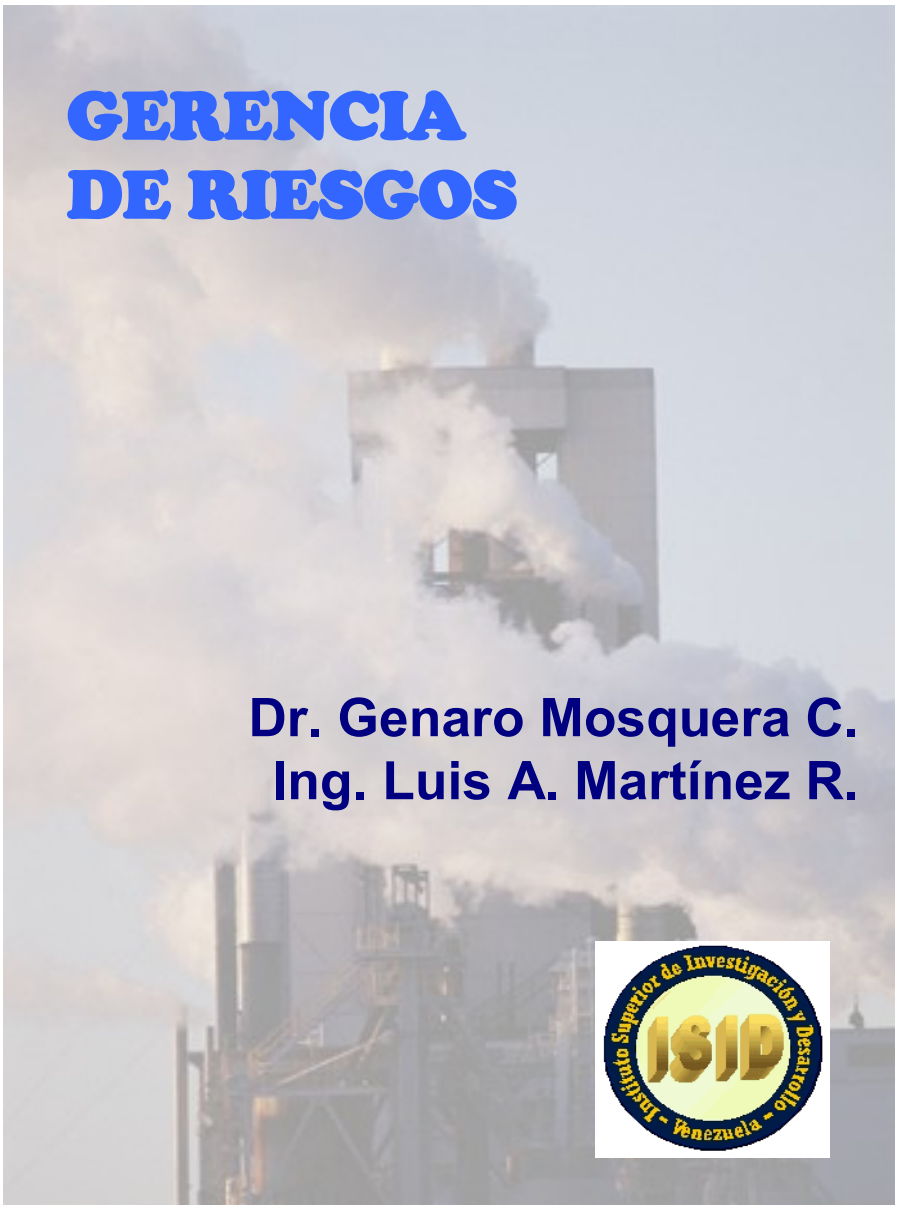
Centro de Altos Estudios Gerenciales
Instituto Superior de Investigación y Desarrollo



GERENCIA DE RIESGOS

Dr. Genaro Mosquera C.
Ing. Luis A. Martínez R.

JUNIO, 2010

Copyright,
1ª. Edición Adaptada en versión digital

Centro de Altos Estudios Gerenciales ISID

CONTENIDO

Introducción

La búsqueda, creación y adopción de métodos, procedimientos y sistemas dirigidos a garantizar una operación más confiable y segura de las plantas industriales, ha ido asumiendo cada vez mayor prioridad, al incrementarse la probabilidad de ocurrencia de accidentes graves asociados a su funcionamiento.

Como consecuencia del impacto que introducen los factores de riesgo en las operaciones, las industrias de alto riesgo han adoptado y puesto en práctica el concepto de "Cultura de la Seguridad", concebida como la actitud que debe prevalecer entre los individuos y las organizaciones ante las cuestiones de seguridad. Cuanto más riesgosas son las operaciones industriales, mayor es el peligro de que una falla o un evento externo indeseado llegue a desencadenar uno o más sucesos accidentales que, de no afrontarse a tiempo y adecuadamente, pueden ocasionar daños severos a las instalaciones y al medio ambiente, y graves lesiones o la muerte de las personas. Siendo así, mayor habrá de ser el esfuerzo en las tareas y medidas de prevención, mejores los medios tecnológicos para combatirlos, y más sofisticadas las técnicas de análisis, para desentrañar los elementos y mecanismos que intervienen en el desarrollo de los fenómenos accidentales y su evolución hacia situaciones incontrolables, cuyas consecuencias suelen traducirse en pérdida de vidas humanas, económicas o tecnológicas, pudiendo inclusive desembocar en una hecatombe ecológica de incalculables proporciones.

Numerosas han sido las iniciativas emprendidas para establecer métodos dirigidos a evaluar las condiciones de riesgo de las plantas industriales: desde métodos determinísticos relativamente sencillos, hasta modelos probabilísticos complejos, basados en el enfoque de la "defensa en profundidad". La experiencia acumulada en este sentido en varios decenios de investigación y aplicación, lleva a concluir que el enfoque más conveniente es aquel donde se conjugan de forma integrada los principios determinísticos de la ingeniería y los métodos probabilísticos, para producir un modelo de apoyo a la toma de decisiones, capaz de adaptarse a las condiciones dinámicas que caracterizan a las operaciones de tipo industrial y de contribuir más eficientemente a la gestión del riesgo.

La estrategia metodológica y las herramientas de cálculo y análisis empleadas en lo que se conoce como Análisis Probabilístico de Seguridad, o APS, han demostrado ser efectivas y versátiles como medios de apoyo de la Gerencia para la toma de decisiones en materia de riesgos. En Venezuela, luego de una serie de pruebas de aplicación realizadas a partir de 1984, en empresas del sector petrolero, químico, alimentario, automotriz, eléctrico, de transporte naviero y terrestre, entre otras, se pudo comprobar su validez y aplicabilidad, y que sus resultados constituyen un aporte efectivo al proceso de toma de decisiones, en pro de la seguridad y la reducción de riesgos, la optimización de las operaciones y la racionalización del mantenimiento.

Parte del material referente al APS contenido en esta publicación, fue extraído de una colección de documentos producidos con fines informativos por la Organización Internacional de Energía Atómica, para los miembros de la comunidad científica mundial.

Conceptos y nociones fundamentales.

Cuando una persona percibe la existencia de una situación de riesgo, su reacción más inmediata es asociarla a la presencia de una condición de peligro que amenaza su seguridad e integridad, al tiempo que el instinto de conservación la induce a tomar algunas precauciones o previsiones para evitar que la amenaza potencial llegue a convertirse en un hecho real que pueda producirle algún tipo de daño.

En la sociedad tecnológica de nuestros días, vivimos inmersos en un mundo de inagotables fuentes de riesgo. Dentro de nuestros hogares o fuera de ellos, nos vemos obligados a vivir y a desenvolvernos inmersos en situaciones de peligro, representadas por la inseguridad personal, los accidentes viales, catástrofes naturales, enfermedades, accidentes del trabajo, sólo por mencionar algunos ejemplos de la cantidad abrumadora de riesgos que atentan en todo momento contra nuestra incolumidad.

Entonces cabe preguntarse: ¿Por qué aceptamos vivir en un ambiente plagado de riesgos y no tomamos medidas para minimizar o eliminar el peligro potencial, obedeciendo los dictámenes de nuestro instinto de conservación, o no recurrimos a la intervención de las autoridades para que actúen de consecuencia? La respuesta, sencillamente, es que no llegamos a percibir tales situaciones como una situación de riesgo que nos puede afectar personalmente.

Cuando el riesgo de muerte es del orden de 10^{-6} personas/año, (una persona en un millón por año) no nos sentimos amenazados, porque la probabilidad de ocurrencia es extremadamente baja. Tendemos a creer, por ejemplo, que la muerte debido a la caída de un rayo es un "hecho del destino" y que nunca seremos víctima de ese fenómeno.

Si el riesgo de muerte es del orden de 10^{-5} o 10^{-4} personas/año, (una entre 100.000 o una entre 10.000 por año), nos preocupamos relativamente, pero confiamos en las medidas que toman, por ejemplo, los organismos públicos para fines de prevención. Típicos de estos casos son los accidentes automovilísticos, incendios, ahogamiento, envenenamiento, entre otros.

Sin embargo, independientemente del valor absoluto del riesgo, el grado de aceptación de éste por parte de los individuos y colectivamente por la sociedad, difiere en función de diversos factores, tales como: los beneficios que se pueden obtener de la actividad de la cual se deriva el riesgo; si el riesgo se asume voluntariamente o si se está expuesto al mismo involuntariamente; la magnitud de las consecuencias asociadas al riesgo, etc.

Es en virtud de razonamientos similares que las comunidades terminan por compartir su entorno con plantas de producción altamente peligrosas, asumiendo que los beneficios directos o indirectos que se desprenden de la actividad de las empresas, son suficientes para compensar los riesgos de su explotación, y lo asumen voluntariamente.

Hasta este punto, se ha hablado del riesgo en términos de amenaza a la integridad de las personas y sus posibles consecuencias; sin embargo, es necesario considerar el fenómeno desde una óptica más amplia e integradora. No se trata solamente del peligro de pérdida de vidas humanas o lesiones personales, sino también de bienes y propiedades en general, de maquinaria, instalaciones, equipos, edificaciones, infraestructura, de la calidad de vida de las comunidades, de la integridad del medio ambiente y la supervivencia de los sistemas ecológicos. Es decir que el riesgo tiene connotaciones de tipo personal, social y tecnológico y, por lo tanto, su definición debe abarcar estas tres vertientes, asociándolas a las actividades de tipo industrial.

Según las Normas COVENIN, *el riesgo es una medida del potencial de pérdida económica o lesión en términos de la probabilidad de ocurrencia de un evento no deseado junto con la magnitud de las consecuencias*, definición un tanto restringida pues involucra solamente dos aspectos de interés en términos de higiene industrial, es decir, la lesión a las personas y el costo económico para la empresa.

Una definición más amplia, que incluya todos los factores que pueden ser afectados por una condición de riesgo, desde el punto de vista de las operaciones industriales, sería:

El riesgo es una medida del potencial de pérdida de vidas, de lesiones a las personas, de daños a la propiedad o al medio ambiente, en términos de probabilidad de ocurrencia de un evento no deseado, junto con el impacto de sus consecuencias.

En este caso, se entiende por "evento no deseado": un fenómeno natural calamitoso (huracán, terremoto, inundación, etc.), una contingencia en el curso de las operaciones de una planta, por ejemplo un suceso desencadenado a raíz de la falla de un equipo, o provocado accidental o intencionalmente por una o más personas (incendios, choques, voladuras, etc.).

Al referirnos a las consecuencias, es necesario distinguir entre aquellas que para la planta o la empresa son de carácter interno, las cuales, a su vez, pueden ser de tipo tangible o intangible, y las consecuencias de naturaleza externa, cuyo impacto se localiza fuera de las fronteras físicas de la fábrica.

Las **consecuencias externas** son representadas por aquellos hechos que afectan en una medida importante a la población y su entorno social y económico, y aquellos que ocasionan serios daños al medio ambiente y los sistemas ecológicos en general.

Entre las **consecuencias internas de tipo tangible** se incluyen: la muerte de trabajadores y las lesiones al personal, los daños a las estructuras de la planta, sus instalaciones, dotaciones y otros bienes, así como las pérdidas económicas resultantes de los daños antes señalados, además de los que acarrea la interrupción de los procesos de producción.

Las **consecuencias internas intangibles** están relacionadas directamente con la imagen que la empresa proyecta hacia el entorno, y pueden llegar a tener efectos inclusive mucho más graves que los daños de tipo material. Entre ellas se incluye; pérdida de la confianza y credibilidad depositada por los clientes, la comunidad y las instituciones u organizaciones

relacionadas con la empresa; disminuida competencia técnica, como consecuencia de los daños a las instalaciones y la pérdida de personal entrenado y experimentado; reducción en la capacidad de competir ventajosamente en los mercados y de emprender o continuar con los planes de desarrollo y crecimiento de la planta.

Anteriormente, se mencionó que en función del sujeto afectado, los riesgos pueden ser considerados como de tipo individual, social o colectivo y tecnológico; seguidamente se precisa la definición del riesgo en base a esta clasificación:

Riesgo individual: el que puede causar daños a la persona expuesta, tales como: muerte, lesiones temporales o permanentes, pérdida de bienes personales, etc.

Riesgo Social o colectivo: del cual pueden desprenderse daños a grupos de personas (muertes, lesionados, etc.) o el impacto social que ocasione, representado por pérdidas económicas, sea en términos monetarios o en días/hombre de producción, pérdida de viviendas, terrenos cultivables afectados, cuerpos de agua contaminados, etc.

Riesgo Tecnológico: aquel por el cual las eventuales consecuencias se expresan en términos de daño a los recursos tecnológicos, tales como: sistemas de producción, sistemas de apoyo de las instalaciones o componentes de los mismos, medios de transporte, etc.

CAPITULO I – CULTURA DE SEGURIDAD

El concepto de Cultura de Seguridad aparece por primera vez en un informe técnico elaborado a raíz del accidente ocurrido en la Central Electronuclear de Chernobil (URSS) en 1986. En el informe se planteaban las bases para establecer los principios básicos de seguridad y se presentaba una serie de recomendaciones para la promoción y difusión de una cultura de la seguridad.

El mencionado documento establecía que la Cultura de la Seguridad se refería a *"…. la dedicación y la responsabilidad personal de todos los individuos que desarrollan cualquier actividad que tenga influencia en la seguridad….."*; estableciéndose además que ella comprende, como elemento clave, *"una preocupación constante por la seguridad"* que conduce a asumir una *"actitud esencialmente crítica, la búsqueda constante de un nivel de excelencia, y el estímulo del sentido de la responsabilidad personal y del autocontrol corporativo en materia de seguridad"*.

Resumiendo, el concepto de Cultura de Seguridad puede ser expresado de la siguiente manera:

Cultura de Seguridad es el conjunto de características y actitudes en organizaciones e individuos que aseguren, como prioridad esencial, que las cuestiones de seguridad reciban la atención que merecen en razón de su significación.

Existe una serie de aspectos generales aplicables a toda clase de actividades, organizaciones e individuos que representan las características universales de la cultura de seguridad, cuyos elementos esenciales son:

- Conciencia individual de la importancia de la seguridad
- Conocimientos y competencia impartidos por capacitación y adiestramiento del personal y por vía de la autoformación.
- Compromiso que requiere la demostración, por parte de los altos niveles gerenciales, de que la seguridad tiene alta prioridad y se han adoptado objetivos de seguridad que son comunes para todos los individuos.
- Motivación a través del liderazgo, autogeneración de actitudes convenientes, así como el establecimiento de un sistema de premios y sanciones
- Supervisión, incluyendo prácticas de auditoría y revisión, y la disposición correcta para responder ante las críticas de los individuos.
- Responsabilidad, a través de la asignación y descripción formal de las funciones, y su plena comprensión por parte de las personas a quienes se les confieren.

En este sentido, el papel de la alta gerencia asume una importancia trascendental, ya que no es posible hablar de cultura de la seguridad, si ésta no emana del vértice de la pirámide jerárquica de dirección, para luego difundirse entre todos los niveles intermedios y llegar finalmente al individuo vinculado directamente con el proceso productivo.

La observancia de una cultura de seguridad se orienta hacia la puesta en práctica, en cada organización, de una política de seguridad, donde se establezcan los compromisos que sirven de guía a todo el personal, haciendo públicos los objetivos y compromisos que la organización se compromete a garantizar. En esta declaración debe quedar claramente definida la responsabilidad en materia de seguridad y que, en todo momento, la seguridad está en un plano superior, por encima de las presiones de la producción y los cronogramas de proyectos. Ella debe crear un ambiente propicio entre los trabajadores, tal que promueva la preocupación constante y el adecuado comportamiento individual por y hacia el mejoramiento de la seguridad.

Resulta obvio que todo lo anterior implica, en materia de gestión, la asignación de recursos, la autorregulación, el establecimiento de compromisos y de los requisitos necesarios que deben cumplir los gerentes, la definición de responsabilidades, el establecimiento y control de las prácticas de seguridad, las necesidades de calificación y capacitación del personal, la existencia de una adecuada política de premios y sanciones y, por último, la adopción de un programa de auditoría, análisis y comparaciones.

La figura a continuación representa la estructura sobre la cual se fundamenta el concepto de Cultura de Seguridad, donde se muestran los elementos principales que lo integran.

1.1 Principios básicos de Seguridad

El establecimiento de una cultura de seguridad se fundamenta en la aplicación de un conjunto de principios, cuyo propósito es el de garantizar una estrategia global en lo referente a medidas de protección y dispositivos de seguridad de las instalaciones. Entre ellos se incluyen los siguientes:

- Defensa en profundidad
- Práctica de ingeniería de eficacia comprobada
- Garantía de calidad
- Factores humanos
- Evaluación y verificación de la seguridad
- Experiencia operacional e investigación en materia de seguridad

1.1.1. Principio de Defensa en Profundidad

En las empresas industriales suelen preverse medidas de protección contra las fallas tecnológicas o humanas que pueden ocurrir durante el proceso de explotación, siendo el principio de defensa en profundidad uno de los más relevantes a los fines de garantizar una estrategia global en lo que respecta a medidas de protección y dispositivos de seguridad de las instalaciones.

Este principio se caracteriza por la creación de múltiples barreras de protección a diferentes niveles, con la particularidad de que el esquema de protección incluye a las mismas barreras, lo cual garantiza una defensa eficaz contra las fallas, de manera que si llegase a ocurrir alguna, existe la contramedida respectiva que contribuirá a evitar el daño a las instalaciones, al medio ambiente, a las personas y a la población en general.

La eficacia de esta concepción se logra mediante la aplicación de dos conceptos relacionados con la **prevención y la mitigación de accidentes**.

Cuando se aplican correctamente, estos conceptos constituyen una garantía para que ninguna falla única, humana o mecánica, termine por ocasionar daños a las personas y al entorno. Si la defensa es realmente eficaz las fallas combinadas tendrían una posibilidad muy remota de causar daños significativos, y en la mayoría de los casos prácticamente ninguna.

En el caso de las centrales nucleares, la aplicación de este principio ofrece, con alto grado de confianza, la posibilidad de preservar las tres funciones de seguridad básica (control de la potencia, enfriamiento y el confinamiento de sistemas radiactivos) reduciendo significativamente el riesgo de afectación de la población y del medio ambiente por contaminación radiactiva

Como norma general, una instalación de alto riesgo no debe mantenerse funcionando si la integridad de una de las barreras físicas existentes está amenazada, ya que se degradaría la

efectividad para contener el vertimiento de sustancias peligrosas, si tuviera lugar un accidente.

Las barreras físicas deben ser diseñadas siguiendo como principio un criterio conservador racional, de manera que se pueda contar con cierto margen de seguridad contra el espectro de posibles fallas a las que pueden estar sometidas. Se incluyen aquí los aspectos humanos vinculados con el principio de defensa en profundidad, que garantizan la integridad de las barreras, tales como: la garantía de calidad, los controles administrativos, las evaluaciones de seguridad, la reglamentación independiente, los límites operacionales, la calificación y capacitación del personal y la cultura de seguridad existentes.

Los responsables del diseño deberán garantizar la idoneidad de las barreras, mediante la aplicación de un conjunto de medidas preventivas contra el surgimiento y para la mitigación de las averías, tanto en los sistemas de producción como los de seguridad. En el caso de los sistemas de seguridad, es vital lograr la independencia funcional de su actuación durante las averías, mediante la aplicación adecuada de los principios de redundancia y de diversidad en el diseño.

Bajo el principio de la defensa en profundidad, no se debe operar a potencia nominal con componentes de la defensa indisponibles, aún pudiendo contar con otros componentes de la misma barrera o de otra barrera sucesiva. La mayoría de los accidentes graves ocurridos por el surgimiento de combinaciones de fallas múltiples, se ha debido a la mala práctica de mantener la planta en operación cuando existen componentes defectuosos ó cuyas funciones se encuentran degradadas en cierta medida.

En este aspecto, debe proveerse vigilancia constante sobre las desviaciones que pudiesen conducir a eventuales fallas durante el proceso de operación, y tomar las medidas correctivas correspondientes, dentro de los márgenes de tolerancia establecidos, de manera tal que se mantenga en todo momento la protección necesaria constituida por las barreras físicas.

Es importante que el diseño contemple márgenes de seguridad suficientemente amplios, a fin de evitar que leves desviaciones de los parámetros de proceso puedan desencadenar situaciones sumamente críticas o anormales en la actividad de explotación de la instalación.

La aplicación del principio de defensa en profundidad comienza por las medidas de prevención para evitar los accidentes, prestando particular atención a los medios para alcanzar la mayor seguridad posible. El primero de ellos está representado por el esfuerzo que se realice en pro de alcanzar alta calidad de diseño, construcción y explotación de la instalación, buscado en todo momento que sean poco frecuentes las desviaciones fuera de los límites normales de operación.

El diseño de los sistemas de seguridad contempla la redundancia, diversidad y separación física suficiente de sus componentes y subsistemas paralelos, con el objetivo de alcanzar por esta vía una reducción significativa de la probabilidad de pérdida de las funciones de seguridad que deben cumplir.

Todos los sistemas y componentes de importancia para la seguridad de la instalación, y los sistemas que garantizan el proceso de producción con altos índices de disponibilidad, son sometidos a un estricto régimen de control, pruebas y ensayos periódicos, con el objetivo de determinar el nivel de degradación que pueden alcanzar durante el proceso de explotación, y de esta forma tomar medidas correctivas que permitan mantener una alta confiabilidad y seguridad de la instalación.

La existencia de un sistema de garantía de calidad, establecido en todas las actividades relacionadas con la operación y el mantenimiento, constituye un elemento de defensa contra el surgimiento de las fallas. En este aspecto, el personal de operación y mantenimiento debe mantenerse entrenado y capacitado en la prevención y mitigación de accidentes, de acuerdo a los programas de preparación del personal, según los lineamientos establecidos en el sistema general de garantía de calidad adoptado por la organización industrial.

De esta forma, se garantiza una sólida preparación que permite mantener una acción de vigilancia permanente, para detectar la degradación o fallas incipientes y por tanto reconocer de forma rápida y oportuna el comienzo de los procesos de avería, a fin de ejercitar las correspondientes medidas correctivas, evitando que las fallas puedan derivar hacia una situación más grave.

Una de las herramientas que ha permitido mejorar sensiblemente los programas de entrenamiento y capacitación del personal de operaciones y de mantenimiento en las industrias de alto riesgo, es el Análisis Probabilístico de Seguridad (APS) mediante el cual se logra dirigir los esfuerzos y recursos hacia los focos vitales de mayor importancia dentro de la actividad de explotación, la optimización de la calidad del diseño, las especificaciones técnicas de planta, los programas de garantía de calidad. Estas y otras aplicaciones de los estudios de APS ayudan a consolidar una defensa en profundidad verdaderamente eficaz.

A través de la mitigación de accidentes, se logra ampliar el concepto de defensa en profundidad, más allá del alcance que establece el principio de prevención de accidentes, en virtud de que existe un grupo de medidas de mitigación, en caso de avería, que permiten reducir considerablemente los efectos del escape de sustancias nocivas dentro y fuera de la instalación y del lugar de emplazamiento de la planta. En este sentido, las disposiciones relacionadas con la mitigación de accidentes se clasifican en tres categorías: las que se contemplan en la gestión de accidentes, los dispositivos técnicos de seguridad y las contramedidas a tomar fuera del lugar de emplazamiento de la fábrica.

1.1.2. Principio de la práctica de ingeniería de eficacia comprobada

Este principio plantea, en esencia, que todo diseño debe ser realizado conforme a criterios sensatos que estén avalados por la experiencia práctica, y que los sistemas y componentes se proyecten, construyan y ensayen con arreglo a procedimientos y normas de calidad, de acuerdo a los objetivos de seguridad de las instalaciones en cuestión.

Toda modificación y mejora a los diseños originales debe ser rigurosamente evaluada y las innovaciones introducidas con extrema cautela. En general, cada actividad que se realiza

estará bajo un sistema estricto de garantía de calidad. Los nuevos diseños, en la medida de lo posible, deben estar sustentados por la experiencia práctica obtenida en instalaciones que se encuentren en funcionamiento, o de los resultados de programas de investigación en instalaciones experimentales.

1.1.3. Principio de la garantía de calidad

La garantía de calidad, como principio, se aplica a toda las actividades relacionadas con las instalaciones industriales, desde la etapa de concepción del diseño hasta la etapa de explotación e incluso su cierre definitivo. Esto asegura con alto grado de confianza que todas las tareas, servicios brindados y artículos suministrados para estas instalaciones satisfagan los requisitos especificados.

Es fundamental para la seguridad, que exista un elevado grado de calidad en el comportamiento de los equipos y en las actuaciones de las personas. Para lograr este objetivo, la práctica de la garantía de calidad prevé someter todo el conjunto de actividades que se realice al control y verificación de su estado, requiriéndose mayor rigurosidad en la medida que aumenta la relevancia de la actividad en relación a la seguridad de la instalación.

En este aspecto adquiere particular importancia la clasificación de todos los componentes, estructuras y sistemas, de acuerdo a sus funciones e importancia para la seguridad. La realización de esta tarea es fundamental pues todo se diseña, fabrica, construye e instala con exigencias de calidad que se corresponden con la clasificación adoptada. Más adelante, se aborda en detalle el tema de la clasificación, atendiendo distintos criterios, entre los cuales se incluye la importancia de los sistemas respecto a la seguridad de las instalaciones.

La existencia de un programa de garantía de calidad ofrece el marco adecuado para alcanzar y demostrar no solamente la calidad del producto, sino también la explotación segura de la instalación, a través de la validación de los diseños constructivos, el suministro y empleo de materiales, los métodos de fabricación, inspección y ensayo, los procedimientos operacionales y otras actividades importantes dirigidas a garantizar el cumplimiento de las especificaciones técnicas y la adecuada calificación y capacitación del personal.

Un elemento esencial de la garantía de calidad lo constituye la elaboración y conservación de la documentación, donde se registran todas las actividades y tareas que deben ser ejecutadas de acuerdo a lo prescrito en las normas y procedimientos correspondientes, sea desde la concepción del diseño hasta la explotación y cierre definitivo de la instalación.

1.1.4. Principio de los factores humanos

En la mayoría de los accidentes, vinculados directa o indirectamente a los procesos industriales, el análisis estadístico ha demostrado que entre sus causas predomina de manera determinante los errores humanos. Por tal razón, resulta ineludible prestar particular atención a la capacitación y entrenamiento del personal encargado de las actividades

relacionadas con la seguridad de las instalaciones, de manera que se encuentre plenamente calificado para el desempeño exitoso de sus funciones.

En el diseño de las instalaciones debe tenerse presente la necesidad de que se incluyan medios y procedimientos de explotación dirigidos a facilitar la toma de decisiones correctas por parte de los operadores, tanto en regímenes de operación normal como de avería; en otras palabras, deberá preverse la posibilidad de evitar, detectar, corregir o compensar los errores que puedan cometerse durante la operación o el mantenimiento de las instalaciones.

En este campo se incluye disciplinas tales como el estudio del comportamiento humano y la aplicación de los procesos más avanzados en el área de la automatización.

1.1.5. Principio de la evaluación y verificación de la seguridad

Este principio plantea que antes de comenzar la construcción y las operaciones en una planta, deberá realizarse una evaluación de la seguridad. La evaluación se acompaña de la documentación respectiva y será objeto de examen por parte de una organización independiente. Posteriormente, la documentación deberá ser actualizada a la luz cualquier información que resulte relevante en función de la seguridad.

Es importante resaltar que la evaluación de la seguridad se efectúa expresamente para descubrir eventuales deficiencias básicas en el diseño. Como toda actividad sometida al principio de garantía de calidad, se exige de manera documental que toda la información generada a raíz de las evaluaciones de la seguridad, debe ser adecuadamente documentada, por cada etapa de trabajo establecida.

El objetivo es lograr un conocimiento profundo de todos los aspectos relacionados con la seguridad. En este aspecto, es importante aclarar que no se trata solamente de cumplir el requisito formal de un documento con la información que demuestre el nivel de excelencia alcanzado; es necesario además que los responsables de las operaciones dominen esta clase de información.

Actualmente, en la evaluación de la seguridad se aplican habitualmente dos métodos complementarios: uno de naturaleza determinística y otro de tipo probabilístico. Ambos métodos se utilizan conjuntamente para evaluar y mejorar el diseño y la explotación de la instalación. Los análisis probabilísticos de seguridad constituyen una herramienta eficaz, puesto que permiten evaluar de manera integral los aspectos de confiabilidad y seguridad vinculados a la instalación desde etapas muy tempranas, facilitan la identificación de los sucesos accidentales, y manejar otras variables asociadas a las actividades de la explotación que requieren la aplicación de un análisis de tipo determinístico.

1.1.6. Principio de la experiencia operacional e investigación en materia de seguridad

Entre las organizaciones industriales debe establecerse un sistema de intercambio, examen y análisis de la experiencia operacional y de los resultados de las investigaciones en materia

de seguridad, de forma tal que entre las plantas prevalezca un ambiente del cual se puedan extraer enseñanzas útiles y se tienda a generalizar las mejores prácticas en materia de seguridad. De esta manera, se logra el objetivo de que ningún suceso pase inadvertido, se disponga de información para introducir correctivos adecuados y se evite que otras plantas incurran en situaciones similares.

Sobre la base de los principios básicos de seguridad antes descritos, la organización responsable de las operaciones y el mantenimiento de la planta industrial deberá diseñar un plan de acción que le permita introducir y difundir la Cultura de Seguridad, comenzando por establecer los lineamientos de política y definir los demás aspectos que contemplan los compromisos a nivel de la gerencia y de los individuos que habrán de asumir en materia de seguridad.

La organización, como máximo responsable de la seguridad de la planta, debe proporcionar todo el equipo, personal, procedimientos y prácticas de gestión necesarios para garantizar en todo momento la explotación segura y confiable de las instalaciones, la cual abarca un conjunto de actividades que deberán sustentarse en los principios básicos de seguridad. De manera resumida estas actividades incluyen:

- Definición de las responsabilidades del personal.
- Ingeniería y ensayos técnicos.
- Capacitación del personal.
- Retroalimentación resultante de la experiencia operacional.
- Realización de la labor de explotación.
- Entrenamiento del personal.
- Acopio de datos de referencia de los sistemas.
- Límites y condiciones.
- Mantenimiento, pruebas e inspección.
- Garantía de calidad de la explotación.
- Procedimiento para la evaluación de la seguridad.
- Validación de los procedimientos de operación normal.
- Procedimientos para la operación normal.
- Procedimientos para protección contra agentes nocivos.
- Procedimientos operacionales de emergencia (POE).
- Capacitación y realización de los procedimientos de gestión de accidentes.
- Instalaciones de respuesta a las emergencias.
- Evaluación de emergencias.

CAPÍTULO II – CLASIFICACIÓN DE LOS SISTEMAS INDUSTRIALES

La clasificación de sistemas industriales es una de las tareas que mayor interés ha suscitado en la industria moderna en general, teniendo en cuenta que el establecimiento de un correcto sistema de clasificación permite asignar y unificar requerimientos y por tanto concentrar esfuerzos hacia los grupos que demandan mayor atención. Sin embargo, los sistemas de clasificación tradicionales adolecen, en su mayoría, de una debilidad distintiva y es que las escalas de clasificación y, por tanto, los requerimientos que les corresponde, son establecidos en base a criterios determinísticos.

En la industria que opera con riesgos potenciales asociados, donde la inclusión de un componente, estructura o sistema en determinada agrupación tiene implicaciones en los requisitos de seguridad, es importante que su clasificación corresponda con exigencias reales según las funciones que habrán de cumplir. Este aspecto debe tomarse en cuenta, debido a que la inclusión de nuevos requisitos de seguridad en el diseño, explotación o mantenimiento de equipos comporta un costo asociado, de manera que éstos se encarecen. Por tanto, es tarea fundamental establecer un correcto balance, de modo que el encarecimiento de los componentes, equipos o sistemas, esté respaldado por la correcta escogencia de los puntos del sistema industrial, haciéndoles corresponder requerimientos específicos para reducir los riesgos.

Seguidamente, se exponen algunas de las formas de clasificación utilizadas en la industria de riesgo potencial y las bases para la implantación de dichos sistemas de clasificación. Una de las tendencias actuales en la clasificación de sistemas, estructuras y componentes es utilizar criterios probabilísticos, a objeto de determinar cuáles de ellos deben diseñarse, operarse y mantenerse según las diferentes gradaciones de los requisitos de seguridad.

2.1. Establecimiento de Criterios de Clasificación de Sistemas Industriales en Instalaciones de Riesgo Potencial

Los criterios de clasificación de los sistemas industriales varían según sus objetivos. Los mismos van desde la necesidad de establecer requisitos funcionales o de seguridad, hasta el simple cumplimiento de requerimientos metodológicos. Entre los tipos de clasificación frecuentemente empleados se pueden mencionar las siguientes modalidades: Clasificación por tipo de sistema; por importancia para la seguridad; por valor económico; por índice de disponibilidad; por requerimientos legales y reglamentarios; por funciones de seguridad; por cumplimiento de requisitos metodológicos; por requerimientos de gestión; por aplicación de criterios de riesgo (APS), los cuales se describen a continuación.

2.1.1. Clasificación por Tipo de Sistema

Los sistemas, atendiendo a la naturaleza de los dispositivos que los constituyen, se pueden subdividir en mecánicos (termomecánicos), eléctricos y automáticos. Estos sistemas se entrelazan y complementan, formando primero los sistemas tecnológicos y finalmente la instalación completa, cuyo objetivo fundamental es cumplir de manera segura el proceso para el cual ha sido diseñada (generación de energía eléctrica, procesamiento de productos químicos, fabricación de bienes de consumo, etc.).

Este tipo de clasificación, basada en la naturaleza de los dispositivos que integran el sistema, se realiza preferentemente para identificar las diferentes áreas que se encuentran asociadas, según determinados grados de especialización, en la solución de problemas específicos relativos al diseño, mantenimiento y otras actividades conexas.

Un reflejo de este tipo de clasificación es el organigrama de mantenimiento de cualquier instalación tecnológica de relativa complejidad, en el cual se pueden identificar las áreas de mantenimiento termomecánico, eléctrico y automático, según sea la naturaleza de los equipos y/o sistemas que conforman la instalación.

Teniendo en cuenta algunas particularidades de los procesos, es posible establecer categorías de menor nivel, como por ejemplo subdividir los sistemas termomecánicos en función del tipo de fluido que contienen, o los sistemas eléctricos en base a los niveles de voltaje. Tales sub-clasificaciones llevan implícito un grado de especialización mayor y algunos requerimientos complementarios. Por ejemplo, en una central termoeléctrica se identifican de manera general sistemas termomecánicos de agua, vapor y gases; sistemas eléctricos de corriente alterna y continua a diferentes niveles de voltaje; sistemas automáticos de instrumentación y de control.

2.1.2. Clasificación por Importancia para la Seguridad

Este tipo de clasificación es común en instalaciones de riesgo potencial, como, por ejemplo, las centrales nucleares y la industria química. Los sistemas, por su trascendencia para la seguridad, pueden dividirse según sean importantes o irrelevantes respecto a la seguridad. La clasificación se basa en que el riesgo de esta clase de industrias, debido a la posible liberación de productos sumamente peligrosos (tóxicos en el caso de la industria química de proceso, o radiactivos en el caso de las plantas nucleares) pueden ocasionar la muerte o daños permanentes a la salud de las personas, destrucción de las instalaciones, daños al medio ambiente y serios problemas económicos.

Es por tanto común que los sistemas que contienen o controlan procesos donde intervienen tales sustancias o productos, sean considerados importantes para la seguridad. También quedan clasificados como importantes los sistemas de mitigación destinados a evitar o disminuir las consecuencias de un accidente, en caso de llegar a producirse. A su vez, dentro de los sistemas importantes, se delimitan sistemas de explotación normal, que se relacionan de forma general con aquellos que participan en el proceso continuo de producción y los de seguridad que, salvo algunas excepciones, se encuentran normalmente a la espera.

También dentro de los sistemas de seguridad, se establece una sub-clasificación relacionada con el tipo de función de seguridad que el sistema cumple. Esta sub-clasificación divide los sistemas de seguridad en: sistemas de seguridad de protección, sistemas de seguridad de localización y sistemas de seguridad de apoyo.

Los sistemas de seguridad de protección son los que realizan directamente las funciones de seguridad de mitigación cuando se alcanzan condiciones de accidente. Los sistemas de seguridad de localización cumplen la misión de confinar el accidente en los límites impuestos por las barreras conformadas por la defensa en profundidad. Los sistemas de seguridad de apoyo constituyen las fuentes de suministro de enfriamiento y de energía, y garantizan el control para el cumplimiento de las funciones de los sistemas de protección y algunos los sistemas de localización.

Teniendo en cuenta la importancia para la seguridad de las funciones que deben cumplir, estos sistemas se caracterizan por exigir requisitos especiales de diseño y operación, como son: elevada resistencia antisísmica, alta confiabilidad de alimentación, de manera que quede virtualmente asegurado su funcionamiento ante situaciones de avería en las que concurren fallas múltiples. Tales requerimientos de diseño y de características operacionales (alimentación confiable) llevan implícito su propio sistema de clasificación, cuya exposición haría innecesariamente extenso este aspecto.

2.1.3. Clasificación por el Valor Económico

Es tradicional que en procesos tecnológicamente complejos existan equipos que representan un componente de costo elevado dentro del costo total de la instalación. Es procedente que para tales equipos existan requerimientos específicos de operación, mantenimiento y conservación, entre otros.

El establecimiento de esa diferenciación es útil cuando se trata de proteger equipos de elevado valor, cuya rotura o destrucción compromete por largos períodos o de forma definitiva la explotación de la instalación. Por ejemplo, en las centrales termoeléctricas de algunos países, existen sistemas de mantenimiento que establecen la categorización de los sistemas por su participación en el ciclo de producción de energía eléctrica; según esta modalidad, los más importantes incluyen: Turbina, Caldera, Transformador Principal de Salida, coincidiendo con los equipos cuyo costo unitario dentro del costo total de la instalación es el más elevado.

2.1.4. Clasificación por Índice de Disponibilidad

Las instalaciones modernas de proceso continuo resultan más económicas en la medida en que se logra aumentar su coeficiente de utilización. Este factor está relacionado directamente con la explotación prolongada del equipamiento que las conforman. Dicha explotación solo es posible si se dispone de un equipamiento de elevada fiabilidad en operación continua, o de un parque de equipos redundantes, capaz de asumir un ciclo prolongado de explotación sin fallas durante el tiempo necesario.

Para establecer una clasificación de equipos relacionada con la disponibilidad, es importante el conocimiento de las características de fiabilidad de los equipos, así como de la influencia sobre este parámetro, o de sus interfases con otros sistemas cuando dicho equipo forma parte de un esquema complejo.

En muchas ocasiones, la clasificación realizada sobre la base de los índices de disponibilidad no está respaldada por datos estadísticos de fallas, que reflejen el comportamiento de los equipos clasificados, y consideran de manera limitada la fiabilidad de los mismos.

La categorización de equipos únicos presentes en el ciclo productivo de un sistema de generación de energía eléctrica, tales como Caldera, Turbina y Transformador principal de salida, que en el sistema SOMCE (Sistema de Organización del Mantenimiento en Centrales Eléctricas) se consideran como pertenecientes a la Categoría "A", entraña no sólo el reconocimiento de su valor económico, sino también la necesidad de su disponibilidad para la producción. Sin embargo, la clasificación SOMCE incluye en la categoría "B", equipos, como las Bombas de Alimentación o de Condensado que al salir de servicio limitan la fiabilidad de la central, lo cual demuestra que los índices de confiabilidad han sido tenidos en cuenta en forma limitada para los fines de la clasificación.

2.1.5. Clasificación por Requerimientos Legales y Reglamentarios

Para el control de instalaciones de riesgo potencial, es común que existan en diferentes países, y en ocasiones incluso por consenso internacional, requerimientos legales y reglamentarios que son de carácter obligatorio para determinados equipos y/o sistemas. Ello hace que su clasificación, desde este punto de vista, tenga especificidades relacionadas con su inspección u otros aspectos y que su control y conservación se adhiera a estas exigencias reglamentarias.

Un ejemplo de esta clasificación, y que adquiere en este caso rango de requerimiento internacional, ocurre en la industria nuclear con algunos equipos sometidos a reglamento de salvaguardia para el control de la no proliferación de las armas nucleares. Entran en este caso la vasija del reactor nuclear y las bombas principales de seguridad.

2.1.6. Clasificación por Funciones de Seguridad

La clasificación por función de seguridad es uno de los criterios de clasificación más modernos. El mismo permite establecer requerimientos de diseño o de otro tipo, según la función de seguridad que deba cumplir el sistema en cuestión.

Lo más novedoso de esta clasificación es que permite jerarquizar por su importancia las diferentes funciones de seguridad, basándose en criterios probabilísticos cuantitativos, que incluyen la probabilidad de que se requiera la función de seguridad y las consecuencias de su fallida intervención. Posteriormente, en base a la importancia relativa de las funciones de

seguridad, se clasifican los sistemas que las desempeñan. En el capítulo dedicado a la Gestión de la Seguridad, se describe en forma más detallada lo atinente a las funciones de seguridad.

2.1.7. Clasificación por requisitos metodológicos

Algunas metodologías y las técnicas de análisis que incorporan utilizan una terminología propia que comporta una clasificación de los sistemas que se analizan. Ejemplo de ello es el Análisis Probabilístico de Seguridad, el cual establece, para las actividades de modelación, la clasificación de los sistemas de mitigación en sistemas frontales y de apoyo.

La clasificación está relacionada fundamentalmente con la necesidad de establecer fronteras entre los diferentes sistemas que se incluyan en el análisis. Son sistemas de seguridad frontales aquellos que ejecutan directamente las funciones de seguridad para mitigar las consecuencias de un accidente. Por otra parte, son sistemas de seguridad de apoyo los que garantizan funciones tales como el enfriamiento, el suministro de energía y el control de los sistemas frontales.

2.1.8. Clasificación por requerimientos de Gestión

Algunas actividades necesitan como soporte una clasificación especializada que facilite su administración o gestión, independientemente de que puedan apoyarse en los criterios de clasificación anteriormente descritos, que establecen la jerarquización de los equipos, sistemas y estructuras en base a su importancia para la seguridad, la disponibilidad u otros requisitos. La gestión del mantenimiento y la gestión de almacenes constituyen ejemplos evidentes de esta necesidad.

Para la realización de las operaciones de mantenimiento, al margen de la prioridad asociada a los equipos más importantes, determinada por algún otro criterio de clasificación, es indispensable una labor organizativa específica. Por consiguiente, en la elaboración de los planes de mantenimiento es importante organizar los equipos y sistemas por grupos, de acuerdo a características comunes, tales como: similitud del equipamiento, intercambiabilidad de partes y piezas de repuesto, necesidad de herramientas especiales, de medidas de seguridad y/o de protección para realizar las reparaciones, etc.

El tipo considerado de agrupamiento aporta una clasificación sumamente útil desde el punto de vista de la organización de los procedimientos de mantenimiento, ya que partiendo de la existencia de equipos agrupados por características comunes, los procedimientos de mantenimiento se minimizan, pues se desarrollan para grupos de equipos en lugar de equipos individuales.

Este tipo de clasificación alcanza mayores resultados en la optimización de la documentación guía para la realización del mantenimiento, cuando se agrupan actividades que pueden estar relacionadas entre sí de alguna forma, ya sea porque se realizan en

secuencia, o porque se ejecutan en equipos de un mismo sistema, constituyendo procedimientos mayores conocidos como gamas de mantenimiento.

Las gamas de mantenimiento alcanzan diferentes niveles de jerarquía y pueden existir gamas para mantenimiento anual, la cuales abarcan a su vez gamas semestrales, que comprenden a su vez varios procedimientos de mantenimiento. Otra peculiaridad de las gamas es que proporcionan un estimado de piezas de repuesto y recursos humanos requeridos, herramientas específicas y secuencias de trabajo. De esta forma se obtienen gamas destinadas al mantenimiento, que sirven simultáneamente a determinados equipos o sistemas.

Adicionalmente, en la elaboración del plan es necesario prever la posibilidad de realizar mantenimientos simultáneos en varios sistemas y equipos, lo cual dependerá, entre otros factores, de la existencia de equipos redundantes, de las limitaciones de tiempo y las configuraciones permisibles de equipos fuera de servicio, según lo establecido en las especificaciones técnicas o en las normas y procedimientos de operación. Este último aspecto conduce a agrupar los equipos según que puedan ser sometidos simultáneamente a labores de mantenimiento, lo cual comporta la necesidad de establecer paquetes de mantenimiento integrados por agrupaciones de equipos que, dadas las características específicas de las condiciones de explotación de la instalación, pueden planificarse para recibir mantenimiento de manera simultánea.

En la actividad de almacenes, la clasificación de partes y piezas de repuesto, independientemente de su categorización primaria por la influencia que tienen sobre la seguridad, la disponibilidad, o el valor económico del equipo que las demande, exige especificidades propias que corresponden, por regla general, al equipo o grupo de equipos (sistemas) que las requieran.

2.1.9. Clasificación por Criterios de Riesgo en base a estudios de APS

La clasificación por aplicación de criterios de riesgo es una modalidad novedosa entre los sistemas de clasificación, que ha sido utilizada con éxito en instalaciones de alto riesgo, como resultante de la aplicación del Análisis Probabilístico de Seguridad.

Esta clasificación se basa en la utilización de criterios probabilísticos cuantitativos, obtenidos a partir de los datos de fiabilidad de equipos, de los procedimientos operacionales y de mantenimiento, de los índices de fiabilidad humana y de los modelos de árboles de fallas y de eventos del APS, mediante los cuales se logra identificar los elementos componentes del sistema que contribuyen en mayor medida a la generación de situaciones de riesgo.

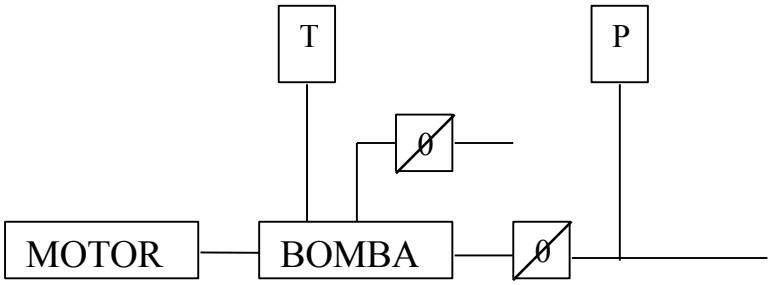
2.2. Sistema de Codificación Coherente

Ninguna actividad en la industria moderna, donde se operan, mantienen y controlan cantidades apreciables de equipos, puede prescindir de un sistema de codificación. Sin embargo, los sistemas de clasificación utilizados en las actividades de gestión suelen presentar problemas a la hora de establecer un adecuado sistema de codificación que permita identificar los equipos y a la vez que tome en consideración criterios específicos de diferentes áreas (mantenimiento, operaciones, almacenes, etc.)

El sistema de codificación, aunque simplifica las tareas, no resuelve por sí solo las complejidades relacionadas con el control de equipos y de las actividades que se desarrollan en la industria moderna, razón por la cual, en una planta industrial de relativa complejidad, donde los procesos y las actividades son altamente dinámicos es indispensable el uso de la informática. Por consiguiente, los sistemas de codificación en instalaciones modernas son también soporte para la automatización del control de las actividades, lo que redunda en ventajas, por cuanto se optimiza el empleo de personal y disminuye tanto la documentación, como los errores humanos relacionados con el control.

Si el sistema de codificación es adecuado, en ocasiones basta solamente el código del equipo para identificarlo y para establecer relaciones con otros parámetros vinculados con su clasificación respecto a otras actividades. Un ejemplo lo constituye el sistema de codificación utilizado para identificar agrupaciones en las órdenes de trabajo de mantenimiento, donde una agrupación es un conjunto de equipos sujeto a mantenimiento simultáneo. En otras palabras, la agrupación constituye un paquete de mantenimiento, que se identifica por el código del equipo más significativo incluido en la agrupación. De esta forma se garantiza un control más adecuado desde el punto de vista de la informática. Un ejemplo concreto puede apreciarse a continuación:

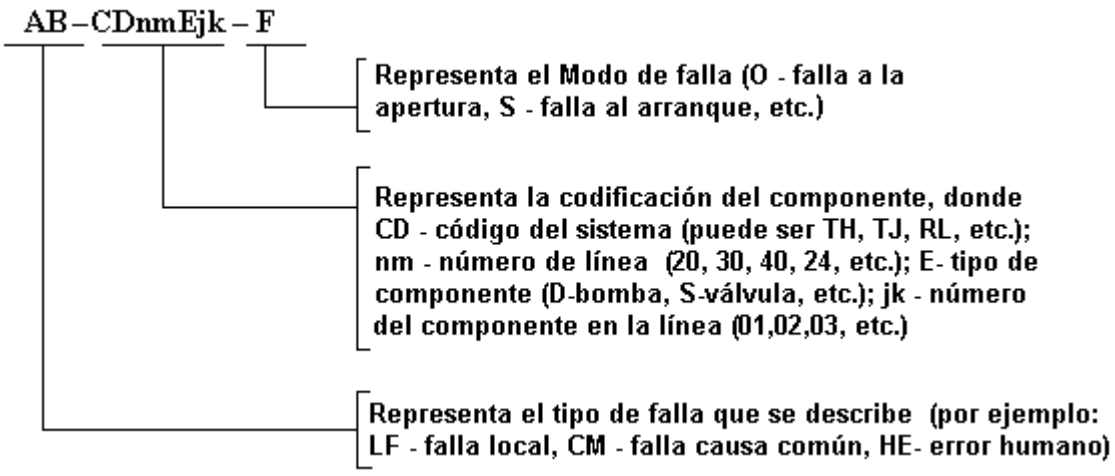
Agrupación TH20D01



que incluye motor, bomba, válvulas, manómetro y termómetro, y se identifica por el código de la bomba motorizada.

Un sistema de codificación adecuado permite además realizar labores de búsqueda automática en los registros de información almacenados en las computadoras. Los registros deben ser únicos para cada equipo, pero deben tener una configuración tal que permita identificar equipos de un mismo sistema, o equipos del mismo tipo u otra característica que resulte de interés para el usuario.

Por ejemplo el sistema de codificación, utilizado en algunas tareas de modelación de APS], tiene la siguiente estructura:



Esta codificación permite la búsqueda por el código completo o sub-código, lo cual ayuda a la localización de componentes en la base de datos por distintos criterios de búsqueda, tales como: tipo de falla, sistema tecnológico, tipo de componente, modo de falla, código de componente, entre otros.

2.3. Bases de Clasificación de Sistemas en Instalaciones de Riesgo Potencial

Cuando se trata de instalaciones de riesgo potencial, el objetivo primordial debe ser la seguridad, razón por la cual la clasificación de sistemas debe enfocarse al establecimiento de requisitos para evitar o minimizar, en caso de que se produzca, la liberación de sustancias nocivas o peligrosas al medio ambiente. Por consiguiente, la clasificación de los sistemas, estructuras y componentes relacionados con la seguridad se hace con el objetivo de establecer requisitos graduales, según la clase o categoría en que se incluyan los sistemas, estructuras y componentes en cuestión.

La clasificación se basa fundamentalmente en dos métodos:

- El método determinístico: que fija requisitos para aquellos sistemas, componentes y estructuras relacionados con la seguridad. Esta modalidad no tiene en cuenta criterios

probabilísticos, es decir, no considera la probabilidad de requerir el funcionamiento de los sistemas de seguridad, ni la fallida acción de sus efectos mitigativos.

- El método probabilístico: que establece requisitos para los sistemas, componentes y estructuras de acuerdo a su importancia relativa, obtenida a partir de criterios probabilistas, tales como:

    - Importancia de la función de seguridad en la cual participan los sistemas, estructuras y componentes, que a su vez dependerá de la probabilidad de requerirse la función y de las consecuencias de su fallida intervención.

    - Importancia de los componentes/sistemas que participan en las funciones de mitigación modeladas en el análisis de riesgo, y obtenidas a partir del peso de la indisponibilidad individual con respecto a la frecuencia total de daño tecnológico de la instalación.

En este caso, se trata de utilizar convenientemente las medidas de importancia RRW (medida de reducción de riesgo) y RAW (medida de incremento del riesgo) o su aplicación (estudios de priorización), para ordenar los componentes según el valor de su contribución a la falla o a la supervivencia del sistema.

Salvo raras excepciones, en la industria convencional se siguen criterios determinísticos para establecer la clasificación de los sistemas y, por consiguiente de los requisitos impuestos sobre las actividades relacionadas con la seguridad (diseño, mantenimiento, etc.).

2.4. Clasificación por Métodos Probabilísticos

Entre las principales ventajas de la clasificación probabilística se cuenta la de establecer requerimientos a los sistemas, estructuras y componentes basados en criterios realistas. La disminución del factor subjetivo en el establecimiento de requerimientos se debe a que la importancia del sistema, estructura y/o componente está basada en valores cuantitativos que representan su impacto sobre el sistema (cuando la medición obedece a la clasificación según la importancia de sistemas y componentes), o el riesgo de no cumplir la función de seguridad (cuando la medición toma en cuenta la clasificación por función de seguridad).

Por otra parte, si los parámetros de riesgo calculados por uno u otro método estuvieran penalizados por incertidumbres elevadas, los resultados obtenidos permitirán al menos determinar los puntos más débiles, por su contribución relativa al riesgo y establecer requerimientos más estrictos en base a prioridades.

Una particularidad importante de la clasificación por funciones de seguridad es que resulta de mayor alcance que la derivada de la determinación de las medidas de importancia. Ello se debe a que la primera abarca tanto sistemas de explotación normal (previstos para evitar que incidentes operacionales conduzcan a situaciones de accidente) como sistemas destinados a mitigar las consecuencias de los accidentes.

2.5 Aplicación de la Clasificación de Componentes y Sistemas por su Importancia, según estudios de APS

Los resultados obtenidos a partir de un estudio de APS pueden servir tanto para corroborar la clasificación realizada de acuerdo a otros criterios, así como para cuestionarla en algunos casos. A continuación se describen algunas aplicaciones en este sentido:

1- Optimización de especificaciones técnicas:

Las especificaciones técnicas de funcionamiento están formadas por un grupo de procedimientos y guías del operador, en las cuales se reflejan los límites y condiciones operacionales de trabajo de la instalación, las acciones que el operador debe realizar para mantenerla dentro de tales límites, así como las actividades que deben ejecutarse para cumplir con las condiciones operacionales.

Precisamente en este último grupo se encuentran las actividades relativas a la prueba periódica de sistemas y componentes, y los límites de tiempo fuera de servicio permisible para ellos.

Es común que en las instalaciones de riesgo potencial existan sistemas encargados de mitigar las consecuencias de los accidentes. Estos sistemas, por regla general, se encuentran a la espera, por lo que al someterlos a un régimen de pruebas periódicas disminuye su probabilidad de fallar, ya que la prueba rompe los mecanismos de falla relacionados con el régimen de espera, como oxidación, acumulación de humedad, etc. A la vez, la prueba periódica puede aportar indisponibilidad ya que, en ocasiones para su cumplimiento, es necesario sacar componentes fuera de servicio o realinear sistemas.

Otro problema surge cuando se detectan fallados los sistemas de mitigación y es necesario repararlos en un tiempo razonable, dentro de límites preestablecidos (tiempo permisible fuera de servicio), los cuales están relacionados con los equipos redundantes disponibles y la importancia de las funciones que dichos sistemas cumplen.

Como resultado de los estudios de priorización, se identifican los componentes que mayor impacto tienen en la reducción del riesgo de la instalación, una vez que se aplica una correcta estrategia de pruebas y se adoptan los tiempos fuera de servicio adecuados. La aplicación práctica del APS en aquellos casos en los cuales se establecían las especificaciones técnicas solamente en base a criterios determinísticos, se identificaron problemas representados por:

- Estrategias de pruebas inadecuadas: intervalos entre pruebas o duración de las pruebas excesivos o deficientes.
- Tiempo permisible fuera de servicio incorrecto.
- Configuraciones críticas (combinación de equipos fuera de servicio que comprometen la seguridad de la instalación).

2- Optimización del mantenimiento:

En una instalación de relativa complejidad, es tradicional disponer de un plan de mantenimiento en el cual se organizan actividades de intervención periódicas planificadas. Sin embargo, por lo general, el plan está elaborado en base a una clasificación de sistemas soportada por criterios determinísticos.

La experiencia de la aplicación del APS en dichas industrias ha permitido detectar deficiencias en la clasificación de los equipos, así como la realización de mantenimientos simultáneos inadecuados.

La solución de estos problemas puede lograrse mediante la determinación de indicadores de priorización por mantenimiento, para resolver el primero de ellos, y la adopción de medidas dirigidas a evitar las configuraciones críticas, para resolver el segundo. Tanto una actividad como la otra implica la realización de una reclasificación de equipos, utilizando los resultados de los estudios mencionados.

Como resultado, el estudio de las configuraciones críticas puede llevar a la reconsideración de los paquetes de mantenimiento, mientras que la priorización por mantenimiento puede conducir al establecimiento de nuevas prioridades, lo cual, lógicamente, introduce modificaciones en el plan de mantenimiento.

3- Optimización de la Garantía de la Calidad:

La Garantía de la Calidad en una industria no se reduce al simple control de la calidad del producto terminado; por el contrario, es el resultado del seguimiento a los atributos de la calidad a lo largo del proceso productivo en todas sus fases. Para lograr tal propósito es indispensable que todos los procesos y actividades de la industria estén desarrollados en base a procedimientos preestablecidos, incluyendo las labores administrativas y las actividades de operación y mantenimiento.

En una clasificación sobre bases probabilísticas, la vigilancia de los equipos relacionados con la seguridad y, por tanto los procedimientos de Garantía de Calidad asociados, habrán de ser más rigurosos mientras mayor sea su impacto en el riesgo de daño tecnológico.

Es por tanto útil para los fines de la Garantía de Calidad, la clasificación de sistemas y componentes, utilizando los recursos de categorización que facilita el APS.

4- Optimización de los requisitos de diseño.

Los requisitos de diseño deberán ser más estrictos para los equipos que mayor importancia tengan para la seguridad. Por ello, una gradación de los requisitos de diseño, de acuerdo a la clasificación obtenida a través de los estudios de importancia aplicando el APS, permitirá enfocar directamente la rigurosidad de los requisitos de diseño a los contribuyentes más importantes por su impacto al riesgo.

5- Optimización de las actividades de parada de planta.

Una de las modalidades más recientes de la aplicación de la metodología de APS es el llamado APS en parada. Hay instalaciones en las cuales, aún después de la parada de la planta, continúan desarrollándose procesos riesgosos de liberación de energía (liberación de energía residual en reactores nucleares) o procesos con reacciones remanentes (en reactores en la industria química) o incluso actividades de mantenimiento que pueden ser fuentes potenciales de accidente (incendio en industrias petroquímicas).

Por las características de los procesos señalados, es necesario que se mantengan activas determinadas funciones de mitigación para el control de accidentes, en caso que llegaran a producirse, aun cuando los riesgos en situación de parada no son de igual magnitud que cuando la instalación se encuentra operando a la potencia máxima de diseño.

Es necesario advertir que durante las paradas, habida cuenta de que los riesgos son menores y se realizan mantenimientos a gran escala, se tiende a un relajamiento de la necesaria cautela, por lo cual puede descuidarse el control de los sistemas de mitigación, o realizarse manipulaciones (desconexión de la red eléctrica o actividades de mantenimiento) que los inhiben para el cumplimiento de sus funciones. En tales condiciones, la situación puede empeorar en caso de accidente.

La realización de los APS en parada va acompañada de la obtención de parámetros similares a los ya explicados para APS en operación (conjuntos mínimos más importantes, ordenamiento según medidas de importancia, estudios de priorización). Por lo tanto, es posible, a partir de estos resultados, optimizar las actividades de parada, otorgando prioridad a los equipos que en dicho estado contribuyen mayormente al riesgo, o evitando las configuraciones críticas cuando deban ejecutarse mantenimientos simultáneos.

A título de ejemplo, a continuación se incluye la tabla de clasificación de equipos pertenecientes a una central de generación termoeléctrica, según los criterios de mantenimiento adoptados por el SOMCE (Sistema de Organización del Mantenimiento de Centrales Eléctricas)

2.6. Clasificación de equipos importantes en centrales eléctricas

Para los fines de la clasificación, se tienen en cuenta los siguientes aspectos:

1. - Importancia del equipo dentro del proceso de producción
2. - Complejidad tecnológica del equipo.
3. - Costo total del equipo.
4. - Recursos necesarios para ejecutar el mantenimiento.

Según los criterios expuestos, los equipos se clasifican en cuatro categorías obedeciendo a las definiciones que las caracterizan, las cuales se describen a continuación:

Equipos Categoría A

- Son los equipos fundamentales en el proceso de producción y su salida para mantenimiento representa la paralización del bloque, estando condicionada por autorización especial.
- Los recursos financieros, materiales y el personal necesario para realizar su mantenimiento implican costos elevados.
- Los ciclos y plazos fijados para el mantenimiento son controlados por la entidad reguladora competente.
- Requieren la intervención de personal altamente especializado, con vasta experiencia y calificación para realizar el mantenimiento.

Equipos Categoría B

- Son equipos cuya parada afecta parcialmente la generación o disminuyen la confiabilidad del proceso de producción.
- Dentro del proceso de producción tienen una importancia menor que los de categoría A.
- Requieren personal de alta calificación para realizar el mantenimiento, aunque en menor grado respecto a lo que se requiere para los equipos categoría A.

Equipos Categoría C

- Son equipos que pertenecen al proceso de producción, pero su salida para mantenimiento no afecta a la generación.
- Dentro del proceso de producción tienen una importancia menor que los de categoría B.
- Los recursos necesarios para mantenimiento son menores que los necesarios para los de Categoría B.

Equipos Categoría D

- Son equipos que no influyen directamente en el proceso de producción.
- Dentro del proceso de producción tienen una importancia menor que los de categoría C.

Al establecerse la clasificación, deben considerarse los aspectos siguientes:

- La clasificación de un equipo primario mecánico corresponderá con la del equipo eléctrico primario correspondiente y viceversa.
- Los equipos que tienen elevada importancia dentro del proceso de producción, pero en cuyo mantenimiento no se utilizan grandes recursos, se considerarán dentro de la clasificación establecida, pero se les añadirá la palabra crítico, lo cual indica que debe prestarse atención especial durante su mantenimiento.

Seguidamente se enumeran los equipos clasificados por categoría.

Clasificación	Equipos
Categoría A	- Caldera - Turbina (incluye condensador) - Generador - Transformador de salida
Categoría B	- Bomba de Alimentar - Bomba de Condensado - Bomba de Circulación de agua de mar - Bomba de Aceite de Arranque - Calentadores de alta presión y de baja - Ventiladores de tiro forzado e inducido - Excitatrices - Grúas mayores de 25 t - Mallas Rotatorias - Bombas de enfriamiento mayores de 15 m3/h - Compresores mayores de 10 m3/h - Transformadores de distribución - Transformadores de servicio de planta - Interruptor de campo - Interruptores mayores de 13.8kv - Transformadores mayores de 33kv - Pilas electrolíticas - Banco de batería de emergencia - Calentadores de Aire Regenerativo - Sistema de regulación de voltaje
Categoría C	- Bombas de aceite de sellaje (Crítico) - Bombas de lubricación de reserva (Crítico) - Eyector Principal - Bombas de enfriamiento menores de 15 m3/h (Crítico) - Extractor de hidrógeno (Crítico) - Bombas de drenaje calentadores de baja presión (C.B.P.) - Bombas de transferencia de condensado o drenaje - Bombas dosificadoras - Compresor de hidrógeno - Compresor de aire acondicionado del mando térmico - Quemadores de petróleo - Bombas de petróleo - Bombas de gasoil - Bomba de suavizamiento de condensado - Bomba de agua cruda - Bomba de agua descarbonatada - Bomba de transferencia de agua - Eyector de sellos - Tanque principal de aceite (Crítico) - Tanque de sellaje

	- Tanque de emergencia de los sellos - Grúas o winches de 6-25 t - Filtros de tratamiento de agua - Filtros de petróleo - Enfriadores - Compresores de menos de 10 m3/h - Bombas de lavado de mallas - Calentadores de petróleo - Eyectores económicos y de arranque - Bombas de condensado de petróleo - Equipos del sistema de limpieza de caldera (lluvia de bolas e inyectores de vapor) - Bombas de ácido y álcali
Categoría D	- Bombas de servicio contra incendio (Crítico) - Bombas del sistema de aire acondicionado - Bombas de transferencia de aceite - Bombas de achique - Bombas de vacío de la casa de electrólisis - Bomba de prueba hidráulica - Bomba de lavado de calentadores de aire (CAR) - Tanque de almacenamiento de aceite - Equipos del sistema de aire acondicionado - Extractores y ventiladores de los edificios - Compresores comerciales - Grúas y winches hasta 5 t - Purificadores de aceite - Equipos de iluminación - Equipos de soldadura - Paneles

2.7. Riesgo y Seguridad

Resulta incuestionable el hecho de que existe una relación muy estrecha entre los sistemas de producción de una planta, los riesgos asociados a la operación y mantenimiento de los mismos, y los sistemas de prevención y protección que hayan sido diseñados y puestos en funcionamiento para reducir tales riesgos hasta límites razonablemente aceptables, teniendo en cuenta tanto el aspecto de la seguridad como el de la economía de la empresa.

En dependencia de la complejidad de las plantas industriales y de la peligrosidad de los procesos productivos, resultará necesario adoptar sistemas y procedimientos de prevención y protección cuyo variedad, diseño y efectividad deberá ajustarse convenientemente a los niveles de seguridad que se desea alcanzar. A continuación y de forma general, se enumeran los sistemas y procedimientos de prevención y protección que pueden contribuir a gerenciar técnicamente la seguridad industrial y optimizar la gestión de riesgos.

SISTEMAS Y PROCEDIMIENTOS DE PREVENCIÓN Y PROTECCIÓN

- Sistemas de detección temprana y monitoreo
- Sistemas de mitigación de accidentes y liquidación de averías
- Planes de contingencia
- Planes de Emergencia
- Auditorías de Sistemas de Seguridad
- Programas de capacitación y adiestramiento
- Análisis Probabilístico de Seguridad (APS)

Los **sistemas de detección temprana y monitoreo** son aquellos que permiten revelar signos de lo que podría constituir el inicio de un suceso accidental. Entre esta clase di sistemas se incluyen los de detección de humo y de calor, que permiten alertar al personal acerca de la presencia de un conato de incendio.

Entre los **sistemas de mitigación de accidentes y de liquidación de averías** se encuentran aquellos que intervienen para evitar o minimizar las consecuencias de un suceso accidental, tales como los sistemas antincendio o de enfriamiento, los sistemas de interrupción del suministro eléctrico en caso de variaciones incontrolables del voltaje, o los sistemas que permiten realizar una parada de planta segura, cuando las condiciones de trabajo así lo exijan.

Los **planes de contingencia** contemplan los procedimientos y acciones que han de tomar los operadores durante la evolución de una secuencia accidental, una vez que las condiciones hayan llegado a rebasar las previstas en el diseño de la instalación, pero antes de que sobrevenga realmente un accidente grave. Esas medidas pudieran alterar o revertir la marcha del accidente. Con ello se persigue llevar las instalaciones a una condición estable y asegurar la integridad de los trabajadores. Los planes de contingencia son sujetos a revisión

permanente y deben ser ensayados periódicamente para mantener al personal debidamente entrenado en su ejecución.

Los **planes de emergencia** están dirigidos a mitigar los efectos sobre el personal y la población que pueden resultar del impacto interno y externo del accidente ocurrido en una instalación. Ello significa que su concepción y ejecución requiere de la participación de diversas organizaciones e instituciones técnicas, incluyendo autoridades y organismos públicos a diferentes niveles.

Estos planes comprenden el conjunto de actividades necesarias, para que en caso de accidente con posible liberación de sustancias nocivas al medio ambiente, se puedan ejecutar todas las acciones requeridas para la protección del personal de la instalación y de la población. Una vez elaborados, los planes se ensayan periódicamente probando sus correspondientes medios de comunicación y logística, y son lo suficientemente flexibles para adaptarse, de acuerdo a las circunstancias, a una variedad de condiciones particulares.

Ciertos componentes de las plantas son clasificados como "importantes para la seguridad" y a causa de su relevancia respecto a la salvaguarda de la salud pública y la seguridad, es necesario implementar un programa de auditoría de **auditoría de los sistemas de seguridad** que deberá aplicarse a todas las actividades vinculadas con equipos importantes para la seguridad. El propósito central del programa es establecer una serie de acciones sistemáticas y planificadas para garantizar plena confianza en que esos equipos en particular se comportarán satisfactoriamente mientras se encuentren en servicio.

El **entrenamiento de los operadores** es un proceso extensivo y continuo, producto de una combinación entre clases en aula, ejercicios en simuladores y actuaciones en la planta, en la medida que ello sea posible y apropiado. Los procedimientos y el entrenamiento deben ser diseñados específicamente para reducir los errores por parte del operador, mediante una mayor familiarización de las personas con las acciones prescritas, reduciendo el esfuerzo de memorización y minimizando la distracción debido a cuestiones de menor importancia.

Es necesario definir cuales sistemas, subsistemas y funciones son relevantes en relación con la seguridad, de modo tal que sea posible focalizar la atención en aquellos requerimientos de mantenimiento que estén dirigidos a satisfacer las metas de seguridad de la planta. Adicionalmente, es importante identificar las funciones que cada uno de los sistemas y subsistemas deben cumplir. Será entonces posible identificar los componentes que dan efectivamente sustento a las funciones de seguridad.

El **Análisis Probabilísticos de Seguridad (APS)** es una herramienta apropiada para seleccionar y evaluar los sistemas, subsistemas y funciones importantes para la seguridad, incorporando la experiencia operativa y de mantenimiento acumulada en la planta. El análisis consiste en la medición de la probabilidad de ocurrencia asociada a las secuencias accidentales y detectar posibles debilidades en los sistemas de seguridad, así como examinar el impacto de las modificaciones que se pretenda introducir, buscando mejorar el desempeño de dichos sistemas.

Las interrelaciones entre los procedimientos operacionales de emergencia (POE), las guías para la gestión de accidentes graves y las acciones fuera de los límites de la planta pueden ser planificadas y evaluadas a través de estudios de APS, con el propósito de minimizar las consecuencias de accidentes severos, considerando todo el espectro de posibilidades y probabilidades de ocurrencia, así como las respuestas de la planta en situación de accidente que se derivan del análisis de una variedad de posibles escenarios configurables mediante el empleo del APS.

Cuando la operación de los sistemas de protección de la planta, normados mediante los procedimientos operacionales de emergencia, no logra liquidar un accidente, se entra en el campo de la gestión de accidentes severos, en cuyo caso se puede recurrir a cualquier medio, interno o externo, para mitigar el accidente y sus consecuencias.

Los resultados del estudio de APS, por ser una fuente adecuada para identificar las secuencias accidentales, clasificarlas por grupos funcionales y facilitar la descripción de las respuestas de la planta y sus puntos vulnerables, puede constituir el primer paso para desarrollar un sistema de gestión de accidentes severos. El APS puede proporcionar sustento al desarrollo de estrategias contra las vulnerabilidades detectadas, así como herramientas de cálculo que facilitan la selección y aplicación de las estrategias, o su rechazo cuando los resultados revelan efectos potencialmente negativos.

La aplicación del APS en esta área en particular, además de la identificación de las secuencias accidentales, apunta hacia el análisis cronológico de los accidentes, identificando las rutas de éxito (estrategias), estableciendo prioridades para reforzar la seguridad, reducir el riesgo y construir las bases para el entrenamiento de los operadores y el desarrollo de los procedimientos.

En el campo de la industria nuclear se habla de accidente severo y situación de emergencia cuando el evento ocasiona daños al reactor y al domo de contención, dando lugar al escape masivo de partículas radiactivas hacia el ambiente externo. También en la industria convencional pueden ocurrir eventos similares, con consecuencias catastróficas. Ejemplo de ello se tiene en Italia (Seveso - 1976), Venezuela (Tacoa – 1982), India (Bophal - 1984) ocasiones en las cuales el desarrollo incontrolable de los accidentes rebasó las fronteras de las plantas, ocasionando entre las comunidades del entorno un número importante de personas fallecidas, daños ecológicos incalculables, destrucción de bienes muebles e inmuebles, así como pérdidas multimillonarias en sistemas, equipos e instalaciones.

CAPÍTULO III - ANÁLISIS Y GESTIÓN DE RIESGOS

Antes de entrar a considerar lo referente al análisis de riesgos y la metodología sugerida para adoptar un modelo de gestión de riesgos basado en el estudio de elementos de tipo probabilístico, se proporciona seguidamente la definición de algunos términos que se utilizan en el desarrollo de este tema.

Accidente: Suceso no deseado que interrumpe o interfiere el desarrollo normal de una actividad, y origina una o más de las siguientes consecuencias: lesiones personales, daños al ambiente, daños materiales.

Suceso Iniciador: Suceso ocurrido, dentro o fuera de la planta, que provoca la alteración de las condiciones de operación normal, al punto de requerirse actuaciones automáticas o acciones manuales, para llevar la planta a una condición segura y estable.

Secuencias accidentales: Cadenas de eventos que culminan en estado de daño a la instalación.

Árbol de eventos: modelo gráfico utilizado para determinar, mediante lógica binaria, los posibles estados finales de la instalación, resultantes de condiciones iniciales previamente establecidas, asociadas a un suceso iniciador.

En primer lugar, examinemos cuáles son las principales fuentes de riesgo en relación con la operación de una empresa industrial:

- Instalaciones y sistemas de producción y de apoyo
- Sistemas de seguridad y protección
- Prácticas y procedimientos operacionales
- Acciones de mantenimiento
- Capacitación y adiestramiento deficientes
- Planes de contingencia y emergencia ineficientes
- Eventos externos y fenómenos naturales

Las instalaciones y sistemas de producción y apoyo, así como los mismos sistemas de seguridad y protección, están sujetos al fenómeno de las fallas que, en determinadas circunstancias, pueden derivar hacia sucesos accidentales de cierta gravedad.

Por otra parte, los procedimientos y prácticas operacionales, por propias deficiencias o por la ausencia de una adecuada supervisión y/o revisión, pueden conducir al establecimiento de condiciones de funcionamiento que exceden los límites de diseño de la maquinaria y generar accidentes de consecuencias imprevisibles. Una situación similar ocurre en el caso de las acciones de mantenimiento, a causa de impericia del trabajador, deficiencias de los procedimientos o descuido por parte de los supervisores.

Una pobre capacitación o entrenamiento de los trabajadores tiene un peso determinante en el desempeño del personal, cuya actuación puede involucrar la comisión de errores o la

omisión de parte de los procedimientos de operación, creando así condiciones propicias para el desarrollo de sucesos accidentales.

Las deficiencias en los planes de contingencia y de emergencia constituyen un foco adicional de riesgo, considerando que son procesos diseñados precisamente para atacar una suceso accidental. Si la concepción de los planes compromete de alguna manera su efectividad, es posible que el accidente que pretende mitigar o combatir supere las barreras de seguridad y se torne totalmente incontrolable, con todas las consecuencias que tal situación podría comportar.

Los fenómenos naturales y los eventos provocados por el hombre tienen la posibilidad de ocasionar grandes pérdidas materiales y de afectar sectores importantes de población en las proximidades del sitio donde ocurren o a lo largo de su trayectoria; tales son los casos de fenómenos como terremotos, huracanes, tornados, inundaciones e impacto de meteoros, o de aquellos provocados por el hombre, tales como: incendios, explosiones y voladuras, caída de aviones, rotura de diques, choque de vehículos, derrame de contaminantes, entre otros.

3.1. Fuentes de riesgo y sucesos iniciadores

Para emprender el proceso de adopción de un modelo de gestión de riesgos, es preciso, en primer lugar, proceder a identificar las posibles fuentes de riesgo y los sucesos iniciadores que pueden dar lugar al desencadenamiento de las secuencias accidentales indeseadas

Sucesos iniciadores externos.

Estos sucesos tienen el potencial de crear las condiciones para que se produzcan fallas y disparos de equipos vitales para la operación normal de la planta. Sin embargo, los iniciadores externos tienen, además, la particularidad de poder afectar también la disponibilidad de los sistemas asignados para hacer frente a las fallas y disparos de equipos que desencadenan la situación accidental. Este aspecto hace que se confiera una importancia especial a la evaluación de los riesgos debido a los SI externos.

Los sucesos iniciadores externos está representados por: incendios, inundaciones y terremotos, caída de aeronaves, vientos extremos, tornados, escape de agentes químicos y proyectiles expelidos por equipos rotatorios.

Sucesos iniciadores internos

Se refieren a los sucesos originados dentro de las fronteras de la planta, cuyas causas se relacionan directamente con el proceso tecnológico (por ejemplo, falla o disparo de equipos, errores del personal de operación, etc.).

Iniciadores especiales de causa común

Se incluyen en esta categoría los sucesos que provocan un desbalance inadmisible en las condiciones de operación normal, que obligan a interrumpir inmediatamente las operaciones y que, adicionalmente, incapacitan a determinados sistemas necesarios para controlar el estado de la planta durante y después de su ocurrencia (por ejemplo, pérdida de la alimentación eléctrica externa, pérdida de agua de enfriamiento, desactivación de sistemas de control, etc.).

Para identificar los sucesores iniciadores internos, se emplean métodos tales como el FMEA (Análisis de Modos y Efectos de Falla), el Diagrama Lógico Maestro o el Árbol de Fallas. En la práctica, los sucesos iniciadores externos, por la dificultades que presenta su modelación, no suelen ser incluidos en los estudios de riesgo.

Por otra parte, en razón del amplio número de sucesos iniciadores que puede resultar del proceso de identificación, es conveniente que al final, éstos queden agrupados en función de los siguientes criterios:

- que requieran la actuación de los mismos sistemas de mitigación (funciones o sistemas de seguridad requeridos) y que los criterios de éxito de tales sistemas sean iguales en todos los casos;

- que impongan las mismas condiciones especiales de reacción a nivel de la planta (acciones manuales o respuestas automáticas);

- que el estado resultante en todas las secuencias de eventos sea el mismo.

3.2. Funciones y Sistemas de Seguridad

Los sucesos iniciadores constituyen el punto de partida de un accidente, sin embargo, la respuesta subsiguiente de los sistemas de la instalación destinados a su mitigación, determinará si el suceso alcanza finalmente la condición de accidente.

Además de la determinación de sus causas y su frecuencia de ocurrencia, el interés en los análisis de riesgo se centra en identificar las vías de desarrollo de los sucesos no deseados. Es por ello que se debe lograr distinguir las secuencias de eventos que culminan en estado exitoso de aquellas que concluyen en una situación de daño a las instalaciones.

A tal efecto, los estados de éxito se refieren a las secuencias que terminan con la neutralización de las condiciones adversas creadas por el iniciador, mientras que un estado de daño se alcanza cuando en el transcurso de la secuencia de eventos no se logra controlar los parámetros que fueron alterados, con lo cual el escenario de la avería empeora hasta concluir con daños de la instalación y consecuencias negativas para la incolumidad de la personas, el medio ambiente y/o la economía.

Las secuencias de eventos que culminen en estados de daño son las que deben ser cuantificadas, para determinar la frecuencia de daño de la instalación debida a todo el

conjunto de iniciadores definidos en el análisis de riesgo. A estas secuencias se les denomina secuencias accidentales.

Para poder determinar las secuencias accidentales, dentro de todas las posibles secuencias de eventos, debe definirse previamente qué y cuáles condiciones configuran el estado de daño a la instalación, ya que de ello depende directamente el número de secuencias a cuantificar y por tanto la frecuencia de daño estimada.

Una vez que hayan sido seleccionados y adecuadamente agrupados los sucesos iniciadores, se requiere determinar la respuesta de la planta ante éstos. Para evaluar la respuesta de la planta se deben definir las funciones de seguridad, es decir, aquellas que deben cumplirse para controlar las fuentes de riesgo de la planta.

Cada función incluye un grupo de acciones que deben realizarse, para evitar estados de daño de la planta tras la ocurrencia de un suceso iniciador. Se trata de un conjunto de acciones que se corresponden con las características del iniciador y que evitan la destrucción o el deterioro apreciable de las barreras que impiden o minimizan, por ejemplo, la fuga de sustancias tóxicas dentro de la planta o hacia el medio ambiente.

Cada función de seguridad debe identificarse con uno o varios sistemas de seguridad diseñados para cumplirlas. Adicionalmente, pueden existir en la planta sistemas que por sus características son capaces de cumplir una o más funciones de seguridad, aunque no estén designados específicamente para ello. Este aspecto es importante, ya que dichos sistemas constituyen reservas de seguridad que pueden contribuir a disminuir el riesgo en una medida apreciable y, por lo tanto, deben considerarse como tales en el análisis.

Del estudio detallado del diseño y operación de la planta se obtiene el listado de sistemas encargados de cumplir las respectivas funciones de seguridad y, por consiguiente, la interrelación entre las funciones y los sistemas, como se aprecia en el ejemplo a continuación:

Ejemplo de Funciones de Seguridad para
Central Electronuclear con Reactor PWR

FUNCIÓN DE SEGURIDAD	OBJETIVO
1. Control de reactividad	Detener el reactor para reducir el nivel de generación de calor al nivel de las posibilidades de evacuación de los sistemas de seguridad.
2. Control de inventario del sistema de refrigeración del reactor	Mantener el combustible rodeado de refrigerante
3. Control de presión del refrigerante primario	Mantener la presión del sistema de refrigeración del reactor en niveles apropiados.
4. Evacuación del calor del combustible nuclear	Transferir el calor generado en el combustible nuclear al sumidero de calor correspondiente.
5. Aislamiento de la contención	Cerrar las válvulas abiertas en las tuberías de sistemas que normalmente atraviesan el recinto de contención, para evitar escapes radiactivos.
6. Control de temperatura y presión en la contención	Mantener protegidas las estructuras de contención y los equipos situados en su interior.
7. Control de gases inflamables	Redistribuir o evacuar el hidrógeno que ingresa a la contención, para evitar su daño por explosión

Interrelación Función / Sistema de Seguridad.

FUNCIÓN DE SEGURIDAD	SISTEMA QUE LA CUMPLE
Control de reactividad	Sistema de Protección del Reactor Sistema de Inyección de Emergencia de alta presión.
Control de inventario del sistema de refrigeración del reactor	Sistema de Inyección de Emergencia de Alta Presión. Sistema de Inyección de Emergencia de Baja Presión
Control de presión del refrigerante primario	Válvulas de Seguridad / Alivio del Compensador de Presión
Evacuación del calor del combustible nuclear	-Sistema de Inyección de Emergencia de Alta Presión -Sistema de Inyección de Emergencia de Baja Presión -Sistema de Agua de Alimentación de Operación Normal. - Sistema de Agua de Alimentación de Emergencia. - Válvulas de Seguridad / Alivio del Compensador de Presión

Los sistemas relacionados se denominan sistemas frontales y se utilizan para la construcción del árbol de eventos de sistemas, como se verá más adelante.

3.3. Fiabilidad de los sistemas de Seguridad

Al igual que las instalaciones y la maquinaria destinadas a los procesos productivos, los sistemas de protección y seguridad también adolecen del fenómeno de las fallas, constituyendo éste un factor sumamente crítico, dadas la implicaciones que tiene la inactivación de tales sistemas sobre la seguridad global de la planta. Adicionalmente, para la elaboración de los árboles de eventos y la evaluación de las probabilidades de daño asociadas a las secuencias accidentales, es necesario conocer las probabilidades de falla de los equipos y sistemas vinculados a las funciones de seguridad.

Por consiguiente, es preciso considerar un programa de evaluación de la fiabilidad y disponibilidad de los sistemas de seguridad, así como establecer un programa de mantenimiento basado en parámetros de riesgo.

Para asegurar que toda actividad de mantenimiento relacionada con la seguridad, sea manejada adecuadamente dentro de los programas de mantenimiento de la planta, se requiere identificar claramente las metas generales de seguridad de la empresa.

Desde la perspectiva del mantenimiento orientado a la seguridad, estas metas son útiles para determinar el impacto de ciertas configuraciones operacionales o de las estrategias de mantenimiento sobre los objetivos declarados de seguridad, y su valoración puede ser utilizada para optimizar la programación de los mantenimientos en el curso de las operaciones o en ocasión de las paradas de planta.

Es necesario definir cuáles sistemas, subsistemas y funciones son relevantes en relación con la seguridad, de modo tal que sea posible focalizar la atención en aquellos requerimientos de mantenimiento que estén dirigidos a satisfacer las metas de seguridad de la planta. Adicionalmente, es importante identificar las funciones que cada uno de los sistemas y subsistemas deben cumplir. Será entonces posible identificar los componentes que dan efectivamente sustento a las funciones de seguridad y evaluar la fiabilidad y disponibilidad de los sistemas, a partir de la confiabilidad de sus componentes más relevantes en relación al riesgo.

3.4. El árbol de eventos de funciones.

Partiendo de las funciones de seguridad definidas, se procede a construir el modelo de respuesta de la instalación ante cada suceso iniciador o grupo de sucesos iniciadores definidos. El método más difundido en los estudios de APS utiliza la técnica de análisis de Árbol de Eventos.

El árbol de eventos es un modelo gráfico que se desarrolla sobre la base de una lógica binaria inductiva, es decir, se parte de una condición inicial (el suceso iniciador), prosiguiendo el análisis hasta culminar con la determinación de posibles estados finales de la planta claramente identificables (éxito o daño), resultantes de la condición inicial considerada.

Los elementos del árbol de eventos se denominan encabezamientos o cabeceras y se colocan ordenadamente de izquierda a derecha, comenzando por el suceso iniciador y continuando con los eventos, que en este caso son las funciones de seguridad requeridas para llegar a una condición de estado estable (ver Fig.1).

El orden de las cabeceras debe reflejar en el modelo las posibles dependencias funcionales, físicas y temporales entre ellas (ver Fig. 2). Así, los eventos que siguen al suceso iniciador se van ramificando en cada nodo, representándose sólo dos estados posibles para cada uno de ellos, el éxito de la función (rama superior) o su condición de falla (rama inferior).

Para una planta, este estado podría definirse como la superación de ciertos límites en una parte determinada de la instalación, a partir de los cuales se producen afectaciones a la salud del personal o de la población de los alrededores, y/o deterioro al medio ambiente exterior.

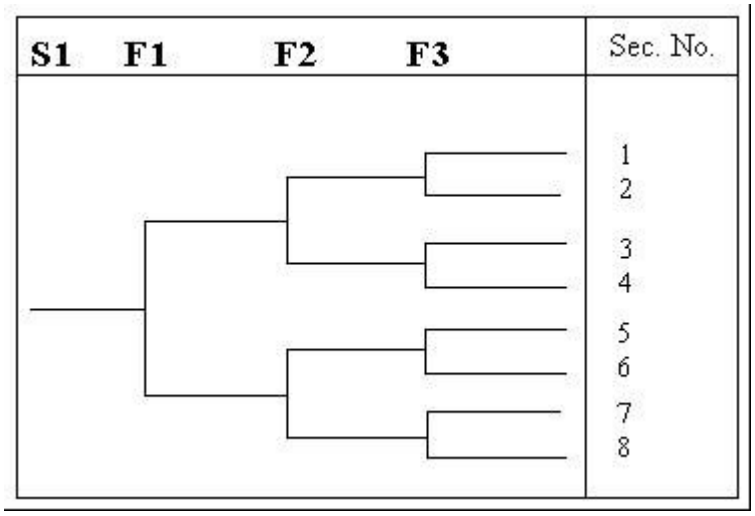


Fig. 1. Árbol de Eventos Hipotético (sin incluir dependencias)

En la Fig. 1 las cabeceras son las siguientes:

SI: Suceso iniciador (o grupo de sucesos iniciadores).
F1: Función de seguridad requerida No.1.
F2: Función de seguridad requerida No.2.
F3: Función de seguridad requerida No.3.

Como puede apreciarse, el número máximo de secuencias de árbol de eventos está determinado por la expresión 2^{n-1}, donde "n" es el número de encabezamientos del árbol. Sin embargo, al incluirse las dependencias entre los eventos que forman las cabeceras, y estando éstas ordenadas de manera adecuada, su número puede disminuir notablemente,

eliminándose secuencias imposibles o ilógicas. En la Fig. 2 puede verse este efecto, dadas las dependencias hipotéticas definidas entre los eventos.

Para que se comprenda cómo se construye un árbol de eventos, teniendo en cuenta todos los factores antes mencionados, considere las dependencias hipotéticas siguientes, a partir de las cuales el árbol representado en la Fig. 1 se convierte en el árbol de la Fig. 2.

Dependencias hipotéticas existentes entre las cabeceras de la Fig. 1.

a. Para mitigar el iniciador son necesarias la función F1 "y" la función F2 "o" la F3. Es decir, de acuerdo con las condiciones establecidas por el iniciador, la función F1 es imprescindible, así como una cualquiera de las otras dos (F2 o F3).

b. F1 debe tener éxito para que el resto de las funciones tengan la posibilidad de cumplirse satisfactoriamente. Esto significa que el éxito de F2 y F3 dependen del éxito de F1.

c. F2 y F3 son independientes entre sí.

Como se observa, en la Fig. 2 se omitieron las ramificaciones correspondientes a la falla de la función F1, ya que las restantes funciones no pueden tener éxito si F1 falla (secuencia No.4 de la Fig. 2). Ello significa que la rama de falla va en este caso directamente a un estado de daño de la planta, debido a que las funciones F2 y F3 no tendrán posibilidad de cambiar el estado final del escenario, aún cuando tenga éxito alguna de ellas.

Por otra parte, se omiten las ramas que siguen al éxito de la función F2 tras el éxito de F1, ya que en este caso el iniciador es mitigado y no se requiere la función F3 para alcanzar el éxito (secuencia No.1 de la Fig. 2).

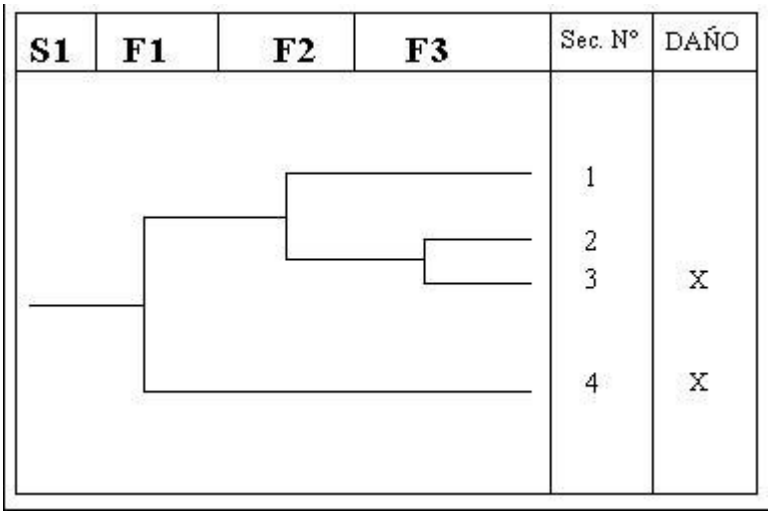


Fig. 2. Árbol de Eventos Hipotético (con dependencias incluidas).

Dicho de otra forma, el éxito o falla de F3 no cambia el estado final de la planta bajo las condiciones de este escenario. En el caso del éxito de F1 y falla de F2, se da oportunidad de éxito o falla de F3, ya que de esta última función depende la posibilidad de culminar el escenario con un estado de éxito o de daño (secuencia No.2, éxito y No.3, daño, Fig. 2). En el árbol de la Fig. 2 se han identificado como secuencias accidentales, las secuencias No. 3 y 4, mientras que las secuencias No. 1 y 2 terminan exitosamente.

3.5. El árbol de eventos de sistemas

Una vez construido el árbol de funciones, se elabora el árbol de eventos de sistemas, donde aparecen los sistemas y subsistemas encargados de su cumplimiento, considerando también en este caso, las dependencias existentes entre tales sistemas.

Los sistemas a incorporar en el modelo, llamados usualmente sistemas frontales, necesitan además de ciertas funciones de apoyo, para poder desempeñar su papel. Estas funciones, así como los sistemas que las garantizan, pueden aparecer o no de manera explícita en el árbol. Como ejemplo de funciones de apoyo, podemos citar: el suministro de alimentación eléctrica, de enfriamiento y lubricación, y de aire comprimido para el caso de válvulas neumáticas e interruptores de potencia.

La Fig. 3 representa el árbol de eventos de un sistema hipotético, construido, a manera de ejemplo, a partir del árbol de funciones de la Fig. 2 y considerando las siguientes dependencias supuestas.

Dependencias hipotéticas existentes entre las cabeceras de la Fig. 3

a. La función F1 la cumplen alternativamente los sistemas S1 y S2.
b. Los sistemas S1 y S2 son física y funcionalmente independientes
c. La función F2 la cumple el sistema S3.
d. La función F3 la cumple el sistema S4.
e. Los sistemas S3 y S4 son totalmente independientes.
f. El sistema S4 depende funcionalmente del sistema S1, por compartir los componentes de mayor contribución a la falla de ambos sistemas.

En la Fig. 3 puede verse el resultado de la omisión de ramas producto del análisis de las dependencias incorporadas. Nótese que en esta figura se ha incluido, además, un sistema de codificación para la falla de cada sistema y el suceso iniciador, cuestión que no se exige para los árboles de funciones. Este último aspecto tiene una importancia crucial para obtener un resultado coherente del análisis, que facilite, además, el seguimiento y la comprensión por parte del usuario del producto, es decir, el propietario de la instalación y otras instituciones que puedan servirse del mismo.

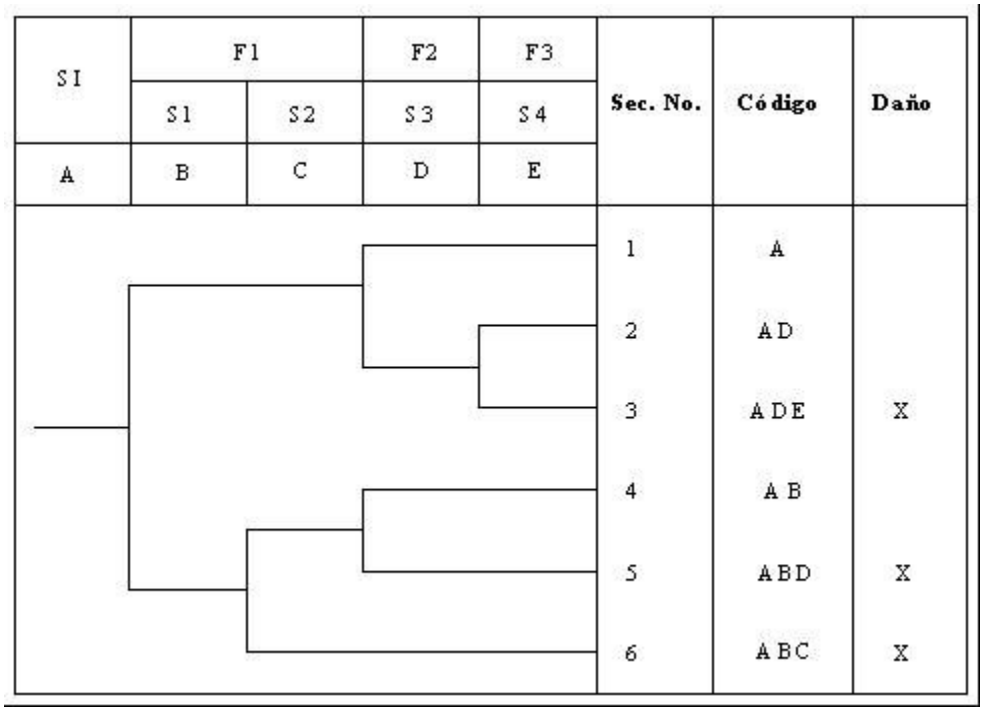
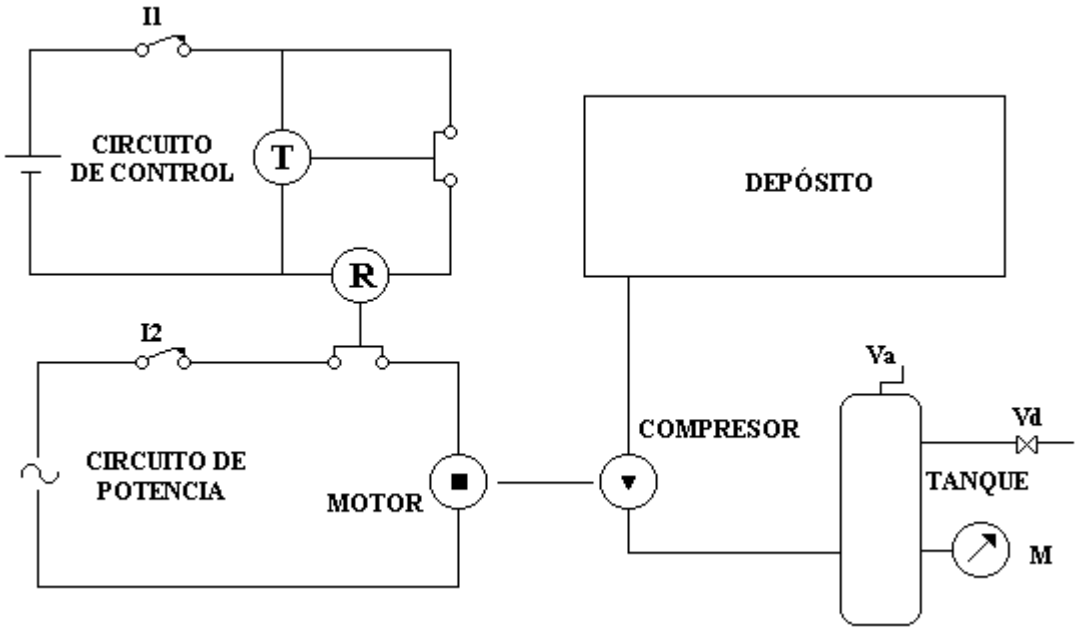


Fig. 3. Árbol de Eventos de Sistemas

3.6. Cálculo de las probabilidades de ocurrencia de estados de daño

Para estimar la probabilidad de daño a la planta, como consecuencia de una secuencia accidental, es necesario en primer lugar evaluar la probabilidad de ocurrencia de cada suceso primario, como resultado de la evaluación de la probabilidad de falla de los componentes que integran cada sistema de seguridad.

Para explicar el proceso de cálculo, nos serviremos como ejemplo del diagrama de una instalación de llenado y descarga de un tanque a presión, en la cual el proceso es controlado por un temporizador y se encuentra bajo la vigilancia de un operador encargado de activar cada ciclo del proceso y controlar que no se exceda la capacidad del tanque y se produzca su rotura por sobrepresión. A continuación se presenta el esquema que representa la instalación en cuestión.



SISTEMA DE LLENADO DE TANQUE A PRESIÓN

Los sistemas de seguridad a considerar en este caso, incluyen la intervención del operador para interrumpir el proceso mediante la desconexión del circuito de potencia o del circuito de control, a fin de evitar que una falla del sistema eléctrico mantenga energizado el moto-compresor de llenado del tanque. Como última medida para evitar el daño, se tiene la válvula de alivio del tanque que debería abrirse cuando se registre un exceso de presión en el tanque.

Los sucesos iniciadores para efectos del análisis son: la falla del timer (T), la falla del relay (R) y la presencia de sobrecorriente en el circuito de potencia (SC).

Luego de construir el árbol de fallas del sistema de llenado, se obtiene la información para determinar cuáles componentes constituyen los sucesos primarios, así como su probabilidad de falla, como se muestra en la Cuadro N° 1.

CUADRO N° 1 - Probabilidades de falla de sucesos primarios (para T = 8.000 horas)

Suceso Primario	**Código**	**λ**	**q_i**
Rotura del Tanque a presión normal	Tpn	1E-8/h	4,00E-5
No abre la válvula de alivio del tanque	Va	3E-4/h	6,21E-1
Manómetro bloqueado o indica menos presión	M	1E-5/h	3,90E-2
El operador no actúa (error humano)	E	1E-2/h	1,00E-2
Los contactos del relay fallan cerrados	R	2,7E-7/h	1,08E-3
Sobrecorriente en el circuito de potencia	SC	1E-8/h	4,00E-5
Los contactos del timer fallan cerrados	T	1E-4/h	3,12E-1
Los contactos del interruptor I1 fallan cerrados	I1	8E-6/h	3,13E-2
Los contactos del interruptor I2 fallan cerrados	I2	8E-6/h	3,13E-2

$q_i = 1 - \{1 - Exp(\lambda \times T)\} / (\lambda \times T)$

El análisis cualitativo y cuantitativo del árbol de fallas de la instalación permite identificar también los denominados Conjuntos Mínimos, es decir las combinaciones mínimas de componentes o sucesos primarios que conduce al evento final no deseado, que en este caso es la rotura del tanque por sobrepresión.

El Cuadro N° 2 muestra los Conjuntos Mínimos y las probabilidades de falla asociadas a los mismos.

CUADRO N° 2.- Probabilidades de falla de los Conjuntos Mínimos

Orden del CM	**CM**	**Probabilidad**
1	Tpn	4,00E-5
2	Va.SC	2,48E-5
3	Va.M.R	2,61E-5
	Va.M.T	7,45E-3
	Va.E.R	6,70E-6
	Va.E.T	1,94E-3
	Va.I2.R	2,10E-5
4	Va.I2.T.I1	1,90E-4
Total		9,78E-3

Nota: La probabilidad del CM es igual al producto de las probabilidades de los sucesos primarios intervinientes.

Después de obtener la estimación de la probabilidades de falla asociadas a los conjuntos mínimos resultantes de la evaluación cuantitativa de los sistemas, se construye el árbol de fallas de las funciones de seguridad, a objeto de determinar cuáles son los conjuntos mínimos, es decir las combinaciones de funciones, sistemas y sucesos primarios, incluyendo los errores humanos, la deficiencias en la estrategias de mantenimiento y otros factores que pueden intervenir en las secuencias accidentales y conducir al estado de daño de la planta.

En el Cuadro N° 3 se observan las probabilidades de falla asociadas a los Conjuntos Mínimos, así como la probabilidad total, que expresa el nivel de riesgo al cual se encuentra expuesta la planta en función de las secuencias accidentales consideradas.

CUADRO N° 3.- Probabilidades de falla de CM de las secuencias accidentales (SA)

Suceso Iniciador	CM	Probabilidad q_i/año
Los contactos del timer fallan cerrados	Va.M.T	7,45E-3
	Va.E.T	1,94E-3
	Va.I2.T.I1	1,90E-4
Total Iniciador T		***9,67E-3***
Los contactos del relay fallan cerrados	Va.M.R	2,61E-5
	Va.I2.R	2,10E-5
	Va.E.R	6,70E-6
Total Iniciador R		***5,38E-5***
Sobrecorriente en el circuito de potencia	Va.SC	2,48E-5
Total Iniciador SC		***2,48E-5***
Probabilidad Total		**9,75E-3**

Nota: La probabilidad de falla es igual a la suma de las probabilidades de falla de las funciones intervinientes.

El gráfico que se muestra a continuación corresponde al árbol de sucesos de sistemas asociado a la instalación de llenado utilizada como ejemplo, donde se indica con la letra E las secuencias que concluyen exitosamente y con la letra D aquellas que terminan produciendo daño a la planta..

Árbol de Sucesos de Sistemas

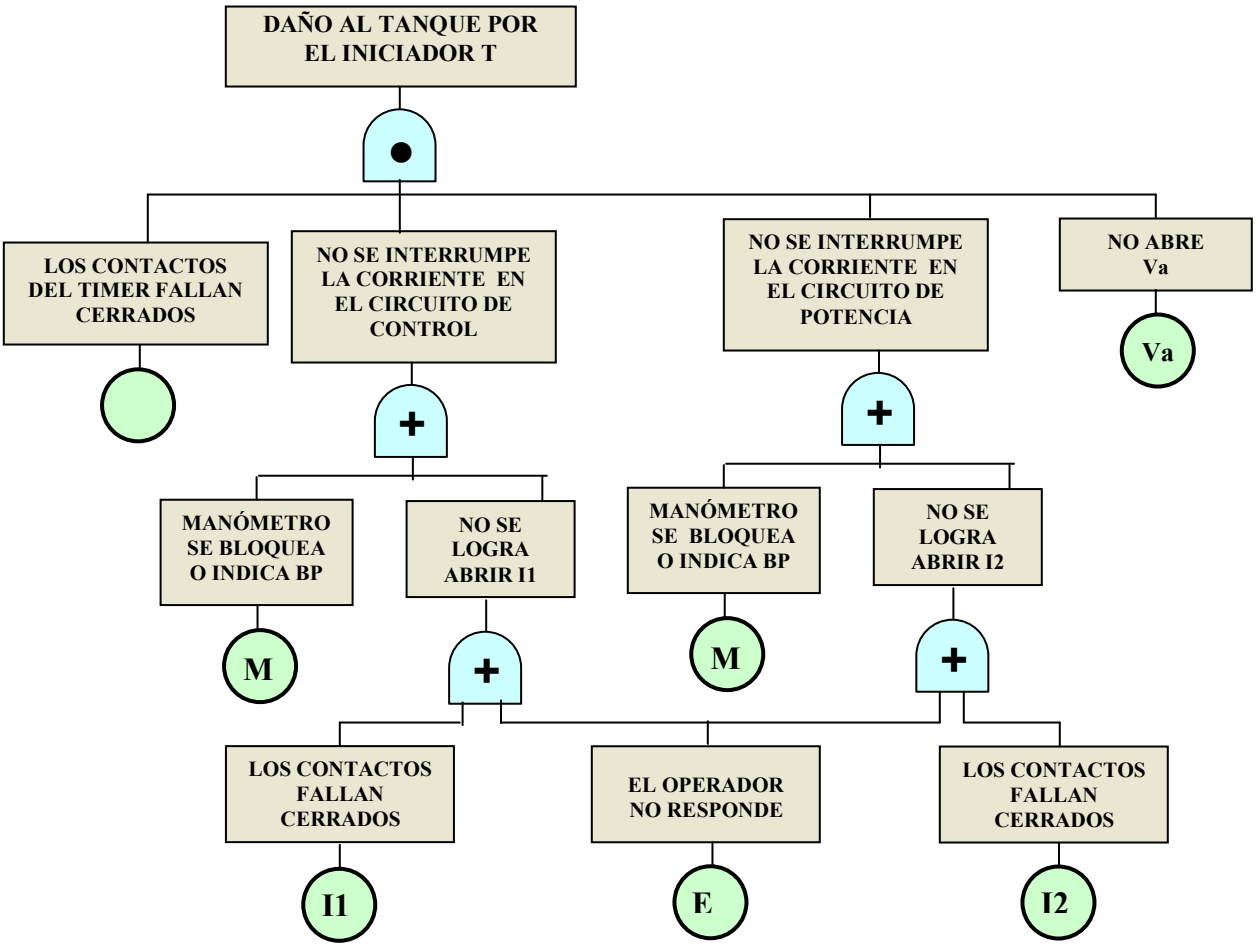
Iniciador	Funciones			Estado final
Los contactos del timer fallan cerrados	Desconexión por el operador		Protección de presión	
	Circuito potencia	Circuito Control	Apertura Va	
				E
				E
				E
				D

Iniciador	Funciones		Estado final
Los contactos del relay fallan cerrados	Desconexión por el operador	Protección de presión	
		Apertura Va	
			E
			E
			D

Iniciador	Funciones	Estado final
Sobrecorriente en el circuito de potencia	Protección de presión	
	Apertura Va	
		E
		D

Para complementar la información, se incluye así mismo el árbol de falla de las funciones de seguridad correspondiente al iniciador T (los contactos del timer fallan cerrados).

ÁRBOL DE FALLA DE LAS FUNCIONES PARA EL INICIADOR T



3.7. Toma de decisiones orientada a la reducción de riesgos

La misión crucial de la gerencia en el manejo de los elementos que revisten importancia respecto a la seguridad y el tratamiento de los factores que influyen en los niveles de riesgo de la actividad industrial, se centra fundamentalmente en lograr que el funcionamiento de las plantas sea una operación segura y confiable. Si bien una proporción substancial del trabajo se destina a ejercer el mayor control posible sobre las potenciales fuentes de riesgo, es innegable que el mantenimiento, aun siendo una actividad rutinaria, es un medio efectivo que contribuye no solamente a optimizar el funcionamiento de los equipos, sino también concurre en el logro de las metas que se plantean tanto en materia de seguridad como desde la perspectiva de la economía general de la empresa.

El mantenimiento centrado en confiabilidad (Reliability Centered Maintenance) y el mantenimiento orientado a la gestión de riesgos (Risk Oriented Maintenance) son enfoques sistemáticos de evaluación dirigidos al desarrollo y optimización de los programas de mantenimiento, y con ellos los índices de seguridad esperados. Ambos métodos representan formas lógicas y sistemáticas de considerar las funciones de los sistemas, subsistemas y componentes, los modos de falla de cada función, la importancia asociada a la función y su probabilidad de falla.

En el caso de los sistemas importantes para la seguridad, el APS es una herramienta única en la tarea de determinar la importancia relativa de los componentes, mediante el empleo de las llamadas medidas de importancia. Por consiguiente, el APS puede ser usado en conexión con el proceso del RCM, a fin de focalizar el análisis en los componentes más importantes desde el punto de vista de la seguridad..

Esta combinación ofrece ventajas en relación con los sistemas importantes para la seguridad y aquellos que son menos importantes, pero cuyo comportamiento tiene alguna influencia sobre la frecuencia de algunos eventos iniciadores de accidente o falla. El APS permite evaluar la significación de los componentes y su mantenimiento (planificado o no) logrando identificar las áreas de mayor impacto para la aplicación de los procesos del RCM, además de proveer la información requerida para la toma de decisiones.

El impacto que se logra mediante modificaciones en las estrategias de mantenimiento, sobre la base del RCM, puede ser evaluado mediante las herramientas del APS, a través de modificaciones controladas de las bases de datos, por ejemplo variando los valores de indisponibilidad de los sistemas analizados, de conformidad con las estrategias que se piense adoptar y modificando tentativamente las ratas de falla en base a criterios técnicos. La re-evaluación de los indicadores de seguridad y disponibilidad pondrán de manifiesto en qué medida se mejora la seguridad y se reduce el riesgo potencial. Además, se podrá extraer información realmente valiosa para tomar decisiones que conduzcan a lograr las metas de seguridad establecidas, manteniéndose dentro de parámetros óptimos de confiabilidad, disponibilidad y economía.