ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA QUÍMICA Y AGROINDUSTRIA

PROPUESTA DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD DEL IRRADIADOR DE COBALTO 60 DEL CENTRO DE IRRADIACIÓN DE LA EPN CON ENFOQUE EN SEGURIDAD FUNCIONAL (IEC 61508)

TESIS PREVIA A LA OBTENCIÓN DE GRADO DE MÁSTER (MSc.) EN SEGURIDAD INDUSTRIAL Y PREVENCIÓN DE RIESGOS LABORALES

DIEGO FERNANDO MONTALUISA IPIALES

DIRECTOR: ING. WILLIAM ESTUARDO VILLACIS OÑATE, MSc.

Quito, febrero 2021

DECLARACIÓN

Yo, Diego Fernando Montaluisa Ipiales, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

_____

Diego Fernando Montaluisa Ipiales

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diego Fernando Montaluisa Ipiales, bajo mi supervisión.

_____

Ing. William Esturado Villacis Oñate, MSc.

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A mi esposa María y a mi hija Sofía, por brindarme todo su apoyo durante todo este periodo de culminación de la Maestría y por soportar las largas horas de ausencia familiar que ha requerido la culminación de esta meta.

A mis padres y hermanos, por apoyarme a seguir creciendo profesionalmente e inculcarme todos los valores que, como persona, se requieren para terminar con éxito este peldaño más en mi vida.

A todos mis colegas del Departamento de Ciencias Nucleares, que me han ayudado con su tiempo y conocimiento durante la elaboración de esta tesis y un agradecimiento especial William Villacis por ayudarme en la dirección de este proyecto.

Un agradecimiento muy especial a Francisco Salgado (D.E.P.), ya que, con él, materialice la idea principal de este proyecto. Gracias a su apoyo como profesor y como persona, me compartió su conocimiento y su tiempo para tener las bases necesarias para terminar con éxito este proyecto de titulación.

A Dios y a todas las personas que me conocen, gracias por aportar de manera directa o indirecta a la culminación de este paso más de mi vida profesional, ya sea con su tiempo, ánimo, conocimiento o buenos y malos momentos, muchas gracias.

Diego F. Montaluisa I

ÍNDICE DE CONTENIDOS

PÁGINA

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PÁGINA

ÍNDICE DE ANEXOS

PÁGINA

RESUMEN

El objetivo del presente trabajo fue realizar un estudio para desarrollar el mejoramiento de los sistemas de enclavamientos de acceso al búnker y del sistema de control de nivel del blindaje húmedo del irradiador de Co-60. Para conseguir este objetivo, se utilizó el enfoque de seguridad funcional establecido por el estándar general IEC 61508 y el estándar específico IEC 61511 de la Comisión Internacional de Electrotecnia. El primer estándar se refiere a los sistemas eléctricos/electrónicos/electrónicos programables relacionados a la seguridad y el segundo a los sistemas instrumentados de seguridad de procesos industriales.

Con base en este enfoque, se desarrolló una propuesta de mejoramiento para los sistemas instrumentados de seguridad del irradiador de Co-60 citados inicialmente, adicionalmente, se utilizó la Metodología APS nivel 1, propuesta por el Organismo Internacional de Energía Atómica (IAEA), con la cual se evaluó cuantitativamente los sistemas instrumentados de seguridad actuales y los diseñados dentro del contexto de escenarios y eventos iniciantes que puedan generar una exposición potencial o sobrexposición del POE que laboran en las instalaciones del irradiador de Co-60.

Los resultados de este estudio fueron nuevas arquitecturas para los sistemas instrumentados de seguridad que, al ser evaluados, se obtuvo una mejora significativa en cuanto al factor de reducción del riesgo de los escenarios planteados. En el caso del primer escenario planteado con relación a una falla mecánica que traba el rack de la fuente de Co-60 en una posición fuera del blindaje húmedo dentro del búnker, el factor de reducción de riesgo obtenido fue de 404 veces, mientras que en el segundo escenario planteado con relación a la pérdida del blindaje húmedo a causa de un evento natural, se obtuvo un factor de reducción de riesgo de 107 veces. Estos factores de reducción de riesgo fueron evaluados para una fuente de Co-60 con una actividad nominal de 50 000 Ci (actividad propuesta para la repotenciación de la instalación), es decir que, el presente trabajo, generó la propuesta para las nuevas arquitecturas de

los SIS y sus directrices para los procedimientos de operación y mantenimiento requeridas por el irradiador de Co-60 para operar con las instalaciones repotenciadas y así mantener la probabilidad de ocurrencia anual de una sobrexposición o exposición potencial del POE dentro de los objetivos de seguridad radiológica establecidos por el Consejo Internacional de Protección Radiológica (ICRP)

INTRODUCCIÓN

En el mundo y en la región latinoamericana se observa un gran interés y dinamismo en el uso de tecnologías de irradiación, en virtud de los beneficios que brinda esta tecnología y sus varias aplicaciones en varios tipos de industria como por ejemplo: en la industria de alimentos; con el propósito de conseguir productos alimenticios inocuos para el consumo humano; en el tratamiento postcosecha de frutas y vegetales con fines de control fitosanitario; en la industria médica: en la sanitización de productos herbolarios, cosméticos y de uso en el cuidado de la salud; en la esterilización de insumos médicos como productos descartables o productos farmacéuticos entre otros (IAEA, 2006).

Dentro de la creciente importancia que tiene en la región el uso de estas tecnologías, el Ecuador ha incursionado en la investigación sobre esta temática utilizando las instalaciones que posee la Escuela Politécnica Nacional, está cuenta desde 1981 con un irradiador de Co-60 que es una instalación de irradiación gamma ubicada en el Centro de Irradiación (CIR) del Departamento de Ciencias Nucleares. Este irradiador contiene una fuente de Co-60 (isótopo radiactivo sintético del cobalto) con el propósito de realizar estudios de las aplicaciones de las radiaciones ionizantes gamma en la industria, en la esterilización, en la conservación de alimentos, investigación de nuevos materiales, etc. La instalación del irradiador de Co-60 es de origen francés, así como todos los equipos requeridos para su funcionamiento, instrumentación de monitoreo y control. La Escuela Politécnica Nacional construyó la infraestructura y blindajes requeridos para la fuente de Co-60 basada en las especificaciones técnicas francesas.

El irradiador de Co-60 en sus inicios contó con una actividad nominal de 20 000 Ci al 15 de abril de 1980, y en febrero de 1991, esta se actualizó con 12 lápices radiactivos, lo que dio un total de 40 700 Ci. El 4 de agosto del 2003 el irradiador de Co- 60 cuenta con una actividad de 7 712 Ci y al 1 de enero del 2020 contaba con una actividad de 888 Ci (Centro de Irradiación, 2020).

El irradiador de Co-60 es una instalación de categoría IV, irradiador panorámico de almacenamiento húmedo para fuentes (IAEA, 2010b), según las guías de seguridad

del Organismo Internacional de Energía Atómica (IAEA por sus siglas en inglés). Esta categorización se basa en el diseño, accesibilidad y blindaje de la instalación de la fuente radiactiva. Esto quiere decir que el irradiador de Co-60 es una instalación en la que, el acceso humano está prohibido a la sala de irradiación (búnker) cuando está fuera de su posición de depósito y la fuente radiactiva es almacenada y completamente blindada por una piscina de agua (blindaje húmedo) cuando la fuente no está en uso.

El principio de protección radiológica frente a las radiaciones ionizantes se basa en tres factores: distancia, tiempo de exposición y blindaje, este último recurso es empleado cuando no son suficientes los parámetros de distancia y tiempo, debido a la naturaleza de la fuente de Co-60 (fuente de radiación ionizante), las instalaciones poseen varias barreras de seguridad y trabaja bajo un sistema de gestión integrado que considera la calidad, seguridad y ambiente, con una especial consideración en la protección radiológica de la instalación para evitar que las personas que laboran, sufran de efectos adversos en su salud o que existan impactos en el ambiente.

Los blindajes que posee el irradiador de Co-60 son:

- Blindaje seco (Búnker): Es el cuarto de irradiación con paredes de hormigón armado de hasta 1,6 m de espesor y una densidad de 2.4 t/m^3 con un área útil de 16 m^2 (4 m x 4 m)
- Blindaje húmedo (Piscina): Es la zona de almacenamiento de la fuente de Co-60 cuando no se encuentra en uso, esta zona está constituida por una piscina de agua tratada de 6,5 m de largo por 2,5 m de ancho y 4,5 m de profundidad. Las paredes están construidas de hormigón armado de 0,4 m de espesor e impermeabilizado con material resistente a la radiación gamma e igualmente pintadas con pintura resistente a la radiación

Adicional a los blindajes, el irradiador de Co-60 posee varios sistemas de seguridad y enclavamientos que garantizan la seguridad de las personas que laboran en el área supervisada y controlada de la instalación durante los procesos de irradiación. Además, estos sistemas permiten alerta al personal en caso de que exista un incremento en la radiación ambiental en el interior del Centro de Irradiación, este

sistema actualmente está constituido por elementos eléctricos, electrónicos y electromecánicos que, a pesar de estar bajo un programa de mantenimiento riguroso, su antigüedad aumenta la probabilidad de fallo de sus elementos constitutivos.

Todos estos sistemas no cuentan con una integridad total de sus elementos eléctricos y electrónicos, debido al deterioro por antigüedad de los componentes que componen dichos sistemas, además, se requiere incorporar otros elementos de seguridad para mejorar las acciones de control en caso de la ocurrencia de eventos no deseados. Además de estas barreras y sistemas de seguridad, el irradiador de Co-60 dispone de protocolos y procedimientos específicos para la administración y operación del irradiador de Co-60 dentro de un sistema de gestión integrado y de un programa de protección radiológica que ejecutan los especialistas del Centro de Irradiación, esto con el objetivo de garantizar la seguridad del personal interno y externo del Centro de Irradiación y evitar o minimizar impactos al ambiente.

Por todo lo anteriormente expuesto, el presente trabajo tiene por objetivo desarrollar una propuesta de mejoramiento con un enfoque en seguridad funcional para los sistema instrumentados de seguridad del irradiador de Co-60, específicamente a los sistemas de enclavamientos principales y el control del nivel de blindaje húmedo del irradiador de Co-60 del Centro de Irradiación de la Escuela Politécnica Nacional basado en el estándar internacional general IEC 61508 y su estándar específico IEC 61511 las mismas que se refieren a los sistemas eléctricos/electrónicos/electrónicos programable relacionados a la seguridad y a los sistemas instrumentados de seguridad que forman parte del Irradiador de Co-60. Vinculado a este enfoque de seguridad funcional, se presentarán directrices para las mejoras a los procedimientos de operación y mantenimiento del irradiador de Co-60. Todo esto se realizó con el objetivo de disminuir el nivel de riesgos que puedan conllevar la operación del irradiador de Co-60 considerando la futura repotenciación y recarga a corto plazo de la fuente a 50 000 Ci.

1 REVISIÓN BIBLIOGRÁFICA

1.1 SEGURIDAD FUNCIONAL

La seguridad funcional es parte de la seguridad global, este concepto trata sobre la confianza con la que un sistema puede llevar a cabo una tarea relacionada con la seguridad cuando esta sea demandada y difiere a otro tipo de seguridades pasivas como pueden ser las seguridades eléctricas, mecánicas o intrínsecas. La seguridad funcional es una forma activa de seguridad. Por tal motivo, dentro de la misma se considera la identificación de fallas peligrosas específicas que podrían llevar a eventos con consecuencias serias o fatales (Meany, 2018).

La seguridad funcional es un concepto ampliamente usado en la industria en general, ya que, involucra la identificación de fallas potenciales que podrían ocasionar lesiones graves e incluso la muerte de personas relacionadas directa o indirectamente a las actividades que se realiza en la industria, además, las directrices proporcionadas dentro de la seguridad funcional también pueden considerarse para minimizar los daños producidos al ambiente o a los activos de la industria. La normativa IEC 61508 se enfoca específicamente a los elementos eléctricos/electrónicos/electrónicos programables que pueden poseer los sistemas de seguridad de las instalaciones en general y esta normativa también se encuentra estrechamente vinculada con varias normativas de seguridad debido a los orígenes y a la historia que comparten durante la evolución de esta normativa, esto se verá con más detalle en la sección 1.1.1.

Para entender de mejor manera los temas tratados en este trabajo, a continuación, se enuncia algunas definiciones de los términos y acrónimos utilizados dentro de la seguridad funcional y que se encuentran en el estándar IEC 61508 y otras fuentes relacionadas, según los siguientes temas:

a) **Sistemas** (IEC, 1997d)

- Equipo bajo control (EUC por sus siglas en inglés). Equipo, maquinaria, aparato o planta usado para manufactura, proceso, transportación, uso médico u otras actividades
- Sistema de control EUC. Sistema que responde a la señal de entrada desde un proceso y/o un operador que genera una señal de salida al EUC para operar de la manera deseada.
- Riesgo del EUC. Es el riesgo latente del EUC o su interacción con el sistema de control EUC (el riesgo del EUC es el punto de referencia, para así poder evaluar independientemente y de ser necesario considerar contramedidas para reducir el riesgo).
- Sistemas relacionados a la seguridad. Son sistemas designado que:
    - Implementan la función de seguridad requerida para alcanzar o mantener un estado seguro para el ECU.
    - Pretende alcanzar la seguridad integrada necesaria para la función de seguridad requerida, ya sea por sí solos o en conjunto con otros sistemas relacionados de seguridad E/E/EP, otra tecnología de sistemas de seguridad o facilidades de reducción de riesgo externo.
- Sistemas electrónicos programables (PES por sus siglas en inglés). Sistemas para control, protección o monitoreo basado en uno o más dispositivos electrónicos programables, incluido todos los elementos de los sistemas como fuentes de poder, sensores y otros dispositivos de entrada, líneas de datos o comunicación, actuadores y otros dispositivos de salida.
- Eléctrico/Electrónico/Sistema electrónico programable (E/E/PE). Igual a los PES.
- Arquitectura. Arreglo de elementos de hardware y/o software en un sistema (British Standard, 2003).

b) Seguridad y riesgo (IEC, 1997d)

- Daño. Lesión física o daño a la salud de las personas ya sea directa o indirectamente como resultado de daños a la propiedad o al ambiente (esto excluye a los daños a la propiedad y al ambiente, esto no se encuentra conforme con las definiciones modernas).
- Peligro. Fuente potencial de daños.
- Situación peligrosa. Circunstancia en la cual las personas son expuestas a peligros.
- Evento peligroso. Situación peligrosa la cual resulta en un daño.
- Seguridad. Libre de riesgo inaceptable.
- Seguridad funcional. Parte de toda la seguridad relacionada a los EUC y a los sistemas de control EUC los cuales dependen del correcto funcionamiento de los sistemas E/E/PE relacionados a la seguridad, otras tecnologías relacionadas a la seguridad y facilidades de reducción de riesgo externo.
- Función de seguridad. Función a ser implementado por un sistema E/E/PE relacionado a la seguridad, otra tecnología relacionada a la seguridad o facilidad de reducción de riesgo externo, el cual pretende alcanzar o mantener un estado seguro para los ECU con respecto a un evento peligroso específico.
- Riesgo. Combinación de la probabilidad de ocurrencia del daño y la gravedad de dicho daño.
- Riesgo tolerable. Riesgo el cual es aceptable en un contexto dado basado en los valores actuales de la sociedad.
- Riesgo residual. Riesgo remanente después de las medidas de protección que han sido tomadas.
- Falla (failure). Finalización de la capacidad de una unidad funcional para realizar una función requerida (British Standard, 2003)
- Avería (fault). Condición anormal que puede causar una reducción en, o pérdida de la capacidad de una unidad funcional (British Standard, 2003).
- Falla de causa común. Fracaso, que es el resultado de uno o más eventos, que causa fallos de dos o más separada canales en un sistema

de múltiples canales, que conducen a un fallo del sistema (British Standard, 2003).

c) Seguridad integrada (IEC, 1997d)

- Seguridad integrada. Probabilidad de que un sistema de relacionado a la seguridad realice satisfactoriamente una función de seguridad requerida bajo las condiciones establecidas y en el tiempo establecido.
- Nivel integrado de seguridad (SIL por sus siglas en inglés). Nivel discreto para especificar los requerimientos de seguridad integrada de las funciones de seguridad a ser asignados a los sistemas E/E/PE relacionados a la seguridad donde el SIL – 4 tiene el más alto nivel de seguridad y el SIL – 1 tiene el más bajo.

d) Otros (IAEA, 2018)

- Comisionamiento. Es el procedimiento de confirmación de que los sistemas instalados funcionan cumpliendo las especificaciones o requerimientos técnicos diseñados.

1.1.1 EL ESTÁNDAR IEC 61508

A inicios de los años 70's las personas que trabajaban en procesos industriales se dieron cuenta que plantas industriales más grandes involucraban mayores inventarios de materiales peligrosos y la práctica común de aprender de los errores ya no era una metodología aceptable. A mediados de los 70´s, ya existía una preocupación por la falta de controles formales o regulaciones sobre las actividades industriales y debido a incidentes con impactos mayores como los ocurridos en Flixborough en junio de 1974 (28 muertes), el incidente de Seveso en 1976 y otros eventos ocurridos como accidentes de ferrocarriles, mantuvieron vivos los intereses en el área de seguridad por lo que el Reino Unido inició con la generación de publicaciones que servían como guías y regulaciones para esta área.

Las técnicas de evaluación de riesgos de procesos de plantas fueron comunes a inicios de los 80’s, pero no existían guías o regulaciones formales o algunas eran fragmentadas. Solamente la sección 6 de la Ley de Salud y Seguridad en el Trabajo de 1974, hacía hincapié en realizar todo lo razonablemente práctico para garantizar la seguridad. Sin embargo, seguido a los desastres de Flixborough, generó una serie de movimientos (incluido la directiva Seveso) las cuales condujeron a la regulación de control de riesgos de accidentes industriales mayores de 1984 (CIMAH por sus siglas en inglés) y su respectiva revisión, además, se generó la regulación de control de riesgos de accidentes mayores de 1999 (COMAH por sus siglas en inglés). Sin embargo, estas regulaciones no especificaban el método de establecer los objetivos de riesgo tolerable para actividades específicas, tampoco se direccionaban las evaluaciones de riesgo ni la especificación de las características de seguridad requeridas en los diseños. La EN 1050 (principios de evaluación de riesgos de 1996) cubría los procesos que involucraban la evaluación de riesgos, pero daba pequeños consejos sobre la reducción de riesgos, la EN 954-1 (seguridad relacionada a las partes de control) daba una guía de cómo reducir los riesgos de sistemas de control, pero no incluía a los controladores lógicos programables (PLC por sus siglas en inglés). Además, en los 80’s proliferaba la creación de software para el control en tiempo real y la seguridad de procesos por lo que se veía la necesidad de una sistemática de cuantificación de fallas, en otras palabras, determinar la tasa de falla de hardware como de software.

En 1989, la Agencia Ejecutiva para la Seguridad y Salud (HSE por sus siglas en inglés) publicó guías en la que fomentaba el enfoque para garantizar la seguridad funcional del equipo programable, esto condujo a la Comisión Internacional de Electrotecnia (IEC por sus siglas en inglés) a trabajar durante los 90’s, la cual culminó en el estándar internacional de seguridad IEC 61508, al que le concierne los sistemas eléctricos/electrónicos/electrónicos programables relacionados a la seguridad, donde las fallas de estos, podría afectar a las personas o el ambiente (Smith & Simpson, 2004) .

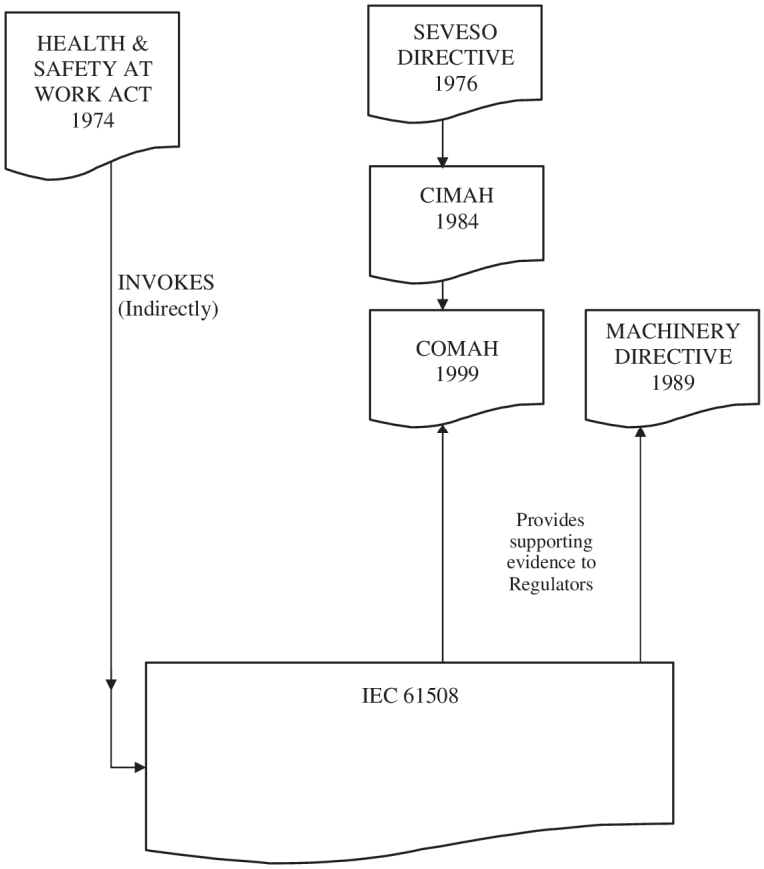


Figura 1.1. Relación de la IEC 61508 con legislaciones actuales del Reino Unido (Smith & Simpson, 2011)

La clave de la seguridad funcional terminó por ser el estándar IEC 61508. Su primera revisión fue publicada en 1998, su segunda revisión se la realizó en 2010 y se trabaja para una nueva revisión desde los inicios del 2017, desde su primera revisión, esta norma ha sido adaptada a varios campos como son: el automotriz (ISO 26262), procesos de control (IEC 61511), computadores lógicos programables -PLC- (IEC 61131 – 6), para maquinarias (IEC 62061), controladores de motores (IEC 61800 – 5 – 2) y muchas otras áreas (Figura 1.2). Estos otros estándares ayudan a interpretar el muy extenso alcance de la IEC 61508 (Smith & Simpson, 2004).

Algunos estándares de seguridad funcional tales como la ISO 13849 y la DO-178/DO-254 han sido derivadas de la IEC 61508, por lo que no es de sorprenderse la similitud de estas otras normativas con la IEC 61508 (Meany, 2018).

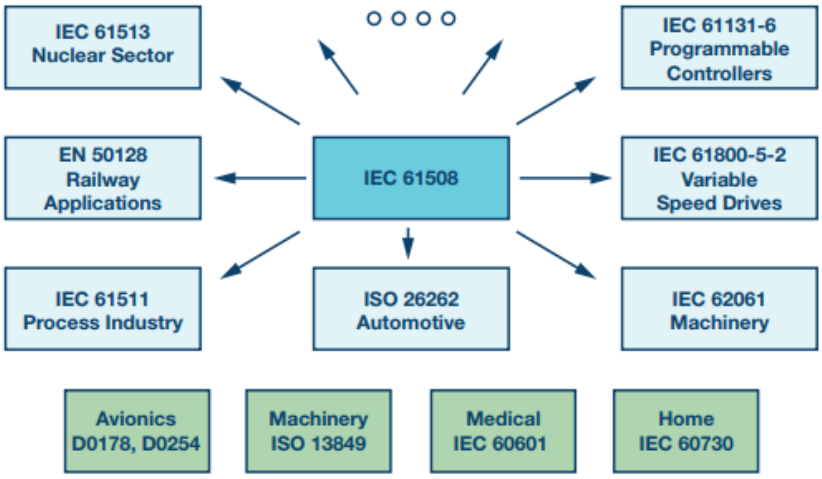


Figura 1.2. Relaciones de la IEC 61508 con otros estándares de seguridad funcional (Meany, 2018)

1.1.2 EL ESTÁNDAR IEC 61511

La primera versión del estándar IEC 61511 se liberó en 2003 bajo el paraguas de la IEC 61511, sin embargo, la diferencia más básica entre los dos estándares es su aplicabilidad. La IEC 61508, es una normativa orientada a los fabricantes de dispositivos y la IEC 61511 es una normativa orientada al usuario y diseñadores de sistemas instrumentados de seguridad.

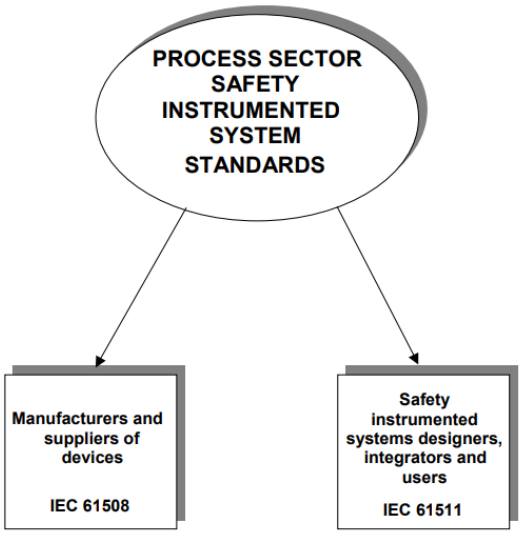


Figura 1.3. Relación entre la IEC61508 y la IEC61511 (British Standard, 2003)

Este estándar internacional direcciona las aplicaciones de sistemas instrumentados de seguridad para los procesos industriales a alcanzar cierto estándar mínimo de seguridad y niveles de rendimiento, para esto también se requiere un proceso peligroso y una evaluación de riesgo que sirve para llevar a cabo las definiciones de las especificaciones para los sistemas instrumentados de seguridad a ser desarrollados (British Standard, 2003). Por tal motivo, los estándares IEC 61508 e IEC 61511 son la base de las directrices relacionadas a la seguridad funcional en varios ámbitos de la industria.

Para entender el enfoque de la seguridad integrada que tiene la normativa IEC 61508 e IEC 61511, se realiza una rápida introducción de ciertos conceptos básicos mencionados en estas normas:

- Enfoque de ciclo de vida
- Ciclo de vida de los SIS
- Objetivos de seguridad
- Nivel de seguridad integrado (SIL por sus siglas en inglés)

1.1.3 ENFOQUE DE CICLO DE VIDA

El estándar IEC 61508 tiene un enfoque de ciclo de vida de la seguridad general, el cual es crucial, este ofrece un modelo de fases de la administración de la seguridad y la vida de un sistema. El propósito del ciclo de vida de seguridad general es forzar que la seguridad se aborde independientemente de los problemas funcionales, para superar así la suposición de que la confiabilidad funcional producirá automáticamente la seguridad de un sistema. Entonces, especificar requisitos de seguridad por separado permite que sean validados independientemente de la funcionalidad, lo que brinda una mayor confianza de seguridad en todas las condiciones de operación y falla. La paradoja, sin embargo, es que las actividades de seguridad no deben llevarse a cabo, o pensarse, como totalmente desconectadas de otros proyectos o actividades operativas. Deben integrarse en una perspectiva total del sistema en las fases del ciclo de vida (IEC, 1997a).

En la Figura 1.4, se muestra la concepción del ciclo de vida de un sistema de seguridad con base en el estándar IEC 61508.

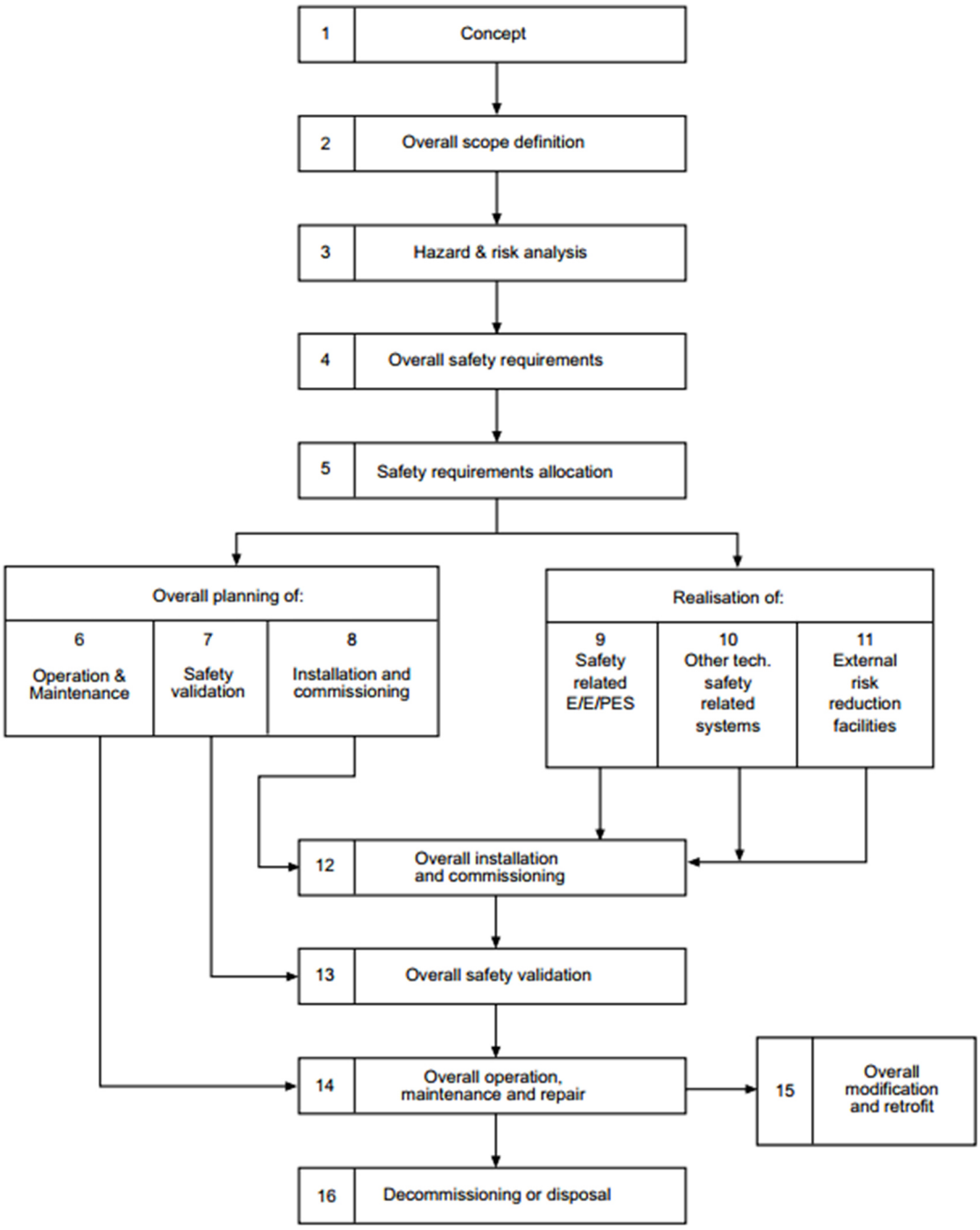


Figura 1.4. Ciclo de vida de la seguridad global
(IEC, 1997a)

En la fase 1 y 2 se indica la necesidad de considerar las implicaciones de seguridad de los EUC y sus sistemas de control, como el nivel de sistema. En la fase 3 los

riesgos son identificados, analizados y evaluados comparándolos con los criterios de tolerancia. En la fase 4, se especifica los requerimientos de seguridad para las medidas de reducción de riesgos. En la fase 5 esta especificación es trasladada a los diseños de las funciones de seguridad y se selecciona las formas de implementación en las fases 9, 10 y 11. Las fases 6, 7 y 8 se refieren a la planificación de los procesos que se pueden considerar en el ciclo de vida del sistema, como son: operación, mantenimiento, validación, instalación y comisionamiento de este. En las fases 12, 13 y 14 se llevan a cabo la planificación de la operación, mantenimiento, validación, instalación y el comisionamiento de los sistemas relacionados a la seguridad. La fase 15 cubre las modificaciones del sistema y sus retroalimentaciones y la fase 16 cubre la puesta en fuera de servicio y la disposición final del sistema, en el fin de su ciclo de vida (Smith & Simpson, 2011).

Como puede observarse, la idea principal que considera el estándar IEC 61508 es tratar la seguridad funcional de un sistema de seguridad en todo su contexto, desde su concepción, planificación, implementación, operación y hasta su disposición final.

1.1.4 EL CICLO DE VIDA DE LOS SIS

La normativa IEC 61511 describe buenas prácticas de ingeniería en la administración de sistemas para el usuario/operador/dueño y de cómo especificar, diseñar, verificar, ingeniar, evaluar, instalar, poner en marcha, validar, operar, mantener documentar y mejorar continuamente el funcionamiento correcto de sus SIS, esto tiene por objetivo prevenir la falla humana y para esto, un acercamiento sistemático se desarrolló por medio del uso de un modelo cíclico como se puede ver en la Figura 1.5. (Basilio, Landrini, & Capelle, 2017)

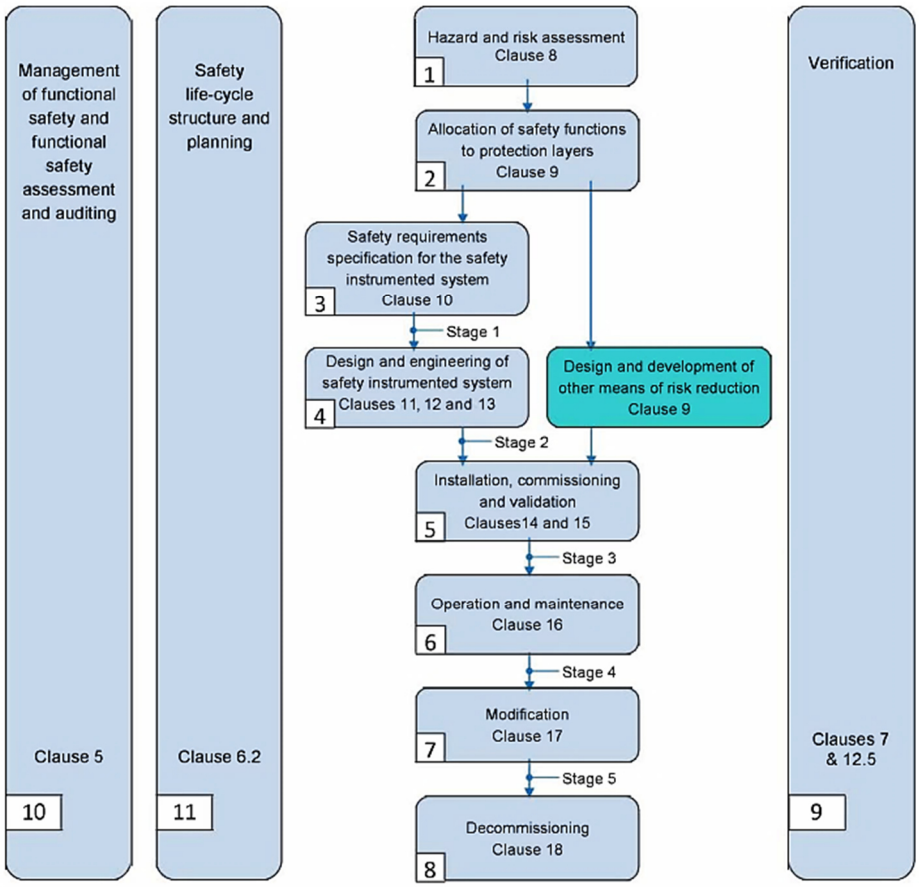


Figura 1.5. Ciclo de vida de los SIS
(Basilio, Landrini, & Capelle, 2017)

El modelo de ciclo que se puede ver en la Figura 1.5 consta de 11 fases dedicadas a los requerimientos, información y tareas que deben realizarse para el acercamiento del enfoque de seguridad funcional. La descripción de estas fases tiene mucha relación con las proporcionadas en la sección 1.1.3.

1.1.5 OBJETIVOS DE SEGURIDAD Y EL NIVEL DE SEGURIDAD INTEGRADO (SIL POR SUS SIGLAS EN INGLÉS)

No existe actividad o equipo con riesgo cero, es decir que ningún equipo físico tiene tasa de falla cero, ninguna persona realiza actividades sin errores y ningún software es infalible, no obstante, la percepción del riesgo en una actividad particular que pueda provocar consecuencias graves exige un nivel de riesgo cero idealmente

(Smith & Simpson, 2004), aunque esto no sea posible en la práctica. En la Tabla 1.1 se detallan algunos ejemplos de riesgos diarios de muerte:

Tabla 1.1. Ejemplos de riesgos diarios de muerte por varias causas

Causas de muerte	**Probabilidad de ocurrencia**
Todas las causas	$1x10^{-3}$ por año
Todos los accidentes	$5x10^{-4}$ por año
Accidentes en la casa	$4x10^{-4}$ por año
Accidentes de tránsito	$6x10^{-5}$ por año
Desastres naturales	$2x10^{-6}$ por año

(Smith & Simpson, 2004).

Por tal motivo, prevalece el concepto de un nivel de riesgo tolerable aceptable para la ejecución de cualquier actividad. Sin embargo, para determinar este nivel de riesgo tolerable es necesario considerar varios factores que pueden afectar el mismo, como pueden ser, el control que se posee de las actividades, la naturaleza del riesgo, el número de personas involucradas, las tecnologías involucradas entre otras.

Una visión general del estándar IEC 61508 e IEC 61511 es la de proporcionar criterios de niveles discretos de seguridad (objetivos de seguridad integrada) que se pueden definir en cuatro categorías, estas pueden ser del SIL 1 a SIL 4, está categorización implica que una SIL 2 tiene una mayor seguridad que una SIL 1 por lo que, si mayor es su categoría mayor es su seguridad, las categorías SIL se pueden definir como se indica en la Tabla 1.2.

Tabla 1.2 Niveles integrados de seguridad (SIL)

Nivel de seguridad integrada (Safety Integrity Level – SIL)	**Tasa de alta demanda (Fallas peligrosas/horas)**	**Tasa de baja demanda (probabilidad de falla en demanda)**
SIL 4	$\geq 10^{-9}$ a $<10^{-8}$	$\geq 10^{-5}$ a $<10^{-4}$
SIL 3	$\geq 10^{-8}$ a $<10^{-7}$	$\geq 10^{-4}$ a $<10^{-3}$
SIL 2	$\geq 10^{-7}$ a $<10^{-6}$	$\geq 10^{-3}$ a $<10^{-2}$
SIL 1	$\geq 10^{-6}$ a $<10^{-5}$	$\geq 10^{-2}$ a $<10^{-1}$

(Ingrey & Lerévérend, 2005)

Estos criterios son utilizados a nivel general entre los fabricantes de elementos eléctricos, electrónicos y electrónicos programables, en donde el nivel más alto

(SIL 4) implica costos elevados y metodologías bastantes complejas para lograr satisfacer los requerimientos para este grado de seguridad integrada, mientras que para un nivel bajo (SIL 1) suele ser suficientes con metodologías apegadas a la buena prácticas de diseño y con un enfoque en la ISO 9001 para garantizar la calidad de la seguridad integrada.

Los conceptos de alta tasa de demanda y baja tasa de demanda que se detalla en la Tabla 1.2, hace referencia a la manera de demanda de una función de seguridad, para un mejor entendimiento de este concepto, se hace la siguiente analogía, en un vehículo, una función de seguridad de alta demanda es el sistema del freno, mientras que una función de baja demanda es el uso del airbag, mientras que el primero es de uso diario ,el segundo talvez se lo use una vez cada diez años, sin embargo, las dos funciones son importantes. Es de interés la combinación de la tasa de fallo y el tiempo de inactividad, lo que se denominaría la probabilidad de falla en demanda (PFD por sus siglas en inglés), este se muestra en el lado derecho de la Tabla 1.2.

1.1.6 ESQUEMA DE ACTIVIDADES REQUERIDAS PARA ALCANZAR EL ENFOQUE DE SEGURIDAD FUNCIONAL

El estándar IEC 61508 ofrece un esquema sistemático a seguir para lograr la seguridad funcional, este esquema se indica en la Figura 1.6, en la que se considera un resumen del enfoque del ciclo de vida de los sistemas visto en la sección 1.1.4.

A continuación, se describen cada una de las fases del esquema resumido del ciclo de vida de la Figura 1.6.

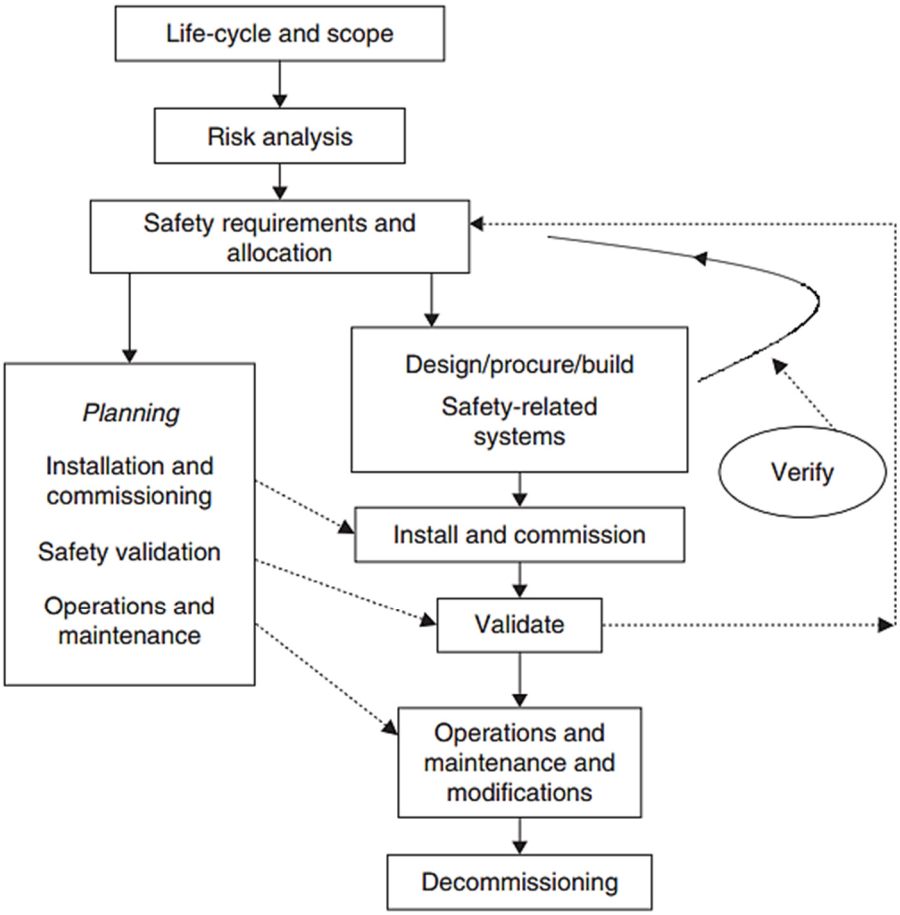


Figura 1.6. Resumen del Ciclo de vida de seguridad de un sistema (Smith & Simpson, 2004)

- El ciclo de vida y el alcance. Es necesario determinar el alcance de los EUC, sus límites y requerimientos funcionales de seguridad, el alcance de los peligros y sus riesgos. Para realizar este paso, se considera la información actual del Centro de Irradiación (sistemas de seguridad, procedimientos, etc.). Se considera también las recomendaciones realizadas por organismos competentes en el ámbito del uso de radiaciones ionizantes como son: Organismo Internacional de Energía Atómica (IAEA), Comisión Internacional de Protección Radiológica (ICRP) entre otros, esto permite tener un sustento formal para las evaluaciones y sus respectivas aplicaciones de las metodologías que se usen a lo largo de este trabajo.
- Análisis de riesgo. Esto involucra la cuantificación de la evaluación del riesgo y considerar las consecuencias de la falla, dentro de este paso, se utiliza la metodología del análisis probabilístico de seguridad (APS) nivel 1

recomendada por el IAEA para instalaciones de irradiación sin reactores nucleares (NRNF’s por sus siglas en inglés). Adicionalmente, se utiliza la metodológica del análisis de modo de fallo y efectos (FMEA por sus siglas en inglés) para determinar las funciones de seguridad y sus modos de fallo.

- Requerimientos de seguridad. En este paso se establece los objetivos de riesgos máximos tolerables de todo el sistema, se asignan las tasas de fallos y sus diferentes modos de fallos. En este punto se definen las funciones de seguridad para establecer sus modos de fallos y sus protecciones, así cada función de seguridad es definida con su propia asignación SIL.
- Planificación. En este paso se realiza la planificación de las fases que conlleva la implementación del sistema de seguridad como son, la instalación, validación de seguridad, operación y mantenimiento.
- Diseño y construcción del sistema de seguridad. Al considerar el estándar IEC 61508, IEC 61511 y otras directrices relacionadas al ámbito de la aplicación de la instalación, significa que en este paso se realiza el diseño y creación de los sistemas de seguridad para los sistemas eléctricos, electrónicos, electrónicos programables de los sistemas de seguridad con base en su aplicación.
- Instalación, puesta en servicio, operación y mantenimientos. Este paso es la implementación de la planificación desarrollada anteriormente, además de esto se considera las posibles modificaciones que se pueden llevar a cabo en el tiempo con respecto a sus funciones de seguridad.
- Poner el sistema fuera de servicio. Definir la manera de realizar la disposición final del sistema de seguridad.

Al considerar el enfoque del ciclo de vida de la seguridad, se puede apreciar que este es extenso, por lo que, el presente trabajo de titulación tiene por objetivo realizar una presentación priorizada de la mayoría de los pasos mencionados en el esquema mostrado en Figura 1.6. relacionados con los SIS más relevantes del irradiador de Co-60.

A continuación, se realiza la descripción teórica de otros temas relevantes que requieren el enfoque de seguridad funcional.

1.2 EVALUACIÓN DE RIESGOS PARA FACILIDADES DE IRRADIACIÓN POR MEDIO DEL ANÁLISIS PROBABILÍSTICO DE SEGURIDAD (APS) NIVEL 1 – GENERALIDADES

El análisis probabilístico de seguridad (APS) provee un enfoque formal para estructurar de forma lógica los sistemas complejos en la que se evalúa las consecuencias de las fallas y se establece una estimación numérica del riesgo. Esta metodología se utiliza en varias industrias de alto riesgo y permite, a través de la medición del riesgo realizar una demostración explicita de la seguridad a través de los diferentes sistemas de una instalación, el esquema general de esta metodología se indica en la Figura 1.7.

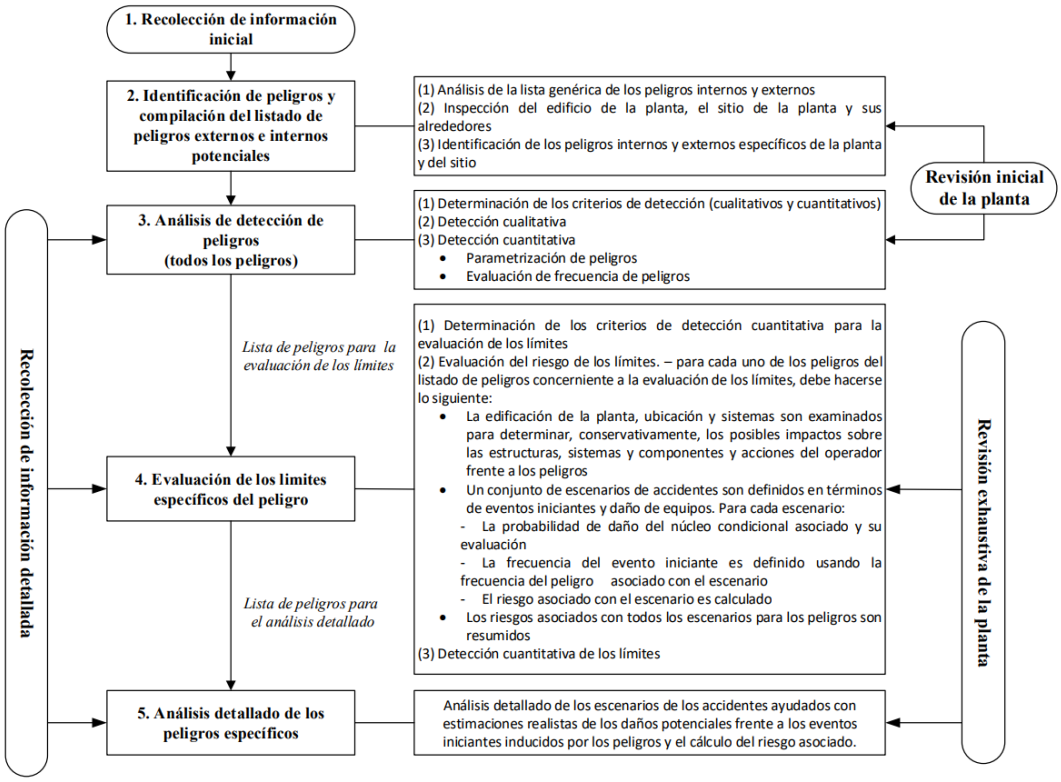


Figura 1.7. Acercamiento global del APS nivel 1 para peligros internos y externos (IAEA, 2010a)

Realizar un estudio con un enfoque APS ayuda a mejorar la seguridad de las plantas, ya que provee a los diseñadores tener un punto de referencia imparcial para categorizar el nivel de seguridad, además, el APS es utilizado ampliamente

para decidir más fácilmente las mejores opciones de seguridad y desarrollar programas de mantenimiento más racionales desde el punto de vista de seguridad. Por todos estos beneficios y otros, el Organismo Internacional de Energía Atómica (IAEA) recomienda el uso de esta metodología para la evaluación de seguridad de instalaciones especiales como plantas de energía nucleares (NPP por sus siglas en inglés). Sin embargo, esta metodología también se puede utilizar para instalaciones nucleares sin reactores (NRNF por sus siglas en inglés), dentro de este tipo de instalaciones se encuentran las siguientes: plantas de tratamiento de desechos nucleares, facilidades de irradiación con gamma, rayos X o electrones, instalaciones de tratamiento con radiaciones ionizantes, etc.

En el presente proyecto se realiza una evaluación basada en el análisis probabilístico de seguridad (APS) y se considera la guía proporcionada por el Organismo Internacional de Energía Atómica IAEA-TECDOC-1267 el cual proporciona una guía de procedimientos para conducir un análisis probabilístico de seguridad para instalaciones nucleares sin reactor. Estos pasos generales se indican en la Figura 1.8.

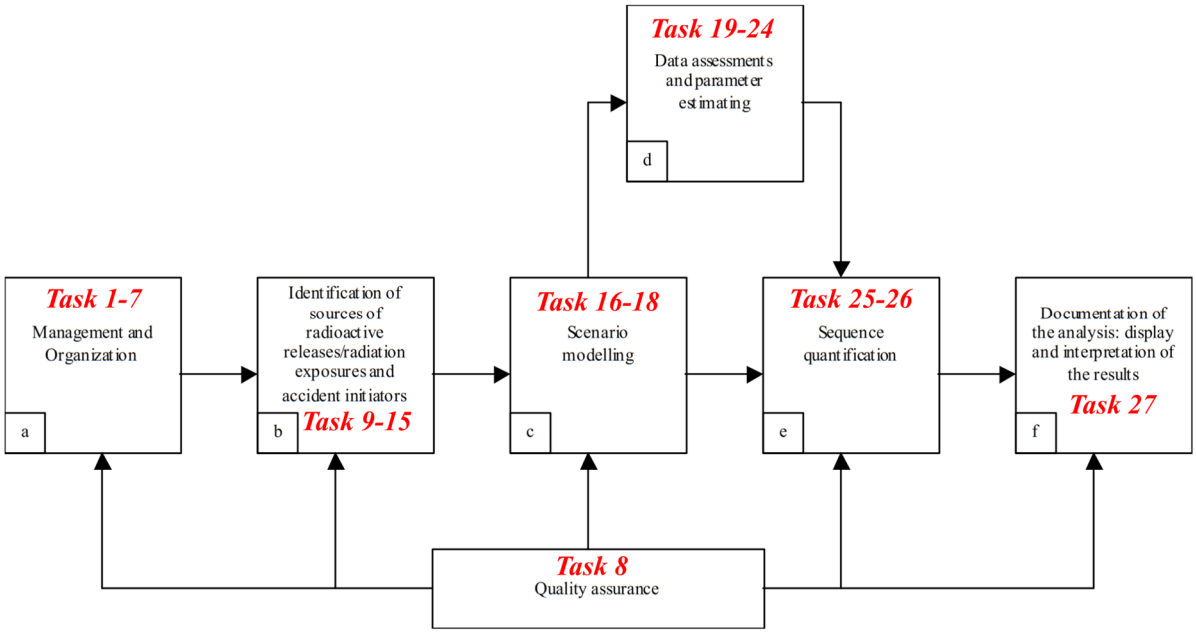


Figura 1.8. Pasos macro para la ejecución de un APS
(IAEA, 2002)

De manera general, el APS se conforma de los siguientes pasos para efectuar el análisis.

A. Gestión y organización del APS.
B. Identificación de fuentes radiactivas de liberación/exposición de radiación y accidentes iniciadores.
C. Modelamiento del escenario.
D. Evaluación de datos y estimación de parámetros.
E. Cuantificación de las secuencias.
F. Documentación del análisis: visualización e interpretación de resultados.

La aseguración de la calidad es considerada en la ejecución de todos los pasos.

1.2.1 PASOS GENERALES DEL APS

Si bien los pasos generales del APS ilustrados en la guía IAEA-TECDOC-1267 sirven para varios tipos de facilidades que trabajan con radiaciones ionizante (excepto reactores nucleares), la profundidad del análisis que se realiza depende del criterio del equipo que lleva a cabo dicho análisis. Por tal motivo, en el primer paso se definen el objetivo y el alcance del APS, lo que otorga límites prácticos para evitar análisis poco relevantes o demasiados complejos que requiere la instalación. Un análisis completo requiere demasiados recursos humanos, tiempo, recopilación de información y es de alta complejidad.

1.2.1.1 Gestión y organización del APS

Dentro de esta actividad se realizan varias tareas que permiten gestionar todas las actividades requeridas para la ejecución del APS. Entre estas actividades se encuentran de manera general:

- Definir el objetivo del análisis.
- El alcance que tendría el APS.
- La administración, metodologías y procedimientos para llevar a cabo la evaluación.

- El equipo de trabajo para realizar la evaluación; dentro de este equipo de trabajo se recomienda seleccionar personal que se encuentre fuertemente vinculada con la operación de la facilidad.
- Entrenamiento, en caso de ser necesario sobre las metodologías a utilizar.
- Recursos y horarios requeridos para dicho análisis.
- La forma de llevar a cabo el aseguramiento de la calidad de los datos recopilados y los resultados obtenidos.

1.2.1.2 Identificación de fuentes radiactivas de liberación/exposición de radiación y accidentes iniciadores

Este paso requiere de la recopilación de toda la información que posee la instalación sobre la operación, sistemas de seguridad, protocolos de emergencia que posee la facilidad, además, en este paso se requiere identificar los posibles eventos iniciantes que podrían derivar en un evento no deseado que pueda producir consecuencias sobre las instalaciones o sobre el personal de la facilidad o de sus alrededores. Este paso permite familiarizar a los participantes del APS con todos los sistemas, procedimientos y protocolos de seguridad que posee la facilidad, este detalle es una de las grandes fortalezas de esta metodología, ya que, en muchos casos, el personal que labora dentro de una facilidad de irradiación no posee todos los conocimientos y procedimientos de seguridad por lo amplio que esto suele ser.

1.2.1.3 Modelamiento del escenario

En este paso se realiza el modelamiento del escenario de un evento iniciante que podría derivar en algún estado no deseado de la facilidad, para este modelamiento, esta guía recomienda el uso de dos herramientas de evaluación que son el Análisis de árbol de eventos (ETA por sus siglas en inglés) y el análisis de árbol de fallos (FTA por sus siglas en inglés).

1.2.1.4 El análisis de árbol de eventos (ETA por sus siglas en inglés)

Es una técnica gráfica deductiva para la representación de secuencias mutuas de eventos iniciadores de acuerdo con el funcionamiento /no funcionamiento de los diversos sistemas diseñados para mitigar las consecuencias. Este método se puede aplicar cuantitativamente como cualitativamente

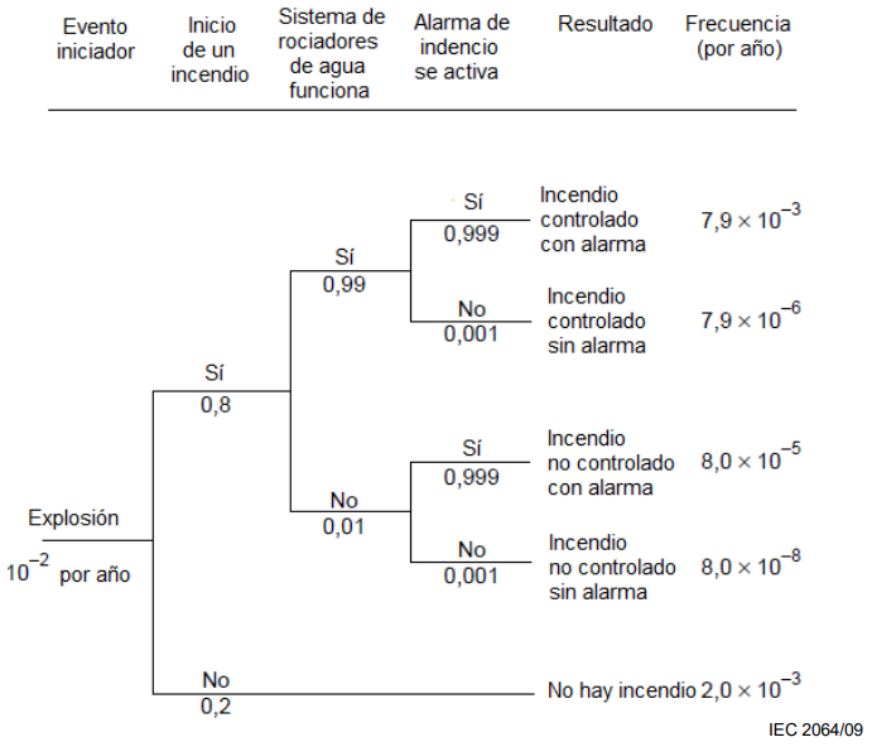


Figura 1.9. Ejemplo de un análisis cuantitativo de árbol de eventos (ETA) (INN, 2013)

Como se puede observar en la Figura 1.9, mediante el despliegue en forma de árbol se puede representar los eventos de agravamiento o de mitigación y los sistemas o barreras de seguridad relacionados.

El análisis ETA se puede utilizar para modelar, calcular y clasificar los diferentes escenarios de accidente que siguen al evento iniciador.

El análisis cuantitativo tiende a considerar por sí mismo la aceptabilidad de los controles, se utiliza con frecuencia para modelar fallas en los que hay múltiples barrearas de protección.

Para esta metodología se requieren los siguientes elementos:

- Lista de eventos iniciadores apropiados.
- Información de las barreras de protección y sus controles, sus probabilidades de falla si se desea un análisis cuantitativo.
- Una comprensión de los procesos en los cuales la falla inicial se intensifica.

El resultado de esta metodología es la descripción cualitativa de los posibles problemas y las estimaciones cuantitativas de las frecuencias o probabilidades del evento y sus combinaciones, por lo que se puede generar una lista de recomendaciones para reducir el riesgo. Estos resultados permiten diagramar de forma clara la influencia del éxito o de la falla de sistemas o de las funciones de mitigación del riesgo, sin embargo, si no se tiene cuidado con la evaluación de elementos comunes, sistemas de utilidad u operadores se puede dar estimaciones optimistas del riesgo.

1.2.1.5 El análisis de árbol de fallos (FTA por sus siglas en inglés)

El árbol de fallos fue originado en la industria aeroespacial y ha sido usado extensamente en la industria de plantas nucleares para calificar y cuantificar los peligros y sus riesgos asociados.

El FTA es una técnica para identificar y analizar factores que pueden contribuir a un evento especificado no deseado. Los efectos causales se identifican deductivamente, se organizan de una manera lógica y se representan gráficamente mediante un diagrama de árbol como se indica en la Figura 1.10, que describe los factores causales y sus relaciones lógicas con el evento superior. Los factores identificados en el árbol pueden ser eventos que están asociados con fallas materiales de componentes, con errores humanos o con cualquier otro evento pertinente que conduzca al evento no deseado. La simbología que se utiliza en la elaboración del diagrama FTA se indica en la **¡Error! No se encuentra el origen de la referencia.**.

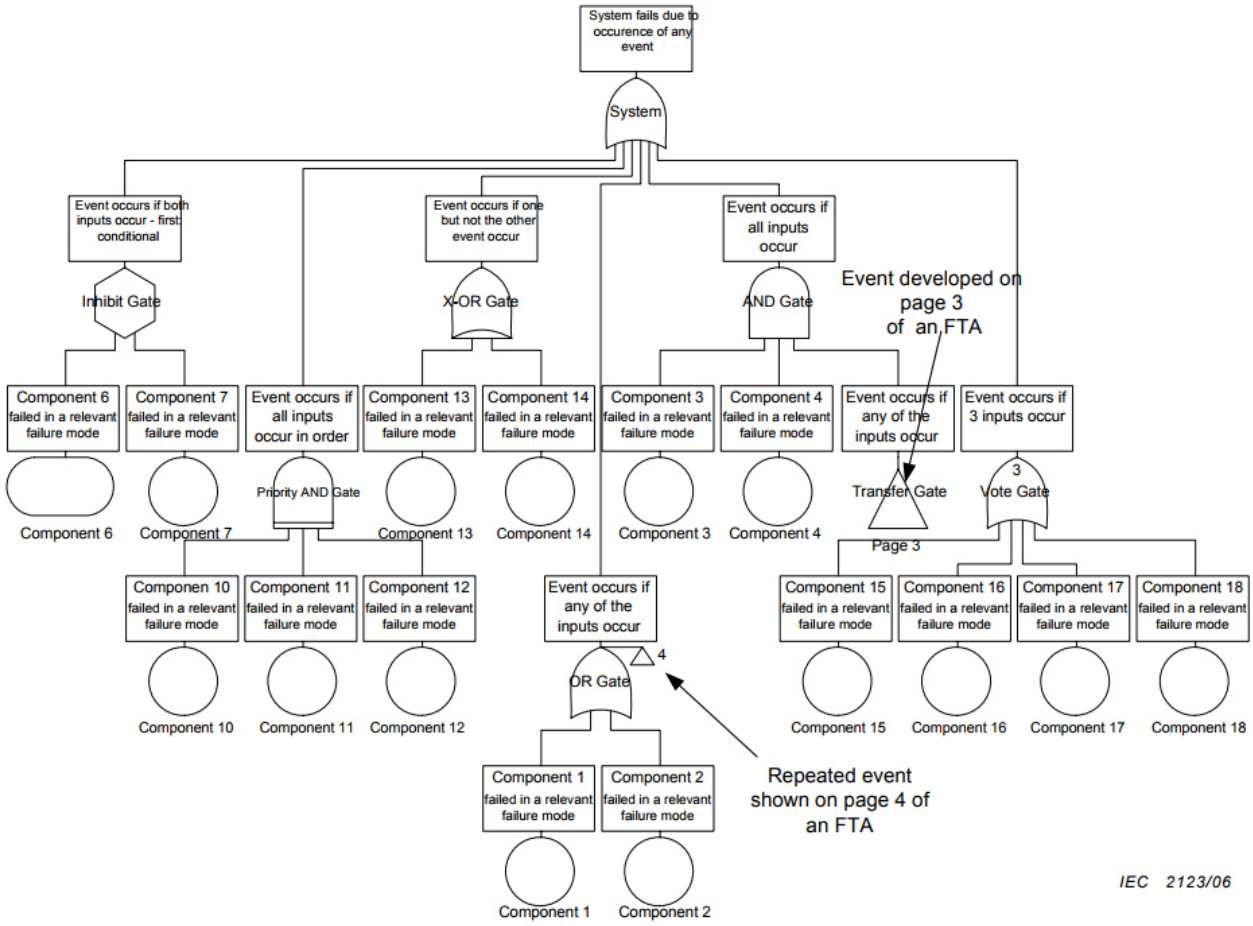


Figura 1.10. Ejemplo de un análisis cualitativo de árbol de fallos (FTA) (IEC, 2006)

Un árbol de fallas se puede usar cualitativamente para identificar las causas potenciales y los caminos por los que puede ocurrir una falla, o cuantitativamente para calcular la probabilidad del evento.

Para el análisis cualitativo se requiere conocer el sistema y las causas de la falla, así como el conocimiento técnico de como el sistema puede fallar, el análisis cuantitativo requiere de datos de las probabilidades de fallo de los componentes del sistema.

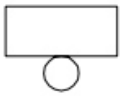
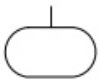
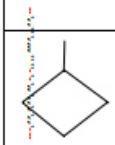
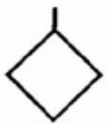
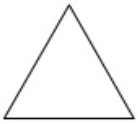
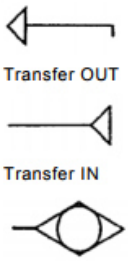
	Symbols		Name	Description	Reliability correlation	Number of inputs
			BASIC EVENT	The lowest level event for which probability of occurrence or reliability information is available	Component failure mode, or a failure mode cause	0
			CONDITIONAL EVENT	Event that is a condition of occurrence of another event when both have to occur for the output to occur	Occurrence of event that has to occur for another event to occur Conditional probability	0
			DORMANT EVENT	A primary event that represents a dormant failure; an event that is not immediately detected but could, perhaps, be detected by additional inspection or analysis	Dormant component failure mode or dormant failure cause	0
			UNDEVELOPED EVENT	A primary event that represents a part of the system that is not yet developed	A contributor to the probability of failure. Structure of that system part is not yet defined	0
			TRANSFER gate	Gate indicating that this part of the system is developed in another part or page of the diagram	A partial fault tree diagram that is shown in other location of the overall system IN means that the develop gate is elsewhere, OUT means that the same gate developed in this place will be used elsewhere	0

Figura 1.11. Símbolos frecuentes utilizados en los FTA
(IEC, 2006)

Para elaborar un árbol de fallas, se define un evento superior, esto puede ser una falla o una consecuencia más amplia de esta falla, las posibles causas inmediatas del modo de falla llevan a identificar al evento superior, este análisis se lo realiza progresivamente más abajo hasta que los análisis no sean procedentes, por ejemplo, en un sistema de hardware, se puede llegar hasta el nivel más bajo de componentes físicos.

Este análisis permite representar gráficamente como puede ocurrir un evento superior y las interacciones donde dos o más eventos pueden ocurrir simultáneamente, lo que permite realizar un análisis lógico de los ajustes de corte de fallas simples en un sistema más complejo.

1.2.1.6 Evaluación de datos y estimación de parámetros

En este paso del APS se realiza la evaluación de las consecuencias de los estados finales no deseados, todos los pasos anteriores a este podrían generar modelos que pueden ser evaluados y analizados de forma cualitativa. Sin embrago, en este paso se requiere realizar los cálculos necesarios para realizar un APS cuantitativo. Además, se requiere realizar análisis profundos sobre las consecuencias que puede sufrir el personal que labora en las facilidades y las personas que se encuentran alrededor en caso de exposición o liberación de material radiactivo, esto se logra por medio de la estimación de tasa de dosis en el interior de la facilidad y en sus alrededores.

1.2.1.7 Cuantificación de las secuencias

En este paso se estima la probabilidad de ocurrencia de los estados no deseados derivados de los eventos iniciantes, además, se considera la probabilidad de ocurrencia de falla de los SIS y se añade a esta, la cuantificación de la estimación de tasa de dosis recibida por el personal en caso de que ocurriera el evento no deseado. Con estos insumos, se puede cuantificar el riesgo de las secuencias analizadas en el APS.

1.2.1.8 Documentación de análisis

En este paso, se refiere a cómo se realiza la documentación de todo el proceso durante el estudio APS, y es criterio del grupo de trabajo, la manera de cómo llevar esta documentación.

Estos pasos resumen todos los que se recomienda realizar para la evaluación por medio de la metodología APS.

Una dificultad que radica en este método es la de obtener datos reales de la confiabilidad de los componentes y sistemas relacionados con la seguridad radiológica. Aun así, una gran ventaja de esta metodología es el alto grado de conocimiento que se adquiere de la instalación estudiada (Alderete & Elechosa, 2006)

1.3 CONFIABILIDAD DE COMPONENTES – GENERALIDADES

La teoría de confiabilidad de componentes requiere de algunos conceptos de probabilidad y entender algunos métodos probabilísticos para su análisis. Las fallas de los equipos ocurren como resultado de una compleja interacción de componentes individuales y la probabilidad global de la falla en un proceso depende altamente de la naturaleza su interacción.

Los datos son recolectados en una tasa de fallo de un componente en particular, estos datos pueden mostrar un promedio de falla del componente luego de un periodo, a esto se le llama la tasa de fallo promedio y es representada por la letra μ, con unidades en fallas/tiempo. La probabilidad que un componente no falle durante un intervalo (0, t) es dado por una distribución de Poisson indicada en la Ecuación [1.1].

$$R(t) = e^{-\mu t} \qquad [\ 1.1]$$

Donde:

R: Confiabilidad de un sistema/componente/equipo

μ: Tasa de fallo del sistema/componente/equipo

t: Tiempo o periodo de evaluación de la confiabilidad

La confiabilidad R se asume que la tasa de fallo es constante en el tiempo, el complemento de la confiabilidad es denominada probabilidad de falla y se define por medio de la Ecuación [1.2].

$$P(t) = 1 - R(t) = 1 - \ e^{-\mu t}$$

[1.2]

Donde:

P: Probabilidad de falla de un sistema/componente/equipos

R: Confiabilidad de un sistema/componente/equipo

μ: Tasa de fallo del sistema/componente/equipo

t: Tiempo o periodo de evaluación de la confiabilidad

La función de densidad de falla es definida como la derivada de la probabilidad de falla como se indica en la Ecuación [1.3].

$$f(t) = \frac{dP(t)}{dt} = \mu e^{-\mu t}$$

[1.3]

Donde:

P: Probabilidad de falla de un sistema/componente/equipos

μ: Tasa de fallo del sistema/componente/equipo

t: Tiempo o periodo de evaluación de la confiabilidad

La función de densidad de fallas es utilizada para determinar la probabilidad P de al menos una falla en un periodo de tiempo $t_0 - t_1$ como se indica en la Figura 1.12. y esta es definida por la Ecuación [1.4].

$$P(t_0 \rightarrow \ t_1) = \int_{t_0}^{t_1} f(t)dt = \int_{t_0}^{t_1} \mu e^{-\mu t} dt = e^{-\mu t_0} - e^{-\mu t_1}$$

[1.4]

Donde:

P: Probabilidad de falla de un sistema/componente/equipos

μ: Tasa de fallo del sistema/componente/equipo

t_0: Tiempo final del periodo de evaluación de la confiabilidad

t_1: Tiempo final del periodo de evaluación de la confiabilidad

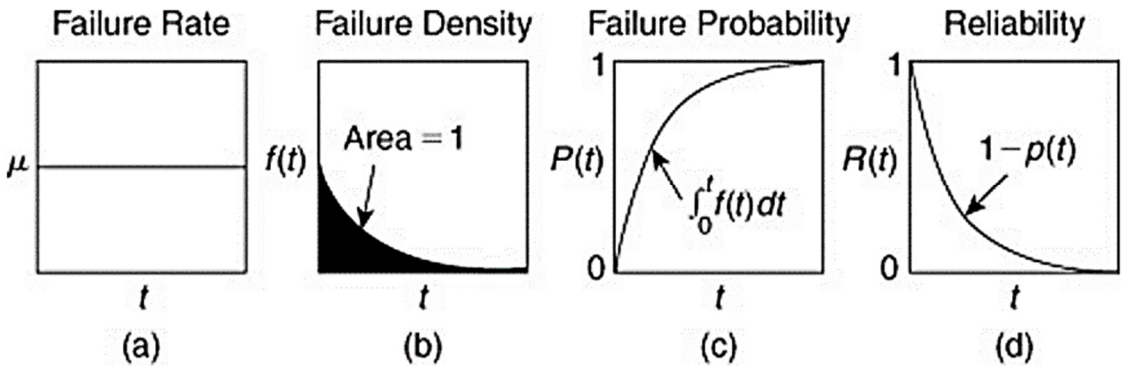


Figura 1.12. Gráficas típicas de los conceptos de confiabilidad: (a) Tasa de fallo, (b) Densidad de fallo, (c) Probabilidad de fallo P(t), (d) Confiabilidad R(t)
(Crowl & Louvar, 2011)

El intervalo entre dos fallas es denominado tiempo promedio entre fallas (MTBF por sus siglas en inglés) y está definida por la Ecuación [1.5].

$$E(t) = MTBF = \int_0^\infty tf(t)dt = \frac{1}{\mu} \qquad [1.5]$$

Donde:

MTBF: Tiempo medio entre fallas

μ: Tasa de fallo del sistema/componente/equipo

Muchos componentes exhiben una típica curva de la tasa de fallo en forma de bañera como muestra la Figura 1.13, la tasa de falla es elevada cuando el componente es nuevo y cuando el componente es viejo, sin embargo, sobre la mitad de la vida útil del componente, la tasa de fallo es aproximadamente constante.

Los procesos pueden tener varias modalidades de interacciones entre sus componentes, los más comunes son las interacciones en serie y en paralelo, frente a estas configuraciones, se requiere entender como interactúan las unidades que se encuentran en serie y en paralelo en relación con la probabilidad de falla, la confiabilidad y la tasa de fallo.

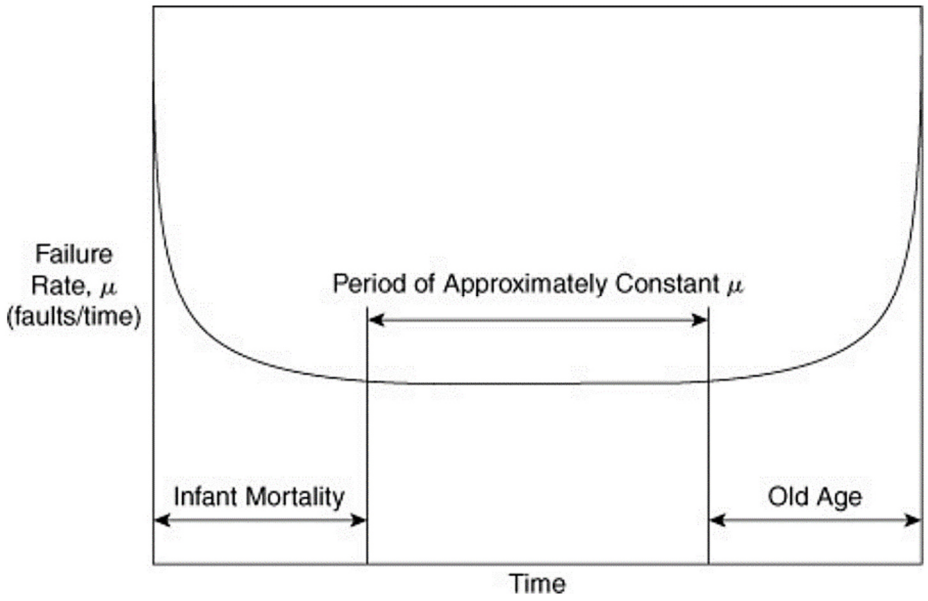


Figura 1.13. Típica curva de tasa de fallo en forma de bañera para hardware.
(Crowl & Louvar, 2011)

Las configuraciones en paralelo requieren que dos componentes fallen simultáneamente para que falle el sistema por lo que se utiliza una compuerta lógica AND para la representación de su vinculación, en cambio en una configuración en serie, es necesario que un componente u otro falle, para provocar el fallo del sistema, por eso se utiliza la compuerta lógica OR para representar esta vinculación Figura 1.14.

En la realidad, para poder determinar la confiabilidad de un sistema se requiere la recolección de los datos de mantenimiento de un proceso para poder calcular los parámetros requeridos en esta teoría. Sin embargo, muchos componentes no pueden ser estimados por las tareas de mantenimiento, ya sea por falta de presupuesto, equipos, o capacitación del personal técnico, por ese motivo, en muchas ocasiones se trabaja con datos genéricos levantados por instancias internacionales o por entidades con la capacidad de hacer este tipo de pruebas o ensayos sobre los componentes que pueden intervenir en un proceso. Por ejemplo:

- IAEA – TECDOC 930: Generic component reliability data for research reactor PSA, International Agency Energy Atomic.
- Military Handbook: Reliability prediction of electronic equipment, Department of Defense of UU.SS.

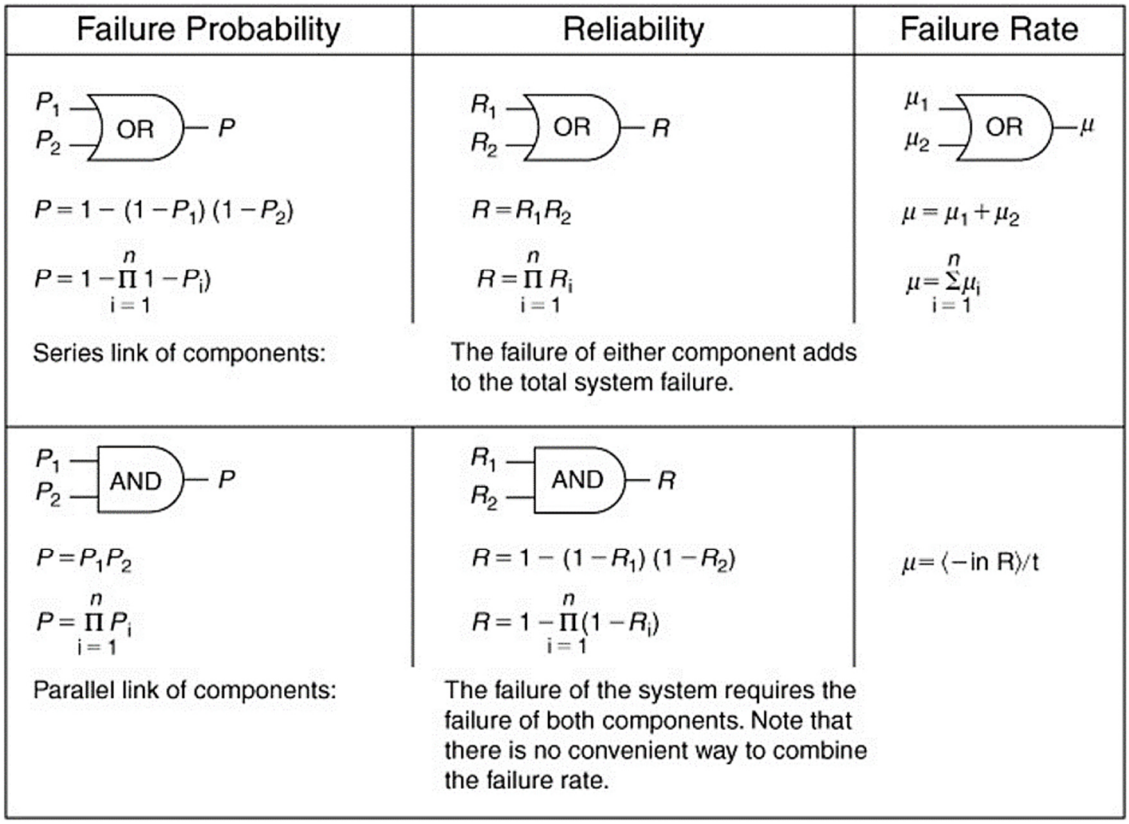


Figura 1.14. Cálculos para las configuraciones en serie y paralelo para la probabilidad de falla, confiabilidad y tasa de falla
(Crowl & Louvar, 2011)

Estas fuentes tienen datos bastante diversos de componentes que intervienen en especial en facilidades de radiaciones ionizantes como son los reactores de investigación, o también en instalaciones en el que intervienen varios componentes eléctricos. Los datos que se pueden obtener de estas fuentes son en general la tasa de fallos/10^6 Horas. A modo de ejemplo, se puede considerar lo siguiente, la tasa de fallo de un motor es de 1,2 cada 10^6 horas. Entonces, para determinar la probabilidad de fallo se realiza el siguiente análisis:

En primer lugar, se requiere de los datos acerca de la tasa de falla por hora de los componentes a ser evaluados y del periodo de evaluación. En la Tabla 1.3 se muestra un ejemplo de cómo se determina la probabilidad de fallo para un motor, la tasa de fallo de este componente es μ = 1,2E-6 (IAEA, 1997). El periodo de evaluación será la cantidad de horas de funcionamiento del componente al año, para esto, se considera que el sistema tiene un tiempo de trabajo igual al del

personal que labora en la instalación por lo que se utiliza el número de horas semanales de trabajo (40 horas semanales establecido en el Código del Trabajo del Ecuador como jornada máxima de trabajo) por semanas laborales al año (para facilitar los cálculos se consideran 50 semanas laborales al año) con lo que se definen 40 x 50 = 2 000 horas. A partir de estos datos se puede determinar la tasa de fallo en el año: μt = 1,20E-6 x 2 000 = 2,40E-3.

Tabla 1.3. Ejemplo de cálculo de probabilidad de fallo

Componente	**Tasa de fallo anual (μt)**	**Confiabilidad** $R = e^{-\mu t}$	**Probabilidad de fallo** $P = 1 - R$
Motor	2,4E-6	9,98E-1	2,00E-3

Todos estos conceptos y otros más son requeridos para una estimación cuantitativa de la confiabilidad de los equipos y de procesos en plantas industriales.

1.4 DETERMINACIÓN DEL NIVEL DE SEGURIDAD INTEGRADO (SIL)

El nivel de seguridad integrada (SIL) es una categorización especificada en el estándar IEC 61508, la cual, considera la máxima taza de falla tolerable que puede tener un componente de un equipo en relación con un peligro específico. Los niveles de seguridad integrada usualmente son descritos por cuatro bandas discretas que son:

- SIL 4: Este nivel de seguridad es el más alto y oneroso para alcanzar, requieren técnicas sofisticadas y costosas.
- SIL 3: es menos oneroso que SIL 4 pero aún requiere técnicas sofisticadas de diseño
- SIL 2: Requiere buenas prácticas de diseño y operación no muy diferentes a ISO 9000.
- SIL 1: Es el mínimo nivel, sin embargo, aún implica buenas prácticas de diseño.

- <SIL 1: Referido en la normativa IEC 61508 como “no seguro”

Para establecer el nivel de seguridad integrado requerido por el sistema, se pueden recurrir a varias técnicas. En este trabajo se mencionan algunas de ellas.

1.4.1 APROXIMACIÓN CUANTITATIVA

Para alcanzar esta aproximación se requiere tener como datos o asumir la frecuencia máxima tolerable para un escenario de riesgo involuntario y tener datos o asumir la probabilidad de eventos peligros que terminan en una fatalidad. Además, se requiere determinar si el sistema de seguridad es de baja demanda o de alta demanda, el objetivo de esta aproximación cuantitativa es la de determinar la probabilidad de falla en demanda (PFD) y por medio de la Tabla 1.2 determinar la asignación SIL correspondiente que requiere el sistema de seguridad.

Si no se tiene información respecto al objetivo de nivel de riesgo para un área específica, se puede considerar la siguiente referencia como se muestra en la Tabla 1.4

Tabla 1.4. Objetivos de niveles de riesgo

Máximo riesgo tolerable de fatalidad	**Riesgo individual (por año)**
Empleado	10^{-4}
Público	10^{-5}
Riesgo aceptable en general	10^{-6}

(Smith & Simpson, 2004)

1.4.2 APROXIMACIÓN GRÁFICA

Cuando no es posible realizar una aproximación cuantitativa para establecer la asignación SIL requerida se puede utilizar juicios cualitativos como el mostrado en la Figura 1.15

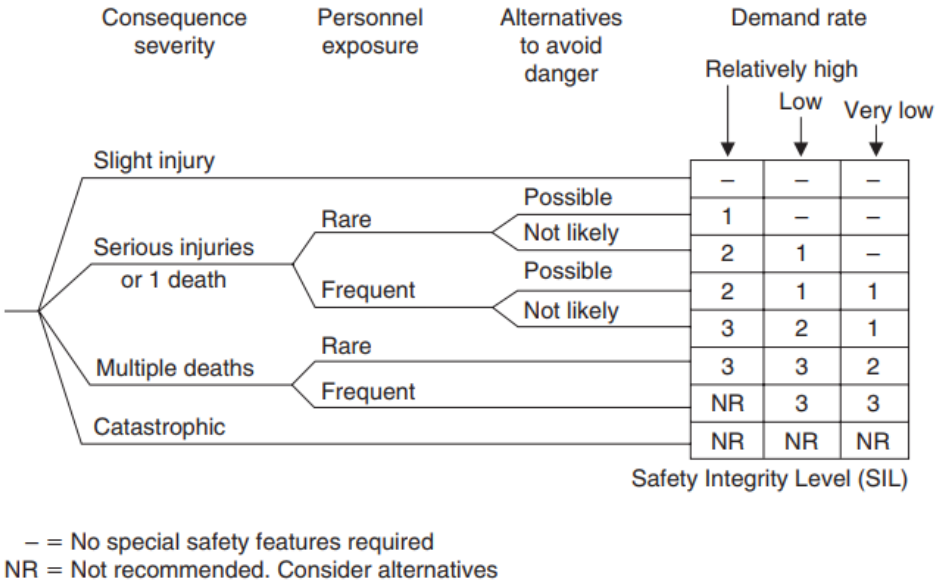


Figura 1.15. Aproximación grafica de riesgo usado para plantas industriales de petróleo y gas off-shore
(Smith & Simpson, 2004)

La aproximación mostrada en la Figura 1.15 es rápida y en muchos casos es imprecisa, en la Figura 1.16 se muestra un gráfico de riesgo calibrado el cual considera el daño como la fatalidad en el establecimiento.

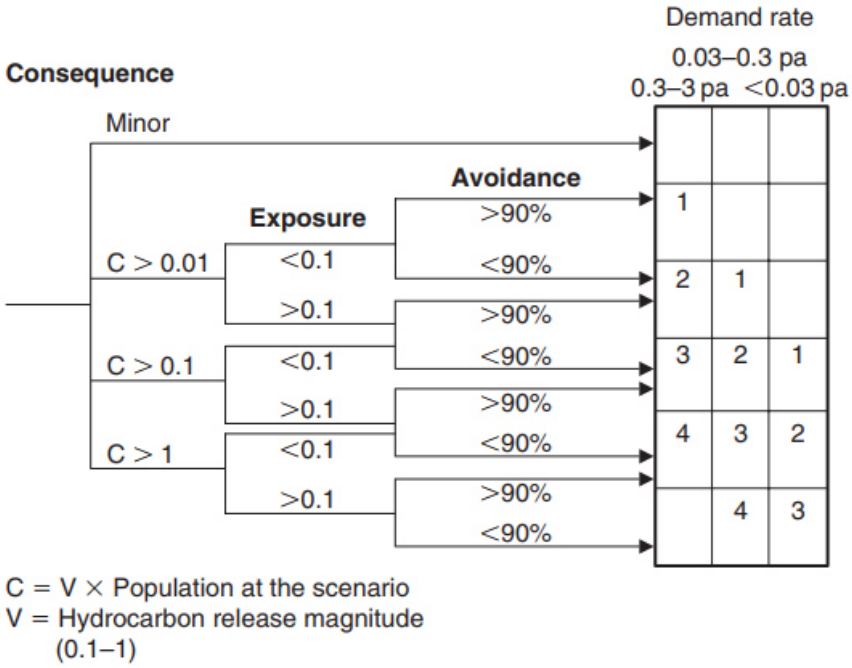


Figura 1.16. Ejemplo de una aproximación gráfica de riesgo calibrado
(Smith & Simpson, 2004)

1.4.3 APROXIMACIÓN DE LA PROBABILIDAD DE FALLA EN DEMANDA (PFD) POR TABLAS

En la aproximación cuantitativa, se necesita el dato del PFD para calcular la asignación SIL que requiere el sistema, por tal motivo, en esta sección se dará una técnica de evaluación por tablas para determinar el parámetro PFD y así poder asignar el grado SIL requerido (técnica sacado del Anexo B de la IEC 61508 parte 6). Para esto se requiere conocer ciertos parámetros de los diseños de los sistemas, por lo que esta técnica requiere de algunos criterios específicos del diseño.

En la Tabla 1.5 se detallan los criterios que se requieren para utilizar la metodología del anexo B del estándar IEC 61508 – parte 6.

Tabla 1.5. Términos y rangos utilizados en el anexo B del estándar IEC61508 – parte 6

Símbolo	Termino (unidades)	Parámetros de rangos utilizados
T_1	Periodo de prueba de calidad (horas)	1 mes (730 h) – para alta demanda 3 meses (2 190 h) – para alta demanda 6 meses (4 380 h) – para alta demanda 1 año (8 760 h) 2 años (17 520 h) – para baja demanda 10 años (87 600 h) – para baja demanda
MTTR	Tiempo medio de restauración (horas)	8 horas
DC	Cobertura del diagnóstico (porcentaje)	1 % 5 % 10 %
β	Fracción de fallas con causas comunes	1 % 5 % 10 %
λ	Probabilidad promedio de fallas (por demanda o por hora)	$0{,}1 \times 10^{-6}$ $0{,}5 \times 10^{-6}$ $1{,}0 \times 10^{-6}$ $5{,}0 \times 10^{-6}$ 10×10^{-6} 50×10^{-6}
PFD_{AVG}	Probabilidad promedio en demanda (horas)	

(IEC, 1997f)

El PFD de un sistema E/E/EP relacionado a la seguridad, se calcula por medio de la combinación de la PFD de todos sus subsistemas que proveen protección en contra de un evento peligroso. Los subsistemas tienen una estructura como muestra la Figura 1.17. En esta estructura se consideran los componentes de entradas y sensores, los componentes del sistema lógico y los componentes de la interfaz de salida y elementos finales.

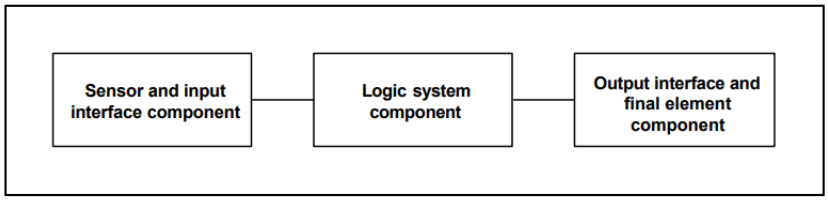


Figura 1.17. Estructura de los componentes de un sistema
(Gruhn & Cheddie, 2006)

Para proceder con esta técnica, es necesario realizar un diagrama en bloques en los que se muestren los componentes de entrada, del sistema lógico y de salida y cada una de estas puede ser representada como estructuras 1oo1, 1oo2, 2oo2, 1oo2D o 2oo3 (estas estructuras se verán en la sección 1.6)

Luego de determinar la estructura del sistema E/E/EP, es necesario determinar los parámetros específicos como son: La cobertura del diagnóstico, la probabilidad de demanda por hora y el factor de causa de falla común. Esto permite determinar el PFD a partir de las tablas dadas en el anexo B del estándar IEC 6508 – parte 6. En la Tabla 1.6 se muestra un ejemplo tomado de dicho anexo.

Tabla 1.6. PFD para un periodo de pruebas de calidad de 6 meses y un MTTR de 8 h

Architecture	DC	λ = 1.0E-07			λ = 5.0E-07			λ = 1.0E-06		
		β=1%	β=5%	β=10%	β=1%	β=5%	β=10%	β=1%	β=5%	β=10%
1oo1 (see note)	0%	1.1E-04			5.5E-04			1.1E-03		
	60%	4.4E-05			2.2E-04			4.4E-04		
	90%	1.1E-05			5.7E-05			1.1E-04		
	99%	1.5E-06			7.5E-06			1.5E-05		
1oo2	0%	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.5E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04
	60%	8.8E-07	4.4E-06	8.8E-06	4.5E-06	2.2E-05	4.4E-05	9.1E-06	4.4E-05	8.8E-05
	90%	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.3E-06	1.1E-05	2.2E-05
	99%	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06
2oo2 (see note)	0%	2.2E-04			1.1E-03			2.2E-03		
	60%	8.8E-05			4.4E-04			8.8E-04		
	90%	2.3E-05			1.1E-04			2.3E-04		
	99%	3.0E-06			1.5E-05			3.0E-05		
1oo2D	0%	2.2E-06	1.1E-05	2.2E-05	1.1E-05	5.5E-05	1.1E-04	2.4E-05	1.1E-04	2.2E-04
	60%	8.8E-07	4.4E-06	8.8E-06	4.4E-06	2.2E-05	4.4E-05	8.9E-06	4.4E-05	8.8E-05
	90%	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.2E-06	1.1E-05	2.2E-05
	99%	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06
2oo3	0%	2.2E-06	1.1E-05	2.2E-05	1.2E-05	5.6E-05	1.1E-04	2.7E-05	1.1E-04	2.2E-04
	60%	8.9E-07	4.4E-06	8.8E-06	4.6E-06	2.2E-05	4.4E-05	9.6E-06	4.5E-05	8.9E-05
	90%	2.2E-07	1.1E-06	2.2E-06	1.1E-06	5.6E-06	1.1E-05	2.3E-06	1.1E-05	2.2E-05
	99%	2.6E-08	1.3E-07	2.6E-07	1.3E-07	6.5E-07	1.3E-06	2.6E-07	1.3E-06	2.6E-06
NOTE For 1oo1 and 2oo2 architectures, the value of β does not affect the average probability of failure.										

(IEC, 1997f)

Cuando se determina los PFD de cada uno de los componentes de la estructura del sistema E/E/EP relacionado de seguridad, se procede a realizar el siguiente cálculo.

$$PFD_{AVG} = \sum PFD_{SE} + \sum PFD_{LS} + \sum PFD_{PE} \quad [1.6]$$

Donde:

PFD_{AVG}: Probabilidad de falla en demanda del sistema E/E/EP relacionado a la seguridad

PFD_{SE}: Probabilidad de falla en demanda de los componentes de entrada y sensores

PFD_{LS}: Probabilidad de falla en demanda de los componentes del sistema de lógica

PFD_{PE}: Probabilidad de falla en demanda de los componentes de salida o elementos finales

De esta manera se calcula el PFD del sistema E/E/EP relacionado a la seguridad, el cual permite determinar el SIL correspondiente en función de su objetivo de seguridad determinado en los requerimientos de seguridad del sistema.

1.4.4 DETERMINACIÓN DEL SIL POR EL ANÁLISIS DE CAPA DE PROTECCIÓN (LOPA POR SUS SIGLAS EN INGLÉS)

Este análisis se basa en una estructura de protección tipo “cebolla” indicada en la Figura 1.18, esta es una de las metodologías para calcular el índice SIL reflejado en los estándares de la IEC 61511 y ANSI-ISA-S84 por ser una técnica exhaustiva y por su carácter semicuantitativo.

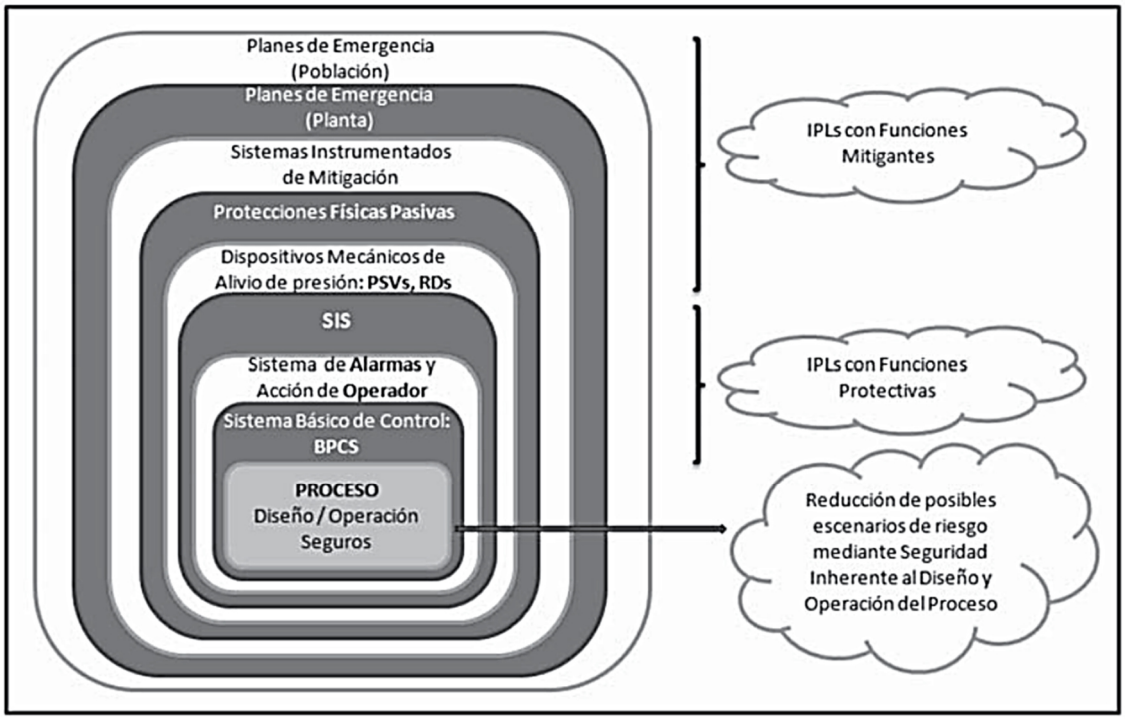


Figura 1.18. Diagrama "cebolla" de las capas de protección de un proceso (Fernandez, et al., 2012)

Esta metodología tiene las siguientes etapas:

- Etapa 1. Identificación de consecuencias y estimación de su severidad.
- Etapa 2. Selección del escenario de estudio.
- Etapa 3. Identificación del suceso iniciador del escenario y determinación de su frecuencia en un año.

- Etapa 4. Identificación de las capas de protección que intervienen en el escenario objeto de estudio y determinar la probabilidad de fallo en demanda (PFD) de las mismas.

La capa de protección es un mecanismo, sistema o acción que es capaz de prevenir o evitar el desarrollo de un escenario hasta llegar a la consecuencia indeseable, este esquema se indica en la Figura 1.19.

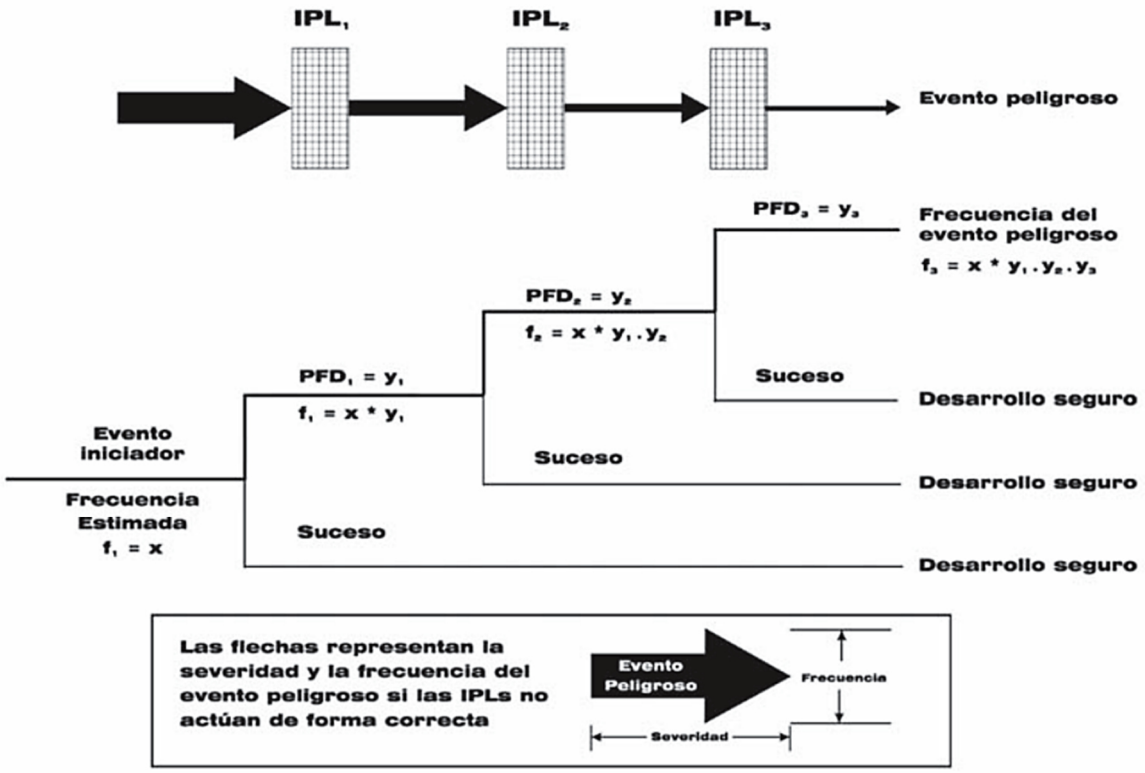


Figura 1.19. Capas de protección y reducción de riesgo
(Fernandez, et al., 2012)

1.5 SISTEMAS INSTRUMENTADOS DE SEGURIDAD – GENERALIDADES

Los sistemas instrumentados de seguridad tienen diferentes connotaciones, debido a que el termino evoluciono desde varios ámbitos, el termino más genérico utilizado es “sistema de seguridad”, pero esto significa diferentes cosas desde el ámbito que se considere, por ejemplo, desde la ingeniería química el término hace referencia a procedimientos y prácticas y no sistemas de control; desde la ingeniería eléctrica,

el término hace referencia a los sistemas de apagado de emergencia usados en los sistemas eléctricos. Cuando el Centro de Seguridad de Procesos Químicos del Instituto Americano de Ingeniería Química, (AIChE CCPS por sus siglas en inglés) publicó las directrices para la automatización de procesos químicos en 1993, el término usado fue “sistemas de enclavamientos de seguridad” (SIS por sus siglas en inglés). Sin embargo, algunos miembros de la Sociedad de Automatización Internacional (ISA por sus siglas en inglés), consideró en la publicación ISA SP84, que los “*enclavamientos”* era solo un subtipo de todos los sistemas de seguridad, por lo que el comité que elaboró la publicación ISA SP84 estableció el término de “sistemas instrumentados de seguridad” para mantener el mismo acrónimo utilizado en la Publicación acerca del Análisis de capas de protección del AIChE CCPS del 2001.

Para definir el término de sistemas instrumentados de seguridad, la normativa ANSI/ISA 91.00.01-2001, utiliza la siguiente definición: instrumentación y control instalado con el propósito de llevar al proceso, o a un equipo específico hacia un estado seguro. Estos pueden ser los sistemas eléctricos, electrónicos, neumáticos, hidráulicos y mecánicos, incluso los sistemas que son programables, en otras palabras. Los sistemas instrumentados de seguridad son sistemas diseñados para responder a condiciones de una planta industrial, que podría ser peligrosa en sí misma, o que, si no se toman medidas, el proceso eventualmente podría derivar en un evento peligroso. Por lo que los sistemas deberían generar las salidas correctas para prevenir o mitigar cualquier evento peligroso o llevarlo a un estado seguro.

La comunidad internacional por medio del estándar IEC 61508 se ha referido a los SIS como sistemas relacionados a la seguridad, pero también combina los acrónimos E/E/EP que hace referencia a eléctricos, electrónicos y electrónicos programables. sí bien este estándar se enfoca a la seguridad de las personas, también se utilizan los mismos conceptos para proteger al equipamiento y al ambiente en general.

Existen algunas consideraciones que están involucrados durante el diseño de los SIS y estas detallan a continuación.

- ***Tecnología.*** Relés electromecánicos, relés de estado sólido, o microprocesador deben considerarse para las entradas y salidas basado en la aplicación del sistema, por ejemplo, para un sistema que requiere 500 entradas y salidas sería muy difícil diseñarlo con tecnología a base de relés, por lo que es requerido un sistema lógico programable como un PLC. Sin embargo, es un error considerar que tener un PLC con un SIL 3 garantizaría la seguridad de todo el sistema, ya que dependen de nivel SIL de los otros componentes que integran el sistema de seguridad. Pero existen otros parámetros que se deben considerar al momento de elegir la tecnología, como son: el presupuesto, el tamaño, el nivel de riesgo, complejidad, flexibilidad, mantenibilidad, interfaz, comunicación, seguridad, etc.
- ***Redundancia.*** Es necesario considerar si el sistema requiere tener redundancia para minimizar la probabilidad de fallo de un sistema de seguridad, dentro de estas consideraciones se podrían analizar varias configuraciones como, por ejemplo: 1oo1, 1oo2, 2oo2, 2oo3, estas configuraciones se revisarán más adelante.
- ***Intervalos de prueba.*** La frecuencia de prueba de los sistemas puede ser: mensuales, trimestrales, anuales o una vez por ronda de trabajo, esto modifica también la probabilidad de fallo de un sistema de seguridad y también es un parámetro para considerar al momento de elegir la redundancia de los componentes.

Los sistemas de seguridad deben ser diseñados como sistemas separados de los sistemas de control, esto para garantizar su funcionamiento en caso de falla de los sistemas de control como se indica en la Figura 1.20.

Sin embargo, si estos requerimientos no pueden ser logrados, entonces todo el sistema de control por entero debe ser considerado como un sistema instrumentado de seguridad.

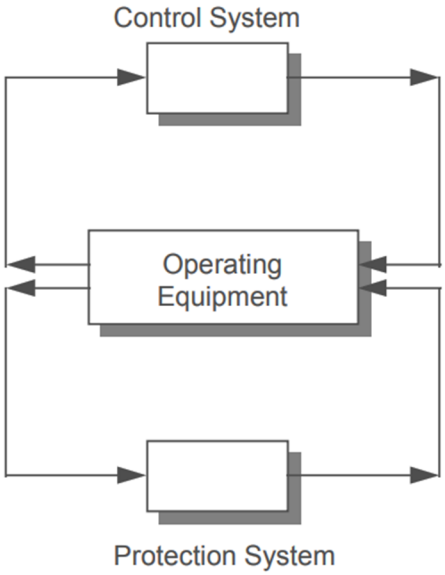


Figura 1.20. Recomendación del Reglamento Ejecutivo de Salud y Seguridad del Reino Unido
(Gruhn & Cheddie, 2006)

1.6 ARQUITECTURAS DE LOS SISTEMAS INSTRUMENTADOS DE SEGURIDAD

Las arquitecturas requeridas por los sistemas instrumentados de seguridad dependen de diferentes factores (el grado SIL que requiere el sistema, tasa de disparos falsos esperados, frecuencia de prueba, tasa de falla de los componentes, el diagnóstico, etc.) sin embargo existen configuraciones de los elementos de entrada, lógicos y de salida que podrían influir en la definición del diseño de un sistema integrado de seguridad. Las arquitecturas también influyen en la redundancia del sistema y es necesario entender cuando el sistema puede ir a un fallo seguro o a un fallo peligroso.

- **Fallo seguro.** Se genera un fallo seguro cuando, como resultado de la falla el proceso va a condiciones seguras.
- **Fallo peligroso**. Se genera un fallo peligroso cuando, ante la demanda de la función de seguridad, el sistema no responde correctamente y deja al proceso en condiciones intolerables de peligro.

A continuación, se describen varias arquitecturas que pueden tener los SIS y se analizan dentro de una función de seguridad de apagado de emergencia. Se

consideró como fallo seguro, el disparo no intencionado de los relés; como fallo peligroso, la no desconexión provocado por la soldadura de los bornes del relé. A modo de ejemplo, se considera que, cada una de estas fallas tendrían una probabilidad de ocurrencia en el año del 4 % y del 2 %, respectivamente (Gruhn & Cheddie, 2006).

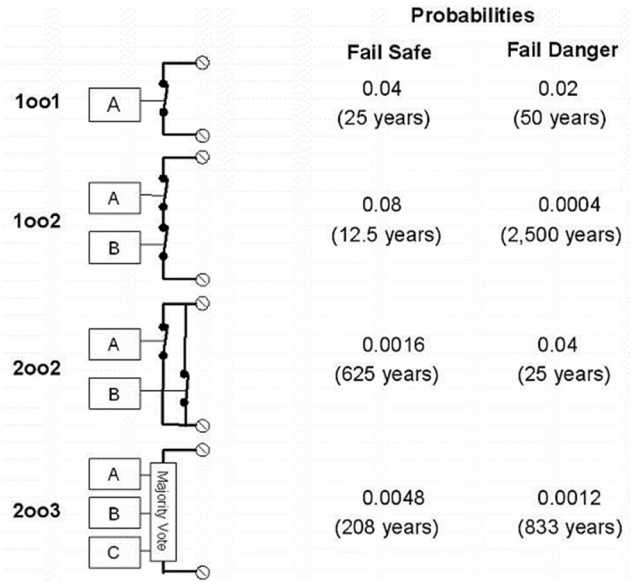


Figura 1.21. Relación de las arquitecturas con las probabilidades de falla (Gruhn & Cheddie, 2006)

1.6.1 ARQUITECTURA 1oo1 (ONE-OUT-OF-ONE)

Esta arquitectura hace referencia a un sistema no redundante como se muestra en la Figura 1.21, si la función de seguridad del relé A es la de un apagado de emergencia, entonces, cuando el relé falla en un modo de disparo no deseado esto generaría un fallo seguro y se asume que la probabilidad de tasa de fallo del relé A en esta configuración es del 0,04 en un año, es decir, el sistema de seguridad tendrá un fallo seguro de 4 veces cada 100 demandas o 1 vez en 25 años. Ahora se considera que el relé pueda tener una falla de soldadura de sus bornes en la bobina, lo cual imposibilitaría la función del apagado de emergencia, lo que genera un fallo peligroso, si se asume para este modo de fallo una probabilidad de tasa de fallo de 0,02, quiere decir que el sistema fallaría 2 veces de cada 100 demandas o 1 vez cada 50 años. Los datos de tasa de fallos que se hacen referencia en estos

ejemplos son solo con fines didácticos, para entender las implicaciones de las diferentes arquitecturas que pueden tener los SIS.

1.6.2 ARQUITECTURA 1oo2 (ONE – OUT – OF – TWO)

Esta arquitectura llamada también dual como se indica en la Figura 1.21, tiene las salidas cableadas en serie, lo que significa que solo requiere un canal para realizar el apagado, existe doble hardware (relé A y B) para cumplir la función de seguridad. Se considera el ejemplo anterior y bajo esta arquitectura se puede decir que un fallo seguro provocado por falsos disparos de los relés duplica su probabilidad de ocurrencia, por el hecho de tener dos veces más hardware que en la arquitectura 1oo1, lo que significa que, en este modo de fallo, la probabilidad de ocurrencia será de 0,08 (0,04 + 0,04), por lo que, el sistema puede fallar 8 veces cada 100 demandas o que puede ocurrir 1 fallo en 12,5 años. Ahora, se asume un evento en el que el modo de fallo no permite que actúe la función de seguridad (este evento puede provocar un fallo peligroso), para que este evento suceda, requiere que fallen los dos componentes del hardware simultáneamente, lo que quiere decir que, en este modo de fallo la probabilidad de ocurrencia será de 0,0004 (0,02 x 0,02), lo cual implicaría que el sistema fallaría 4 veces cada 10 000 demandas o puede fallar 1 vez cada 2 500 años.

1.6.3 ARQUITECTURA 2oo2 (TWO – OUT – OF – TWO)

En esta arquitectura, las salidas son cableadas en paralelo como se indica en la Figura 1.21, esto significa que, para cumplir la función de seguridad de un apagado de emergencia, se deben desconectar los dos relés simultáneamente. Se considera el ejemplo anterior, esta arquitectura tiene una probabilidad de ocurrencia de un fallo seguro de 0,0016 (0,04 x 0,04), lo que quiere decir que este fallo seguro podría ocurrir 16 veces por 10.000 demandas o 1 vez cada 625 años, sin embargo, la probabilidad de ocurrencia de un fallo peligroso se mantiene en 0,04 (0,02 + 0,02),

lo que implica que, el sistema podría tener un fallo peligroso 4 veces de cada 100 demandas o 1 vez cada 25 años.

1.6.4 ARQUITECTURA 2oo3 (TWO – OUT- OF – THREE)

En esta arquitectura se aprovecha de las ventajas de las dos arquitecturas anteriores, la 1oo2 y 2oo2 y se considera en el hardware el uso de tres relés, relé A, B y C (Figura 1.22), desde esta configuración es necesario analizar las fallas en combinaciones duales (A, B; A, C; B, C). Al analizar un fallo seguro por falsos disparos se tendría que analizar la probabilidad de ocurrencia del sistema para producir en todas sus combinaciones un fallo seguro, así, si fallan simultáneamente dos relés se podría producir un fallo seguro del sistema, por lo que, la probabilidad de un fallo seguro estaría dado por la expresión: (A x B) + (A x C) + (B x C). Se asume los valores del ejemplo anterior y se puede decir que la probabilidad de un fallo seguro de esta arquitectura sería igual a (0,04 x 0,04) + (0,04 x 0,04) + (0,04 x 0,04) = 0,0048, lo que equivale a decir que esta arquitectura tendría un fallo seguro cada 208 años, aproximadamente.

Para que la arquitectura genere un fallo peligroso, también se tiene la misma expresión a la anterior, ya que si fallan simultáneamente dos relés el sistema no podría ejecutar su función de seguridad de una desconexión de emergencia, así se puede calcular su probabilidad de falla de la misma manera (A x B) + (A x C) + (B x C). Al considerar los datos del ejemplo anterior, la probabilidad de un fallo peligroso es igual a (0,02 x 0,02) + (0,02 x 0,02) +(0,02 x 0,02) = 0,0012, lo que quiere decir que el sistema tendría un fallo peligroso cada 833 años, aproximadamente.

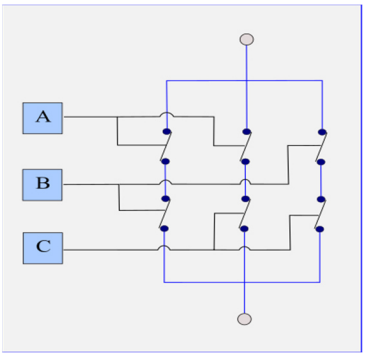


Figura 1.22. Arquitectura 2oo3

1.6.5 DIAGNÓSTICO EN LAS ARQUITECTURAS

En las arquitecturas revisadas previamente, se considera el diagnóstico manual de elementos que forman parte de los SIS, sin embargo, existen configuraciones en las que el diagnóstico del elemento es automático y permite reducir las probabilidades de los fallos.

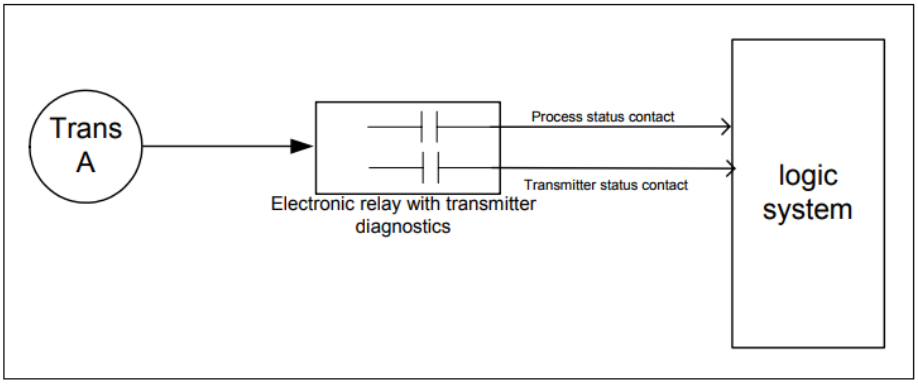


Figura 1.23. Arquitectura con diagnostico 1oo1D
(Gruhn & Cheddie, 2006)

En las arquitecturas con diagnóstico, se tienen los estados lógicos que se indican en la Tabla 1.7. En la Tabla 1.7 se ilustra la lógica de estados de una arquitectura 1oo1D, en la cual se puede apreciar la influencia del diagnóstico en la determinación de una falla. Con este antecedente a continuación se indica cómo pueden variar las arquitecturas de forma resumida. Hay que considerar que estas arquitecturas pueden ser implementadas en los elementos de entrada y salida de un SIS.

Tabla 1.7. Lógica de estado de una arquitectura 1oo1D

Condición	**Estado del proceso detectado por el transmisor** **1 = Sin disparo** **0 = Con disparo**	**Estado del transmisor detectado por diagnóstico** **1 = Sin falla** **0 = Falla detectada**	**Lógica del estado de la arquitectura 1oo1D**
1	1	1	OK
2	0	1	Disparo
3	1	0	Disparo o alarma
4	0	0	Disparo o alarma
Nota: Una alarma siempre debe ser generada si existe una falla del transmisor.			

(Gruhn & Cheddie, 2006)

Tabla 1.8. Resumen de arquitecturas comunes de los SIS

Sensores	
1oo1	Usado si los componentes reúnen los requerimientos de desempeño
1oo1D	El diagnostico puede ser proveído por un monitor de alarma adicional o puede ser construido dentro del mismo (ejemplo: sensor con certificado de seguridad)
1oo2	Dos sensores son instalados, pero solo uno es requerido para un apagado de emergencia, esta configuración es más segura que la 1oo1, pero genera más disparos falsos.
1oo2D	El diagnostico puede ser proveído por un monitor de alarma adicional o puede ser construido dentro del mismo, esta configuración es tolerante a fallas y puede sobrevivir seguro por si solo o a fallas peligrosas y continuar a operar apropiadamente.
2oo2	Dos sensores son instalados y los dos son requeridos para un apagado de emergencia, esta arquitectura es menos segura que la 1oo1, pero tiene menos falsos disparos
2oo3	Tres sensores son instalados y dos son requeridos para un apagado de emergencia, así como la 1oo2D, esta configuración también es tolerante a fallos y puede sobrevivir seguro por si solo o a fallas peligrosas y continuar a operar apropiadamente
Elementos finales	
1oo1	Con simple elemento, Usado solo si esta cumple los requerimientos de desempeño
1oo2	Con dos elementos finales instalados, pero solo se requiere de uno para activar un apagado de emergencia. esta configuración es más segura que la 1oo1, pero genera más disparos falsos
2oo2	Con dos elementos finales instalados, pero requiere de dos para un apagado de emergencia, esta arquitectura es menos segura que la 1oo1, pero tiene menos falsos disparos

(Gruhn & Cheddie, 2006)

2 PARTE EXPERIMENTAL

El desarrollo de la parte experimental del presente proyecto está basado en el enfoque de la seguridad funcional del estándar general IEC61508 y en especial en el modelo de ciclo de vida de los SIS del estándar IEC61511.

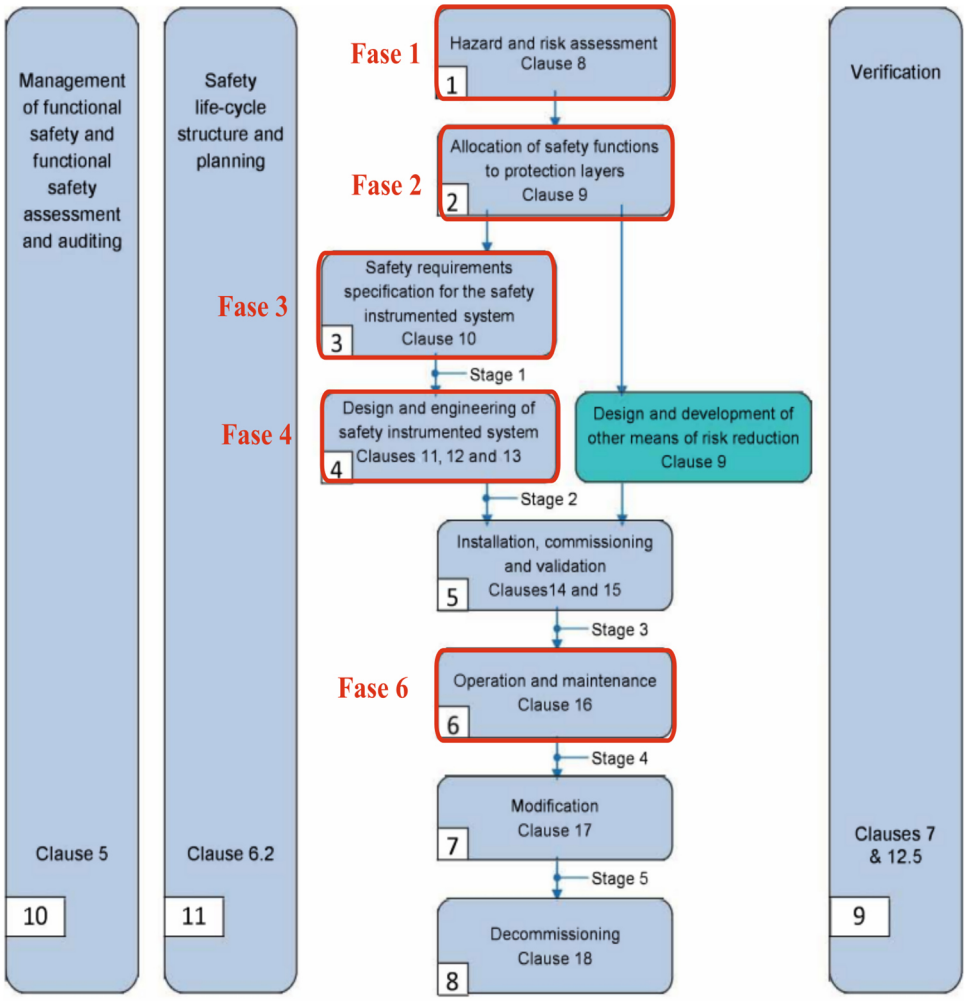


Figura 2.1 Fases del ciclo de vida de los SIS desarrollados en el presente proyecto

Sin embargo, debido a que el enfoque de seguridad funcional mostrado en la Figura 1.4 es bastante amplio, se realizaron ciertas priorizaciones a los análisis efectuados, por lo que se realizó el diseño conceptual concernientes a los sistemas de enclavamientos y control de nivel del blindaje húmedo, que son los SIS más relevantes del irradiador de Co-60. Por lo anteriormente mencionado, para el desarrollo del presente proyecto se consideraron las fases: 1, 2, 3, 4 y 6 del ciclo

de vida de los SIS como se indica en la Figura 2.1. A continuación, se detallan las metodologías utilizadas en la ejecución de cada una de las fases desarrolladas del presente trabajo.

2.1 FASE 1: EL ANÁLISIS DE PELIGROS Y RIESGOS

Para esta fase se consideró la metodología recomendada por el IAEA, la cual es el Análisis Probabilístico de Seguridad (APS) nivel 1 que está orientado a instalaciones de radiaciones ionizantes sin reactores nucleares, para realizar este análisis se recurrió al documento técnico IAEA – TECDOC – 1267, en el cual se visualizó de manera general las tareas específicas que se deben realizar para llevar a cabo un APS nivel 1 completo, como se indica en la Figura 2.2.

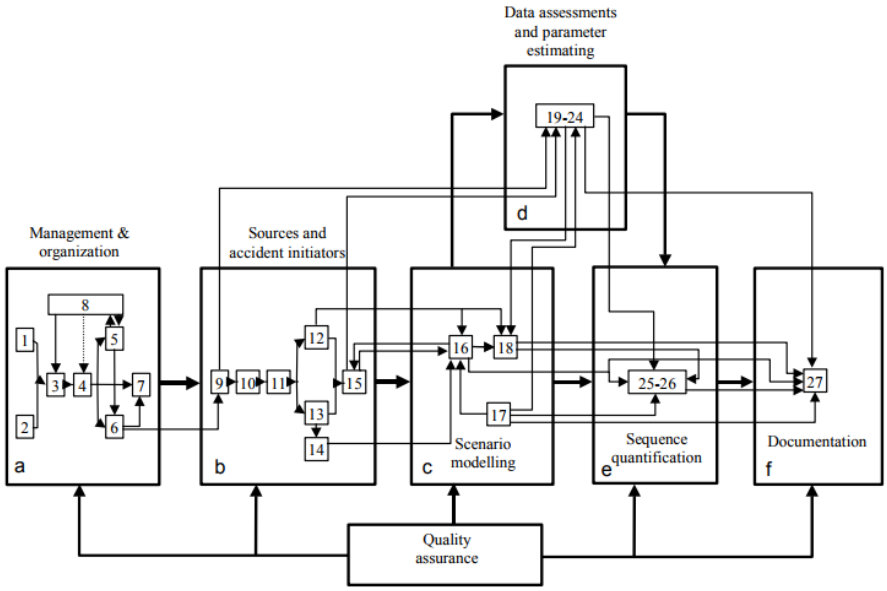


Figura 2.2. Las 27 tareas de un APS de una instalación nuclear sin reactor. (IAEA, 2002)

La metodología que se llevó a cabo para este APS fue por medio de reuniones con funcionarios del Irradiador de Co-60 como son: el Oficial de Seguridad Radiológica (OSR) de la Instalación, el operador y encargado de mantenimiento del irradiador de Co-60 y demás personas involucradas en procesos relacionados como dosimetría y servicio de irradiación. Además, se recurrió a la investigación de bibliografía relacionado a la práctica de Irradiación industrial.

El APS llevado a cabo en este proyecto se encuentra priorizado, con el objetivo de tratar los SIS más relevantes del irradiador de Co-60, además, se tiene en cuenta las siguientes consideraciones:

1. El objetivo general del APS que se desarrolló es el de evitar la sobrexposición o una exposición potencial del POE.
2. El alcance del APS que se desarrolló es sobre los SIS del Irradiador de Co-60, pero dentro de este proyecto solo se considera a detalle: el sistema de enclavamiento de la puerta del búnker y el sistema de control de nivel del blindaje húmedo.

Se consideraron las perspectivas de las regulaciones internacionales para determinar los objetivos de seguridad para la exposición potencial del POE como se indica en la Tabla 2.1.

Tabla 2.1. Rango de probabilidades de ocurrencias de eventos en un año

Categorización de eventos	**Probabilidad de ocurrencia del evento en el año**
Secuencia de eventos que conducen a dosis tratadas como parte de la exposición normal	10^{-1} a 10^{-2}
Secuencia de eventos que conducen a efectos estocásticos solamente, pero sobre los límites de dosis	10^{-2} a 10^{-5}
Secuencia de eventos que conducen a dosis donde algunos efectos de la radiación son determinísticos	10^{-5} a 10^{-6}
Secuencia de eventos que conducen a dosis donde la muerte es el resultado más probable.	$< 10^{-6}$

(ICRP, 1993)

Estas probabilidades de ocurrencia establecidos por el ICRP en el año 1993 son los objetivos de seguridad que se consideraron en el APS, sin embargo, para determinar la correspondencia de estos límites de ocurrencia, es necesario relacionarlos con las dosis efectivas recibidas por el POE, para lo cual se consideró la siguiente referencia mostrada en la Tabla 2.2.

Tabla 2.2. Límites de exposición potencial de un individuo

Dosis efectiva máxima (mSv)	Probabilidad de ocurrencia del evento en el año
< 50	10^{-1} a 10^{-2}
1 - 500	10^{-2} a 10^{-5}
200 – 5 000	10^{-5} a 10^{-6}
> 2 000	$< 10^{-6}$

(IAEA, 2002)

Las referencias de las Tabla 2.1 y Tabla 2.2 permitieron establecer una región como indica en la Figura 2.3 con la que se pudo definir si los sistemas diseñados cumplen o no con el objetivo de seguridad estipulado por las normativas internacionales.

Figura 2.3. Límites para exposiciones potenciales
(ICRP, 1993)

En la Tabla 2.3, se detallan las metodologías que se desarrollaron en el presente proyecto para el APS. La justificación de las tareas que no se consideran en la Tabla 2.3 se detallan a continuación:

La tarea 7 no aplica, debido a que, los recursos y horarios definidos para la ejecución del APS son propios de la instalación sin recurrir a recursos y horarios adicionales.

Tabla 2.3. Descripción de las metodologías utilizadas en las tareas del Paso A del APS

A: ADMINISTRACIÓN DE LA ORGANIZACIÓN		
Tarea APS	**Descripción**	**Metodología usada**
Tarea 1	Objetivo	Reunión con el grupo de trabajo definido
Tarea 2	Alcance	Reunión con el grupo de trabajo definido
Tarea 3	Administración del proyecto	Sin metodología especifica
Tarea 4	Método y procedimiento	
Tarea 5	Equipo de trabajo	Definición del grupo de trabajo por medio de consulta directa con el OSR y el coordinador de la instalación
Tarea 6	Entrenamiento	Capacitaciones requeridas
Tarea 7	Recursos y horarios	No aplica
Tarea 8	Aseguramiento de la calidad	No aplica

Para la tarea 8, es necesario indicar que el CIR posee un sistema de gestión integrado que permite asegurar la calidad de las actividades realizadas en la instalación. Sin embargo, desde el punto de vista del APS, esta tarea no aplica en la priorización de las actividades del presente proyecto, debido a que, esté es un tema de detalle respaldada con documentación, si bien es importante esta tarea, se la dejará para una implementación futura en el CIR.

En la Tabla 2.4 se indican los criterios para la selección de la metodología usada en el presente proyecto

Tabla 2.4. Criterios de metodologías requeridas por el APS e identificación general de metodología usada en el presente proyecto

		Profundidad del análisis			
		Simple	**Intermedio**	**Detallado**	**Metodología usada**
Tareas APS		**Cualitativo a semicuantitativo**	**Semi - cuantitativo**	**Cuantitativo**	
Tarea 9	Familiarización	simple, menor esfuerzo	← →	detallada y diversa	Documentación y reuniones en grupo
Tarea 10, 11	Identificación de peligros, Selección de eventos Iniciantes	Sistemática simple o evaluación de ingeniería	← →	Sistemática detallada (FMEA, HAZOP)	FMEA
Tarea 12	Estados finales no deseados		← →	Desarrollo detallado	Documentación y reuniones en grupo
Tarea 13	Identificación de medidas de seguridad	Documentación simple, menor esfuerzo	← →	Desarrollo detallado	Documentación y reuniones en grupo
Tarea 14	Información de medidas de seguridad		← →	Desarrollo detallado	Documentación y reuniones en grupo
Tarea 15	Agrupación de eventos iniciantes	Incluido en la tarea 10 a 12 (simple agrupamiento)	← →	Desarrollo detallado	Documentación y reuniones en grupo
Tarea 16	Modelamiento de la secuencia de eventos	Modelamiento simple o evaluación de ingeniería	← →	Modelamientos complejos (FTA, ETA)	Análisis de árbol de eventos (ETA), Análisis de árbol de fallos (FTA)
Tarea 17	Análisis del rendimiento Humano	Simple (juzgamiento)	← →	Análisis detallado (HRA, TA, etc.)	No se cuenta con un análisis específico.
Tarea 18	Análisis de consecuencias	Análisis simple	← →	Análisis detallado	Documentación detallada
Tarea 19 a 24	Estimación de parámetros	Pocos parámetros, casos delimitadores, frecuencias cualitativas	← →	Muchos parámetros, mejores estimaciones	Documentación detallada Estimación de tasa de dosis por medio de cálculos basados en IAEA-TECDOC-1162
Tarea 25, 26	Cuantificación de la secuencia	Simple (dosis y frecuencia cualitativa)	← →	Complejo (análisis de incertidumbres, sensibilidad de análisis, distribuciones)	Documentación detallada.
Tarea 27	Documentación	Básica	← →	Documentación detallada	Documentación general

(IAEA, 2002)

2.1.1 METODOLOGÍA FMEA

La metodología FMEA utilizada en el desarrollo del APS (tarea 10 y 11) tiene algunas características que permite aprovechar de mejor manera los resultados de la misma, si bien el análisis FMEA realizado no es a detalle, este permitió definir los sistemas de seguridad y sus elementos vinculantes para determinar las funciones de seguridad de los sistemas implementados actualmente y así se pudo realizar una evaluación más específica, centrándonos en los sistemas de seguridad propuestos en el objetivo específico de este proyecto, que son: el sistema de enclavamiento de la puerta del búnker y el sistema de control de nivel de agua. Esta metodología también permite tener criterios de priorización de los análisis requeridos. Sin embargo, debido a la metodología integrante que se propone en el APS, fuera del presente proyecto se realizaron mayores análisis, que se extendieron a todos los sistemas de seguridad involucrados con los eventos iniciantes que puedan terminar en una exposición potencial del POE

2.1.2 METODOLOGÍA FTA

La metodología FTA utilizada en el desarrollo de este proyecto se detalló en la sección 1.2.1.5, pero el análisis que se realizó en este proyecto fue cuantitativo, para lo cual se utilizó referencias bibliográficas, debido a que los procedimientos actuales de operación y mantenimiento del Irradiador de Co-60 no proporcionan la información necesaria para poder desarrollar los análisis con datos reales como es el tiempo medio entre fallas (MTBF) o la tasa de fallo al año de los componentes básicos de los SIS, las referencias bibliográficas utilizadas, son para recabar datos de confiabilidad con el objetivo de poder efectuar dichos análisis con mayor criterio, las fuentes consultadas fueron las siguientes:

- IAEA-TECDOC-930 Generic Component reliability data for research reactor PSA (IAEA, 1997).
- MIL-HDBK-217F: Military Handbook, Reliability Prediction of Electronic Equipment (Department of Defense, 1991).
- Guidelines for Hazard Evaluation Proocedures (AIChE, 2008).

- Reliability and lifetime of LEDs (Lutz & Ritzer, 2020).
- Structural reliability Analysis and Prediction (Melchers & Beck, 2018).
- Lee's Loss Prevention in the Process Industries (Mannan, Lee's Loss Prevention in the Process Industries, 2005a).
- Reliability of uninterruptible power supplies (ABB, 2018).
- Fichas técnicas de fabricantes.

Para calcular la probabilidad de fallo de los sistemas de seguridad determinados en los FTA, se utilizó la teoria de confibilidad de componentes de la sección 1.3, para lo cual se utilizó la Ecuación [2.1]

$$PF(T) = 1 - R(T) = 1 - \ e^{-\lambda T} \qquad [2.1]$$

Donde:
PF: Probabilida de fallo al año
R: Confiabilidad del sistema al año
λ: Tasa de fallo por hora
T: horas laborales al año

La metodología usada para determinar la probabilidad de fallo a partir del diagrama FTA es la indicada en la Figura 2.4.

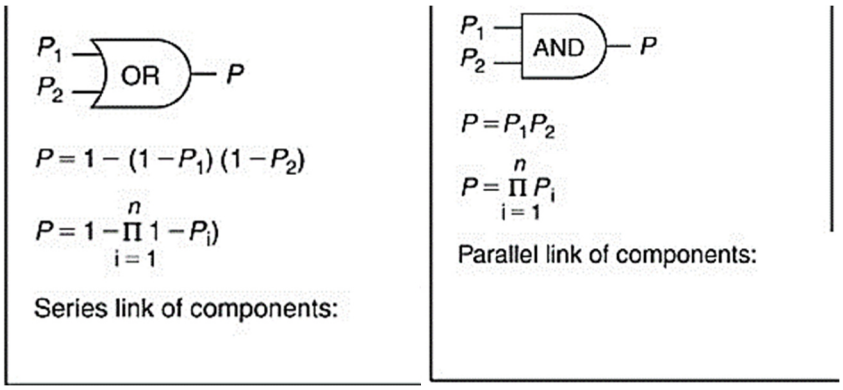


Figura 2.4. Metodología para el cálculo de probabilidad de fallo en un diagrama FTA (Crowl & Louvar, 2011)

La probabilidad de fallo de un sistema que tiene una lógica con operador AND viene dada por la Ecuación [2.2]:

$$P = \prod_{i=1}^{n} P_i$$

[2.2]

Donde:

P: Probabilidad de fallo del sistema

P_i: Probabilidad de los componentes básicos (desde *i* hasta el *n*)

La probabilida de fallo de un sistema que tiene una lógica con operador OR viene dado por la Ecuación [2.3]

$$P = \prod_{i=1}^{n} (1 - P_i)$$

[2.3]

Donde:

P: Probabilidad de fallo del sistema

P_i: Probabilidad de los componentes básicos (desde *i* hasta el *n*)

El factor de reducción de riesgo se define con la Ecuación [2.4]

$$RRF = \frac{Frecuencia\ de\ accidentes\ anuales\ (probabilidad\ de\ ocurrencia\ anual)}{Frecuencia\ de\ accidentes\ tolerables\ (objetivos\ de\ seguridad)}$$

[2.4]

Donde:

RRF: Factor de reducción de riesgo

2.1.3 METODOLOGÍA ETA

La metodología ETA utilizada en el desarrollo del proyecto se detalló en el subcapítulo 1.2.1.4, y al igual que la metodología anterior, existen ciertos factores que no se han analizado en este proyecto debido a la falta de información, por lo que, se recurrio a referencias bibliograficas para determinar ciertos datos, como por ejemplo, las probabilidades de fallo de estructuras civiles o probabilidades de fallo del factor huano. Con estas consideraciones, la manera para determinar la

frecuencia de ocurrencia de un evento no deseado basado en los diagramas ETA fue por medio de un operador AND, por tal motivo, se utilizó la Ecuación [2.2] para relacionar todas las probabilidades involucradas en el diagrama ETA.

2.1.4 ESTIMACIÓN DE DOSIS EFECTIVAS RECIBIDAS POR EL POE

Para el cálculo de la estimación de las dosis efectivas se utilizó la metodología basada en la referencia IAEA-TECDOC-1162, en el que se encuentran procedimientos genéricos para la evaluación y respuesta durante una emergencia radiológica (IAEA, 2000). La Ecuación [2.5] del procedimiento E1 de este documento técnico, se detalla el cálculo requerido para la estimación de dosis efectiva y tasa de dosis que considera una fuente puntual de radiación.

$$E_{ext} = \frac{A \times CF_6 \times T_e \times (0{,}5)^{\frac{d}{d_{1/2}}}}{X^2} \qquad [2.5]$$

Donde:

E_{ext}: Dosis efectiva desde una fuente puntual [mSv]

A: Actividad de la fuente

- En [kBq] si se utiliza el factor CF_6 en [mSv/h]/[kBq]
- En [Ci] si se utiliza el factor CF_6 en [mSv/h]/[Ci]

T_e: Duración de la exposición [h]

CF_6: Factor de conversión para el Co-60

- 2,5E-07 [mSv/h]/[kBq]
- 9,5E+00 [mSv/h]/[Ci])

X: Distancia desde la fuente puntual [m]

$d_{1/2}$: Valor medio de la capa para el Co-60 [cm]

- Agua: 10,99
- Concreto: 5,2
- Aire: 9,42E+3

d: Espesor del blindaje [cm]

Nota: Si se desea realizar el cálculo sin blindaje, se debe establecer el espesor del blindaje d = 0

Por medio de la metodología APS, se realizó una evaluación rápida de los SIS actuales, y se consideró la información proporcionada por el Centro de Irradiación y el personal del Irradiador de Co-60 y la información investigada en la bibliografía mencionada, con el objetivo de tener una línea base para la justificación de la actualización de los SIS, con miras a la repotenciación y recarga de la fuente de Co-60 a 50 000 Ci que está proyectado a futuro en las instalaciones del irradiador.

2.2 FASE 2: ASIGNACIÓN DE LAS CAPAS DE SEGURIDAD DEL SISTEMA

Una vez definidas las funciones de seguridad por medio de la metodología FMEA en la Fase 1 (capítulo 2.1), se realizó la asignación de las capas de seguridad en las que se definieron capas de prevención y capas de mitigación. Sin embargo, en el presente proyecto solo se mencionan las capas en las que intervienen los SIS de la puerta del búnker y del control de nivel del blindaje húmedo. Además, en esta fase se definió el nivel SIL que requiere la instalación, esto se realizó inicialmente por medio de una aproximación gráfica indicada en la sección 1.4.2, la misma que se muestra en la Figura 2.5.

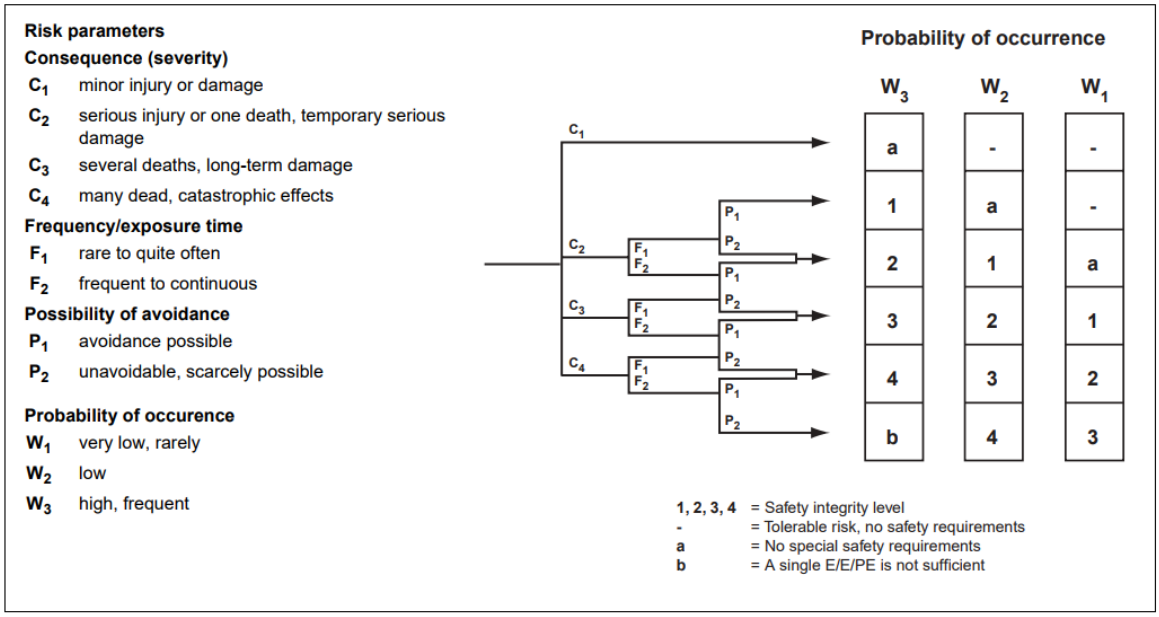


Figura 2.5. Metodología de determinación del índice SIL por una aproximación gráfica (Ingrey & Lerévérend, 2005)

Luego, se realizó la determinación del PDF de los SIS en base a la metodología LOPA explicada en la sección 1.4.4, y también se utilizó la metodología FTA y ETA, con el objetivo de determinar si los diseños evaluados cumplen con los objetivos de seguridad establecidos en la Fase 1 (capítulo 2.1. Análisis de peligros y riesgos).

2.3 FASE 3: DESARROLLO DE LAS ESPECIFICACIONES DE LOS REQUERIMIENTOS DE SEGURIDAD (SRS)

En esta fase, se desarrollaron las especificaciones de los requerimientos de seguridad que tendrán los SIS y basado en el enfoque de seguridad funcional, en esta etapa se definieron las especificaciones a partir de los siguientes criterios:

- El tipo de proceso o aplicación del irradiador de Co-60.
- El peligro relacionado a la exposición potencial del POE y del público en general.
- Las instalaciones que se encuentran en los alrededores del irradiador de Co-60.
- Las condiciones ambientales que pueden afectar el funcionamiento de los SIS.
- La guía de seguridad especifica No SSG – 08 del IAEA y normativas proporcionadas por el reglamento de seguridad radiológica del Ecuador.
- Los tipos de suministros de energía que son necesarios para los SIS.

Además de estos criterios, y basado en algunos criterios del enfoque de seguridad funcional, para los SIS en esta etapa se especificó lo siguiente (Gruhn & Cheddie, 2006):

- La lógica de funcionamiento de cada uno de los SIS.
- La arquitectura requerida por los SIS.
- El grado SIL requerido por la función de seguridad del SIS.
- Los requerimientos de intervalos de pruebas de los SIS.
- Los modos de fallos y respuestas deseadas de los SIS.
- Interfaces entre los SIS y las unidades lógicas de control.

2.4 FASE 4: DISEÑO E INGENIERÍA DE LOS SIS

Para esta fase es necesario recordar que las instalaciones del Centro de Irradiación pertenecen a un área específica como es el área de aplicaciones con radiaciones ionizantes, por lo que en esta etapa se desarrollaron los diseños de ingeniería y se consideró la información y directrices proporcionadas por la coordinación del CIR y por el IAEA en la Guía de Seguridad especifica No. SSG-8 en la que se refiere a la Seguridad Radiológica de las instalaciones de irradiación de rayos gamma, electrones y rayos X (IAEA, 2010b)

2.5 FASE 6: OPERACIÓN Y MANTENIMIENTO

Para esta fase del enfoque de seguridad funcional se tuvieron en cuenta ciertas recomendaciones de la normativa IEC61511 como son (Gruhn & Cheddie, 2006):

- Actividades de operaciones rutinarias y anormales.
- Pruebas de verificación y actividades de mantenimiento y reparación.
- Procedimientos, mediciones y técnicas a usarse.
- Registro de procedimientos adyacentes.
- Registro de todas las fallas de los sistemas de seguridad.
- Competencia del personal.
- Entrenamiento del personal.

Las siguientes fases (fase 5 y de la 7 a la 11) del ciclo de vida del diseño de los SIS no se analizaron en esta propuesta, ya que, el presente proyecto solo tiene por objetivo general, determinar una propuesta general para los SIS requeridos en las funciones del enclavamiento de la puerta de ingreso al búnker y el sistema de control de nivel de agua, así como la propuesta de la operación y mantenimiento de los sistemas mencionados.

3 RESULTADOS Y DISCUSIÓN

3.1 DESCRIPCIÓN DEL IRRADIADOR DE Co-60

El irradiador de Co-60 se encuentra ubicado en el Centro de Irradiación (edificio 7) de la Escuela Politécnica Nacional. El Centro de Irradiación que se muestra en la Figura 3.1, dispone de una fuente de Co-60 categoría IV, esta tuvo una actividad de 20 000 Ci en el año 1980, en 1991 se realizó una recarga hasta los 40 700 Ci (Villacis, 2019). Esta fuente está compuesta por 12 lápices radiactivos, sin embargo, por el paso del tiempo esta fuente de Co-60 ha decaído y basado en la información proporcionada por el personal del Irradiador de Co-60, la actividad a la fecha del 1 de enero del 2020 es la indicada en la Tabla 3.1.

(a) (b)

Figura 3.1. Edificio del Centro de Irradiación: a) Vista aérea del edificio del CIR, b) Entrada posterior al edificio del CIR
(Villacis, 2019)

El irradiador de Co-60 es de categoría IV (Irradiadores panorámicos de almacenamiento en medio húmedo de la fuente) lo que quiere decir que es un irradiador de acceso humano controlado en el que la fuente se almacena y se blinda totalmente en una piscina llena de agua cuando no se utiliza, la fuente es expuesta en dentro de una sala de irradiación que se mantiene inaccesible durante su operación, principalmente por un sistema de entrada controlada (IAEA, 2010b), el irradiador de Co-60 se indica en la Figura 3.2.

Tabla 3.1. Detalle de la actividad actual de la fuente de Co-60

No. Lápiz	No. Fuente	Actividad (Ci) (01-12-1990)	Actividad Actual (Ci) (01-01-2020)
1	552	3 344	73,0
2	553	3 240	70,7
3	554	3 395	74,1
4	555	3 529	77,0
5	556	3 261	71,2
6	557	3 230	70,5
7	558	3 582	78,2
8	559	3 312	72,3
9	560	3 261	71,2
10	561	3 529	77,0
11	562	3 498	76,3
12	563	3 519	76,8
ACTIVIDAD TOTAL (Ci)		40.700	888,0

Centro de Irradiación, 2020

(a) (b)

Figura 3.2. Irradiador de Co-60 del Centro de irradiación: a) Blindaje húmedo (piscina), b) blindaje seco (búnker)

Las características principales del Irradiador de Co-60 son (Villacis, 2019):

- Capacidad de la fuente: 150 000 Ci
- Actividad actual aproximada: 888 Ci.
- Geometría de la fuente: cilíndrica de 17 cm de diámetro alrededor de la cual están distribuidos los 12 lápices.

- Flujo de ventilación: 500 m^3/h.
- Concentración mínima de ozono: <0,025 ppm.
- Geometría de la cámara de irradiación (búnker): Cúbica
    - Área interna de la cámara de irradiación: 16 m^2 (4 m x 4 m).
    - Volumen interno de la cámara de irradiación: 41 m^3 (4 m x 4m x 2,60 m).
    - Paredes de la cámara de irradiación: Paredes de 1,5 m de espesor construidas en hormigón armado con densidad de 2,35 g/cm^3.
    - Techo de la cámara de irradiación: conformado por 9 bloques de hormigón armado, en una configuración traslapada, 4 bloques de 4,58 m x 1,10 m x 0,70 m en la capa inferior y 5 bloques de 5,14 m x 1,00 m x 0,70 m en la capa superior.
- Piscina: se encuentra construida con paredes de hormigón armado de 0,40 m de espesor y tiene las siguientes dimensiones:
    - Largo: 6,50 m.
    - Ancho: 2,50 m.
    - Profundidad: 4,50 m.

  Esta piscina se encuentra aislada por medio de pasamanos metálicos colocados en los 3 costados libres de la piscina

El ingreso a la cámara de irradiación es por medio de una puerta construida de hormigón y plomo, forrada con planchas de acero de un peso aproximado de 10 t, la misma que está accionada por un sistema electromecánico y por un motor de 3 HP, esta se abre a una velocidad de 2,6 m/min.

El irradiador de Co-60 se encuentra en estado de para, por lo que, su operación se limita a las actividades de comprobación de los sistemas de instrumentación de la instalación y estas son realizadas por el POE del CIR. Por todo lo anteriormente mencionado, se puede decir que, la operación anual del irradiador es igual a las horas laborales del POE que son 40 horas semanales o 2 000 horas anuales (el número de horas laborales se estableció en la sección 1.3.).

3.2 DEFINICIÓN DE LOS SIS DEL IRRADIADOR DE Co-60

En Tabla 3.2 se describen las características iniciales de los SIS que posee el irradiador de Co-60 con relación a la exposición potencial del POE o del público en general. Esto es el resultado de la recopilación de la información realizada por la metodología APS

Tabla 3.2. Descripción de los SIS del Irradiador de Co-60 relacionados a la exposición potencial del POE (condición inicial)

CÓDIGO	SIS	Función	Efecto potencial de la falla
SS1	Sistema de detección de radiación interior	Detectar niveles de radiación en el interior del búnker	Exposición potencial del POE
SS2	Sistema de enclavamiento de acceso al búnker	Prohibir la apertura de la puerta del búnker mientras la fuente de Co-60 se encuentra expuesta	Exposición potencial del POE
SS3	Sistema de detección de radiación exterior	Detectar niveles de radiación sobre los niveles permitidos en el área restringida (sobre la piscina)	Exposición potencial del POE y público en general
SS4	Sistema de control de nivel de blindaje húmedo	Mantener el nivel del blindaje húmedo lo suficientemente alto para contener los niveles de radiación debajo de los límites permitidos	Exposición potencial del POE y público en general
SS5	Punto de ronda	Verificar la salida de todo personal del búnker antes de un proceso de irradiación	Exposición potencial del POE
SS6	Sistema de enclavamientos de la de subida de la fuente de Co-60	Evitar que el rack de la fuente de Co-60 pueda salir de su trayectoria normal de trabajo	Exposición potencial del POE

3.2.1 Sistema de detección de radiación interior – SS1 (condición inicial)

El sistema de detección de radiación interior cumple con la función de medir el nivel de radiación dentro del búnker por medio de un sensor especial (cámara de ionización). La señal del sensor de radiación es acondicionada por un equipo electrónico/electromecánico llamado preamplificador de señal, este componente se conecta por medio de cableados de señal al cofre de detección de niveles de radiación y por medio de un relé electromecánico hacia el cofre de alarmas. En este cofre se tienen elementos electrónicos que permiten determinar los umbrales de activación de las señales de alarma, este sistema se lo definió con el siguiente diagrama de bloques que se muestra en la Figura 3.3 y la descripción de los componentes de este sistema se detallan en la Tabla 3.3.

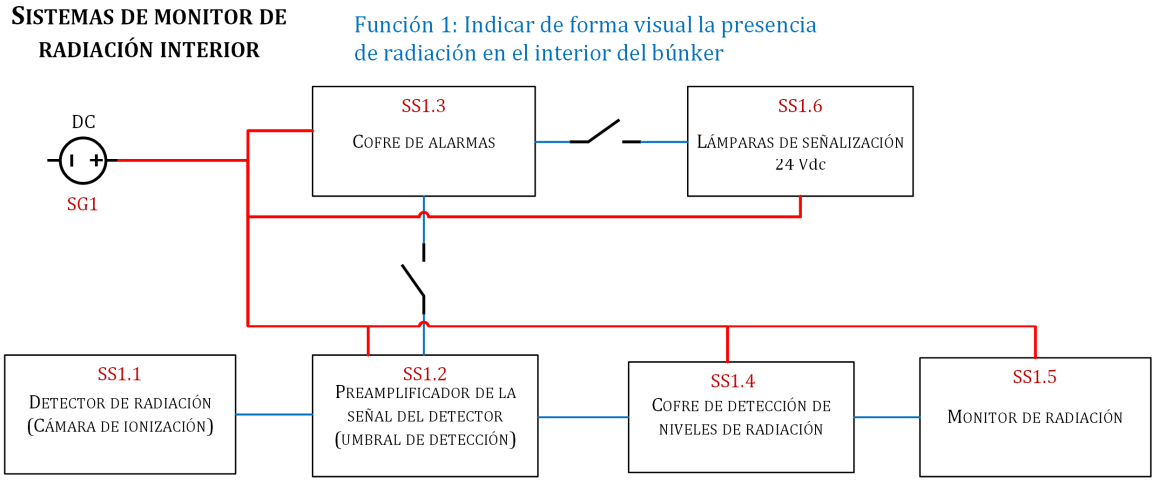


Figura 3.3. Diagrama de bloques del sistema de monitor de radiación interior (condición inicial)

Tabla 3.3. Descripción del Sistema de detección de radiación interior (condición inicial)

Código	Descripción del componente	Función	Modo de falla potencial
SS1.1	Detector de radiación (cámara de ionización)	Detectar las radiaciones ionizantes	Falla por funcionamiento
SS1.2	Preamplificador de la señal del detector	Acondicionar la señal proveniente del detector	Falla por funcionamiento
SS1.3	Cofre de alarmas	Acondicionar las señales umbrales para la activación de alarmas	Falla de contactos
SS1.4	Cofre de detección de niveles de radiación	Acondicionar las señales para la visualización en el monitor de radiación	Falla de contactos
SS1.5	Monitor de radiación	Visualizar los niveles de radiación	Falla de funcionamiento
SS1.6	Lámparas de señalización	Visualizar estados de alarma	Falla de funcionamiento
SG1	Fuente de alimentación de 24Vdc	Proporcionar el suministro de energía al sistema	Falla de funcionamiento

3.2.2 Sistema de enclavamiento de acceso al búnker – SS2 (condición inicial)

El sistema de enclavamiento de acceso al búnker recibe la señal común desde el detector de radiación y el preamplificador de señal, pero, en el cofre de alarmas se tiene un ramal independiente para controlar el bloqueo electromecánico de la puerta del búnker, este sistema se lo definió con el siguiente diagrama de bloques que se muestra en la Figura 3.4 y la descripción de los componentes de este sistema se detallan en la Tabla 3.4.

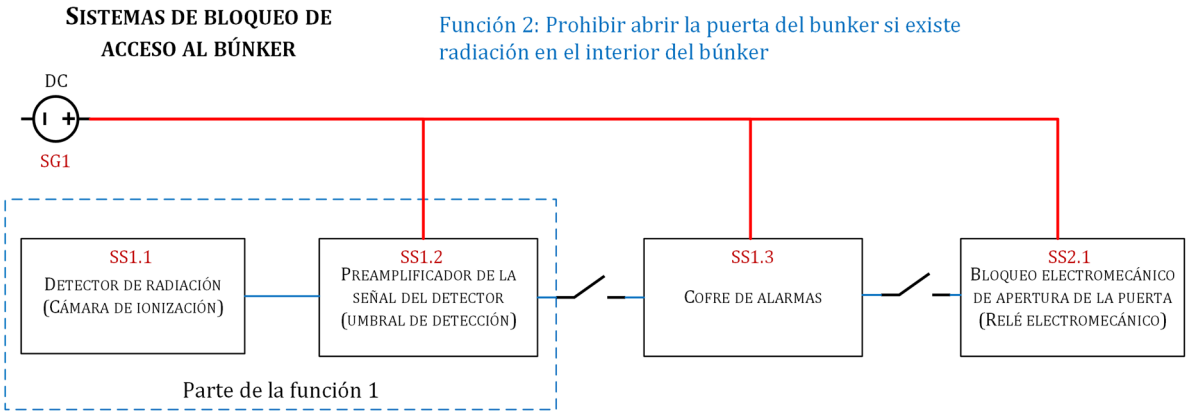


Figura 3.4. Diagrama de bloques del sistema de bloqueo de acceso al búnker (condición inicial)

Tabla 3.4. Descripción del sistema de bloqueo de acceso al búnker (condición inicial)

Código	Descripción del componente	Función	Modo de falla potencial
SS2.1	Cofre de alarmas	Acondicionar las señales umbrales para la activación de alarmas	Falla de contactos
SS2.2	Bloqueo electromecánico de apertura de la puerta (relé electromecánico)	Deshabilitar el control de apertura de la puerta del búnker	Falla de contactos
SG1	Fuente de alimentación de 24Vdc	Proporcionar el suministro de energía al sistema	Falla de funcionamiento

3.2.3 Sistema de detección de radiación exterior – SS3 (condición inicial)

El sistema de detección de radiación exterior consta de un detector de radiación de área que dispone de un UPS para el suministro de alimentación. El sistema se lo definió con el siguiente diagrama de bloques que se muestra en la Figura 3.5 y la descripción de los componentes de este sistema se detallan en la Tabla 3.5.

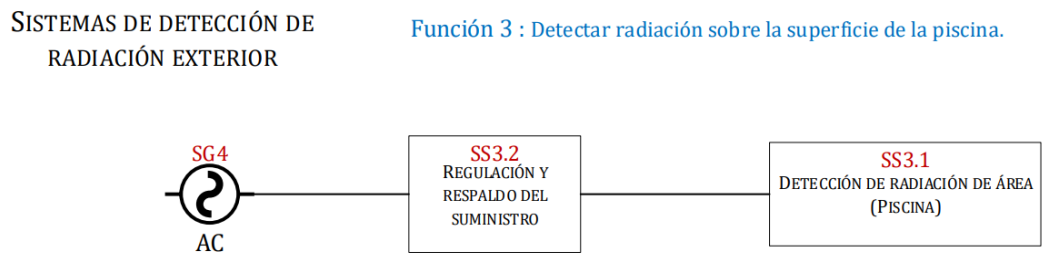


Figura 3.5. Diagrama de bloques del sistema de detección de radiación exterior (condición inicial)

Tabla 3.5. Descripción del sistema de detección de radiación exterior (condición inicial)

Código	Descripción del componente	Función	Modo de falla potencial
SS3.1	Detector de radiación de área	Detectar las radiaciones ionizantes	Falla de funcionamiento
SS3.2	UPS 110 Vac	Suministrar alimentación ininterrumpida al detector	Falla de funcionamiento
SG4	Fuente de alimentación de 110 Vac	Suministrar alimentación al sistema (110 Vac)	Falla de funcionamiento

3.2.4 Sistema de control de nivel de blindaje húmedo – SS4 (condición inicial)

El sistema de control de nivel de blindaje húmedo posee dos líneas de reposición de agua, la primera utiliza un sensor de nivel de mercurio que detecta si el nivel de agua ha bajado aproximadamente 3 cm (reposición por evaporación) y activa una electroválvula que suministra el agua a partir de una cisterna de reserva. La segunda, es un sistema mecánico, que por medio de una válvula manual con flotador permite el ingreso de agua desde el suministro principal agua. Hay que recalcar que dentro de este análisis no se realizó el análisis de la válvula manual directa, ya que este es parte de un sistema de emergencia. Este sistema se definió con el siguiente diagrama en bloques que se muestra en la Figura 3.6 y la descripción de los componentes de este sistema se detallan en la Tabla 3.6.

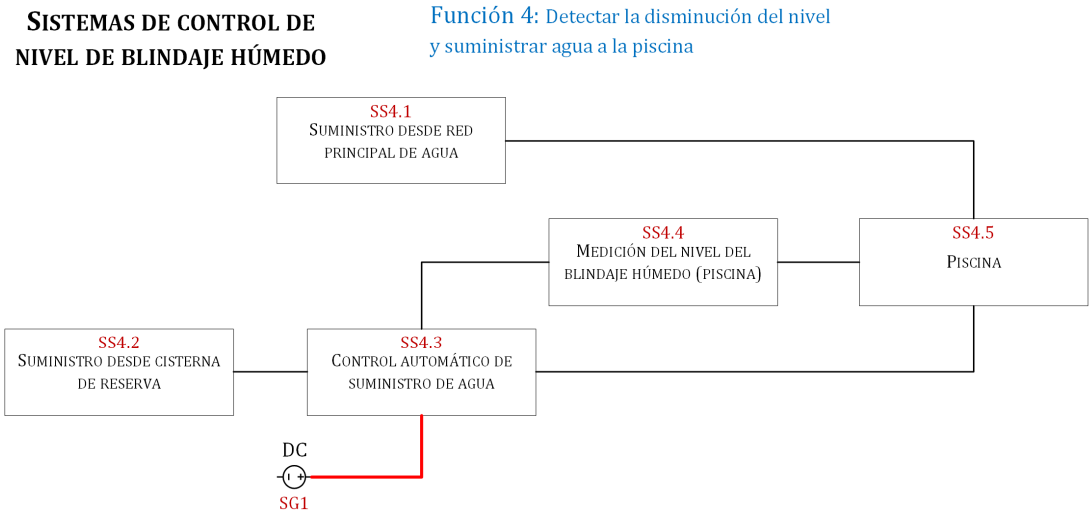


Figura 3.6. Diagrama en bloques del sistema de control de nivel de blindaje húmedo (condición inicial)

Tabla 3.6. Descripción del sistema de control de nivel de blindaje húmedo (condición inicial)

Código	Descripción del componente	Función	Modo de falla potencial
SS4.1	Suministro desde la red principal de agua	Suministrar agua a la piscina si el nivel ha disminuido más de 80 cm desde la red principal de agua	Falla de funcionamiento
SS4.2	Suministro desde la cisterna de reserva	Suministrar agua a la piscina desde la cisterna de reserva	Falla de funcionamiento
SS4.3	Control automático de suministro de agua	Controlar el suministro de agua a la piscina por medio de la electroválvula	Falla de funcionamiento
SS4.4	Medición del nivel del blindaje húmedo (piscina)	Detectar la disminución del nivel de agua (máximo 3 cm)	Falla de funcionamiento
SS4.5	Piscina	Almacenar el blindaje húmedo	Falla por deterioro
SG1	Fuente de alimentación de 24Vdc	Suministrar alimentación a la electroválvula	Falla de funcionamiento

3.2.5 Sistema de enclavamientos de la subida del rack de la fuente de Co-60 – SS6 (condición inicial)

El sistema de enclavamientos de subida/bajada del rack de la fuente de Co-60 cuenta con finales de carrera que envían señales al control electromecánico del motor de izaje y al control del freno electromagnético del motor que cumplen con la función de evitar que el rack de la fuente de Co-60 pueda descarrilarse, lo que provoca que el rack se trabe mecánicamente fuera de la posición de blindaje. Este sistema se definió con el siguiente diagrama de bloques que se muestra en la Figura 3.7 y la descripción de los componentes de este sistema se detallan en la Tabla 3.7.

SISTEMAS ENCLAVAMIENTOS DEL SISTEMA DE SUBIDA FUENTE

Función 6: Evitar que la fuente de Co-60 suba mas de lo debido y se trabe mecánicamente

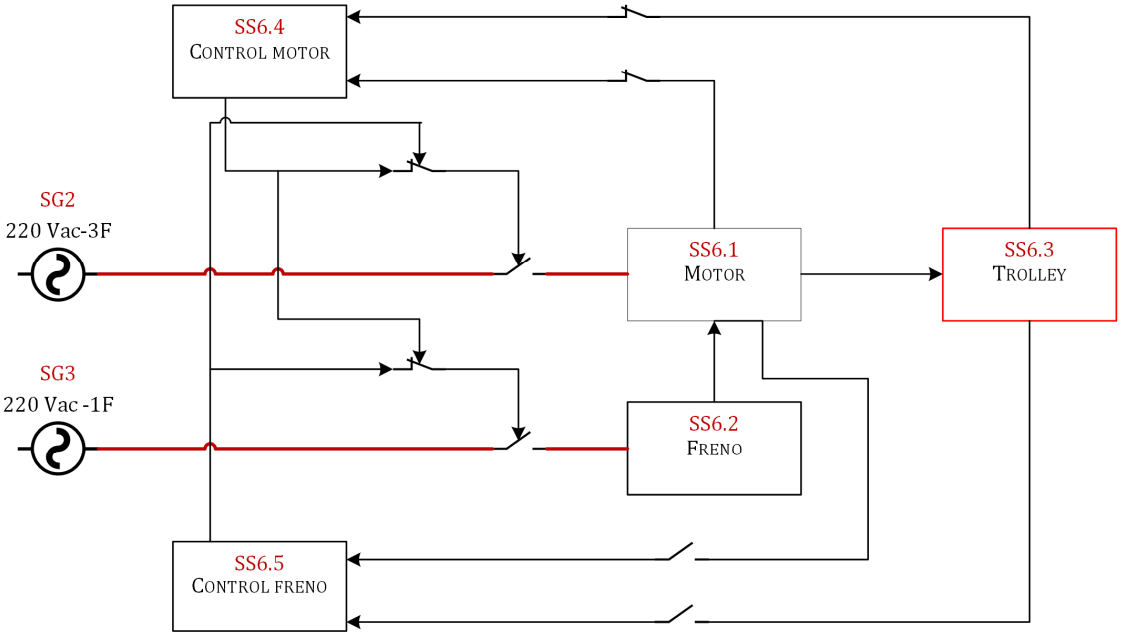


Figura 3.7. Diagrama de bloques del sistema de enclavamientos de subida de la fuente de Co-60 (condición inicial)

Tabla 3.7. Descripción del sistema de enclavamientos de la subida del rack de la fuente de Co-60 (condición inicial)

Código	Descripción del componente	Función	Modo de falla potencial
SS6.1	Motor	Proporcionar el movimiento de subida del rack	Falla de funcionamiento
SS6.2	Freno (electromagnético)	Detener inmediatamente el movimiento del rack	Falla de funcionamiento
SS6.3	Trolley (sistema mecánico)	Enrollar el cable de acero del rack	Falla de funcionamiento
SS6.4	Control electromecánico del motor	Controlar la activación del motor	Falla de contactos
SS6.5	Control electromecánico del freno	Controlar la activación del freno	Falla de contactos
SG2	Fuente de alimentación de 220 Vac – 3F	Suministrar alimentación de energía al motor	Falla de funcionamiento
SG3	Fuente de alimentación de 220 Vac – 1F	Suministrar alimentación de energía al freno electromagnético	Falla de funcionamiento

3.3 DESARROLLO DEL APS NIVEL 1 DEL SISTEMA (EVALUACIÓN INICIAL)

El personal del CIR proporciono la información relacionada al irradiador de Co-60 y a través de reuniones se desarrolló el APS nivel 1 inicial del sistema considerando las recomendaciones del IAEA-TECDOC-1267. La lista completa de la información recopilada para el APS se detalla en el ANEXO IX.

Para el desarrollo de los eventos iniciantes, se consideró la información concerniente a los criterios proporcionados por la Guía de seguridad específica No. SSG-8, que en su párrafo 4.1 indica las cuestiones que se deberían examinar en una evaluación de seguridad (IAEA, 2010b):

- Pérdida de control de acceso.
- Pérdida del control del sistema establecido para el desplazamiento de fuentes radiactivas, incluido un bastidor de la fuente que se quede atascado en la posición no blindada.
- Pérdida de la integridad de sistemas o componentes, comprendidas la integridad del blindaje, la encapsulación de fuentes selladas y la integridad de la piscina.

Nota: No se mencionan todos los criterios de evaluación indicados en Guía especifica No. SGG-8, ya que, los demás criterios hacen referencia a cuestiones generales de irradiadores y a sistemas diferentes a los SIS priorizados en este proyecto.

3.3.1 DEFINICIÓN DE EVENTOS INICIANTES Y ESCENARIOS

Los escenarios tratados en el APS dentro de este proyecto son relacionados directamente con los criterios de análisis que hace hincapié en la SSG-8. De tal manera que, se definieron los siguientes eventos iniciantes con base en el estudio “Análisis Probabilístico de seguridad en una planta semiindustrial de irradiación que tiene una fuente de Co-60 de 50 000 Ci” (Villacis, 2019).

- EVI5. El rack de la fuente de Co-60 queda trabada fuera de la posición de reposo (posición no blindada).
- EVI6. Disminución del nivel de blindaje húmedo donde reposa la fuente de Co-60 debido a una falla de la integridad de la piscina.

Sin embargo, durante las reuniones con el equipo de trabajo del irradiador de Co-60, se detallaron de mejor manera los escenarios planteados:

- Escenario EVI5. El rack de la fuente de Co-60 tiene una falla de los enclavamientos del sistema de subida y bajada del rack de la fuente al momento de subir hacia la posición de irradiación (fuente expuesta) lo que provoca que el rack se quede trabado fuera del blindaje húmedo, el operador del irradiador realiza procedimientos anormales para abrir la puerta e intentar destrabar la fuente.
- Escenario EVI6. Durante un evento natural (terremoto de magnitud entre 7 y 7,9 M_L) la estructura de la piscina colapsa, por lo que, el nivel del blindaje húmedo baja rápidamente, esto sucede cuando no hay personal en el área del irradiador de Co-60.

En la Tabla 3.8 se indican de forma general los SIS que interactúan con los eventos iniciantes EVI5 y EVI6 para prevenir la materialización de los eventos no deseados (sobreexposición del POE y del público en general). Para la elaboración de está matriz se consideró la configuración inicial de hardware encontrado en las instalaciones del irradiador de Co-60 y la información recopilada en el APS.

Tabla 3.8. Visualización general de los SIS que interactúan con los eventos iniciantes EVI5 y EVI6 (estado inicial)

		SIS del irradiador de Co-60 (estado inicial)					
Situación no deseada	**Código evento iniciante**	**Sistema de detección de radiación interior – SS1**	**Sistema de enclavamiento de acceso al búnker – SS2**	**Sistema de detección de radiación exterior – SS3**	**Sistema de control de nivel de blindaje húmedo – SS4**	**Punto de ronda – SS5**	**Sistema de enclavamientos de la función de subida/bajada de la fuente de Co-60 - SS6**
Exposición potencial del POE	EVI5	X	X				
	EVI6			X	X		

3.3.2 DIAGRAMAS FTA DE LOS SIS QUE INTERVIENEN CON EL EVENTO INICIANTE EVI5

3.3.2.1 Diagrama FTA del sistema de detección de radiación interior – SS1 (condición inicial)

Los diagramas FTA que se muestran en las Figuras 3.8 y 3.9, describen el análisis inicial de la falla del aviso de forma visual del sistema de detección de radiación interior – SS1 del irradiador de Co-60.

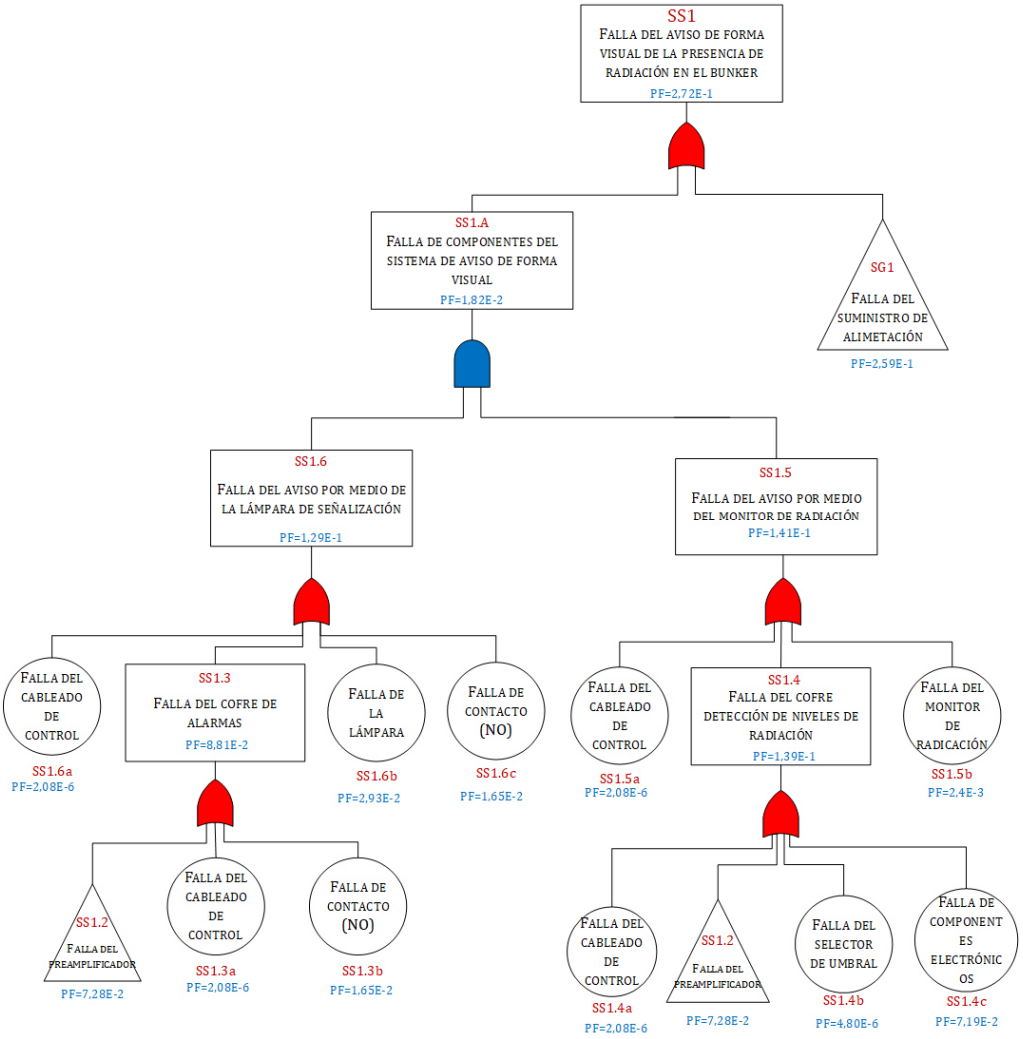


Figura 3.8. Diagrama FTA del sistema de detección de radiación interior – SS1 (condición inicial)

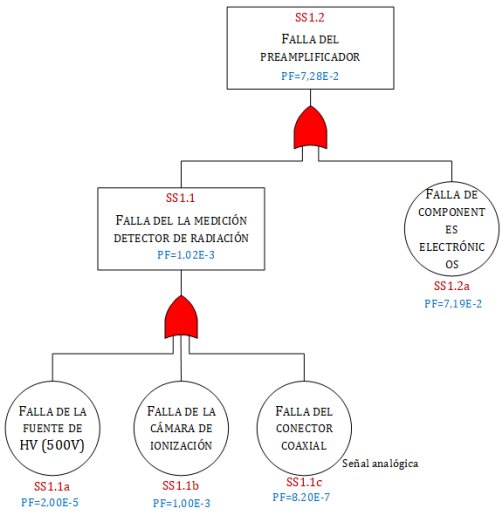


Figura 3.9. Diagrama FTA del sistema de detección de radiación interior – SS1.2 (condición inicial)

En la Figura 3.10. se observa el diagrama FTA que describe el análisis inicial de la falla del sistema general SG1 (suministro de alimentación) del irradiador de Co-60.

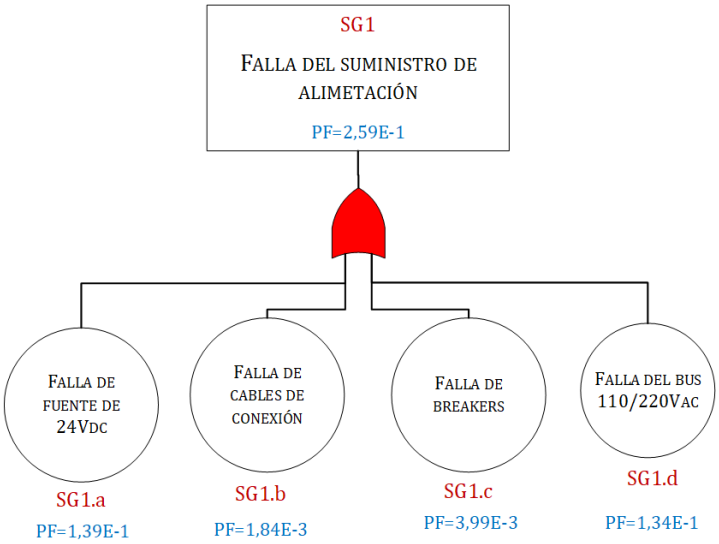


Figura 3.10. Diagrama FTA del suministro de alimentación SG1 (condición inicial)

En el Anexo I se detallan los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos de los diagramas FTA desarrollados en las Figuras 3.8, 3.9 y 3.10. Además, se realizó un análisis comparativo con base a los resultados obtenidos por el cálculo de las probabilidades de falla y la metodología FTA en donde se concluyó que los componentes básicos que más influyen en el falla del SS1 (falla de aviso de forma visual de presencia de radiación en el búnker) son: el SG1.a y el SG1.d, ambos componentes están relacionados con el SG1 (falla del suministro de alimentación), este análisis se ilustran en la Figura 3.11.

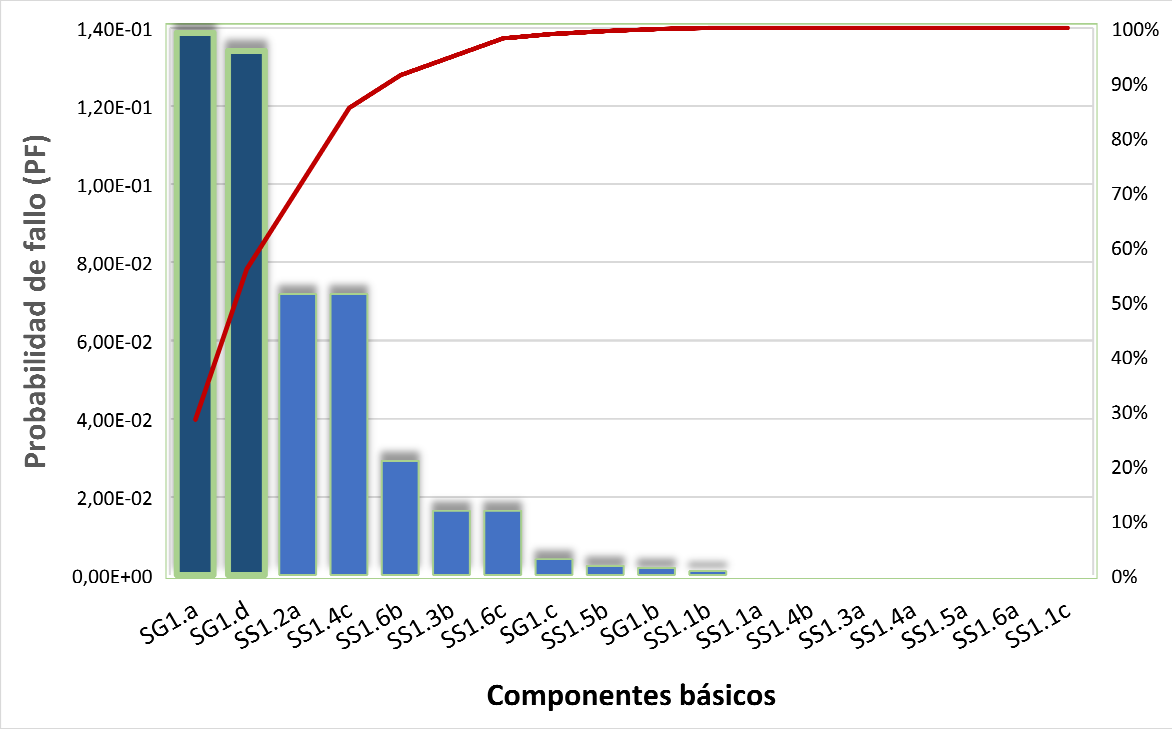


Figura 3.11. Análisis comparativo de las probabilidades de falla de los componentes básicos del SS1 (condición inicial)

3.3.2.2 Diagrama FTA del sistema de enclavamiento del acceso al búnker – SS2 (condición inicial)

El diagrama FTA que se muestra en la Figura 3.12, describe el análisis inicial de la falla del bloqueo electromecánico de apertura del sistema de enclavamiento de acceso al búnker – SS2.

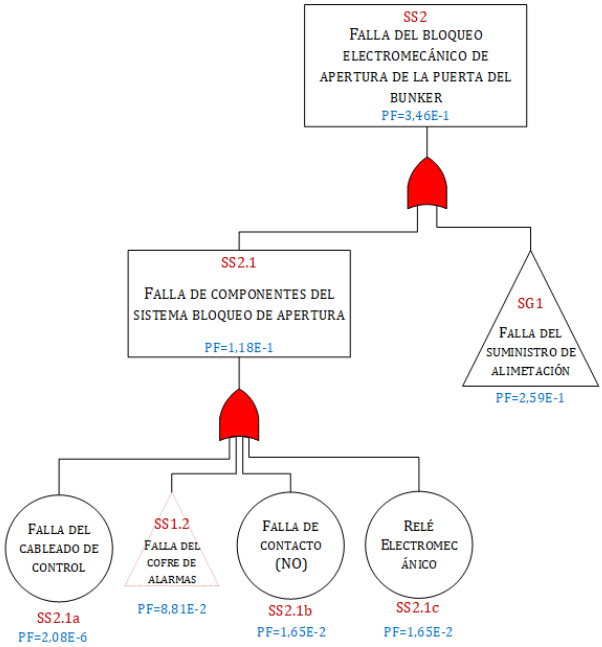


Figura 3.12. Diagrama FTA del sistema de enclavamiento de acceso al búnker – SS2 (condición inicial)

El sistema de enclavamiento de acceso al búnker – SS2 tiene ciertos componentes en común con el sistema de detección de radiación interior – SS1, esto se puede observar en la Figura 3.4. Por tal motivo, Los diagramas FTA de los componentes SG1 y SS1.2 se encuentran detallados en la sección 3.3.2.1. Los resultados de los cálculos para determinar las probabilidades de fallo (PF) de los componentes básicos del diagrama FTA de la Figura 3.12. se detallan en el Anexo I. De igual manera que en el sistema de detección de radiación interior, se realiza un análisis comparativo para identificar los componentes que más influyen en la falla del sistema de enclavamientos de acceso al búnker - SS2. Por medio de esto, se concluyó que los componentes que más influyen en la falla del bloqueo electromecánico de apertura de las puertas del búnker son los relacionados con el SG1 (falla del suministro de alimentación). El análisis comparativo se puede observar en la Figura 3.13

Figura 3.13. Análisis comparativo de las probabilidades de falla de los componentes del SS2 (condición inicial)

3.3.3 DIAGRAMAS FTA DE LOS SIS QUE INTERVIENEN EN EL EVENTO INICIANTE EVI6

3.3.3.1 Diagrama FTA del sistema de detección de radiación exterior – SS3 (condición inicial)

El diagrama FTA que se muestra en la Figura 3.14 describe el análisis de la falla de detección de la radiación en la superficie de la piscina del sistema de detección de radiación exterior – SS3 instalado.

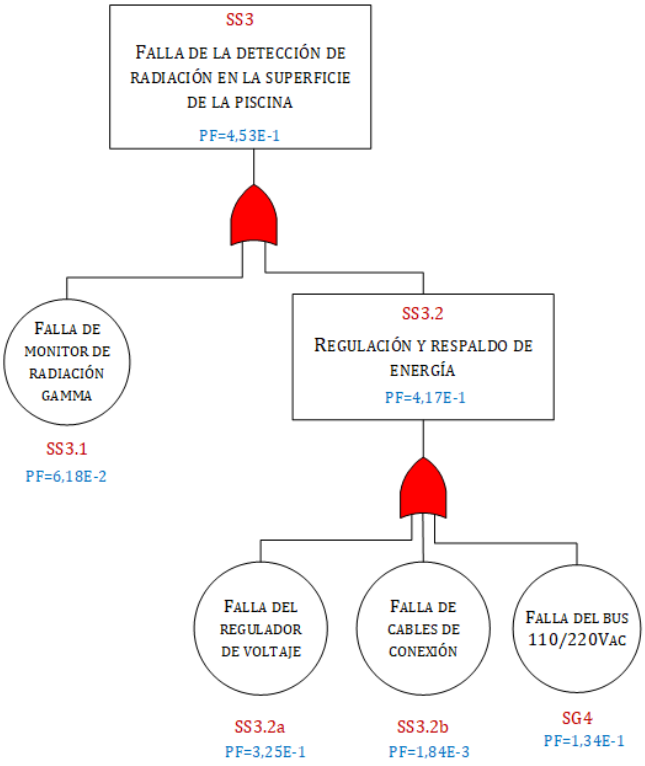


Figura 3.14. Diagrama FTA del sistema de detección de radiación exterior – SS3 (condición inicial)

En el Anexo I se detallan los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos del diagrama FTA del sistema de detección de radiación exterior. Con estos resultados se realizó un análisis comparativo en conjunto con metodología FTA y se determinaron que los componentes básicos que tienen más probabilidad de fallo en el SS3 (falla de detección de radiación en la superficie de la piscina) es el SS3.2a (falla del regulador de voltaje). El análisis comparativo se ilustra en la Figura 3.15.

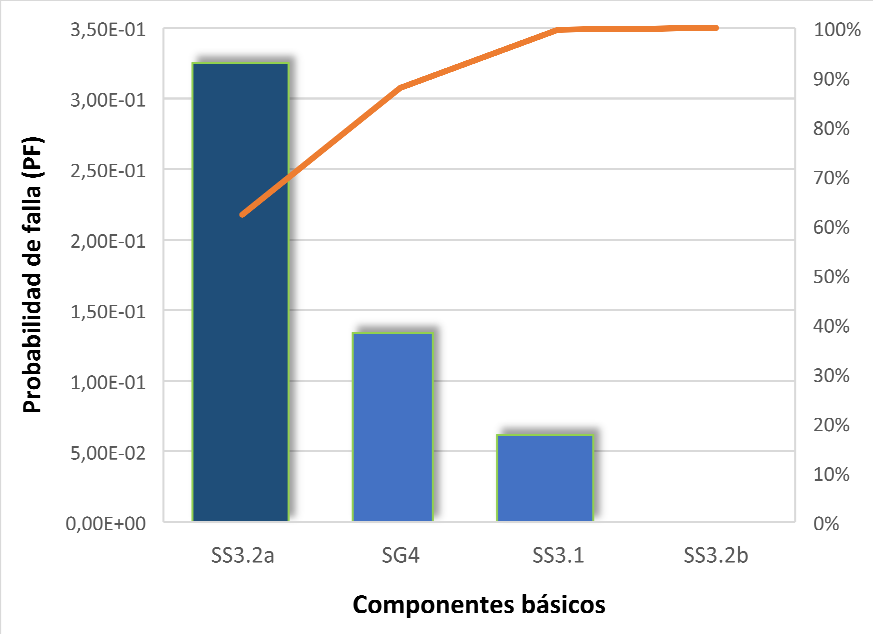


Figura 3.15. Análisis comparativo de las probabilidades de falla de los componentes del SS3 (condición inicial)

3.3.3.2 Diagrama FTA del control de nivel del blindaje húmedo – SS4 (condición inicial)

El diagrama FTA que se muestra en la Figura 3.16, describe el análisis de la falla de la reposición del sistema de control de nivel de blindaje húmedo – SS4 instalado. Se puede observar que también influye en la falla un sistema general que es el SG1, este sistema ya ha sido analizado previamente en el subcapítulo 3.3.2.1.

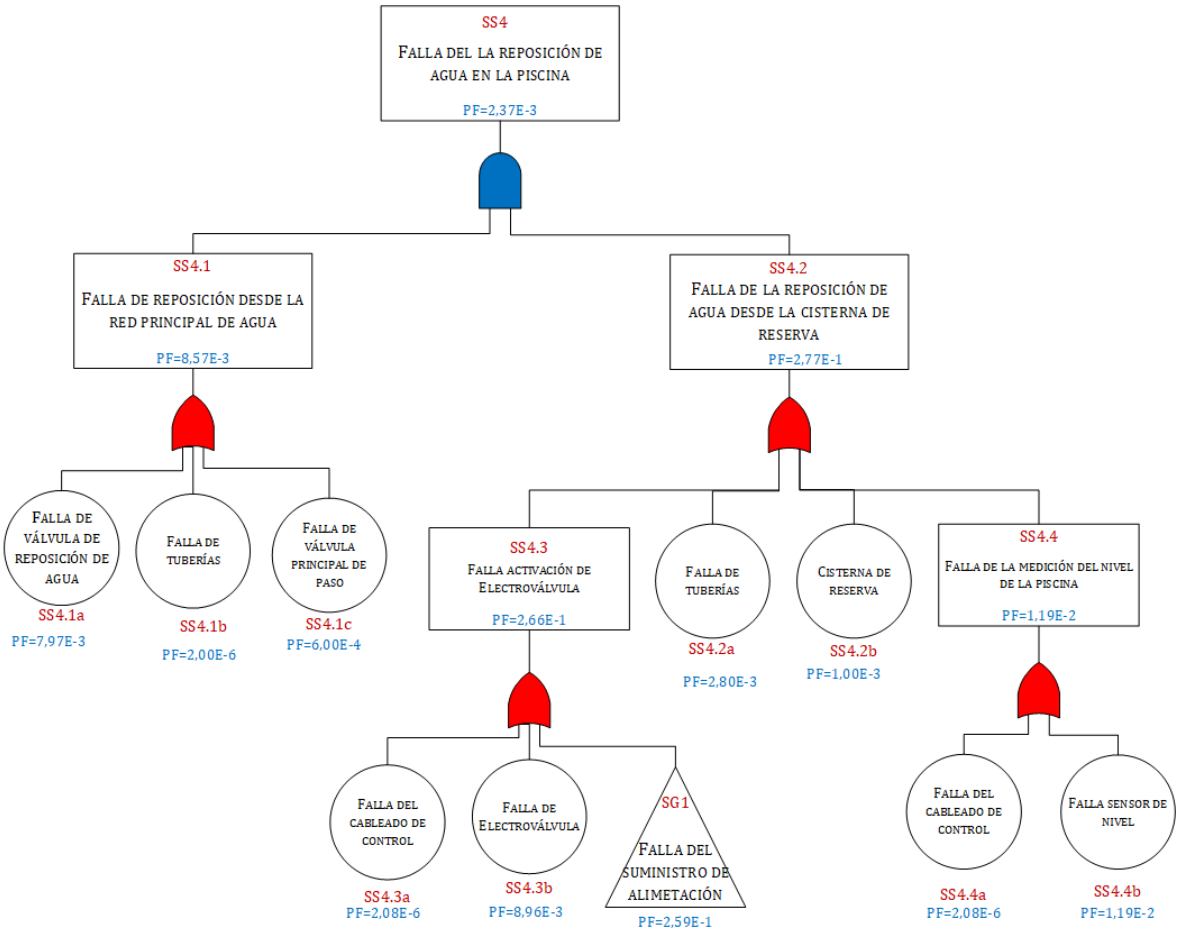


Figura 3.16. Diagrama FTA del control de nivel de blindaje húmedo – SS4 (condición inicial)

En el Anexo I se detallan los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos del diagrama FTA del sistema de control de nivel de blindaje húmedo. Con los resultados obtenidos y con ayuda de la metodología FTA se realizó un análisis comparativo para determinar cuál es el componente que más influye en la probabilidad de falla en la reposición del agua en la piscina del SS4. Como resultado de este análisis se concluye que la falla del SG1(falla del suministro de alimentación) es la más relevante para el control de nivel del blindaje húmedo - SS4. Esto se ilustra en la Figura 3.17.

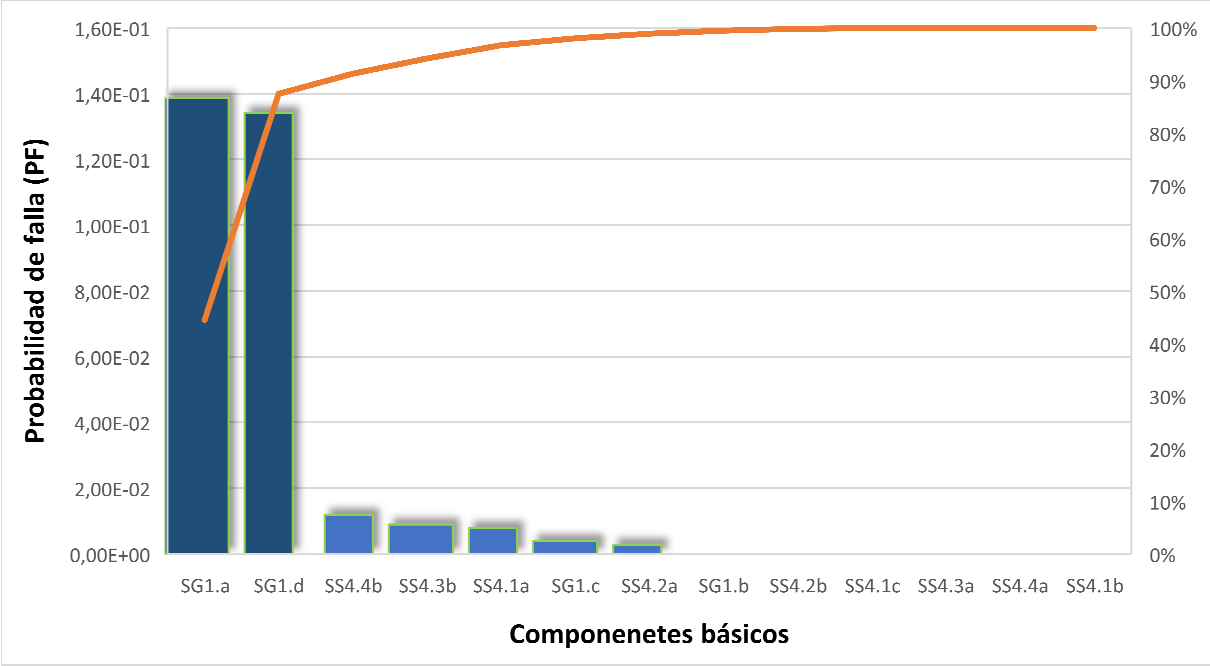


Figura 3.17. Análisis comparativo de las probabilidades de falla de los componentes del SS4 (condición inicial)

3.3.4 DIAGRAMAS FTA DE LOS SISTEMAS ADICIONALES

3.3.4.1 Diagrama FTA del sistema de enclavamientos de sistema de subida de rack de la fuente de Co-60 – SS6

El sistema de enclavamientos de la subida del rack de la fuente de Co-60 no interviene en los análisis del EVI5 ni EVI6, sin embargo, se realizó el respectivo análisis FTA con el objetivo de determinar la probabilidad de ocurrencia en un año un accidente que puede derivar en que el rack de la fuente se trabe durante un proceso de subida sin que el operador se diera cuenta. Por tal motivo, en la Figura 3.18 se muestra el FTA que describe la secuencia de falla de la subida del rack de la fuente del Sistema - SS6.

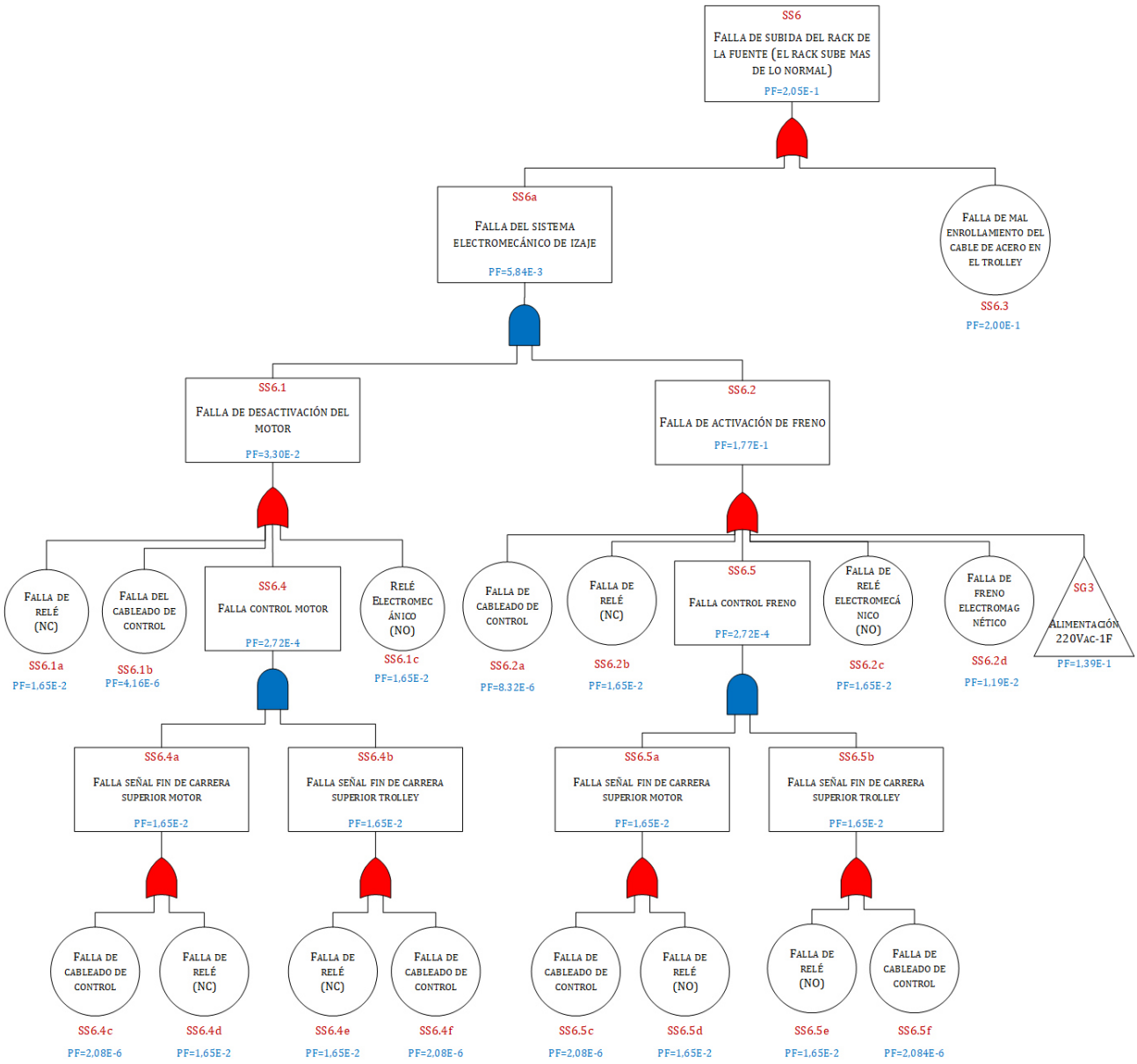


Figura 3.18. Diagrama FTA del sistema de enclavamientos de la subida del rack de la fuente de Co-60 – SS6

En la Figura 3.19. se muestra el diagrama FTA desarrollado del sistema general SG3 que trabajan en conjunto con el sistema de enclavamientos de subida del rack de la fuente – SS6.

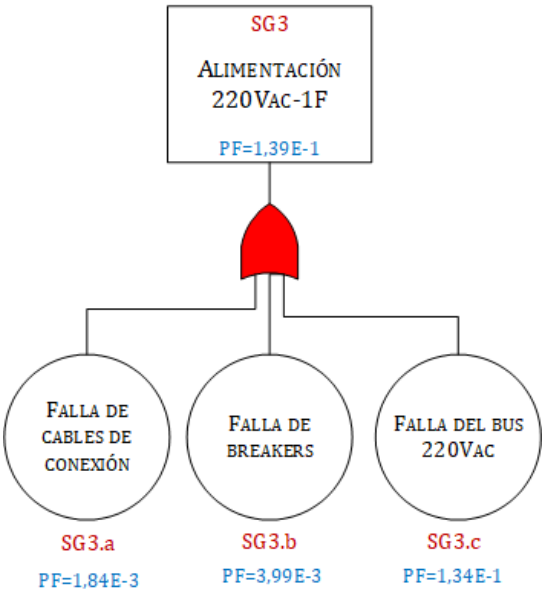


Figura 3.19. Diagrama FTA de la alimentación de 220 Vac SG3

En el Anexo I se detallan los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos de los diagramas FTA que influyen en el sistema de enclavamientos de la subida del rack de la fuente de Co-60. Además, se realizó un análisis comparativo de las probabilidades de falla y con la ayuda de la metodología FTA se determinó el componente básico que tienen más probabilidad de fallo durante la subida del rack de la fuente del SS6. Por lo que se concluye que el SS6.3 (falla del enrollamiento del cable en el trolley) es el que más influyo en la falla del SS6, esto se puede observar en la Figura 3.20. La probabilidad de falla del componente básico SG3.c no tiene mucha relevancia debido a que este influye en la falla de la activación del freno (SS6.2) que se encuentra redundante con la falla de la desactivación del motor (SS6.1), lo que disminuye considerablemente su influencia, esto se puede observar en el diagrama FTA de la Figura 3.18.

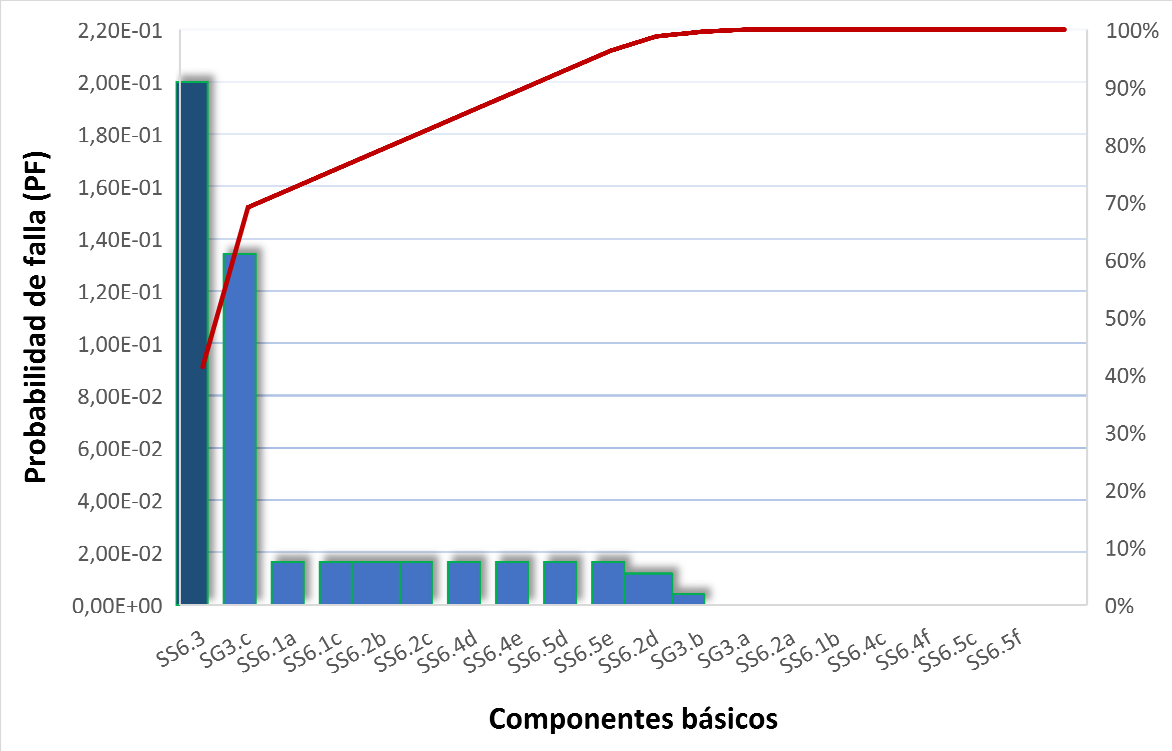


Figura 3.20. Análisis comparativo de las probabilidades de falla de los componentes básicos del SS6

3.3.5 DIAGRAMAS ETA DE EVENTOS INICIANTES

3.3.5.1 Análisis del evento iniciante EVI5

Este análisis se realizó con base al escenario definido en el inicio del subcapítulo 3.3.1, a partir de este escenario, se determinó que el evento iniciante requiere que ocurran dos incidentes que son:

1. El rack de la fuente de Co-60, se queda trabado en la posición sin blindaje dentro del búnker, debido a una falla de los finales de carrera instalados o al enrollamiento del cable en el sistema de izaje del rack de la fuente (falla del sistema de enclavamientos de la subida del rack de la fuente de Co-60 -SS6)
2. Al tener material para irradiar (cajas) el operador pierde visibilidad de la fuente de Co-60 por medio de la ventana, por lo que, una vez terminada la irradiación, el operador procede a realizar todo el proceso de desarmado del irradiador de Co-60, e ingresar al búnker sin seguir con el procedimiento

establecido de ingresar al búnker con un detector manual o portátil (falla por error humano).

Para el primer incidente, se determinó la probabilidad de ocurrencia de un accidente al año en 2,05E-1. Esto se lo realizó con base en la probabilidad de fallo al año del SIS – SS6 mostrado en la Figura 3.18. Para el segundo incidente, debido a que no se tiene información relacionada a la probabilidad de falla por error humano, se determinó la probabilidad de fallo al año basado en bibliografía. La probabilidad de fallo que se definió para este incidente es la relacionada a la siguiente actividad: El personal en diferentes turnos de trabajo no verifica el estado del hardware a menos que lo requiera la lista de verificación o una directiva escrita, esta actividad tiene una estimación de probabilidad de fallo de 1,00E-1 al año, el dato es recuperado del subcapítulo 14.25 “Assessment of human error: proccess operation” de la referencia: Lees’ Loss Prevention in the process Industries (Mannan, 2005a),

Con base en las probabilidades de fallo definidas de los dos incidentes antes mencionados y las probabilidades de fallo de los SIS SS2 y SS3 se estableció el siguiente diagrama ETA para el EVI5, que se indica en la Figura 3.21.

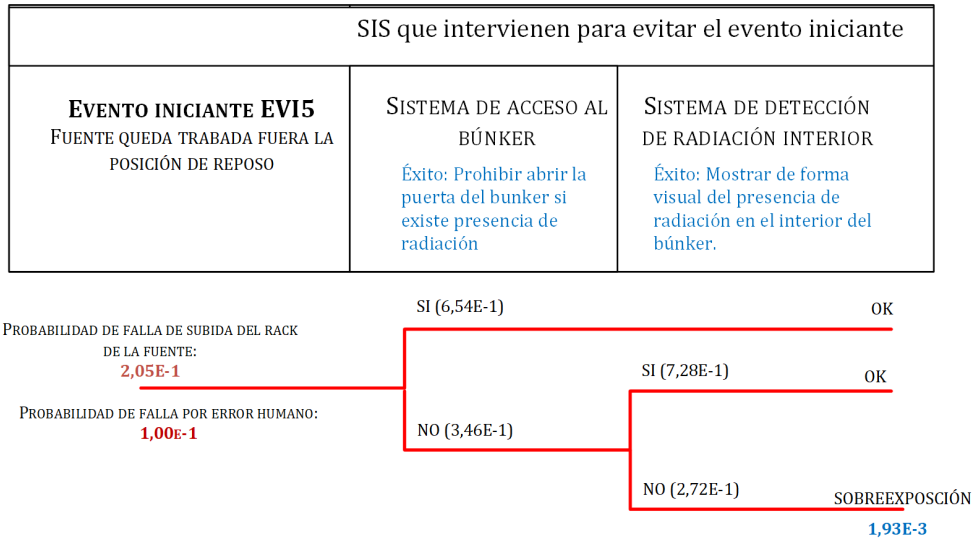


Figura 3.21. Diagrama ETA del evento EVI5 (condición inicial)

3.3.5.2 Análisis del evento iniciante EVI6

Este análisis se lo realizó con base en el escenario definido en el inicio del subcapítulo 3.3.1. Se determinó que, este evento iniciante requiere que ocurran dos incidentes que son:

1. La ocurrencia de un sismo de gran magnitud.
2. el colapso de la estructura civil de la piscina (resguardo del blindaje húmedo).

Para la estimación de la probabilidad de ocurrencia de los incidentes antes mencionados, se refirió a bibliografía y se determinó los siguientes datos.

Para el primer incidente en el capítulo 15 de la referencia Lees' Loss Prevention in the process Industries (Mannan, Lee's Loss Prevention in the Process Industries, 2005a), indica que la probabilidad de ocurrencia en el mundo de un sismo de gran magnitud (> 8 M_L) es de 1 y para un sismo grande de 7,0 a 7,9 M_L es de 10 al año, basado en esta información, para el APS se consideró la probabilidad de ocurrencia de 10 eventos al año, como se indica en la Figura 3.22.

M_L	*Gutenberg and Richter description*	*Annual frequeney*
>8.0	Great earthquakes	1
7.0-7.9	Major earthquakes	10
6.0-6.9	Destructive shocks	100
5.0-5.9	Damaging shocks	1,000
4.0-4.9	Minor strong shocks	10,000
3.0-3.9	Generally felt	100,000

Figura 3.22. Ocurrencia de terremotos al año a nivel mundial
(Mannan, 2005a)

Para el segundo incidente se consideró la referencia Structural reliability analysis and prediction (Melchers & Beck, 2018), en el que menciona la tasa de fallo (colapso) de una estructura de ingeniería en 1,00E-3. Con base en esta información y con las probabilidades de fallo determinadas para los SIS SS3 y SS4 se definió el diagrama ETA indicado en la Figura 3.23.

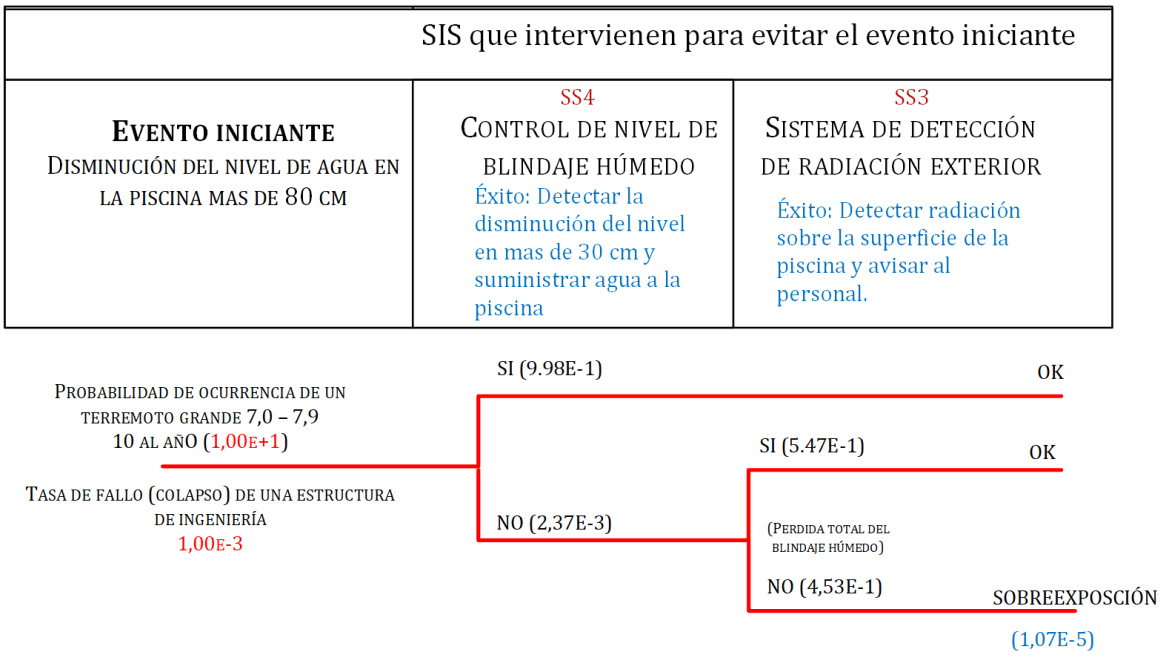


Figura 3.23. Diagrama ETA del evento iniciante EVI6 (condición inicial)

3.3.6 ESTIMACIÓN DE DOSIS EFECTIVA RECIBIDA POR EL POE

Basado en la probabilidad de ocurrencia del evento iniciante EVI5, se realizó la estimación inicial de la dosis efectiva recibida por el POE en dos casos que se indican en la Figura 3.24.

- Punto de estimación A (0,3 m de la fuente de Co-60): cuando el operador ingresa al búnker para retirar las cajas que se irradiaron y es el punto más crítico de la evaluación
- Punto de estimación B (3,8 m de la fuente de Co-60): cuando el operador realiza la operación de la apertura de la puerta.

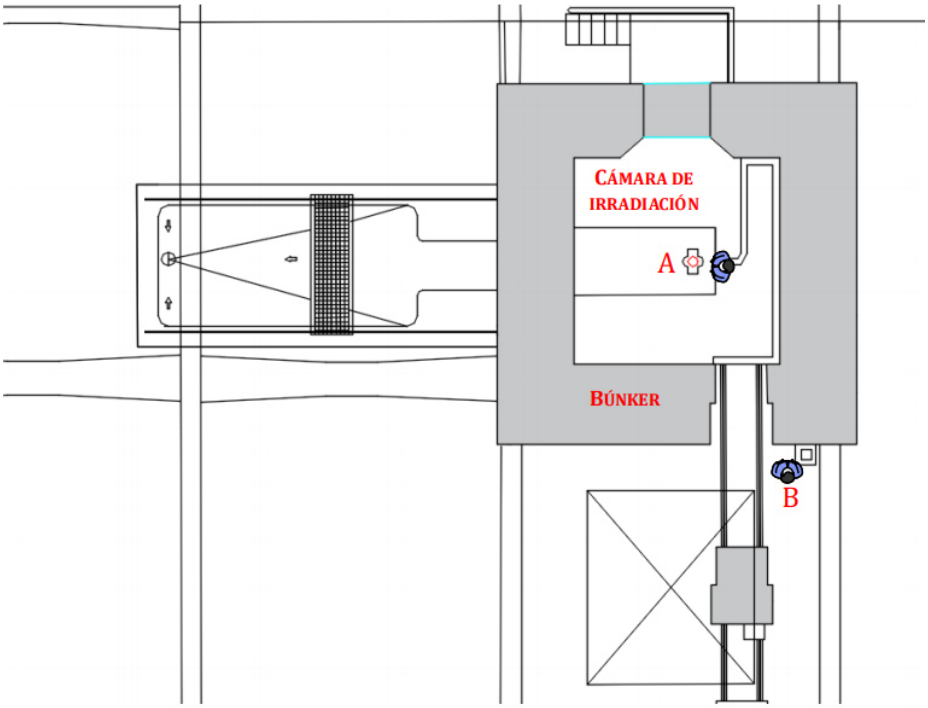


Figura 3.24. Puntos de estimación de dosis efectiva recibida por el POE para el EVI5

Para cada uno de estos puntos de evaluación se consideró que la actividad de la fuente de Co-60 es de 888 Ci al 01/01/2020 (Tabla 3.1) y que la actividad futura de fuente de Co-60 que sería de 50 000 Ci, con una exposición de 1 minuto en este escenario. Para la estimación de la dosis efectiva se utilizó la Ecuación [2.5] y se presentan los resultados en la Tabla 3.9.

Tabla 3.9. Estimación de dosis efectiva en los puntos A y B

Estimación de dosis efectiva		
Tiempo de exposición:		**1 minuto**
	Probabilidad anual	Dosis efectiva (mSv)
Punto A (888 Ci)	1,92E-03	1521,11
Punto B (888 Ci)	1,92E-03	9,48
Punto A' (50.000 Ci)	1,92E-02	85648,15
Punto B' (50.000 Ci)	1,92E-02	533,82

De igual manera, basado en la probabilidad de ocurrencia del evento iniciante EVI6, se realizó la estimación de la dosis efectiva recibida por el POE con base al tercer caso que se indica en la Figura 3.25.

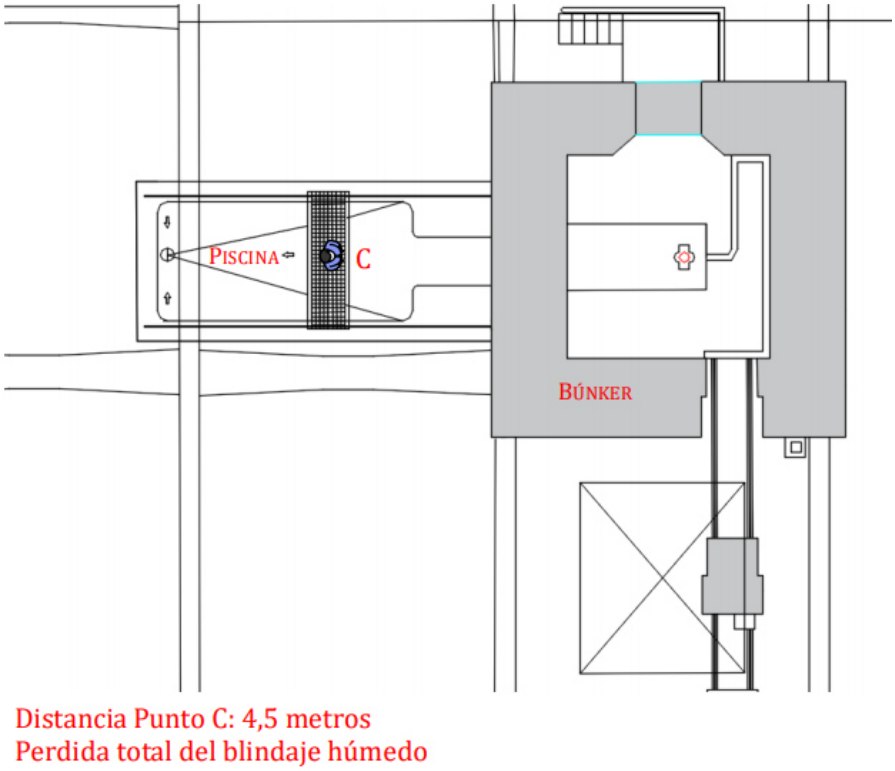


Figura 3.25. Punto de estimación de dosis efectiva recibida por el POE para el EVI6

- Punto C (4,5 m de la fuente de Co-60): cuando un operario o POE se acerca a la piscina para verificar el nivel de esta.

Para este punto de evaluación se consideró la actividad al (01/01/2020) de la fuente de Co-60 que es de 888 Ci (Tabla 3.1) y la actividad futura de la fuente de Co-60, que sería de 50 000 Ci, con una exposición de 1 minuto en este escenario. Para la estimación de la dosis efectiva se utilizó la Ecuación [2.5] y se presentan los resultados en la Tabla 3.10.

Tabla 3.10. Estimación de dosis efectiva en el punto C

Estimación de dosis efectiva		
Tiempo de exposición:	**1 minuto**	
	Probabilidad anual	Dosis efectiva (mSv)
Punto C (888 Ci)	1,07E-05	6,76
Punto C' (50.000 Ci)	1,07E-05	381,66

3.3.7 DISCUSIÓN DE LOS RESULTADOS OBTENIDOS

Como último paso para el APS, se relacionan los datos obtenidos de la estimación de dosis efectiva recibida con la probabilidad de ocurrencia anual y se hace una comparativa con los objetivos de seguridad establecidos en la Tabla 2.2, estos resultados se los puede visualizar en la Figura 3.26.

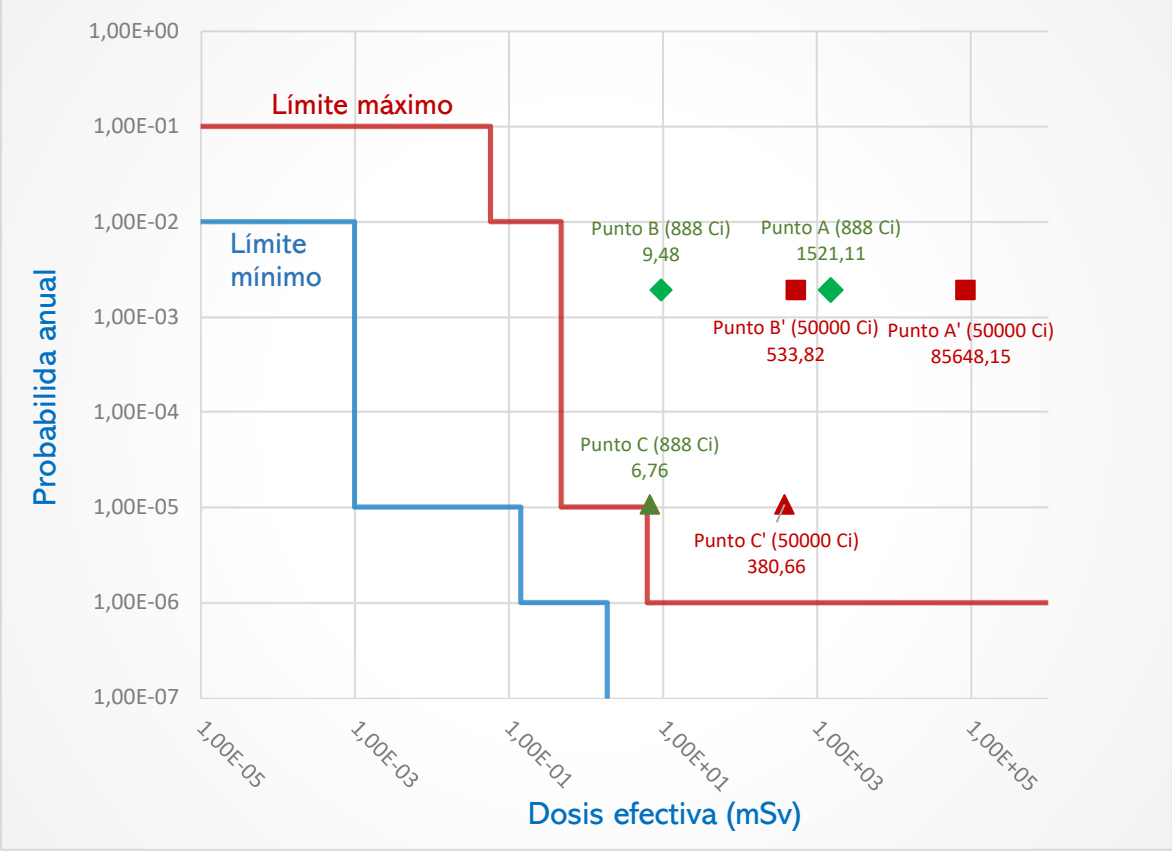


Figura 3.26. Relación de datos obtenidos de la dosis efectiva, probabilidad anual de ocurrencia de la exposición potencial y límites de los objetivos de seguridad de los puntos A, B y C evaluados a 888 Ci y 50 000 Ci con 1 minuto de exposición del POE

Por medio de la comparación de los resultados obtenidos con los límites de los objetivos de seguridad proporcionados por el ICRP (ICRP, 1993), se puede apreciar que los SIS actuales no cumplen con los objetivos de seguridad para la ejecución de estas actividades. Sin embargo, existen otras barreras adicionales de seguridad que están fuera del alcance de este proyecto como son: el uso de dosímetros electrónicos, capacitaciones del personal recurrentes entre otras. Además, se debe considerar que el irradiador actualmente está en estado de para (al momento no presta servicios), por lo que, la probabilidad de ocurrencia basado en las 2 000 h laborales se reduce.

Con todo lo expuesto anteriormente, se determinó que, para la repotenciación de la fuente de Co-60 a 50 000 Ci es necesario actualizar los SIS que posee el irradiador de Co-60 con el objetivo de entrar en la región de los objetivos de seguridad incluso sin la necesidad de recurrir a barreras adicionales que minimicen la probabilidad anual de ocurrencia de una exposición anual del POE.

Para este objetivo, en el siguiente capítulo se procedió a generar la propuesta de diseños de ingeniería requeridos por los SIS evaluados en este proyecto.

3.4 ESPECIFICACIONES DE LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SIS

Para las especificaciones de los requerimientos de seguridad de los SIS, se consideró la guía de seguridad especifica No. SSG 8 y varios criterios proporcionados a partir de las normativas IEC 61508, IEC 61511 entre otras.

En esta etapa se elaboraron los requerimientos de seguridad de los diferentes SIS, dentro del alcance de este proyecto. Estos se detallan en la Tabla 3.11.

Tabla 3.11. Especificaciones de los requerimientos de seguridad generales de los SIS

SIS	Funcionamiento	Arquitectura	SIL requerido	Modos de fallo del SIS	Interfaz
SS1- Sistema de detección de radiación interior	Detectar los niveles de radiación dentro del búnker de manera continua en Sv/h, Bq/l - R/hr, Ci/cc	Dos tipos de conexión al Módulo de control lógico (conexiones de diferente tecnología)	No especificado	Fallo del detector (cámara de ionización) Fallo del módulo de acondicionamiento	RS-485/RS-232 4-20 mA SPDT contactos de relés
SS2 - Sistema de enclavamientos de acceso al búnker	Bloquear el control de apertura de la puerta del búnker	Dos tipos de conexiones con diversas tecnologías (digital y eléctrica)	SIL 1	Fallo de contactos de los relés	4-20 mA SPDT contactos de relés
SS3 - Sistema de acceso al búnker con el detector portátil	Obligar el uso del detector portátil para ingresar al búnker	1oo1	SIL 1	Fallo de funcionamiento de dispositivos Fallo de contactos de relés	SPDT contactos de relés
SS5 - Control de nivel del blindaje Húmedo	Controlar el nivel del blindaje húmedo 1. Reponer el agua en caso de disminuir 3 cm el nivel del blindaje 2. Abrir la reposición desde la red principal de agua en caso de disminuir 50 cm el nivel del blindaje húmedo	Sistema redundante de reposición de agua para el nivel crítico de 50 cm Sistema simple para reposición del agua para el nivel de 3 cm	SIL 1	Fallo de funcionamiento	4-20 mA SPDT contactos de relés

- La alimentación de todos los SIS es a través de una fuente de alimentación de 110/220 Vac por UPS y con una fuente de 24Vdc de seguridad
- El intervalo de prueba de todos los SIS es de 6 meses

No constan las especificaciones de todos los SIS requeridos por el irradiador de Co-60, debido a que, el alcance de este proyecto se centra en los sistemas de enclavamiento de acceso al búnker y de control de nivel del blindaje húmedo.

3.5 DISEÑO DE INGENIERÍA DE LOS SIS (ARQUITECTURAS)

Por medio de la información proporcionada por la metodología APS y las especificaciones de la Tabla 3.11 se definió el diseño de los siguientes SIS para el irradiador de Co-60, con relación a una exposición potencial del POE o del público en general. El detalle de los SIS diseñados se indica en la Tabla 3.12.

Tabla 3.12. Descripción de los SIS del Irradiador de Co-60 relacionados a la exposición potencial del POE (diseño)

CÓDIGO	SIS	Función	Efecto potencial de la falla
SS1	Sistema de detección de radiación interior	Detectar niveles de radiación en el interior del búnker	Exposición potencial del POE
SS2	Sistema de enclavamiento de acceso al búnker	Prohibir la apertura de la puerta del búnker mientras la fuente de Co-60 se encuentra expuesta	Exposición potencial del POE
SS3	Sistema de prohibición de ingreso al búnker sin detector portátil	Prohibir o forzar el ingreso al búnker del irradiador con el uso del detector portátil	Exposición potencial del POE
SS4	Sistema de detección de radiación exterior	Detectar niveles de radiación sobre los niveles permitidos en el área restringida (sobre la piscina)	Exposición potencial del POE y público en general
SS5	Sistema de control de nivel de blindaje húmedo	Mantener el nivel del blindaje húmedo lo suficientemente alto para contener los niveles de radiación debajo de los límites permitidos	Exposición potencial del POE y público en general
SS6	Punto de ronda	Verificar la salida de todo personal del búnker antes de un proceso de irradiación	Exposición potencial del POE
SS7	Sistema de enclavamientos de la función de subida de la fuente de Co-60	Evitar que el rack de la fuente de Co-60 pueda salir de su trayectoria normal de trabajo	Exposición potencial del POE
SS8	Sistema de alarmas interiores	Advertir al personal POE y público en general de niveles anormales de radiación en el área restringida del irradiador de Co-60	Exposición potencial del POE y público en general

3.5.1 Sistema de detección de radiación interior – SS1 (diseño)

El sistema de detección de radiación interior cumple con la función de detectar la radiación al interior del búnker por medio de un una cámara de ionización que trabaja como un contador Geiger Müller, la señal detectada es enviada al monitor de radiación que posee puertos de interfaz digital para conectarse con el PLC y conectores con salidas de relés normalmente abiertos (NO) y normalmente cerrados (NC). La señal utilizada en este SIS es de la interfaz digital, la cual es conectada al PLC y este en función de su programación, permite visualizar los niveles de radiación en la pantalla HMI. El PLC también tiene la capacidad de dar respuesta según los niveles umbrales mediante la activación de la lámpara de señalización, este sistema se lo definió con el siguiente diagrama de bloques mostrado en la Figura 3.27. y la descripción de los componentes diseñados de este sistema se detallan en la Tabla 3.13.

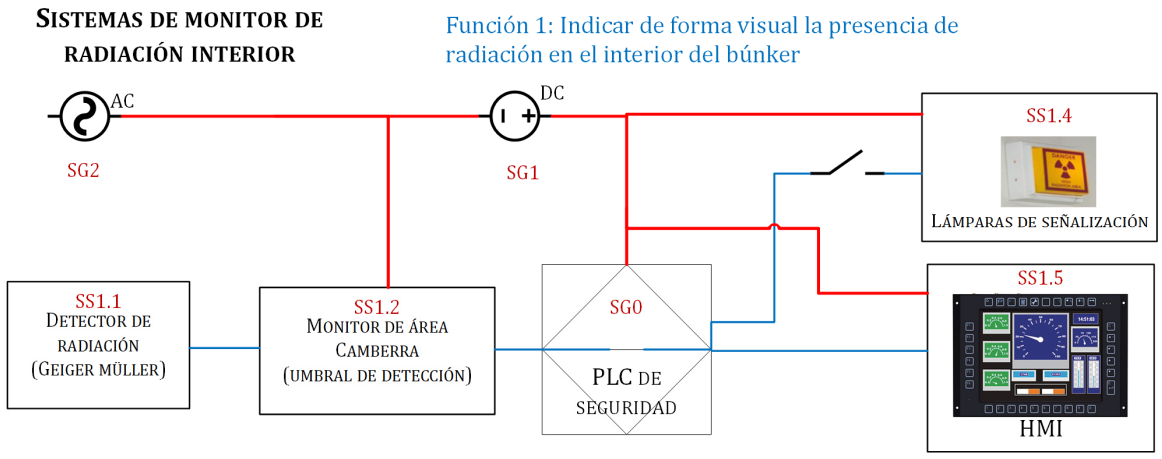


Figura 3.27. Diagrama de bloques del sistema de monitor de radiación interior (diseño)

Tabla 3.13. Descripción del Sistema de detección de radiación interior (diseño)

Código	Descripción del componente	Función	Modo de falla potencial
SS1.1	Detector de radiación (cámara de ionización como contador Geiger Müller)	Detectar las radiaciones ionizantes	Falla por funcionamiento
SS1.2	Monitor de área	Acondicionar la señal proveniente del detector	Falla por funcionamiento
SS1.4	Lámpara de señalización de estado de irradiación	Acondicionar las señales para la visualización en el monitor de radiación	Falla por funcionamiento
SS1.5	Visualizador de niveles de radiación por HMI	Visualizar los niveles de radiación	Falla de funcionamiento
SG0	Controlador Lógico Programable (PLC) de seguridad	Realizar todas las lógicas de control y seguridad gestionadas por software	Falla de funcionamiento
SG1	Fuente de alimentación de 24 Vdc	Proporcionar el suministro de energía al sistema	Falla de funcionamiento
SG2	Fuente de alimentación de 110/220 Vac con UPS regulado	Proporcionar el suministro de energía al sistema	Falla de funcionamiento

3.5.2 Sistema de enclavamiento de acceso al búnker – SS2 (diseño)

El sistema de enclavamiento de acceso al búnker recibe la señal común desde el detector de radiación y el preamplificador de señal, pero en el cofre de alarmas tiene un ramal independiente para controlar el bloqueo electromecánico de la puerta del búnker. Este sistema se lo definió con el diagrama de bloques mostrado en la Figura 3.28 y la descripción de los componentes se detallan en la Tabla 3.14.

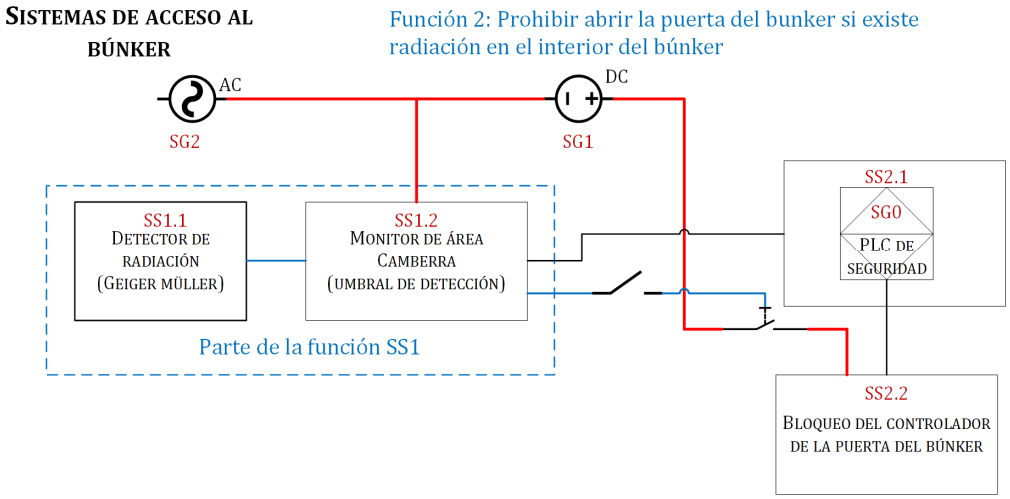


Figura 3.28. Diagrama de bloques del sistema de bloqueo de acceso al búnker (diseño)

Tabla 3.14. Descripción del sistema de bloqueo de acceso al búnker (diseño)

Código	Descripción del componente	Función	Modo de falla potencial
SS2.1	Bloqueo digital de control de puerta de búnker por PLC	Deshabilitar el control de apertura de la puerta del búnker por medio de lógica de control en el PLC	Falla de funcionamiento
SS2.2	Bloqueo electromecánico de apertura de la puerta (relé electromecánico)	Deshabilitar el control de apertura de la puerta del búnker	Falla de contactos
SG0	Controlador Lógico Programable (PLC) de seguridad	Realizar todas las lógicas de control y seguridad gestionadas por software	Falla de funcionamiento
SG1	Fuente de alimentación de 24 Vdc	Proporcionar el suministro de energía al sistema	Falla de funcionamiento
SG2	Fuente de alimentación de 110/220 Vac con UPS regulado	Proporcionar el suministro de energía al sistema	Falla de funcionamiento

3.5.3 Sistema de acceso al búnker con detector portátil de radiación – SS3 (diseño)

Este sistema tiene como elemento principal un detector de radiación portátil, el cual dentro de los procedimientos establecidos para la operación del irradiador de Co-60 es de uso obligatorio para el ingreso al búnker. Este SIS se añadió con la

finalidad de generar una barrera física adicional para que el POE no ingrese sin el detector portátil. El sistema se lo definió con el siguiente diagrama de bloques mostrado en la Figura 3.29 y la descripción de los componentes de este sistema diseñado se detallan en la Tabla 3.15.

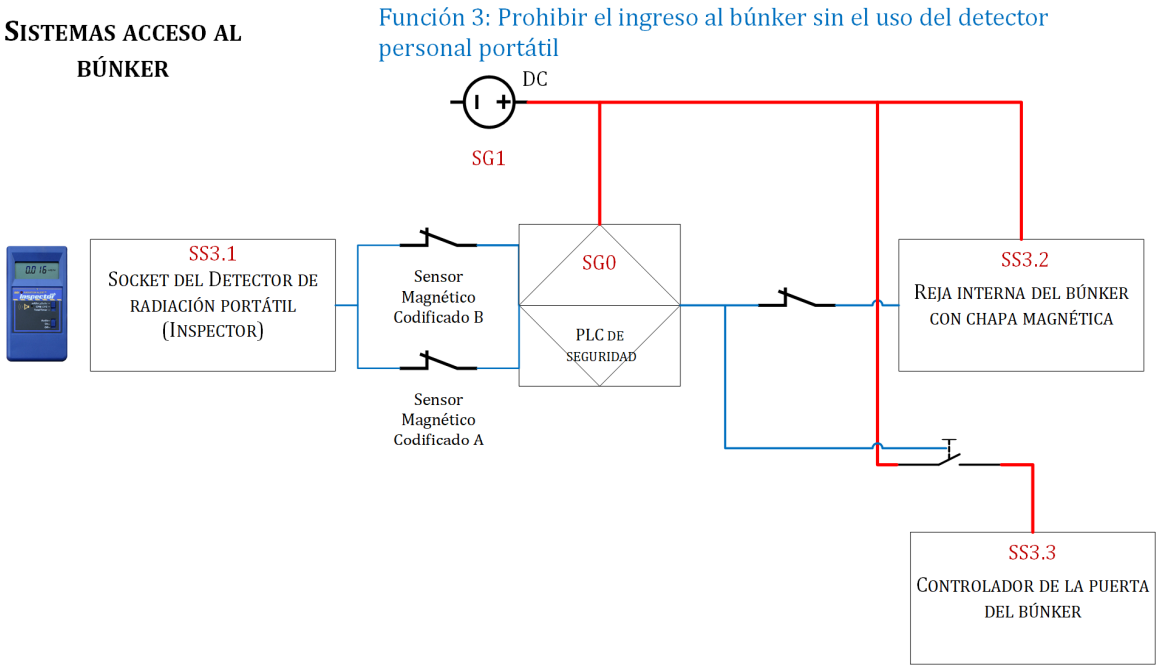


Figura 3.29. Diagrama de bloques del sistema de acceso al búnker con detector portátil de radiación (diseño)

Tabla 3.15. Descripción del sistema acceso al búnker sin detector portátil de radiación (diseño)

Código	Descripción del componente	Función	Modo de falla potencial
SS3.1	Detector de radiación portátil (con sistema codificado)	Deshabilitar toda operación si no se toma el detector de radiación portátil de su socket	Falla de funcionamiento
SS3.2	Reja interna del búnker con chapa magnética	Prohibir el ingreso físico al interior del búnker	Falla de funcionamiento
SS3.3	Bloqueo de controlador de la puerta del búnker	Deshabilitar el control de la puerta del búnker	Falla de funcionamiento
SG0	Controlador Lógico Programable (PLC) de seguridad	Realizar todas las lógicas de control y seguridad gestionadas por software	Falla de funcionamiento
SG1	Fuente de alimentación de 24Vdc	Proporcionar el suministro de energía al sistema	Falla de funcionamiento

3.5.4 Sistema de detección de radiación exterior– SS4 (diseño)

El sistema de detección de radiación exterior consta de un detector de radiación de área que dispone alimentación de 110 Vac regulado por UPS para el suministro de alimentación, este detector envía la señal de los niveles de radiación hacia el PLC de seguridad. El sistema se lo definió con el siguiente diagrama de bloques que se muestra en la Figura 3.30 y la descripción de los componentes de este sistema diseñado se detallan en la Tabla 3.16.

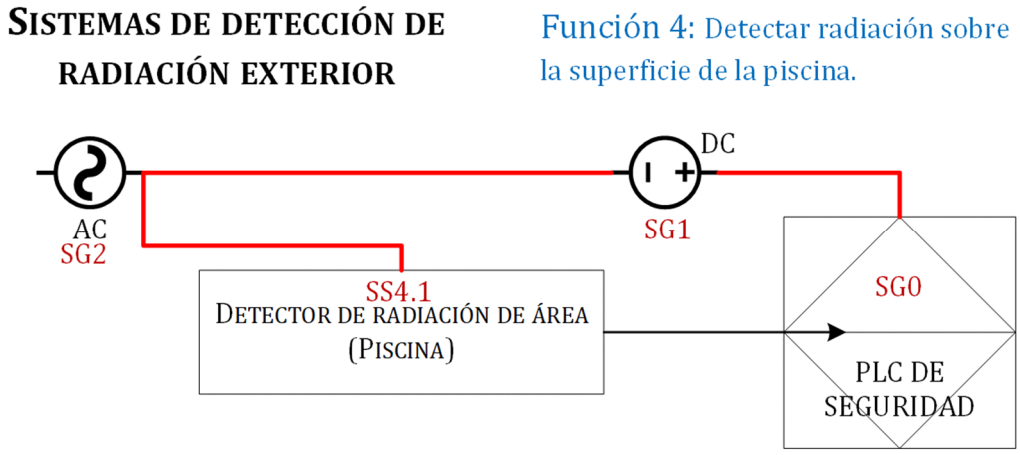


Figura 3.30. Diagrama de bloques del sistema de detección de radiación exterior (diseño)

Tabla 3.16. Descripción del sistema de detección de radiación exterior (diseño)

Código	Descripción del componente	Función	Modo de falla potencial
SS4.1	Detector de radiación de área	Detectar niveles de radiación sobre la piscina	Falla de funcionamiento
SG0	Controlador Lógico Programable (PLC) de seguridad	Realizar todas las lógicas de control y seguridad gestionadas por software	Falla de funcionamiento
SG1	Fuente de alimentación de 24 Vdc	Proporcionar el suministro de energía al sistema	Falla de funcionamiento
SG2	Fuente de alimentación de 110/220 Vac con UPS regulado	Proporcionar el suministro de energía al sistema	Falla de funcionamiento

3.5.5 Sistema de control de nivel de blindaje húmedo – SS5 (diseño)

El sistema de control de nivel de blindaje húmedo diseñado posee dos sistemas de reposición de agua controlado desde el PLC y un sistema de reposición sin influencia del PLC. Además, el sistema se diseñó con un sensor de nivel continuo, lo que permite determinar lógicas de control más elaboradas, sin embargo, se consideró solo la lógica actual de funcionamiento, es decir, el sensor de nivel activa el suministro desde la cisterna cuando el nivel de agua de la piscina ha disminuido 3 cm o activa el suministro desde la red principal si el nivel de la piscina ha disminuido 50 cm. Este sistema se lo definió en un diagrama de bloques como se muestra en la Figura 3.31 y la descripción de los componentes de este sistema diseñado se detallan en la Tabla 3.17.

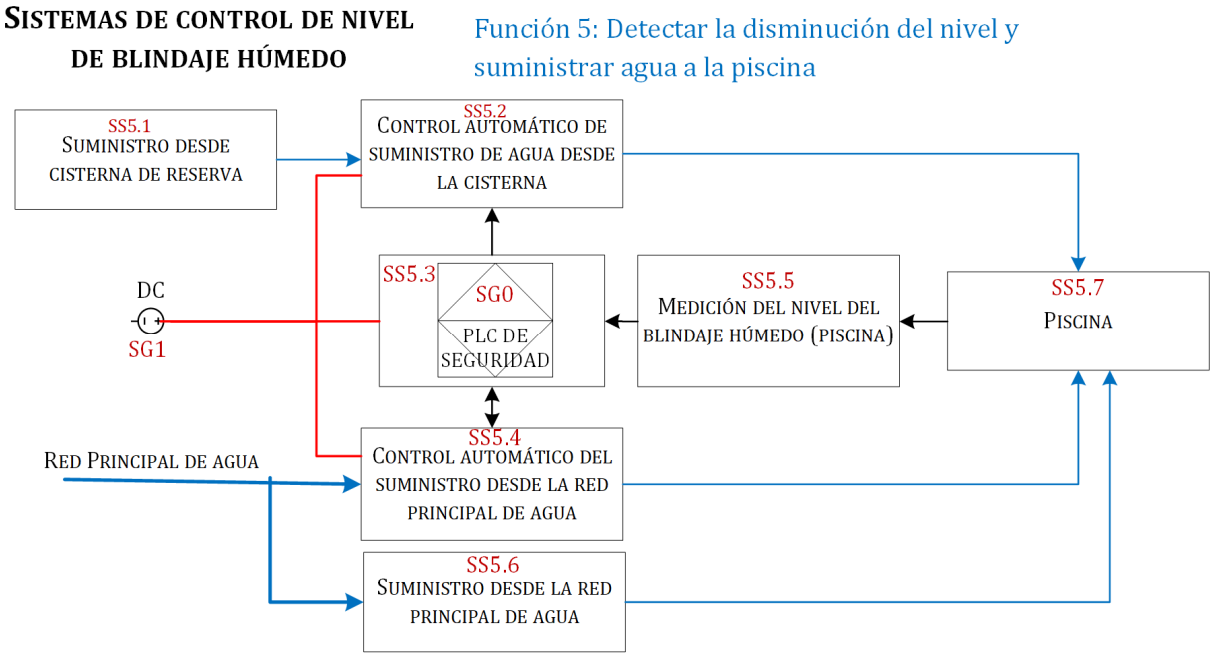


Figura 3.31. Diagrama en bloques del sistema de control de nivel de blindaje húmedo (diseño)

Tabla 3.17. Descripción del sistema de control de nivel de blindaje húmedo (diseño)

Código	Descripción del componente	Función	Modo de falla potencial
SS5.1	Suministro desde la cisterna de reserva	Almacenar un volumen de agua de reserva para reposición del nivel del blindaje húmedo	Falla por deterioro
SS5.2	Control automático de suministro desde la cisterna de reserva	Suministrar de manera automática el agua a la piscina desde la cisterna de reserva	Falla de funcionamiento
SS5.3	Control automático de suministro desde la cisterna de reserva	Realizar todas las lógicas de control y seguridad gestionadas por software	Falla de funcionamiento
SS5.4	Control automático de suministro desde la red principal de agua	Suministrar de manera automática el agua a la piscina desde la red principal de agua	Falla de funcionamiento
SS5.5	Medición del nivel del blindaje húmedo (piscina)	Detectar la disminución del nivel de agua	Falla de funcionamiento
SS5.6	Suministro desde la red principal de agua	Suministrar agua a la piscina si el nivel ha disminuido demasiado	Falla de funcionamiento
SS5.7	Piscina	Almacenar el blindaje húmedo	Falla por deterioro
SG1	Fuente de alimentación de 24Vdc	Suministrar alimentación a la electroválvula	Falla de funcionamiento
SG0	Controlador Lógico Programable (PLC) de seguridad	Realizar todas las lógicas de control y seguridad gestionadas por software	Falla de funcionamiento

3.5.6 Sistema de alarmas interiores – SS8 (diseño)

El sistema de alarmas interiores se encarga de gestionar todos los eventos anormales del irradiador de Co-60 y mostrarlos por medios audibles o visuales al POE, con el objetivo de alertar de problemas en el irradiador. Este sistema cuenta con varias interfaces de comunicación como son: balizas con bocinas, envío de SMS para celular y envío de correos electrónicos. Este sistema se lo definió en un diagrama de bloques como muestra la Figura 3.32 y la descripción de los componentes de este sistema diseñado se detallan en la Tabla 3.18.

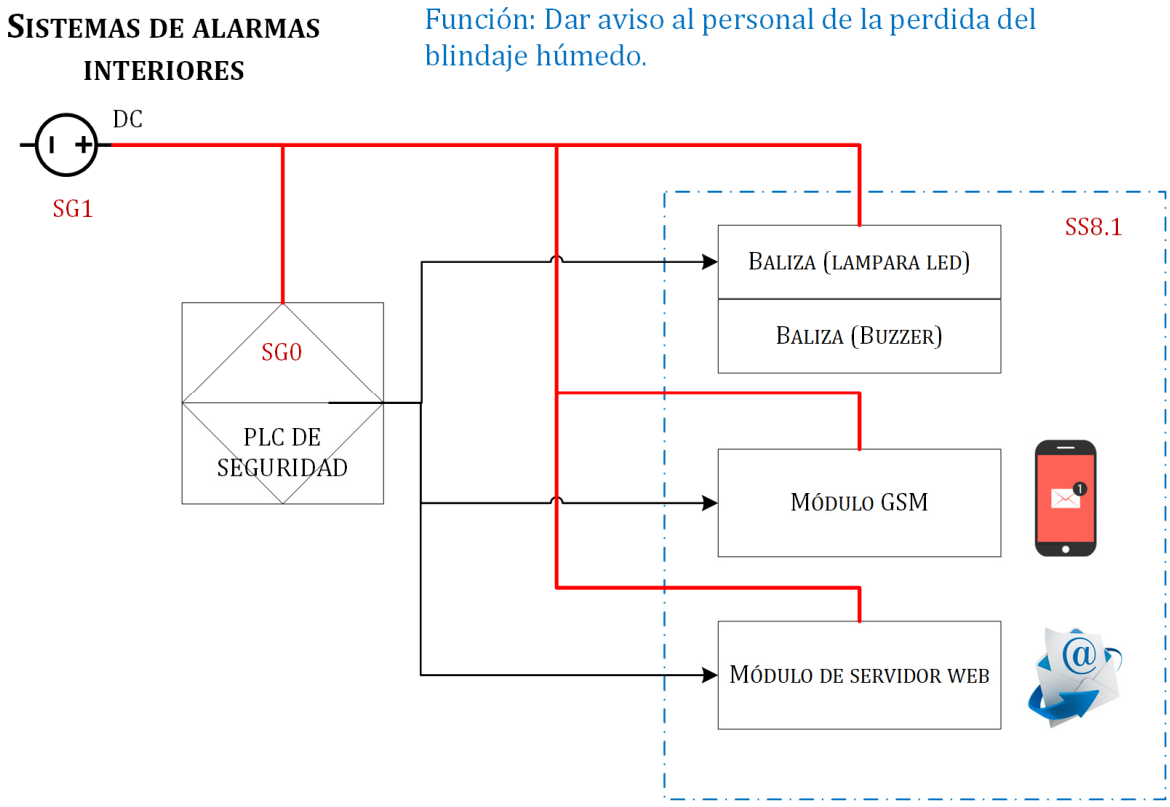


Figura 3.32. Diagrama de bloques del sistema de alarmas interiores (diseño)

Tabla 3.18. Descripción del sistema de alarmas interiores (diseño)

Código	Descripción del componente	Función	Modo de falla potencial
SS8.1	Baliza	Generar señales de advertencia audibles como visuales al POE de los niveles anormales de radiación en el área restringida	Falla de funcionamiento
SS8.1	Módulo GSM	Notificar al personal pertinente del irradiador de Co-60 por medio de mensajes de texto en casos de niveles de radiación anormales en el área restringida	Falla de funcionamiento
SS8.1	Módulo de servidor WEB	Notificar al personal pertinente del irradiador de Co-60 por medio de correos electrónicos en casos de niveles de radiación anormales en el área restringida	Falla de funcionamiento
SG0	Controlador Lógico Programable (PLC) de seguridad	Realizar todas las lógicas de control y seguridad gestionadas por software	Falla de funcionamiento
SG1	Fuente de alimentación de 24Vdc	Proporcionar el suministro de energía al sistema	Falla de funcionamiento

3.6 DESARROLLO DEL APS NIVEL 1 DEL DISEÑO REALIZADO

Considerando los mismos eventos iniciantes EVI5, EVI6 y los diseños propuestos en el subcapítulo 3.5 para los SIS en este proyecto, se desarrolló el respectivo APS para el Irradiador de Co-60 con el objetivo de definir su nivel de riesgo, con base en los objetivos de seguridad planteados. En la Tabla 3.19 se detalla de forma general los SIS diseñados que interactúan con los eventos iniciantes EVI5 y EVI6 para evitar o minimizar la exposición potencial del POE o del público en general. Para la elaboración de está matriz se consideró la configuración de hardware propuesto para el diseño de las instalaciones del irradiador de Co-60.

Tabla 3.19. Visualización general de los SIS diseñados que interactúan con los eventos iniciantes EVI5 y EVI6

		SIS del irradiador de Co-60 (diseño)							
Situación no deseada	**Código evento iniciante**	**Sistema de detección de radiación interior – SS1**	**Sistema de enclavamiento de acceso al búnker – SS2**	**Sistema de acceso al búnker con el detector de radiación portátil -SS3**	**Sistema de detección de radiación exterior – SS4**	**Sistema de control de nivel de blindaje húmedo – SS5**	**Punto de ronda – SS6**	**Sistema de enclavamientos de la función de subida/bajada de la fuente de Co^{60} – SS7**	**Sistemas de alarmas interiores – SS8**
Exposición potencial del POE	EVI5	X	X	X					
	EVI6				X	X			X

3.6.1 DIAGRAMAS FTA DE LOS SIS QUE INTERVIENEN CON EL EVI5

3.6.1.1 Diagrama FTA del Sistema de detección de radiación interior – SS1 (diseño)

Los diagramas FTA que se muestra en las Figuras 3.33, 3.34 y 3.35, describen la secuencia de la falla del aviso de forma visual de la presencia de radiación en el búnker del sistema de detección de radiación interior SS1 diseñado.

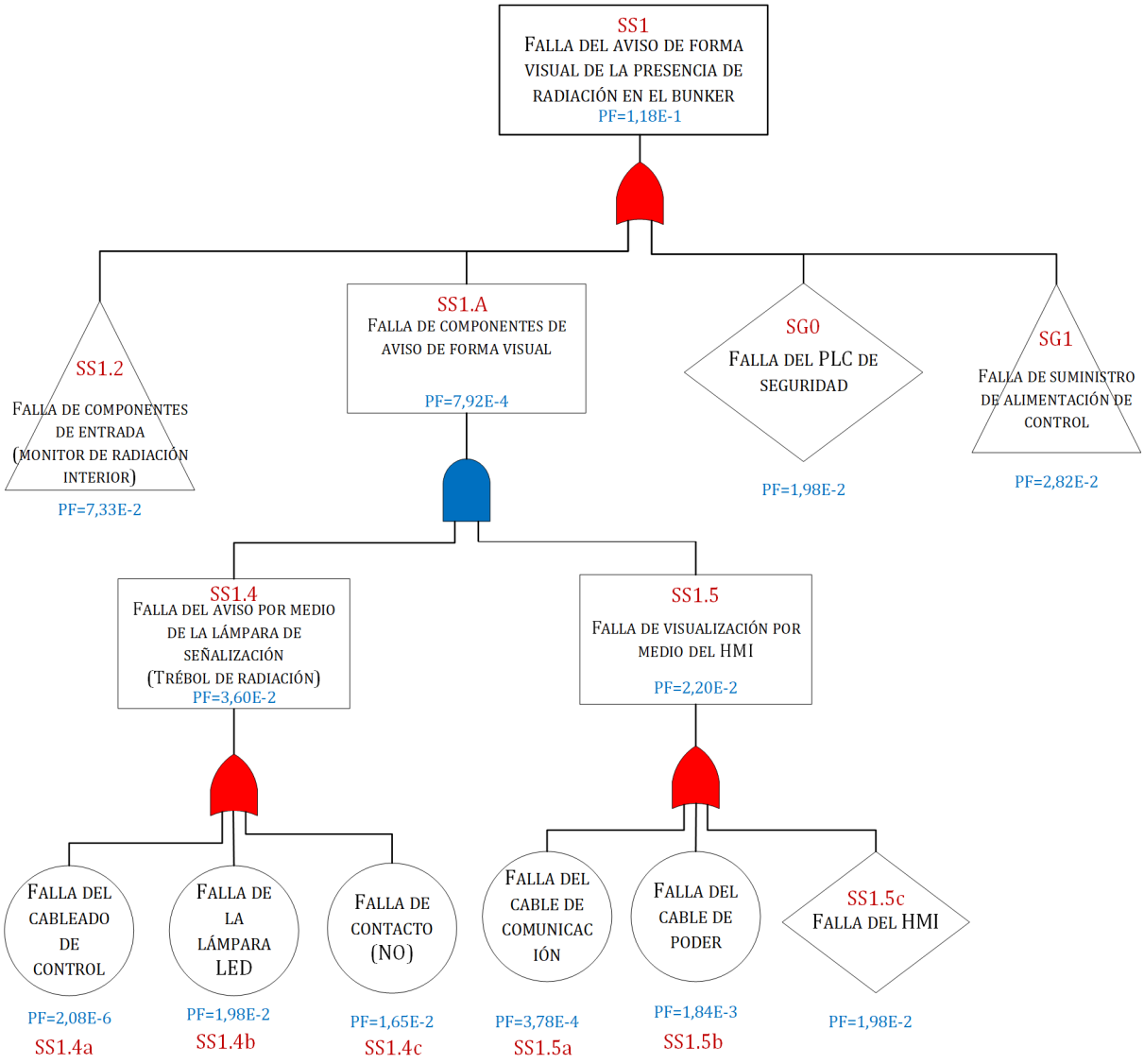


Figura 3.33. Diagrama FTA del sistema de detección de radiación interior – SS1 (diseño)

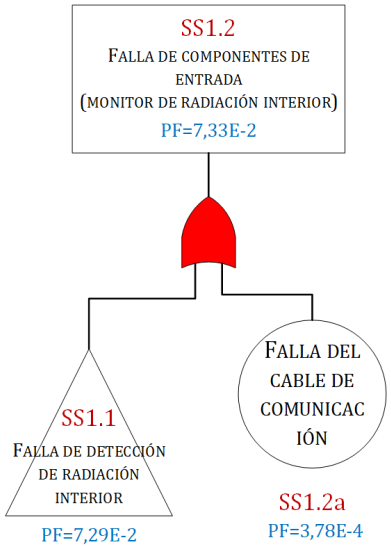


Figura 3.34. Diagrama FTA del sistema de detección de radiación interior -SS1.2 (diseño)

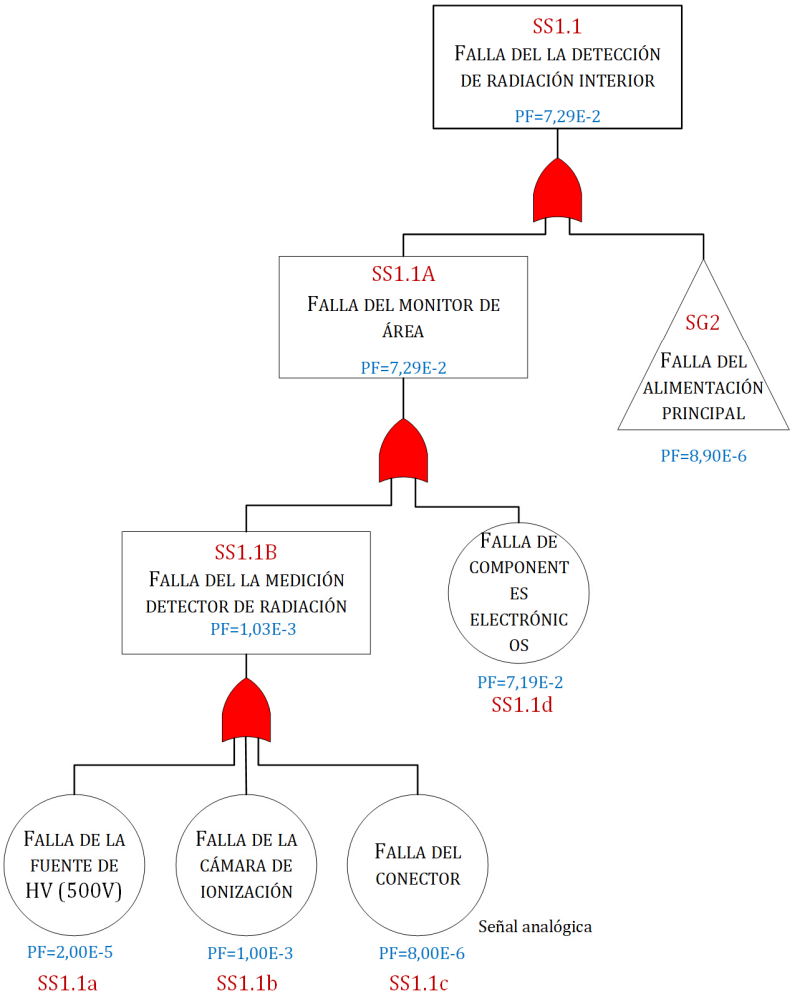


Figura 3.35. Diagrama FTA del sistema de detección de radiación interior – SS1.1 (diseño)

El diagrama FTA que se muestran en la Figura 3.36. describe la secuencia de falla del suministro de alimentación de control de los sistemas de seguridad de los SIS del irradiador de Co-60.

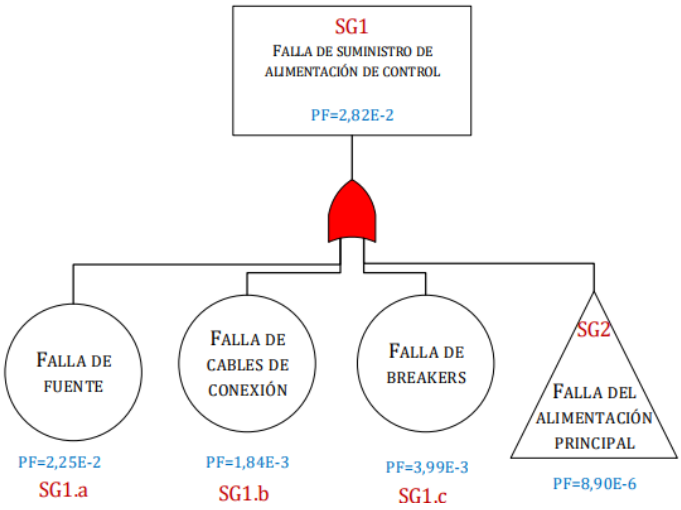


Figura 3.36. Diagrama FTA de sistema general de alimentación de control – SG1 (diseño)

El diagrama FTA que se muestran en la Figura 3.37. describen la secuencia de falla del suministro de alimentación principal del irradiador de Co-60.

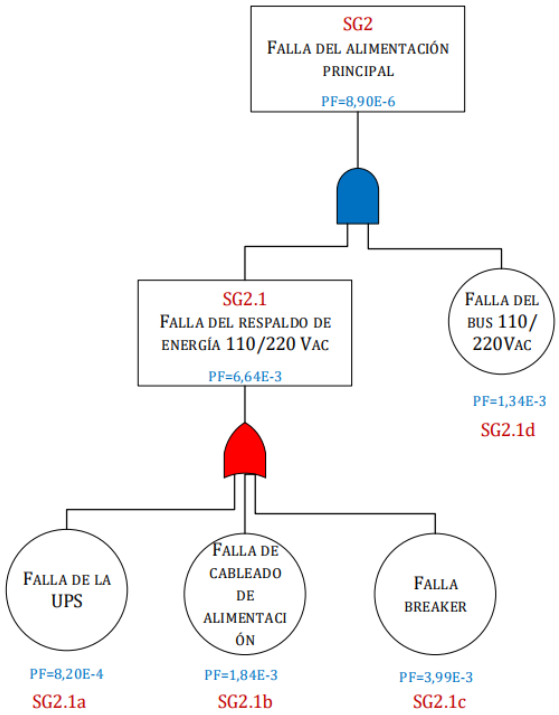


Figura 3.37. Diagrama FTA del sistema general de alimentación principal – SG2 (diseño)

En el ANEXO II se detallan los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos de los diagramas FTA del sistema de detección de radiación interior SS1 diseñado. A partir de estos, se realiza un análisis comparativo para identificar los componentes más influyentes en la falla analizada. Los componentes básicos de la alimentación principal (SG2) y de los componentes actuadores finales (SS3.A) se omitieron del análisis, ya que sus componentes se encuentran en una configuración redundantes y la probabilidad de falla de los conjuntos SG2 y SS3.A son pequeñas y no influyen en el SS1. Por otro lado, se puede identificar que el componente que más influye es el SS1.1d relacionado con la falla del monitor de radiación de área (SS1.1A), esto se puede observar en la Figura 3.38.

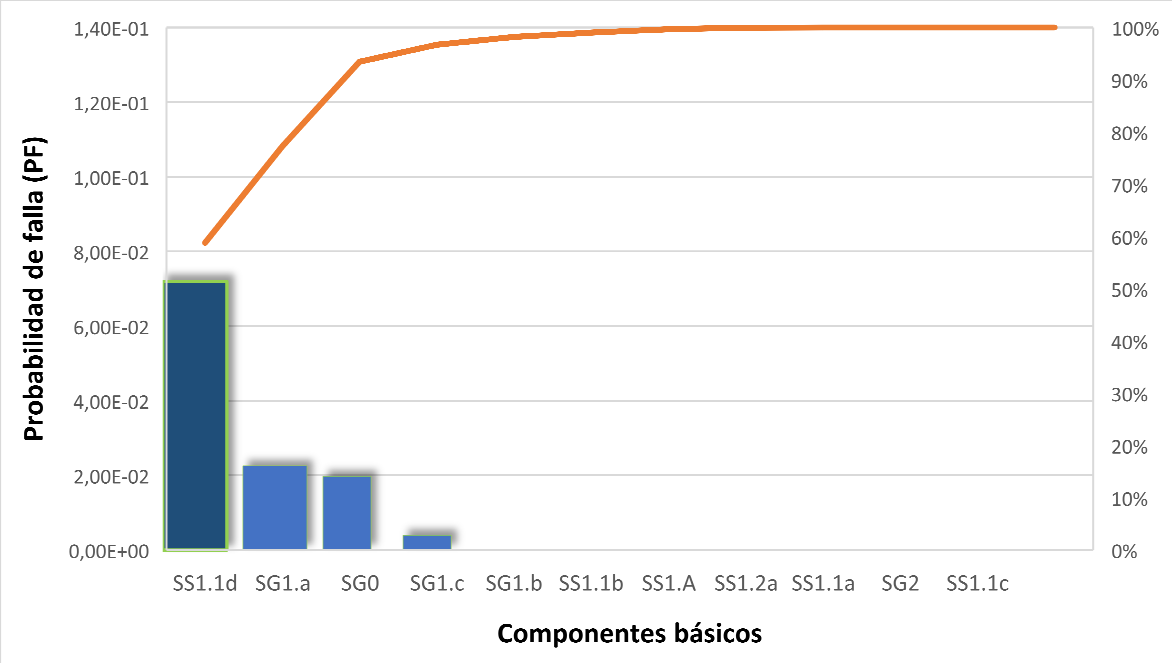


Figura 3.38. Análisis comparativo de las probabilidades de falla de los componentes básicos del SS1 (diseñado)

3.6.1.2 Diagrama FTA del sistema de enclavamientos de acceso al búnker – SS2 (diseño)

El diagrama FTA de la Figura 3.39. describe la secuencia de falla de la prohibición de la apertura de la puerta del búnker del sistema del enclavamiento de acceso – SS2. Este diagrama tiene en común algunos componentes del SS1 como son: la

detección de radiación interior (SS1.2) y la alimentación principal (SG2), estos se detallaron en la sección 3.6.1.1.

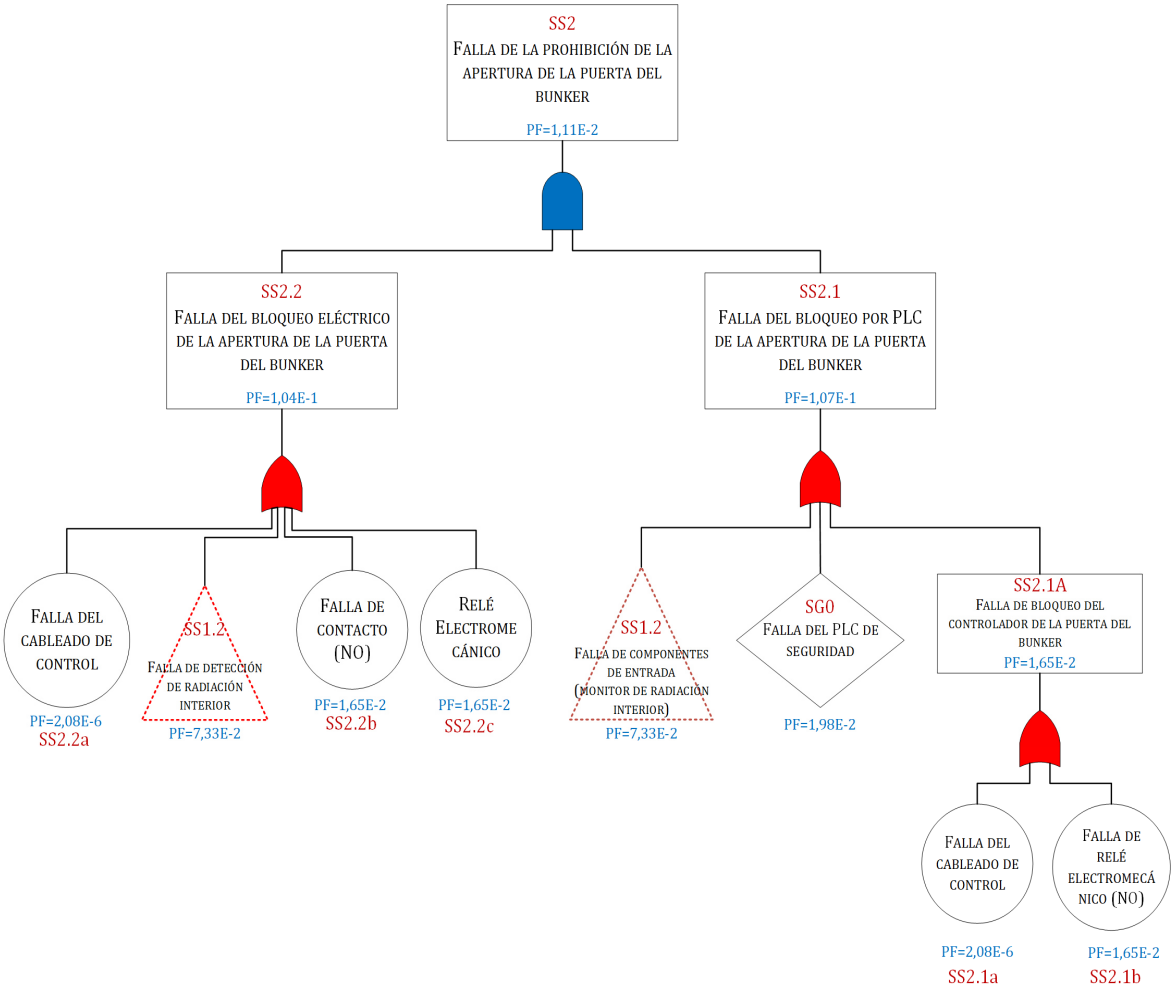


Figura 3.39. Diagrama FTA del sistema de enclavamiento de acceso al búnker – SS2 (diseño)

En el ANEXO II se detallan los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos del diagrama FTA del sistema de enclavamiento de acceso al búnker – SS2 diseñado, con base a estos, se realizó el análisis para determinar el componente básico que más influye en la falla del SS2, de igual manera al diagrama FTA del SS1, los componentes básicos de la falla de la alimentación principal (SG2) se omitieron, ya que en conjunto, tiene una probabilidad de falla baja. Por otro lado, se puede identificar que el componente que más influye en la falla del SS2 es el SS1.1d que se encuentra relacionado con el monitor de radiación de área (SS1.1A), esto se puede observar en la Figura 3.40.

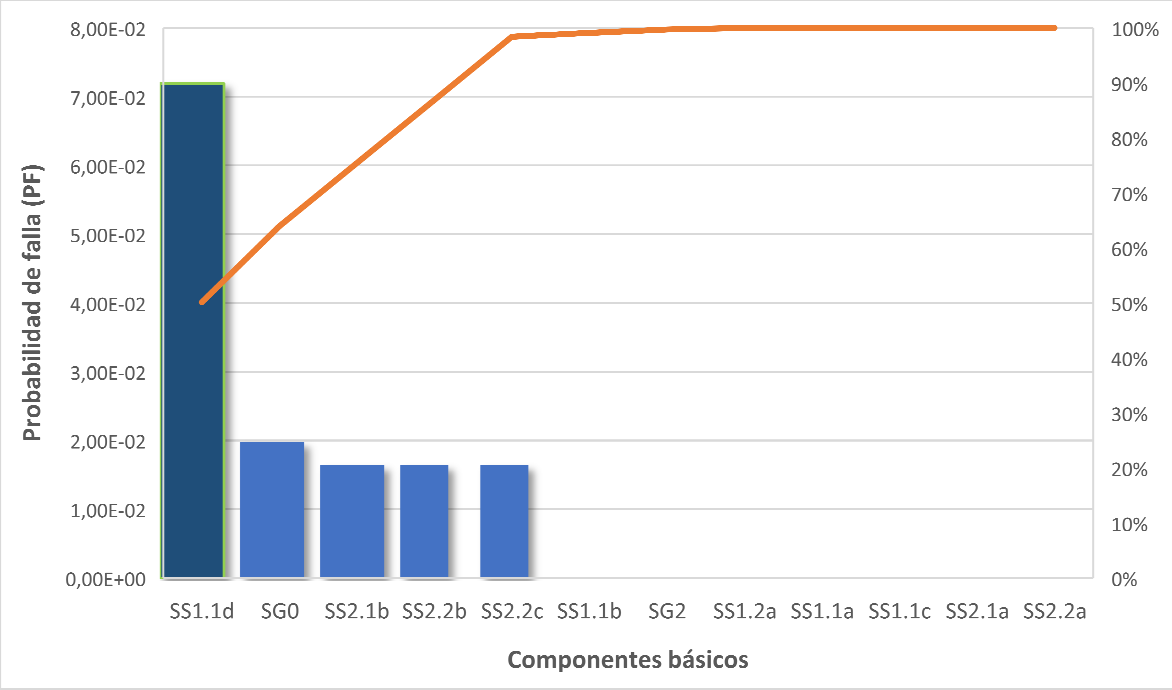


Figura 3.40. Análisis comparativo de las probabilidades de falla de los componentes del SS2 (diseñado)

3.6.1.3 Diagrama FTA del sistema de acceso al búnker con detector portátil – SS3 (diseño)

El diagrama FTA que se muestra en la **¡Error! No se encuentra el origen de la referencia.**. describe la secuencia de la falla de la prohibición del ingreso al búnker sin detector portátil del sistema de acceso al búnker.

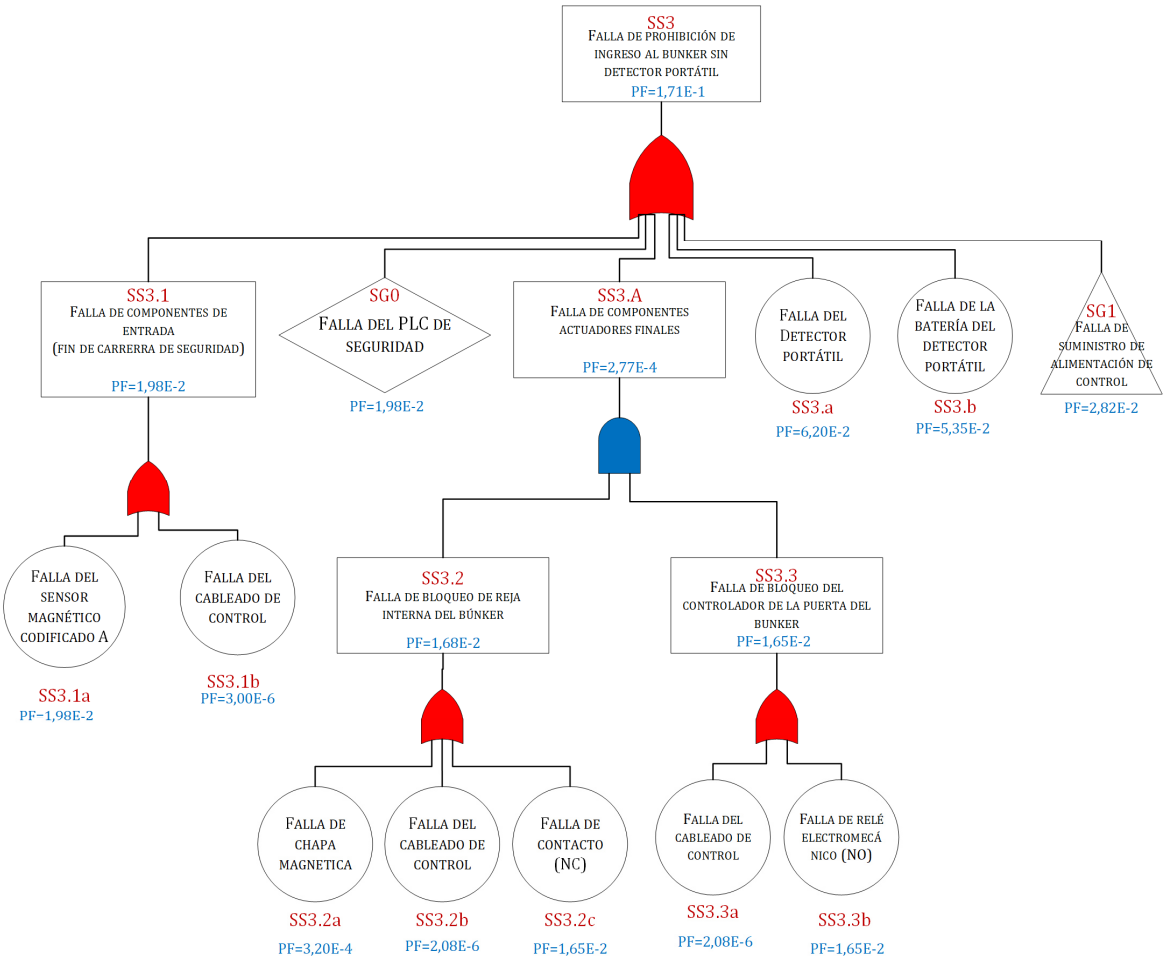


Figura 3.41. Diagrama FTA del sistema de acceso al búnker con detector portátil de radiación – SS3 (diseño)

Las probabilidades de fallo (PF) de los componentes básicos del diagrama FTA del sistema de acceso al búnker con un detector portátil se detallan en el ANEXO II. Por medio de los resultados obtenidos y la metodología FTA se realizó un análisis comparativo de los componentes para determinar los componentes más influyentes del sistema de acceso al búnker con detector portátil de radiación – SS3.

El detalle del componente SG1 y SG2 relacionados al suministro de alimentación se realizan en la sección 3.6.1.1. Los componentes básicos de las fallas de los actuadores finales (SS3.A) y falla de suministro de alimentación principal se omiten de este análisis por tener una configuración redundante y por tener una probabilidad de falla baja en su conjunto. De todo este análisis se puedo determinar que el componente más influyente en el SS3 son los relacionados con la falla del monitor

de radiación portátil (SS3.a) y la batería del este (SS3.b). Esto se puede observar en la Figura 3.42

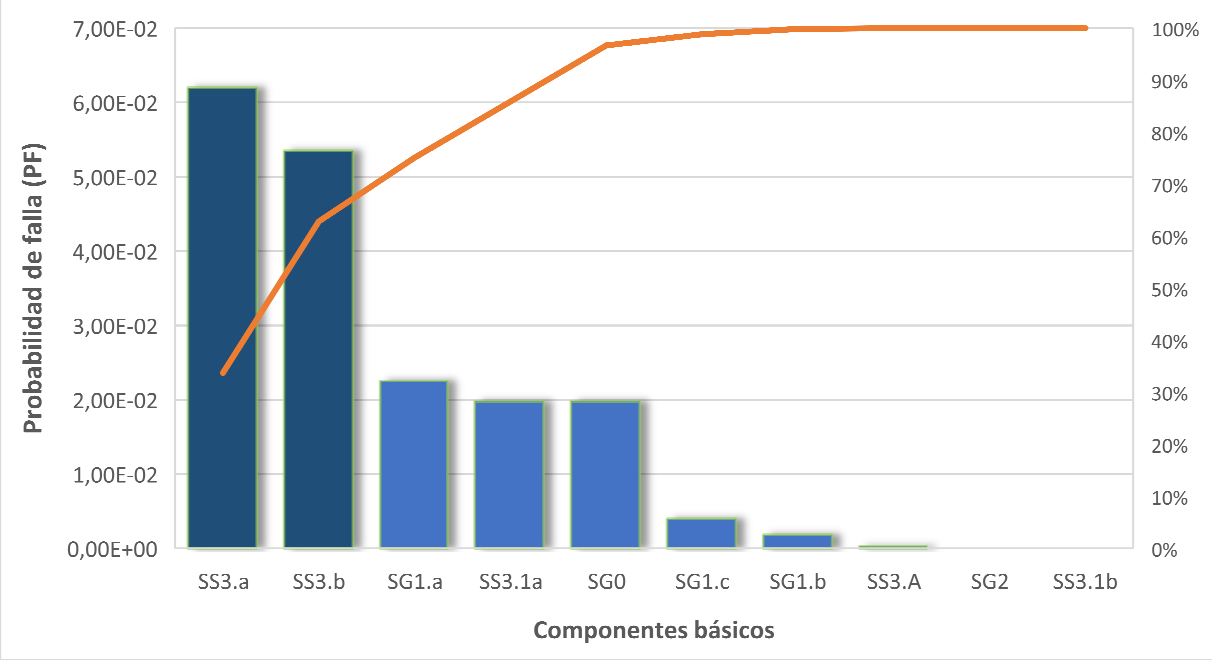


Figura 3.42. Análisis comparativo de las probabilidades de falla de los componentes básicos del SS3 (diseñado)

3.6.2 DIAGRAMAS FTA DE LOS SIS QUE INTERVIENE EN EL EVENTO INICIANTE EVI6

3.6.2.1 Diagrama FTA del sistema de detección de radiación exterior – SS4 (diseño)

La secuencia de la falla de la detección de radiación en la superficie del sistema de detección de radiación exterior se describe en el diagrama FTA que se muestra en la Figura 3.43. El detalle de los diagramas FTA de los componentes del SG1 y SG2 se lo realizó en la sección 3.6.1.1.

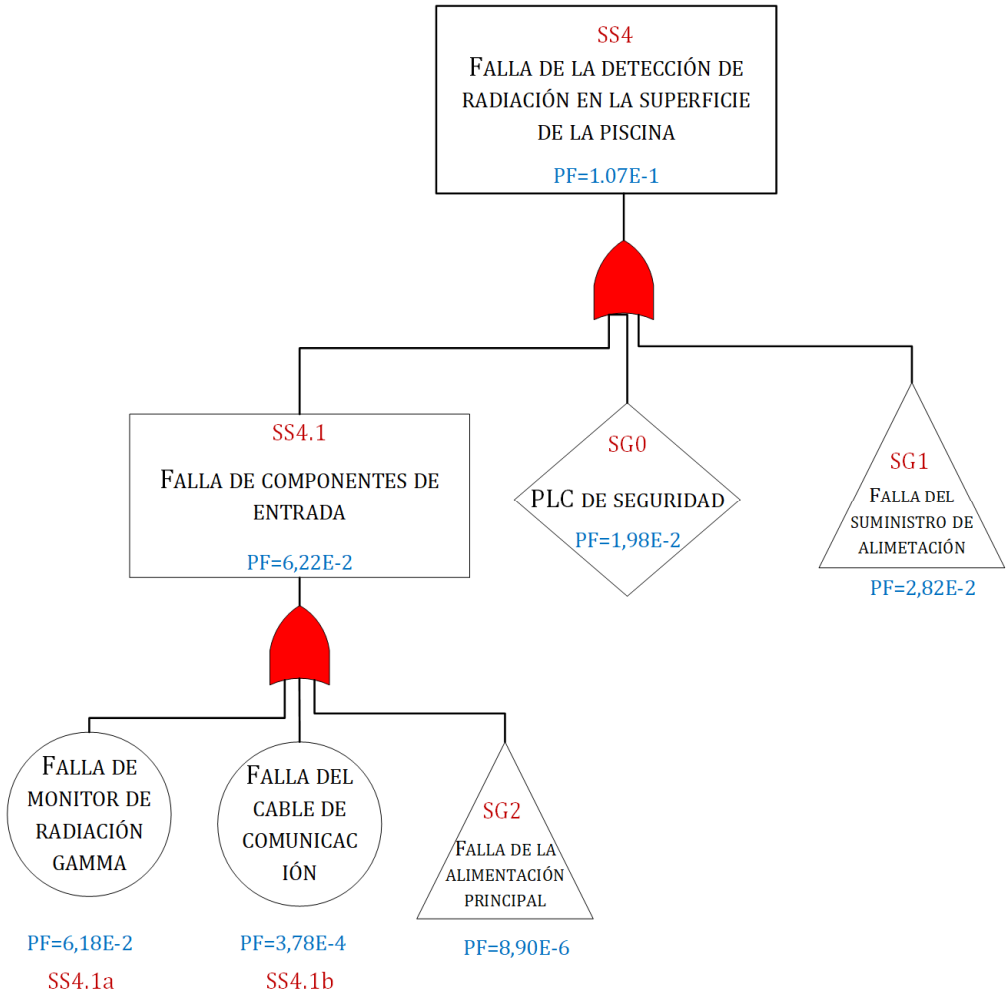


Figura 3.43. Diagrama FTA del sistema de detección de radiación exterior – SS4 (diseño)

Los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos del diagrama FTA del sistema de detección de radiación exterior se detallan en el ANEXO II. A partir de estos resultados y por medio del análisis con la metodología FTA se realiza una comparación para determinar los componentes básicos más influyentes en la falla del sistema de detección de radiación exterior - SS4. En este análisis se omitieron los componentes básicos que influyen en la falla de la alimentación principal (SG2) por ser despreciable en comparación a los otros componentes básicos. A través de este análisis se identificó que el componente que más influye en la falla del SS4 es el monitor de radiación gamma (SS4.1a). Esto se puede observar en la Figura 3.44.

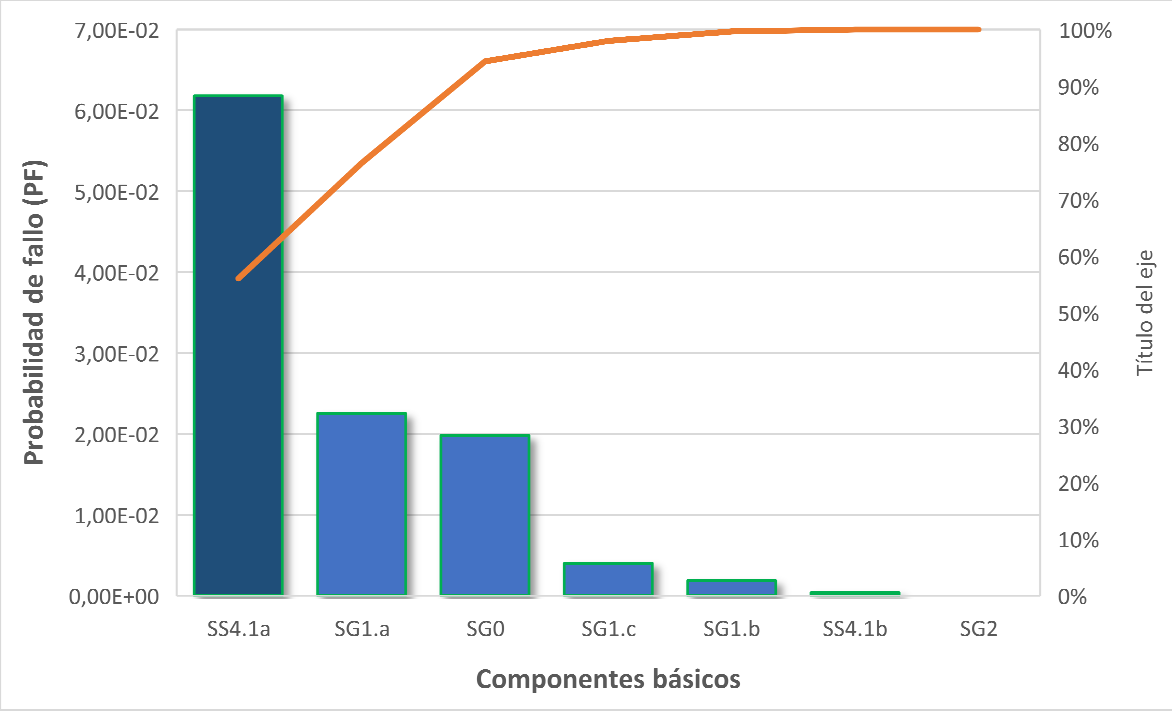


Figura 3.44. Análisis comparativo de las probabilidades de falla de los componentes básicos del SS4 (diseño)

3.6.2.2 Diagrama FTA del control de nivel de blindaje húmedo – SS5 (diseño)

Los diagramas FTA que se muestran en las Figuras 3.45, 3.46 y 3.47 describen la secuencia de la falla de la reposición del agua en la piscina del control de nivel de blindaje húmedo (piscina) diseñado.

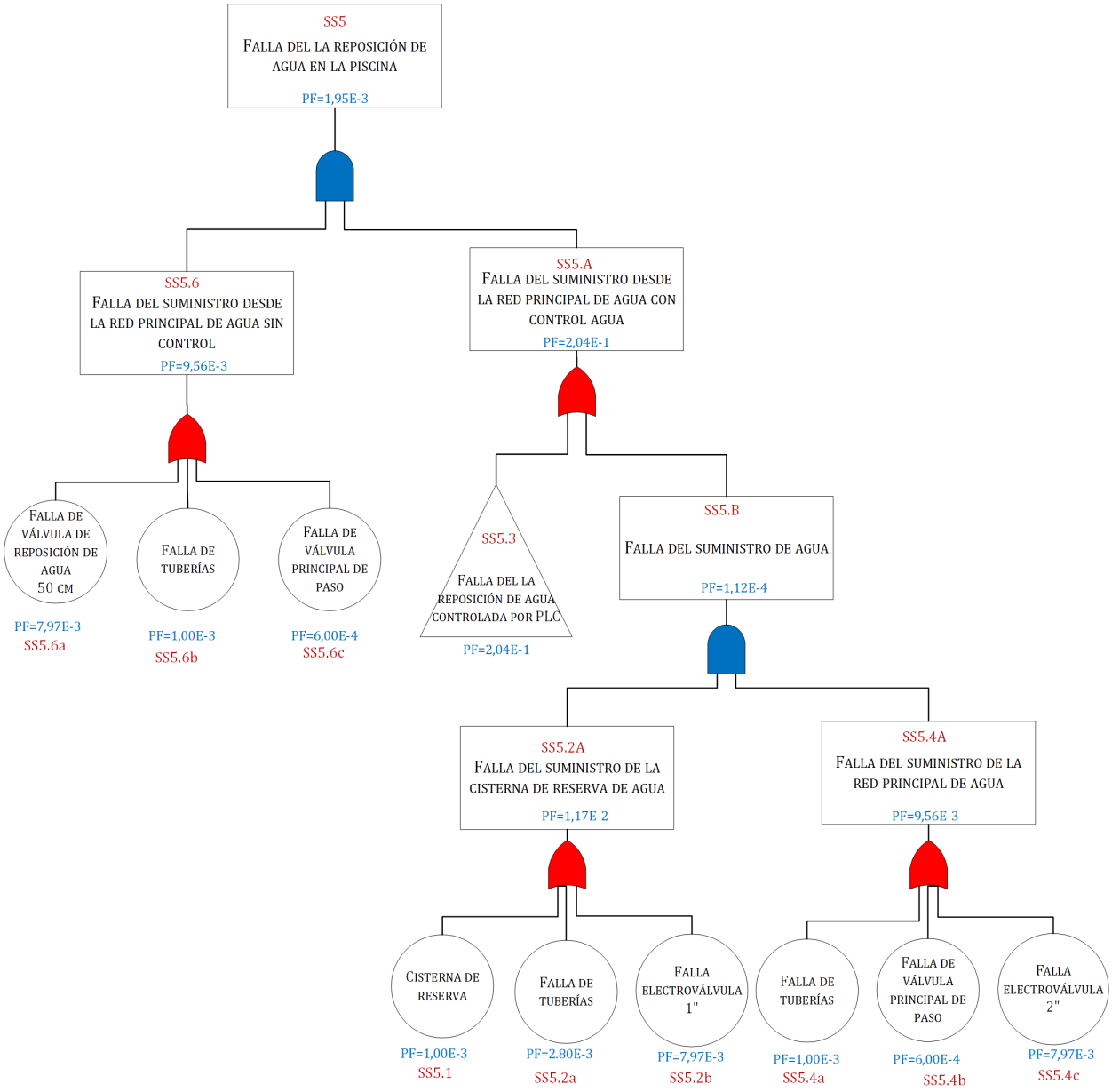


Figura 3.45. Diagrama FTA del control de nivel del blindaje húmedo – SS5 (diseño)

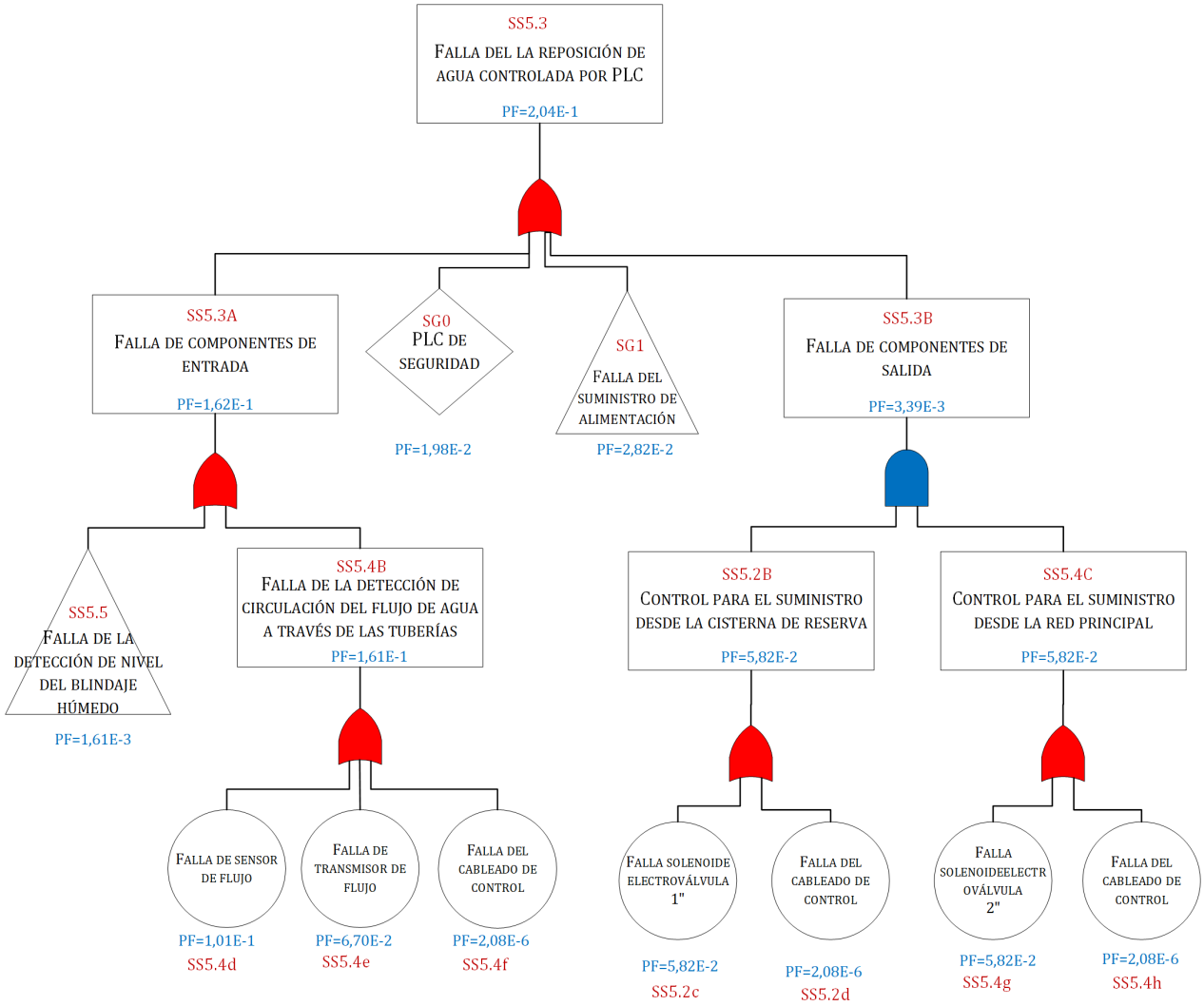


Figura 3.46. Diagrama FTA del control de nivel del blindaje húmedo – SS5.3 (diseño)

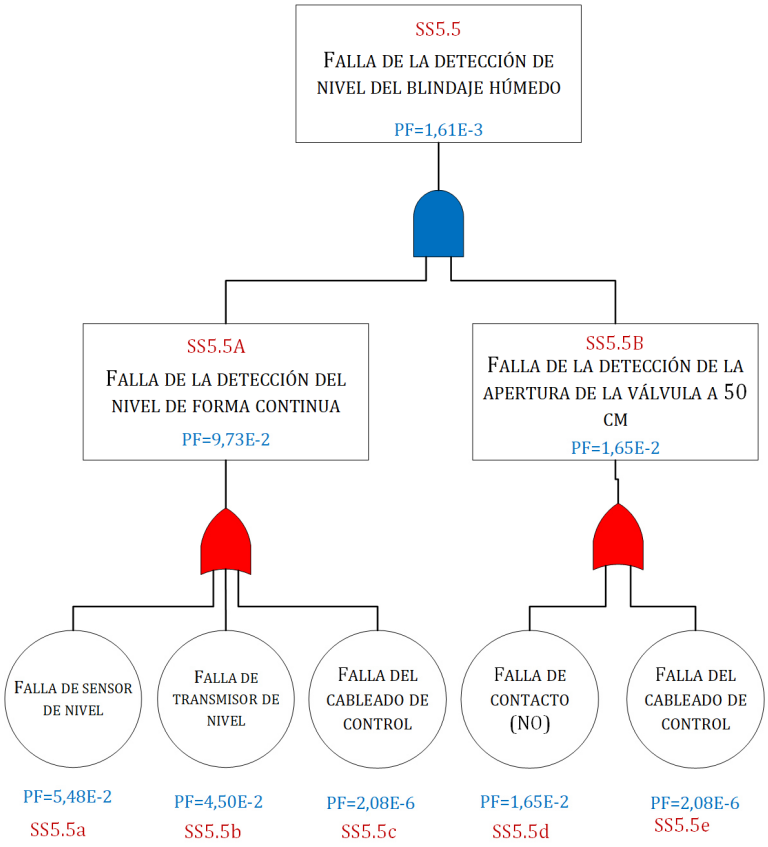


Figura 3.47. Diagrama FTA del control de nivel del blindaje húmedo – SS5.5 (diseño)

Los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos de los diagramas FTA del sistema de control del nivel de blindaje húmedo se detalla en el ANEXO II. A partir de estos resultados y de la metodología FTA se realizó un análisis comparativo de las probabilidades de fallo de los componentes básicos del sistema de control de nivel de blindaje húmedo - SS5. En este análisis comparativo se omitieron los componentes básicos relacionados a la falla del suministro del agua (SS5.B), falla de componentes de salida (SS5.3B), falla de detección del nivel de blindaje húmedo (SS5.5) y falla de la alimentación principal (SG2). Esto debido a que sus configuraciones redundantes disminuyen la influencia de estos en la falla general del sistema SS5. Además, se pudo identificar que los componentes que más influyen en la falla del sistema de nivel de blindaje húmedo son la falla del sensor de flujo (SS5.4d) y la falla del transmisor de flujo (SS5.4e). Esto se puede observar en la Figura 3.48.

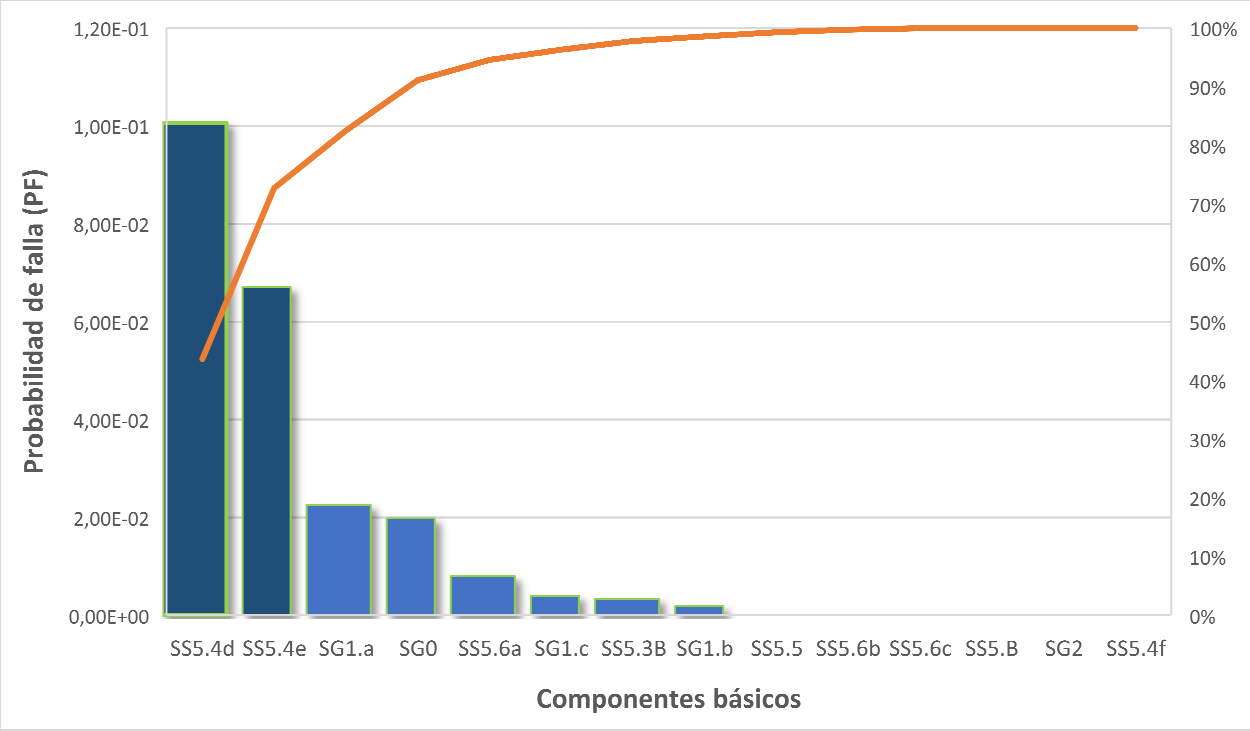


Figura 3.48. Análisis comparativo de las probabilidades de falla de los componentes básicos del SS5 (diseño)

3.6.2.3 Diagrama FTA del sistema de alarmas interiores – SS8 (diseño)

El diagrama FTA que se muestra en la Figura 3.49. describe la secuencia de falla del aviso al personal de la pérdida del blindaje húmedo del sistema de alarmas interiores diseñado.

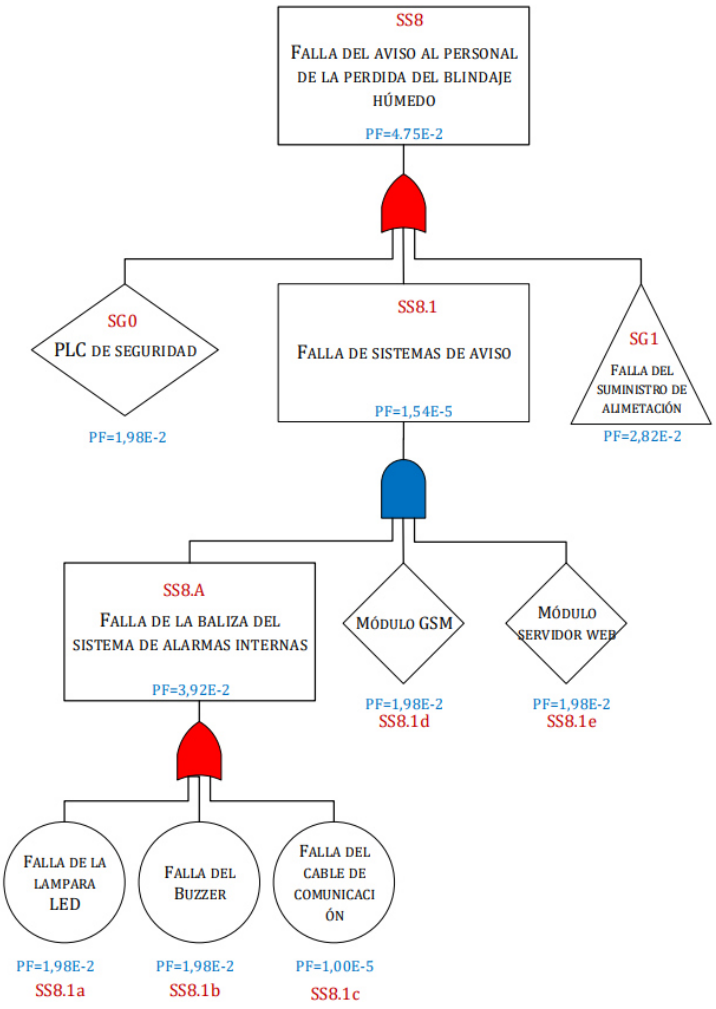


Figura 3.49. Diagrama FTA del sistema de alarmas interiores – SS8 (diseño)

Los resultados de los cálculos realizados para determinar las probabilidades de fallo (PF) de los componentes básicos del diagrama FTA del sistema de alarmas interiores – SS8 se detallan en el ANEXO II. A partir de la metodología FTA y de los datos de las probabilidades de fallo, se realiza un análisis comparativo para determinar el componente básico más influyente en la falla de aviso al personal de la pérdida del blindaje húmedo. Con base al anterior análisis se determinar que este sistema tiene más probabilidad de falla los componentes relacionados a la falla del suministro de la alimentación (SG1) y la falla del PLC (SG0). Esto se puede observar en la Figura 3.50.

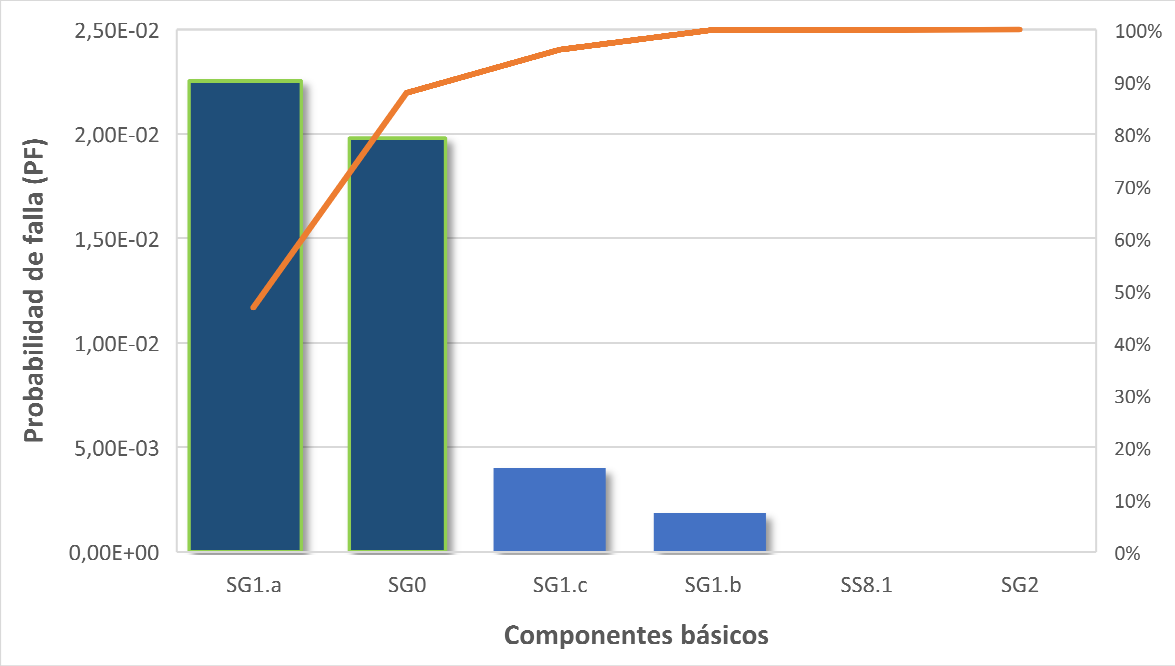


Figura 3.50. Análisis comparativo de las probabilidades de falla de los componentes básicos del SS8 (diseño)

3.6.3 DIAGRAMAS ETA DE EVENTOS INICIANTES

3.6.3.1 Análisis del evento iniciante EVI5

Para este análisis se tuvieron las mismas consideraciones mencionadas en la sección 3.3.5.1, sin embargo, la diferencia radica en que, para este análisis se consideró un SIS adicional que obliga a que el operador ingrese con un detector portátil al búnker. Este nuevo sistema tiene el objetivo de reducir la ocurrencia anual de la exposición potencial del POE. Además, para los SIS diseñados se siguieron las especificaciones de los requerimientos de seguridad mostrados en la Tabla 3.11.

En la Figura 3.51 se indica el diagrama ETA que se elaboró con base al evento iniciante EVI5 y los sistemas SS1, SS2 y SS3 de los SIS diseñados que se detallaron en la Tabla 3.12.

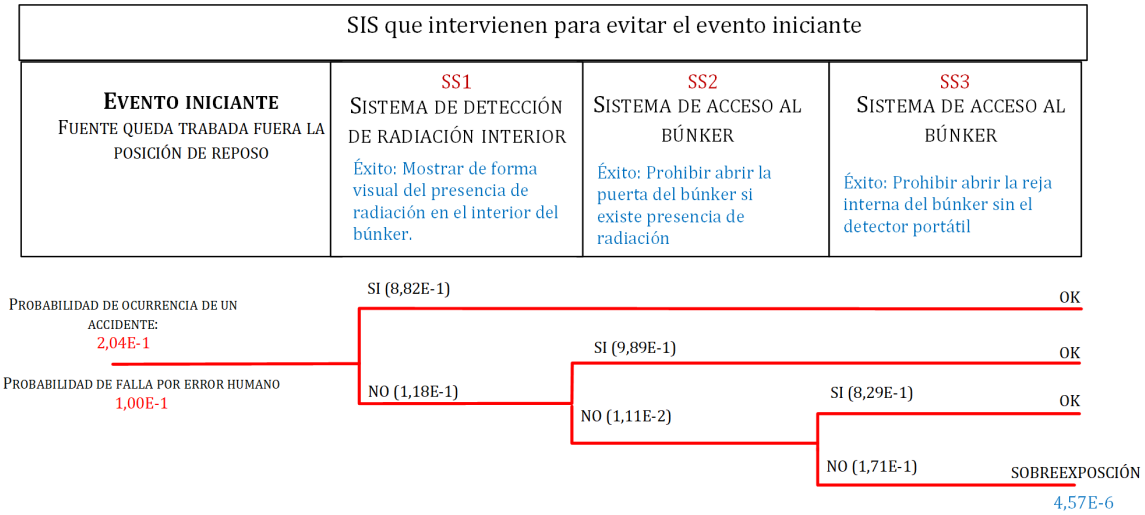


Figura 3.51. Diagrama ETA del evento iniciante EVI5 (diseño)

3.6.3.2 Análisis del evento iniciante EVI6

Para este análisis se tuvo las mismas consideraciones mencionadas en el subcapítulo 3.3.5.2 con el objetivo de reducir la ocurrencia anual de la exposición potencial del POE. Además, para los SIS diseñados se siguieron las especificaciones de los requerimientos de seguridad mostrados en la Tabla 3.11. En la Figura 3.52 se indica el diagrama ETA que se elaboró con base al evento iniciante EVI6 y los Sistemas SS4, SS5 y SS8 de los SIS diseñados que se detallaron en la Tabla 3.12

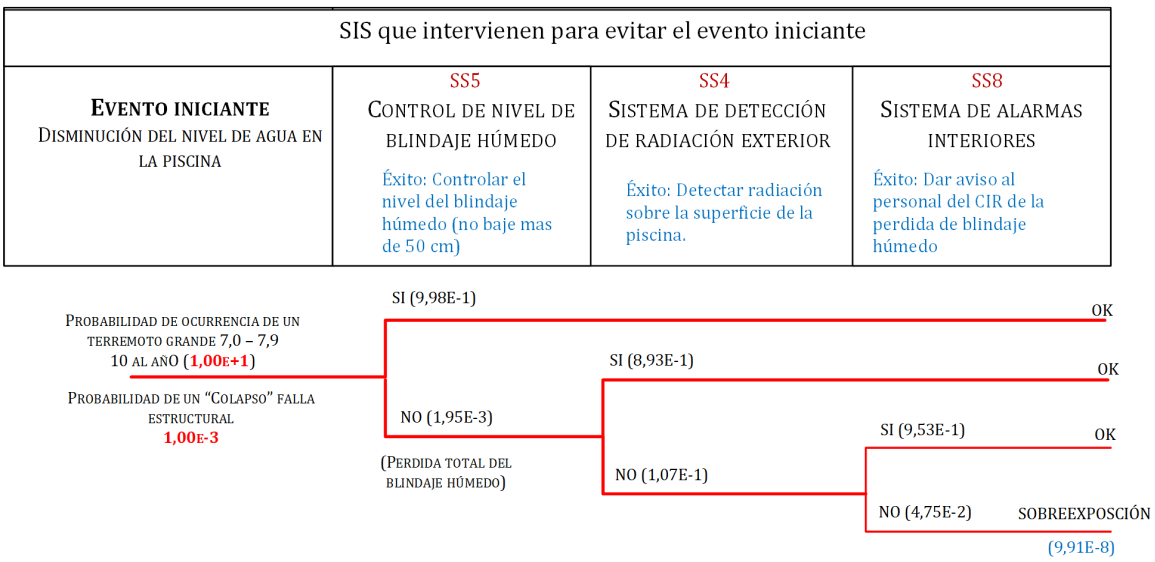
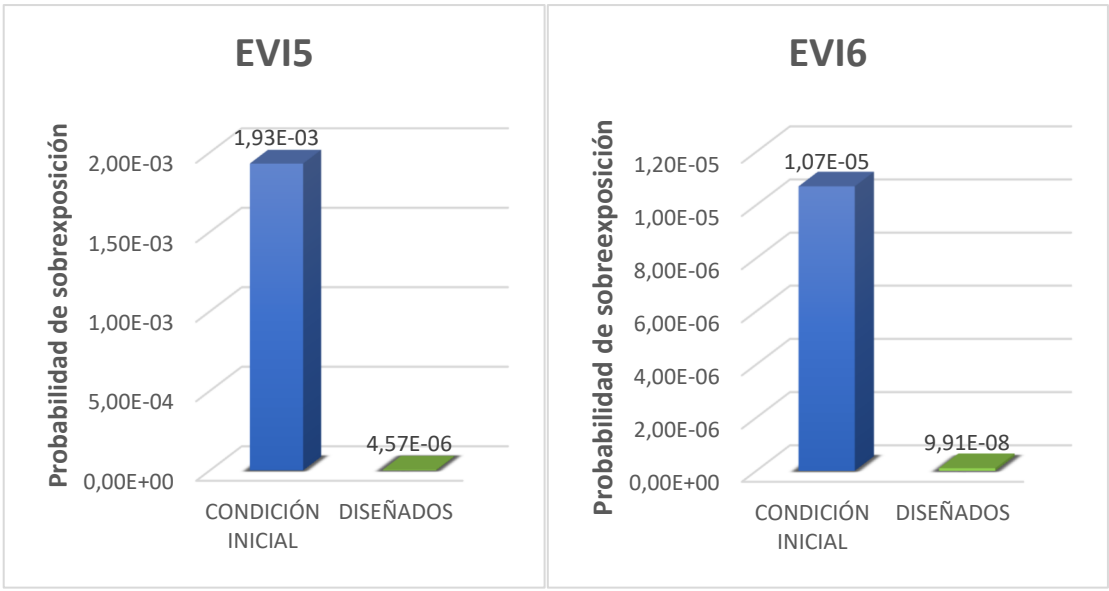


Figura 3.52. Diagrama ETA del evento iniciante EVI6 (diseño)

Además, se realizó una comparación de las probabilidades de sobreexposición para el POE, considerando los sistemas instrumentados de seguridad en condiciones iniciales diseñados para los eventos iniciantes EVI5 y EVI6, esto se ilustra en la Figura 3.53.



(a) (b)

Figura 3.53. Comparación de las probabilidades de sobreexposición considerando los SIS en condiciones iniciales y los SIS diseñados: a) Comparación con respecto al evento iniciante 5, b) Comparación con respecto al evento Iniciante 6

3.6.4 ESTIMACIÓN DE DOSIS EFECTIVA RECIBIDA POR EL POE

Las estimaciones de las dosis efectivas recibidas por el POE son las mismas a las calculadas en la sección 3.3.6, en el que se consideró que la evaluación en esta etapa es para 50 000 Ci, ya que el diseño de los nuevos SIS elaborados tiene por objetivo trabajar con la fuente de Co-60 repotenciada. Por lo tanto, los datos de las estimaciones recibidas en los puntos A, B y C son:

Tabla 3.20. Estimación de dosis efectiva en los puntos de evaluación A, B y C para 50 000 Ci con los diseños desarrollados

Estimación de dosis efectiva		
Tiempo de exposición:		**1 minuto**
	Probabilidad anual	Dosis efectiva (mSv)
Punto A' (50 000 Ci)	4,57E-06	85 648,15
Punto B' (50 000 Ci)	4,57E-06	533,82
Punto C' (50 000 Ci)	9,91E-08	381,66

3.6.5 DISCUSIÓN DE LOS RESULTADOS OBTENIDOS

Se realizó una comparación de los resultados obtenidos entre los SIS en condiciones iniciales y los SIS diseñados. Se consideraron los puntos de evaluación A y B relacionado al EVI5 y al punto C relacionado con el EVI6. Además, se consideró la actividad de la fuente de Co-60 en 50 000 Ci

En la Figura 3.54. Se puede observar los resultados cuantitativos obtenidos. Por medio de la metodología del APS, se puede apreciar que los SIS diseñados han tenido una reducción considerable en cuanto a la probabilidad de ocurrencia anual de una exposición potencial del POE. Para los puntos de evaluación considerados con el evento iniciante EVI5, el factor de reducción del riesgo es de 404 veces y para el evento iniciante EVI6 el factor de reducción del riesgo es de 107 veces, el detalle para la determinación del factor de reducción de riesgo se encuentra en el ANEXO VIII.

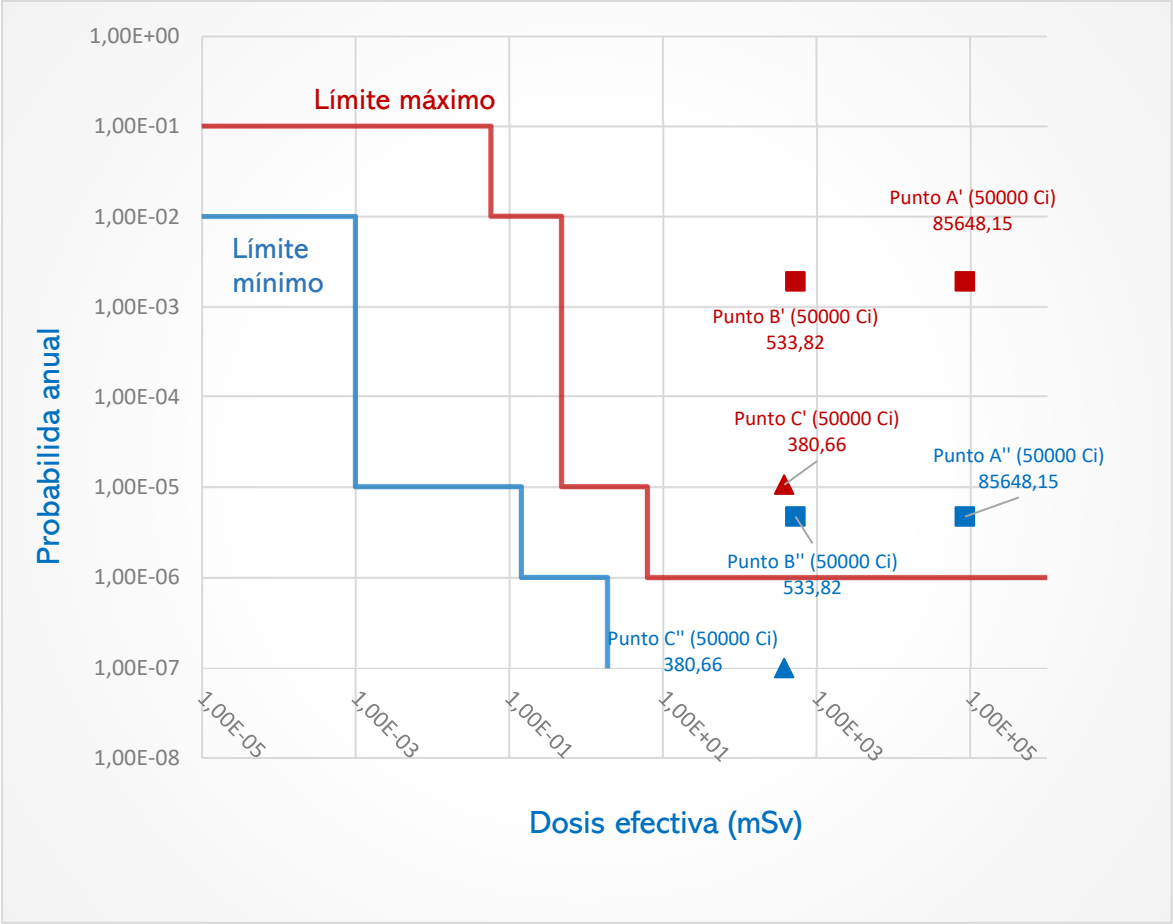


Figura 3.54. Comparación de resultados entre los SIS iniciales y los SIS diseñados.

- SIS iniciales del Irradiador de Co-60: Puntos A', B' y C' de color rojo
- SIS diseñados del irradiador de Co-60: Puntos A'', B'' y C'' de color azul

Los SIS relacionados con el EVI6 si cumplen con los objetivos de seguridad planteados, por lo que no es necesario modificar o añadir más barreras o sistemas de seguridad, sin embargo, es imprescindible que en la implementación de los sistemas se consideren las especificaciones de los requerimientos de seguridad definidos en la Tabla 3.11.

Se puede observar con relación al evento iniciante EVI5, es que aún no están dentro de la región definida por nuestros objetivos de seguridad, por tal motivo, para los SIS que intervienen con este evento iniciante, es necesario realizar alguna modificación adicional o si es posible añadir otra barrera de protección. Sin embrago, para que el evento EVI5 esté dentro de los objetivos de seguridad radiológica (menor a 1,00E-6) se requiere una reducción del riesgo de 5,75 veces.

Lo que significa que no requiere incrementar el grado SIL, sino que, solo es necesario mejorar los SIS que puedan intervenir con el evento iniciante en mención.

Por lo anteriormente mencionado, se puede decir que, una opción a evaluar para alcanzar el objetivo de seguridad con relación al evento iniciante EVI5, es mejorar el sistema de enclavamientos de subida del rack de la fuente de Co-60 – SS6 de los sistemas actuales indicado en la Tabla 3.2. Esto debido a que, el SIS – SS6 influye directamente en la probabilidad de ocurrencia de un accidente como se indica en la sección 3.3.5.1. Esta opción sería la más viable para no incurrir en costos exagerados para la implementación de los nuevos diseños de los SIS.

3.7 PROPUESTA DE PROCEDIMIENTOS DE OPERACIÓN Y MANTENIMIENTO

Desde el punto de vista de seguridad funcional, se consideró generar las directrices requeridas para los procedimientos de operación y mantenimiento de los siguientes SIS diseñados y que son los que tienen la funcionalidad de prevenir las consecuencias de los eventos iniciantes, sin embargo, es necesario recalcar que, debido al alcance del presente proyecto solo se definieron las directrices para los procedimientos de los siguientes SIS:

- Sistema de enclavamiento de acceso al búnker – SS2
- Sistema de control de nivel del blindaje húmedo – SS5

El sistema integrado de gestión del CIR posee varios procesos y procedimientos de los SIS evaluados inicialmente. Sin embargo, para los SIS diseñados en este proyecto, se detallan en los siguientes subcapítulos las directrices que se deberían adicionar al sistema integrado de gestión del CIR y a los procedimientos de operación y mantenimiento del irradiador de Co-60 y sus registros respectivos. Esto se lo debe hacer una vez que los sistemas diseñados sean implementados, considerando las características finales de los componentes instalados en los SIS.

3.7.1 DIRECTRICES PARA LOS PROCEDIMIENTOS DEL SISTEMA DE ENCLAVAMIENTO DE ACCESO AL BÚNKER – SS2

Las directrices más importantes que requiere el sistema de enclavamientos de acceso al búnker indicado en la Figura 3.55 se detallan a continuación.

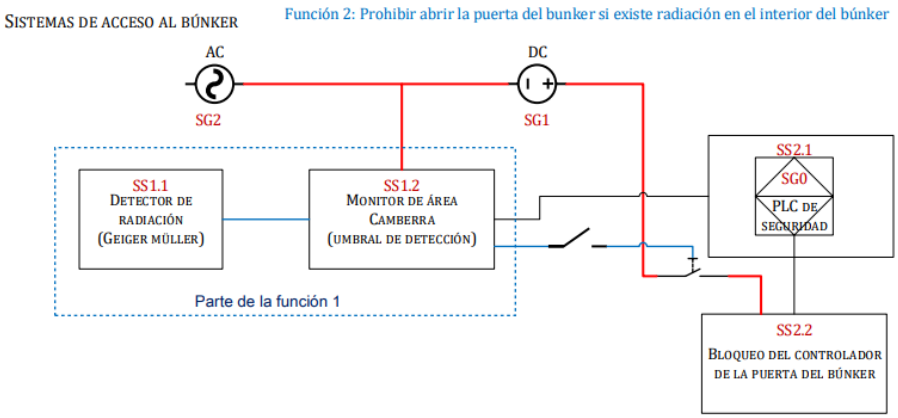


Figura 3.55. Diagrama de bloques del Sistema de enclavamientos de acceso al búnker – SS2 (diseño)

3.7.1.1 Actividades de la operación rutinaria del SIS - SS2

- Previo a iniciar un proceso de irradiación se realizará una prueba de verificación del estado de componentes del SIS – SS2 desde el HMI.
- El sistema iniciará su funcionamiento con la activación del punto de ronda, no requiere de una activación manual del sistema, debido a que este comenzará automáticamente una vez que el irradiador este armado y la puerta se cierre para iniciar un proceso de irradiación.
- Para desactivar el funcionamiento del sistema, se deberá bajar la fuente de Co-60 a una posición blindada y la disminución del nivel de radiación por debajo del umbral de seguridad establecido detectado por el sistema, habilitará automáticamente el control de la apertura de la puerta.

Nota: es necesario recordar que el SIS - SS2 depende del detector de radiación que forma parte del SS1 y este se encuentra en un punto caliente en el exterior

del búnker para determinar la presencia de radiación en el interior de esté, por lo que, durante el proceso de irradiación no se debería apagar el detector de radiación, mover el detector de radiación para otro uso o mover la sonda de detección.

3.7.1.2 Actividades de la operación en condiciones anormales del SIS – SS2

1. Pérdida de energía eléctrica de la red principal. El sistema de control del irradiador de Co-60 debe poseer un sistema adicional de respaldo de energía que permita la funcionalidad del detector de radiación y del SIS – SS2, por tal motivo, en caso de pérdida de energía eléctrica de la red principal, se verificará por medio de una inspección visual el funcionamiento del detector de radiación y si es posible el nivel de radiación al interior de búnker (el nivel debería ser bajo ya que, el sistema de control del irradiador desactiva el freno del rack de la fuente de Co-60 y esta debería descender por gravedad)

2. El nivel de radiación en el detector no desciende por debajo del umbral de seguridad establecido. Si al terminar un proceso de irradiación, el nivel de radiación no disminuye por debajo del umbral de seguridad, se debe prohibir cualquier operación y proceder a realizar una inspección de los sistemas en compañía del Oficial de Seguridad Radiológica con estricto respeto a los procedimientos de protección radiológica establecidos por el Centro de irradiación para posibles incidentes radiológicos.

3. El control de la puerta no se habilita luego de que el nivel de radiación está por debajo del umbral de seguridad establecido. Si al terminar un proceso de irradiación no se puede habilitar el control de la puerta aun cuando el nivel de radiación está por debajo del umbral de seguridad establecido, se debe reiniciar el detector de radiación y revisar si no existe algún mensaje de advertencia en el HMI del irradiador de Co-60.

3.7.1.3 Actividades de pruebas de verificación del SIS – SS2

La verificación del sistema de seguridad se realizará por medio de una forma digital a través del HMI del sistema de control del irradiador de Co-60, este sistema tendrá una opción de verificación del estado de los componentes que conforma el SIS. Esta verificación determinará si el bus de comunicación con el detector de radiación está funcionando y si el detector de radiación responde a las solicitudes del sistema de control del Irradiador de Co-60. Además, esta prueba verificará si existe conectividad con el sistema de control de apertura de la puerta, esta conectividad debe estar en el rango de 4 a 20 mA para indicar su estado idóneo para el funcionamiento, esta verificación se la realizará al inicio de un proceso de irradiación.

Además de la verificación del estado de los componentes, se realizará la comprobación de la funcionalidad por medio del uso de fuentes de prueba y la modificación del umbral de seguridad del detector de radiación. Estas pruebas se realizarán con referencia a los procedimientos especificados por el fabricante del detector de radiación y con cumplimiento estricto de las normativas de protección radiológica, esta prueba de verificación de funcionalidad se las recomienda realizar con una periodicidad de 6 meses.

3.7.1.4 Actividades de mantenimiento del SIS – SS2

Para realizar las actividades de mantenimiento se deberá ingresar en el HMI a la funcionalidad de mantenimiento para entrar en un modo seguro de trabajos de mantenimiento (en esta función de mantenimiento se deshabilita el control de subida de la fuente de Co-60)

Las actividades de mantenimiento se realizarán con una periodicidad de 6 meses y estas actividades involucran la prueba de verificación de la funcionalidad del sistema y la prueba de verificación del estado de componentes, además se deberán reajustar los bornes correspondientes a las conexiones del SIS – SS2

3.7.1.5 Registros del SIS – SS2

Los registros requeridos para el sistema de control de acceso al búnker diseñado son:

a) Registros de operación:

- Registro de la medición del nivel de radiación en cada proceso de irradiación.
- Registro de las fechas y horas en las que el sistema ha pasado el umbral de seguridad, ya sea hacia arriba o hacia abajo.

b) Registros de mantenimiento

- Registro del tiempo de mantenimiento (preventivos o correctivos) del SIS-SS2 en horas (MTTR).
- Registro de fallas del SIS – SS2 (fallas funcionales o fallas de componentes).
- Registro de todas las demandas de seguridad durante el acondicionamiento del umbral de seguridad.
- Registro de las fechas y horas de la realización de las verificaciones del estado de componentes y de la verificación de la funcionalidad del sistema.

Estos registros se deben incorporar al sistema de gestión integrado del CIR cuando se implementen el SIS – SS2 diseñado.

3.7.2 DIRECTRICES PARA LOS PROCEDIMIENTOS DEL SISTEMA DEL CONTROL DE NIVEL DEL BLINDAJE HÚMEDO – SS5

Las directrices más importantes que requiere el sistema de control de nivel de blindaje húmedo indicado en la Figura 3.56 se detallan a continuación.

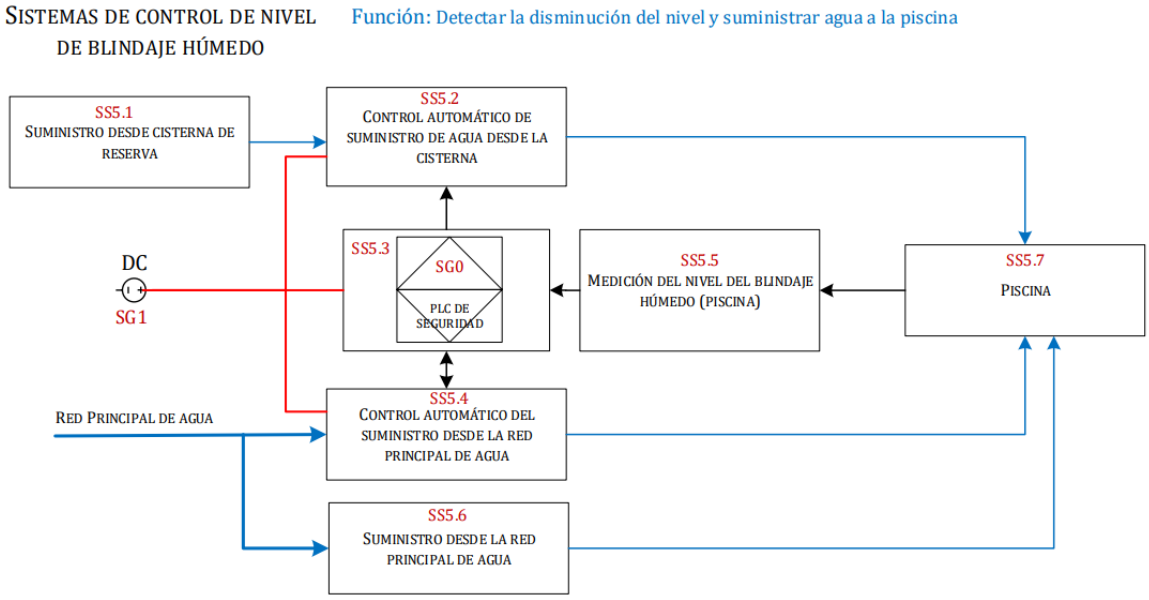


Figura 3.56. Diagrama en bloques del sistema de control de nivel de blindaje húmedo (diseño)

3.7.2.1 Actividades de la operación rutinaria del SIS – SS5

- El sistema trabaja de manera continua e independiente al proceso de irradiación y de forma automática. Se realizan verificaciones periódicas del estado de los componentes del SIS – SS5.
- Si el sensor de nivel continuo detecta una disminución de más de 3 cm de la superficie. Se activa la reposición de agua desde la cisterna de reserva. Si luego de un tiempo no se restablece el nivel del agua, se activa la reposición desde la red principal de agua.
- Si el sensor de nivel continuo detecta una disminución de más de 50 cm de la superficie, se activa la reposición de agua desde la red principal.
- Si el nivel de agua no se restablece, se activará la reposición desde la red principal de manera mecánica y automática por medio de la válvula de boya y se generará una señal de alerta al sistema de alarmas interiores.

3.7.2.2 Actividades de la operación en condiciones anormales del SIS – SS5

1. Pérdida de energía eléctrica de la red principal. El sistema de control del irradiador de Co-60 debe poseer un sistema adicional de respaldo de energía que permita la funcionalidad del SIS – SS5, por tal motivo, en caso de pérdida de energía eléctrica de la red principal, el sistema deberá ser operativo, es decir que debe seguir cumpliendo sus funciones de seguridad.

2. Se activa la reposición de agua desde la cisterna y no se restablece el nivel del blindaje. En este caso, el sistema registrará la eventualidad y lo notificará al operador del irradiador por medio de la pantalla HMI para que se realice una revisión del nivel de agua de la cisterna de reserva y una verificación del funcionamiento de electroválvulas, si los sistemas están funcionales, se debe verificar alguna fuga en la piscina***.***

3. Se activa la reposición de agua desde la red principal y no se restablece el nivel. En este caso, el sistema deberá enviará una señal al sistema de alarmas interiores para verificar inmediatamente la funcionalidad del sistema, electroválvulas, sensores de nivel, conexiones etc.

4. Se activa la válvula de boya. En este caso, el sistema enviará una señal al sistema de alarmas interiores y se deberá atender este evento de forma urgente, ya que puede significar la pérdida de la integridad estructural de la piscina.

3.7.2.3 Actividades de pruebas de verificación del SIS – SS5.

El sistema tendrá incorporado una prueba de verificación de componentes, la misma que se puede realizar bajo demanda desde el HMI. Esta prueba se la ejecuta de manera periódica y será un proceso vigilado por el oficial de protección radiológica de ser necesario, sin embargo, es requerido almacenar la fuente en el búnker previo a esta verificación.

3.7.2.4 Actividades de mantenimiento del SIS – SS5

Las actividades de mantenimiento de este sistema serán la verificación de funcionalidad de circuitos de reposición de agua y el funcionamiento de electroválvulas y componentes del sistema, además se deberán ajustar las conexiones de todos los componentes que son parte de este sistema, luego de esto se realizará una prueba de verificación del estado de los componentes.

Una vez al año se verificará la funcionalidad y la calibración del sensor de nivel, ya sea en el sitio por medio de herramientas o equipos que permitan hacer esta actividad o por medio del retiro del sensor del sistema para realizar las pruebas de calibración fuera de la piscina.

La prueba de verificación de la funcionalidad del sistema será solo 1 vez al año y es necesario realizar previamente una prueba de verificación del estado de los componentes del sistema.

3.7.2.5 Registros del SIS – SS5

Los registros requeridos por el sistema de control de nivel de blindaje húmedo son:

a) Registros de operación:

- Registro de la medición del nivel de agua en la piscina en forma de histórico
- Registro del de fecha hora y el tiempo de activación de los sistemas de reposición de agua
- Registro de fechas y horas de las pruebas de verificaciones de estado automáticas y sus resultados

b) Registros de mantenimiento.

- Registro del tiempo de mantenimiento (preventivos o correctivos) del SIS-SS2 en horas (MTTR)
- Registro de fallas del SIS – SS2 (fallas funcionales o fallas de componentes)

- Registro de todas las demandas de seguridad durante el acondicionamiento y puesta en marcha del sistema
- Registro de las fechas y horas de la realización de las verificaciones del estado de componentes y de la verificación de la funcionalidad del sistema.

Estos registros se deben incorporar al sistema de gestión integrado del CIR cuando se implementen el SIS – SS5 diseñado.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

1. Por medio de la aplicación de la metodología APS nivel 1 cuantitativa y referencias bibliográficas, se estableció que para los sistemas de seguridad actuales existe la probabilidad de ocurrencia de una exposición potencial para el POE con un nivel de riesgo fuera de los límites de seguridad radiológica establecidos por el Consejo Internacional de Protección Radiológica (ICRP) con relación a la probabilidad de falla de los sistemas de seguridad y en relación a dos eventos iniciantes analizados en el presente proyecto bajo el supuesto de 2000 horas laboradas al año.

2. Se determinaron las arquitecturas de los SIS necesarias para el sistema de enclavamientos del acceso al búnker y para el sistema de control de nivel del blindaje húmedo con base a las especificaciones de los requerimientos de seguridad proporcionados por el enfoque de la seguridad funcional de los estándares IEC 61508 e IEC 61511.

3. La reevaluación con la metodología APS nivel 1 cuantitativa de los sistemas rediseñados con el enfoque de seguridad funcional cumplieron con los límites de seguridad radiológica permitidos (para exposiciones > a 2 000 mSv la probabilidad de ocurrencia anual debe ser < 1,00E-6) establecidos por el Consejo Internacional de Protección Radiológica (ICRP) para una operación del irradiador de Co-60 con una actividad de 50 000 Ci.

4. Se propusieron las directrices y lineamientos más adecuados para la ejecución de las actividades de operación y mantenimiento del sistema de enclavamiento de acceso al búnker y de control de nivel de blindaje húmedo, basado en las recomendaciones de los estándares IEC 61508 e IEC 61511 con el objetivo de garantizar que los SIS funcionen dentro de las especificaciones de los requerimientos de seguridad establecidos.

5. Con la metodología APS y con el enfoque de seguridad funcional se logró rediseñar los sistemas de seguridad y se obtuvo un factor de reducción de riesgo de 404 veces para el evento no deseado de exposición potencial para el POE por encima de los 2 000 mSv (dosis efectiva) generado por el evento iniciante que se consideró en el caso de que el rack de la fuente de Co-60 se trabara fuera de su blindaje. Así mismo se logró un factor de reducción de riesgo de 107 veces para el evento no deseado de exposición potencial para el POE por encima de los 2 000 mSv (dosis efectiva) generado por un evento iniciante relacionado a la pérdida del blindaje húmedo por un evento natural.

6. La metodología FTA utilizada dentro del APS permitió identificar los componentes básicos más críticos de los SIS actuales como son: las fuentes de alimentación y el mal enrollamiento del cable y en los SIS diseñados de determino como los componentes básicos más críticos como son: el detector de radiación, el detector de radiación portátil, el sensor de flujo, falla de la fuente de control, esto permitió rediseñar estos sistemas de una manera más sistemática y eficiente.

7. El enfoque de seguridad funcional proporcionado por el estándar IEC 61508 es global al ciclo de vida de los sistemas de seguridad analizados en este proyecto, sin embargo, por el alcance de este proyecto, este enfoque permitió tener las directrices requeridas para el rediseño de los sistemas y su repotenciación con el objetivo de que del Irradiador de Co-60 preste los servicios de irradiación con una fuente de Co-60 con una actividad nominal de 50 000 Ci.

8. La metodología APS permitió que el personal del Irradiador de Co-60 obtuviera un mayor conocimiento acerca de sus sistemas de seguridad tanto preventivos como de mitigación, lo que mejoró el nivel de conciencia de los requerimientos de seguridad de las instalaciones y su intervención en el desarrollo de estos.

4.2 RECOMENDACIONES

1. Se recomienda realizar un estudio de la probabilidad de falla estructural de la piscina ante un sismo, ya que esta contiene el blindaje húmedo, esto permitirá mejorar los resultados obtenidos por la metodología APS.

2. Se recomienda realizar un estudio para el análisis del error humano en el que se evalúe al personal del Irradiador de Co-60, esto permitirá mejorar los resultados obtenidos por la metodología APS.

3. Basado en el enfoque de seguridad funcional, se recomienda realizar un análisis de probabilidad de fallo de los sistemas de seguridad informática y del software diseñado que se implementarán en el futuro por medio de un Controlador Lógico Programable (PLC).

4. Basado en el enfoque de seguridad funcional, se recomienda establecer los parámetros operacionales que deben cumplir los sistemas instrumentados de seguridad en la fase de instalación, verificación y puesta en marcha del irradiador de Co-60.

5. Basado en el ciclo de vida de los sistemas de instrumentados del enfoque de seguridad funcional, se recomienda establecer los procedimientos requeridos para la modificación, puesta en fuera de servicio de los sistemas instrumentados de seguridad.

6. Se recomienda reforzar los procedimientos de mantenimiento por medio de metodologías que permitan establecer parámetros como son el tiempo medio de reparación (MTTR) o el tiempo medio entre fallos (MTBF), estos parámetros son de gran importancia para obtener datos reales requeridos para los análisis de confiabilidad de los sistemas de instrumentación y de seguridad.

5 REFERENCIAS BIBLIOGRÁFICAS

[1] ABB. (2018). White Paper - Reliability of uninterruptible power supplies. Recuperado el 2020, de https://power-backup.ro/wp-content/uploads/2018/04/White_Paper_Relibility_150506.pdf

[2] AIChE. (2008). *Guidelines for Hazard Evaluation Proocedures* (Third ed.). New York: Center for Chemical Process Safety.

[3] Alderete, F., & Elechosa, C. (2006). Análisis Probabilistico de seguridad en Plantas Industriales de Irradiación. *Primer Congreso Americano del IRPA 2006* (pág. 9). México: Autoridad Regulatoria Nuclear - Argentina.

[4] Basilio, A., Landrini, G., & Capelle, T. V. (2017). *Safety Instrumented Systems, Manual for Plant Engineering and Mantinance* (4th ed.). Villasanta, Italy: G. M. International s.r.l.

[5] British Standard. (2003). *BS IEC 61511-1: Functional safety - Safety instrumented systems for the process insdutry sector: Framework, definition, system, hardware and software requirements.*

[6] Charlwood, M., Turner, S., & Worsell, N. (2004). *Resaerch report 216: A methodology for the assignment of safety integrity levels (SILs) to safety-related control function implemented by safety related electrical, electronic and progrmmable electronic control systems of machines.* Norwich, United Kingdom: HSE, Health & Safety Executive.

[7] Crowl, D. A., & Louvar, J. F. (2011). *Chemical Process Safety, Fundamentals with applications* (Third ed.). Boston: Prentice Hall.

[8] Department of Defense. (1991). *MIL-HDBK-217F: Military Handbook, Reliability Prediction of Electronic Equipment.* Washigton DC.: Department of Defense United States of America.

[9] Fernandez, I., Camacho, A., Gasco, C., Macias, A. M., Martin, M. A., Reyes, G., & Rivas, J. (2012). *Seguridad Funcional en Instalaciones de Procesos: Sistemas Instrumentados de Seguridad y Analisis SIL.* Madrid: ISA sección española.

[10] FESTO. (2017). *Seguridad Funcional en la Industria de procesos.* Recuperado el 2020, de www.festo.com: https://www.festo.com /net/SupportPortal/Files/448240/Broschuere_Safety_PA_es_V03_M.pdf

[11] Gruhn, P., & Cheddie, H. (2006). *Safety Instrumented System: Desing, Analisys and Justification* (Segunda ed.). North Carolina, United States of America: ISA - the Instrumentation, System and Automation Society.

[12] Gulland, G. W. (2014). Methods of Determining Safety Integrity Level (SIL) Requirements - Pros and Cons. *Practical Elements of Safety*. doi:https://doi.org/10.1007/978-0-85729-408-1_6

[13] IAEA. (1997). *IAEA-TECDOC-930 Generic Component reliability data for research reactor PSA .* Vienna: IAEA.

[14] IAEA. (2000). *IAEA - TECDOC - 1162 Generic procedures for assessment and response during a radiological emergency.* Vienna: IAEA.

[15] IAEA. (2002). *IAEA-TECDOC-1267 Procedures for conducting probabilistic safety assessment for non-reactor nuclear facilities.* Vienna: IAEA.

[16] IAEA. (2006). *IAEA-TECDOC-1494 Case studies in the application of probabilistic safety assessment technique to radiation source.* Vienna: IAEA.

[17] IAEA. (2010a). *Specific Safety Guide No. SSG 3: Development and application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants.* Vienna: IAEA.

[18] IAEA. (2010b). *Specific Safety Guide No. SSG-8: Radiation Safety of Gamma, Electron and X Ray Irradiation Facilities.* Vienna: International Atomic Energy Agency (IAEA).

[19] IAEA. (2018). *N-P-2.10 Commissioning guidelines for Nuclear Power Plants.* Vienna: IAEA.

[20] ICRP. (1993). *Protection from Potential Exposure: A conceptual framework - ICRP Publication 64.* Tarrytown: International Commission on Radiological Protection (ICRP).

[21] ICRP. (1997). *Protection from Potential Exposure: Application to Selected Radiation Source - ICRP Publication 76.* Eastbourne: International Commission on Radiological Protection (ICRP).

[22] IEC. (1997a). *IEC - 61508-1 Functional Safety of electrical/electronic/ programmable electronic safety-related system: General requirements.*

[23] IEC. (1997b). *IEC - 61508-2 Functional Safety of electrical/electronic/ programmable electronic safety-related system: Requirements for electrical/electronic/programmable electronic safety-related system.*

[24] IEC. (1997c). *IEC - 61508-3 Functional Safety of electrical/electronic/ programmable electronic safety-related system: software requirement.*

[25] IEC. (1997d). *IEC - 61508-4 Functionl Safety of electrical/electronic/ programmable elecronic safety-releated system: Definition and abbreviations.*

[26] IEC. (1997e). *IEC - 61508-5 Functional Safety of electrical/electronic/ programmable electronic safety-related system: Examples and methods for the determination of safety integitiy levels.*

[27] IEC. (1997f). *IEC - 61508-6 functional Safety of electrical/electronic/ programmable electronic safety -related system: Guidlines on application of parts 2 and 3.*

[28] IEC. (2002). *Functional Safety and IEC 61508: A basic guide.* Recuperado el 2019, de www.ida.liu.se: https://www.ida.liu.se/~simna73/teaching/SCRTS/IEC61508_Guide.pdf

[29] IEC. (2006). *IEC - 61025 Fault Tree Analysis (FTA)* (Second ed.). Geneva: International Electrotechnical Commission - IEC.

[30] Ingrey, A., & Lerévérend, P. (2005). *Manual Safety Interity Level.* Germany: Pepperl+Fuchs.

[31] INN. (2013). *Gestión de Riesgo - Técnicas de evaluación del riesgo (Nch - ISO 31010)* (Primera ed.). Santiago de Chile: Instituto Nacional de Normalización - INN.

[32] ITT Corporation. (2013). *Understanding Safety Integrity Level (SIL) and its effects for Field Instrumentes.* Recuperado el 2020, de www.mafiadoc.com: https://mafiadoc.com/understanding-safety-integrity-level-sil-automationcom_5a1f240f1723ddfeeddc9417.html

[33] Keshk, A. B., & Aly, R. A. (2012). Re-assessment for industrial Cobalt 60 Irradiator maintaining radiation safety. *Arab Journal of Science and Application*, 357 - 374.

[34] Lutz, T., & Ritzer, M. (2020). *Reliability and lifetime of LEDs.* Recuperado el 2020, de www.osram-os.com: https://dammedia.osram.info/media/

resource/hires/osram-dam2496614/Reliability%20and%20lifetime%20of%20LEDs.pdf

[35] Mannan, S. (2005a). *Lee's Loss Prevention in the Process Industries* (Third ed., Vol. 1). Burlington: Elsevier Butterworth Heinemann.

[36] Mannan, S. (2005b). *Lee's Loss Prevention in the Process Industries* (Third ed., Vol. 2). Burlington: Elsevier Butterworth Heinemann.

[37] Mannan, S. (2005c). *Lee's Loss Prevention in the Process Industries* (Third ed., Vol. 3). Burlington: Elsevier Butterworth Heinemann.

[38] Meany, T. (2018). *Functional Safety for Integrated Circuit.* Analog Devices Inc. Norwood: Analog Devices Inc.

[39] Melchers, R. E., & Beck, A. T. (2018). *Structural reliability Analysis and Prediction.* Hoboken: Wiley & Sons Ltd.

[40] MTL Instruments Group plc. (2002). *An Introduction to Functional Safety and IEC 61508: Aplication note.* Recuperado el 2020, de www.mtl-inst.com: https://www.mtl-inst.com/images/uploads/datasheets/App_Notes/AN9025.pdf

[41] NEA/CSNI. (2007). *Use and develpment of probabilistic safety assessment.* Paris: OECD.

[42] Nuclear Regulatory Commission. (1981). *Fault Tree Handbook - NUREG 0492.* Washington: U.S. Nuclear Regulatory Commission.

[43] Smith, D. J., & Simpson, K. G. (2004). *Functional Safety* (Segunda ed.). Oxford: Elseiver Butterworth-Heinemann.

[44] Smith, D. J., & Simpson, K. G. (2011). *Safety Critical Systems Handbook: A straightfoward guide to Functional Safety, IEC 61508 (2010 Edition) and related standars* (third ed.). Elseiver Ltd.

[45] Stamatis, D. H. (2003). *Failure Mode and Effects Analysis.* Milwuake: American Society for Quality.

[46] Venegas, F. (2014). La Seguridad Funcional en la Industria de Procesos. *Tesis previa a la obtención del grado de Magister en Control y Automatización Industriales*. Cuenca, Ecuador: Salesiana, Universidad Politécnica.

[47] Villacis, W. (2019). Análisis Probabilístico de seguridad en una planta semi-industrial de irradiación que tiene una fuente de Co60 de 50000 Ci. UBA-FIUBA/ARN.