Propuesta armonizada del estándar ISA 18.2 e ISA/IEC-62443 bajo un enfoque integral para la empresa WISEPLANT.

Universidad del Cauca

Cristian Javier Muñoz Osorio

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Programa de Ingeniería en Automática Industrial

Popayán, Cauca

2022

Propuesta armonizada del estándar ISA 18.2 e ISA/IEC-62443 bajo un enfoque integral para la empresa WISEPLANT.

Universidad del Cauca

Trabajo de grado para optar por el título de Ingeniero en Automática Industrial

Cristian Javier Muñoz Osorio

Director: MsC. Oscar Amaury Rojas Alvarado

Asesor de la empresa: Ing. Maximillian G. Kon

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones

Programa de Ingeniería en Automática Industrial

Popayán, Cauca

2022

Agradecimientos

Especialmente agradezco a mis padres, puesto que sin sus sacrificios y valores hacia mi nada de esto sería posible, han sido un equipo excepcional y mi formación y mis logros obtenidos y por obtener se los debo a ellos. Además, siempre he sentido la guía de Dios en mi camino por lo que, agradezco a todas esas circunstancias y coincidencias que me han puesto acá.

Agradecimientos a la Universidad del Cauca puesto que en sus aulas me he formado técnicamente y extra clases me he formado crítica y personalmente. Al ingeniero Oscar Amaury por inspirarnos en las clases a tomar amor por la automatización y por darme la oportunidad de participar en este proyecto de gran importancia en el contexto actual e histórico. Al ingeniero Maximillian Kon y la ingeniera Ximena Rengifo por su tiempo, sus enseñanzas y sobre toda su confianza puesta en mí.

Quiero agradecer finalmente a mis compañeros de clases por apoyarme académica y personalmente en diferentes situaciones, a mis compañeros de otras facultades y a todas esas personas con las que me crucé y me inspiraron siempre, a ser mejor.

Resumen

El presente trabajo expone lo realizado en colaboración con la Multinacional "Wiseplant". En donde se indagó sobre la gestión de alertas cibernéticas en tecnologías de la operación (OT). Se tomaron dos de los estándares más influyentes con relación a la gestión de alarmas y a la ciberseguridad industrial y se obtuvo lo más importante de cada uno. Tomando como base el estándar ISA 18.2 en relación a la gestión de alarmas, se manejó un contexto histórico en investigaciones y avances desarrollados alrededor de este estándar, se analizaron los errores y desastres que han sucedido y que dieron paso a la necesidad de realizar algunas normas y su evolución hasta el día de hoy. En la ciberseguridad industrial, se tomó como referencia la norma ISA/IEC-62443 siendo esta la más completa y más manejada por las industrias, especialmente por Wiseplant.

Se identificó un problema de gran dimensión y con considerables consecuencias en la ciberseguridad industrial, específicamente en el sector de las tecnologías de operación (OT). Se encontró, que la racionalización de alertas no se estaba realizando correctamente y que las gestiones actuales obedecen a estándares y normas vigentes hechas para procesos de hace 10 o 20 años [1]. En vista de que los procesos industriales actuales están envueltos en nuevas tecnologías (IIOT, BigData, etc.) y cuya producción automatizada es cada vez mayor [2], la gestión de sus alertas se convierte en un pilar fundamental de la industria para su correcto funcionamiento. Por esto, se tomaron los dos estándares o normas expuestos y se unificaron tomando lo más relevante de cada uno en relación con la gestión de alertas cibernéticas. De esta manera, se propuso un modelo gráfico que describe el respectivo ciclo de vida para la gestión de alertas cibernéticas, realizado apropiadamente para las necesidades actuales de la industria y basado en la norma ISA/IEC-62443 y el estándar ISA 18.2.

En ambos estándares se realizó un análisis para determinar lo más relacionado a la gestión de alertas cibernéticas, entre esta información se encuentran ambos modelos gráficos, con su respectivo ciclo de vida y se desglosaron las actividades o fases que lo componen para observar las similitudes entre ambos estándares y juntarlas en un único modelo propuesto, cuya finalidad sea la correcta racionalización de la gestión de alertas cibernéticas. De la misma manera en que se especifican los estándares que se tomaron como base, también se especifica las fases, actividades y entradas del modelo desarrollado, además de una tabla, donde se muestran las entradas y salidas de las actividades para un mejor entendimiento en caso de una posterior aplicación.

Índice

Página

Índice de figuras

Página

Índice de tablas

Página

Introducción

La cuarta revolución industrial ha despejado ciertos límites en el mundo actual en entornos como la producción, el Big Data, el manejo de información, la gestión de alarmas, el mantenimiento predictivo, etc. Entre estos temas, muchos se han trabajado desde la tercera revolución industrial [3], pero ahora con la facilidad que brinda la industria 4.0 con el internet de las cosas, hay muchos temas que se pueden mejorar y hay otros que es necesario optimizarlos.

Las alarmas por ejemplo, siempre han sido un elemento importante para la conservación y la producción de bienes y servicios en el ser humano [4]. Sin embargo, a través del tiempo se han observado tantos cambios en la tecnología y en la industria que el problema ya no es la alarma en sí, si no la gestión de alarmas [5]. Alrededor de esta, se han generado diversos inconvenientes debido a la cantidad de alarmas que se procesan actualmente y la cantidad de fallos que pueden suceder si el operario no realiza la lectura correcta de los históricos de alarmas o simplemente se hace un cambio de turno erróneo [6]. Debido a estos errores que han causado hechos trágicos y catastróficos se han creado diferentes organizaciones, artículos y estándares que contribuyen a la buena práctica de la gestión de alarmas. Entre estos se encuentra el estándar ISA 18.2 cuyo objetivo y contenido van encaminados a generar una mejora continua en la empresa o proceso, con respecto a las alarmas [7].

Se debe tener en cuenta que las alarmas no solo son importantes para controlar la producción sino también para cuidar los activos y la información de la empresa en general. Debido a que en esta era digital se han elevado los ataques informáticos [7], es de suprema importancia tener alarmas o también llamadas en ciberseguridad industrial alertas cibernéticas, que nos permitan saber si tenemos intrusos en nuestra red o en nuestra empresa, de esta manera se pueden realizar acciones que eviten pérdidas económicas o desastres mayores.

El concepto de alertas cibernéticas se tiene paralelamente en la ciberseguridad industrial y en la norma guía ISA/IEC-62443 [9]. La correcta gestión de alertas cibernéticas permite desarrollar e implantar las medidas de seguridad necesarias para que los operarios o quienes estén a cargo de su gestión, garanticen un nivel de seguridad adecuado tanto a amenazas físicas, como cibernéticas, por medio de contramedidas tecnológicas, procedimentales y físicas. Una herramienta en tecnologías de la información (IT) importante para tal propósito actualmente se conoce como la gestión de incidentes [8].

La gestión de incidentes en seguridad de la información, es un proceso para detectar, reportar, valorar, responder, tratar y aprender de los incidentes de la seguridad de la información [9]. Muchas de las organizaciones desarrollan una estrategia de seguridad cibernética equivocada asumiendo que si protegen a los activos cibernéticos están protegiendo a los receptores de riesgos. Esta hipótesis de trabajo es errónea, simplemente porque en el ámbito de las tecnologías de operaciones (OT) muy posiblemente se está dispuesto a aceptar la pérdida de un activo cibernético, pero no se

puede aceptar la pérdida de una vida humana. Además, un buen diseño de la planta (considerando a los sistemas de control como una parte integral), es de sustancial importancia y actualmente, es un aspecto ignorado por los practicantes de la seguridad de la información.

Las tecnologías de operaciones (OT) en general, hacen referencia a los sistemas de producción y control y en su mayoría carecen todavía de soluciones integrales de seguridad [10]. Es necesario tener en cuenta, que la gran mayoría de los sistemas industriales en uso fueron desarrollados hace más de una década con la práctica ausencia de consideraciones sobre ciberseguridad [6].

A partir de esto se han creado diferentes prácticas, mismas prácticas que se utilizan en Tecnologías de la información (IT), en donde se desconocen las diferentes disciplinas de riesgo propias de los entornos industriales, como Sistemas Instrumentados SIS, funcionales y de procesos [11]. Esto acarrea un problema cada vez más común en el que se desconoce la naturaleza de los riesgos que se pueden presentar y por ende se limita la toma de decisiones por parte del operario frente a amenazas de fuerte impacto [12].

Actualmente las empresas de IT están muy entusiasmadas en ocupar un escenario protagónico en este nuevo terreno de las OT. Sin embargo, surgen los siguientes interrogantes:

- ¿Están las plantas industriales implementando sistemas de gestión de alertas de seguridad cibernética razonables y adecuados a los entornos industriales?
- ¿Están los proveedores típicos de sistemas de alertas de seguridad de las tecnologías de la información en condiciones adecuadas para atender las necesidades del piso de planta?

Por lo anterior, se propuso desarrollar una guía que oriente a las empresas a tomar decisiones acertadas en este campo, en este caso, unificando dos estándares que han sido pilares en los temas de gestión de alarmas y ciberseguridad industrial. Proponiendo un modelo cuyo objetivo y contenido permita una correcta gestión de alertas cibernéticas para brindar información real del proceso y dar la posibilidad de intervenir en el momento y la situación indicada con el fin de evitar fallos inesperados [13].

I. Capítulo 1: Estándar 18.2 “Management of alarm systems for the process industries”

1.1. Situaciones e Historia de la gestión de alarmas

El inicio de la gestión de alarmas se puede referenciar con los inicios de los sistemas de control o los DCS (sistemas de control distribuidos) dando por consiguiente que esta surge tras diversos problemas que ocurrían en los procesos y la industria en general a partir de la tercera revolución industrial. Tras el surgimiento de estos DCS se aumentó la posibilidad de tener en la industria producción en masa, procesos controlados y por consiguiente gran cantidad de alarmas. Esta cantidad de alarmas no fue del todo positivo [14].

Por ejemplo, a inicios de los noventa, se produjeron algunos incidentes en los sistemas de control de diferentes industrias. Para esto, distintas empresas ofrecieron productos y servicios que permitieron resolver parte del problema. En 1991, la Asociación de Usuarios de Materiales y Equipos de Ingeniería (EEMUA: Engineering and Equipment Materials Users’ Association) emitió la publicación N.° 191 sobre la gestión de sistemas de alarmas [15]. En 1994, se formó el Consorcio de Gestión de Situaciones Anormales (ASM: Abnormal Situation Management Consortium), que comenzó a estudiar distintos aspectos del problema [16].

Además hay ciertas leyes o guías que se han desarrollado para el beneficio de las empresas y operarios derivada de la buena práctica de la gestión de alarmas.

La Administración de Seguridad y Salud Ocupacional de los Estados Unidos (OSHA: Occupational Safety and Health Administration) ha emitido ciertos requerimientos para los sistemas de alarmas en el Código Federal de Regulaciones, Título 29, Parte 1910.119 (29 CFR 1910.119): “Gestión de Seguridad de Procesos con Materiales Químicos Altamente Peligrosos” [17]. Estos requerimientos se vinculan con la documentación de alarmas críticas y con el entrenamiento que reciben los operadores para poder entender cómo funcionan y actuar dentro de los límites de operación de las alarmas, teniendo en cuenta la consecuencia de la desviación y los pasos para corregirla o evitarla.

Antes, agregar alarmas era costoso y difícil, por lo que se debía verificar dos veces antes de implementarlas. Hoy en día, los avances en hardware y software permiten implementar alarmas a menor costo, sin limitaciones de espacio y con pocas modificaciones. Por lo tanto, se pueden crear algunas alarmas innecesarias. Lo que hace que, el operador no pueda evaluar muchas alarmas, lo que amenaza seriamente la seguridad del proceso.

En el otro extremo, se puede tener un sistema subalarmado, cuyos aspectos negativos están a la par de los de un sistema sobre alarmado. Por ende, lo recomendable es disponer de un sistema que tenga las alarmas necesarias para lograr una operación segura y eficiente [20].

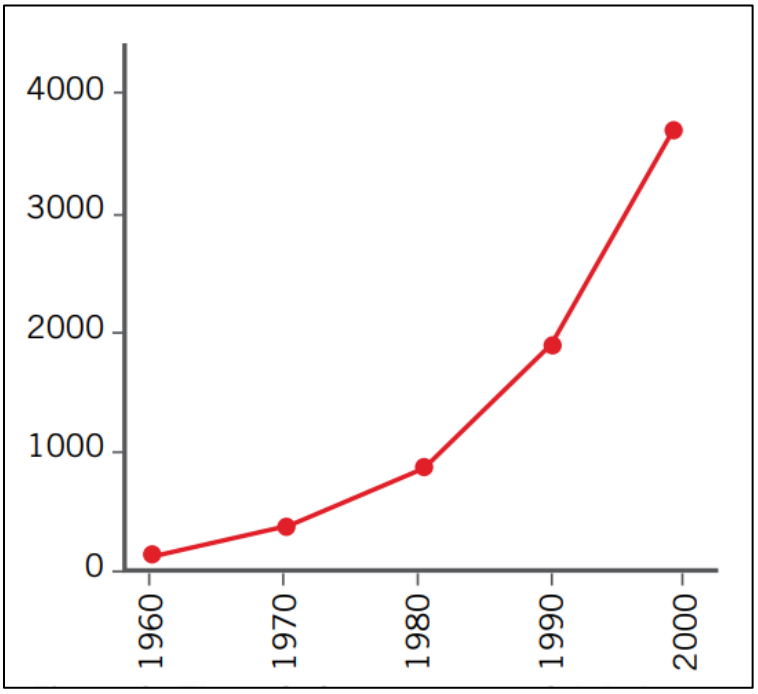

Figura 1: Crecimiento exponencial de las alarmas configuradas por operador. [13]

La motivación para la gestión de alarmas se basa en mejorar el entorno de trabajo del operador (su ergonomía), prevenir su sobrecarga, evitar paradas accidentales, brindar mayor seguridad para las operaciones y mejorar así la confiabilidad de la planta.

"La gestión de alarmas, no obstante, es un proceso continuo que nunca acaba de estar completo. Por tanto, una de las claves para crear un buen programa de gestión de alarmas es saber que NO se trata tan solo de un proyecto, sino de un proceso continuo. La norma ISA-18.2 sugiere que la gestión de alarmas no consista simplemente en hardware o software, sino en el proceso de trabajo o el ciclo de vida de la gestión de alarmas." [18]

1.2. Línea temporal de la gestión de alarmas

La gestión de alarmas ha tenido cambios importantes a lo largo de su historia, todos estos contribuyen a lo que es hoy en día el estándar ISA 18.2 y la gestión de alarmas en procesos industriales a nivel general. Entre los cambios más importantes está:

1990: Tras reconocer que la Gestión de Alarmas se había convertido en un problema, los usuarios de Sistemas de Control Industriales se unieron y formaron en 1990 la "Alarm Management Task Force" (AMTF), que era una junta de asesoramiento dirigida por Honeywell, y en la que participaban miembros de las industrias química, petroquímica y de operaciones de refinado [19].

1994: Se creó el "Abnormal Situation Management Consortium" (ASM) para estudiar distintos aspectos del problema.

1999: EEMUA (Engineering and equipment materials users Association) en el reino unido creó la EEMUA 191(Alarm system- A guide to Design, Management and procurement) en colaboración con el ASM.

2003: La Sociedad Internacional de Automatización (ISA) reunió un grupo de trabajo para preparar recomendaciones prácticas o estándares para Sistemas de Alarmas de procesos industriales. Este trabajo se apoyó en las recomendaciones de la EEMUA 191 [20].

2009: Se publica el primer estándar internacional de ISA conocido como ISA 18.2 "Management of Alarm Systems for the Process Industries" dirigido a la gestión de alarmas.

2016: Se actualiza el estándar con los aspectos observados en las industrias al implementar lo publicado en el año 2009, tales aspectos como la identificación y racionalización, diseño básico de alarmas, métodos de alarmas mejorados y avanzados, entre otros [21].

1.3. Casos críticos de mala gestión de alarmas

En el área de ataques informáticos se pueden traer a colación muchos y se podría pensar que en este momento están sucediendo muchos en muchas partes del mundo. A colación se presenta uno de los más recientes y más delicados que sucedieron actualmente, el de un «hacker» que intentó envenenar el sistema de aguas de una ciudad de la Florida con soda cáustica, pues según el canal de noticias CNN el autor o los autores intentaron aumentar el nivel de soda cáustica en las aguas que se distribuyen en esta ciudad de unos 15.000 habitantes [22].

Afortunadamente en el anterior caso no se efectuó tal hecho, sin embargo, hay otros accidentes que se derivan de una errónea o nula gestión de alarmas, debido a que, en su mayoría presentaban grandes cantidades de alarmas, provocando que las realmente importantes y críticas fueran ignoradas y no se realizaran las acciones preventivas. Por lo que se entiende que, una correcta toma de decisiones se deriva de una óptima gestión de alarmas y se pueden evitar consecuencias catastróficas en un ambiente tan hostil como lo es, el sector industrial. Por esto, se puede comprender también la importancia de la ciberseguridad industrial e incluida en esta, la correcta gestión de alertas cibernéticas. Con el propósito de, además de salvaguardar la empresa de manera general, también proteger y salvaguardar vidas humanas.

Entre estos accidentes se encuentra: La Plataforma petrolífera Piper Alpha, 1988 con 167 muertos, Milford Haven, 1994 con 26 heridos, Buncefield, UK, 2005 con 43 heridos, la Refinería BP, Texas, 2005 con 15 muertos y 180 heridos [23] y Deepwater, Golfo de México, 2010 con 11 muertos [24], entre otros.

Para entender la importancia de la gestión de alarmas se tomaron dos ejemplos de los más catastróficos para su posterior análisis:

1.3.1. Plataforma petrolífera Piper Alpha / Año 1988

Descripción: Una acumulación de errores y decisiones cuestionables dieron lugar a una fuga de gas que finalmente explotó en una plataforma offshore. Esto causó un incendio catastrófico, 167 muertos y billones de dólares en daños.

Caso: Antes de la explosión se liberaron 45 kg de gas licuado que deberían haberse detectado, pero había dos problemas con el Sistema de Alarmas para fugas de gas. Por un lado anunciaba falsas alarmas, haciendo que al final todas fuesen ignoradas, y por otro había problemas de recogida de datos en Sala de Control debido al diseño de los paneles. [25]

Figura 2: Plataforma Petrolífera Piper Alpha incinerada. (Año 1988) [26]

1.3.2. Refinería Texaco en Milford Haven / Año 1994

Descripción: Las inestabilidades y perturbaciones causadas en la planta por una fuerte tormenta eléctrica, dieron lugar a una combinación de fallos en los equipos, el Sistema de Control y la gestión, que terminaron cinco horas más tarde con una importante explosión. Como consecuencia 26 personas resultaron heridas y se produjeron daños por valor de 48 millones de Libras [27].

Caso: La investigación realizada por el Gobierno británico concluyo que los factores clave que contribuyeron a incapacitar la refinería para reconocer y contener los acontecimientos sucedidos fueron:

1. Demasiadas alarmas y mal priorizadas.

2. Los displays de Sala de Control no ayudaban a los Operadores a entender la situación.

3. En los 11 minutos previos a la explosión, los dos Operadores tuvieron que reconocer y actuar sobre 275 alarmas.

Figura 3: Refinería Texaco en Milford Heaven con combustión incontrolada. (Año 1994) [28]

1.4. Situación actual

Las organizaciones y estándares publicados a lo largo de la historia en beneficio de la gestión de alarmas han servido de apoyo para que el estándar internacional ISA 18.2 tenga la rigurosidad y confiabilidad suficiente para ser implementada y solucionar en gran parte los incidentes que sucedían con la gestión de alarmas.

El estándar ISA 18.2 presenta una completa guía que da como resultado un ciclo de vida en pro de la mejora continua de la gestión de alarmas. Este ciclo de vida se compone de diez factores con siete principales. Estos son:

1. Filosofía de alarmas: Documento inicial que indica los requerimientos y reglas de la gestión de alarmas. En base a esto formar un comité con los involucrados en la gestión de alarmas, recomendado con la compañía de un experto.
2. Identificación: Se identifican la necesidades de cada alarma.
3. Racionalización: Se realiza todas las evaluaciones necesarias para determinar la prioridad de todas y cada una de las alarmas. En base a esto se eliminan o se le asigna una mayor prioridad a la que se necesaria. Además se le asignan los límites a las alarmas y la acción que debe realizar el operador.
4. Diseño detallado: En esta se realizar el diseño de alarmas, el diseño del HMI y el diseño avanzado de los límites y prioridades de las alarmas. Este diseño se debe realizar acorde a las especificaciones con gamas de colores, formas y sonidos según la prioridad para llamar la atención del operador.
5. Implementación: Se realiza la prueba y verificación de las etapas anteriores y la instrucción y acoplamiento de los operarios.
6. Operación: Ya implementado el sistema de alarmas se recomienda un plan de entrenamiento para refrescar conocimientos y procedimientos en el tema de manejo de alarmas.
7. Mantenimiento: En este estado se estipula cuando una alarma sale fuera de servicio para repararla, reemplazarla o por pruebas. Como medida de seguridad se recomienda que haya una lista con todas las alarmas en mantenimiento.

En conjunto, estos siete factores junto con otras tres actividades dan el ciclo de vida para la mejora continua en la gestión de alarmas de procesos industriales, observado en la figura 4.

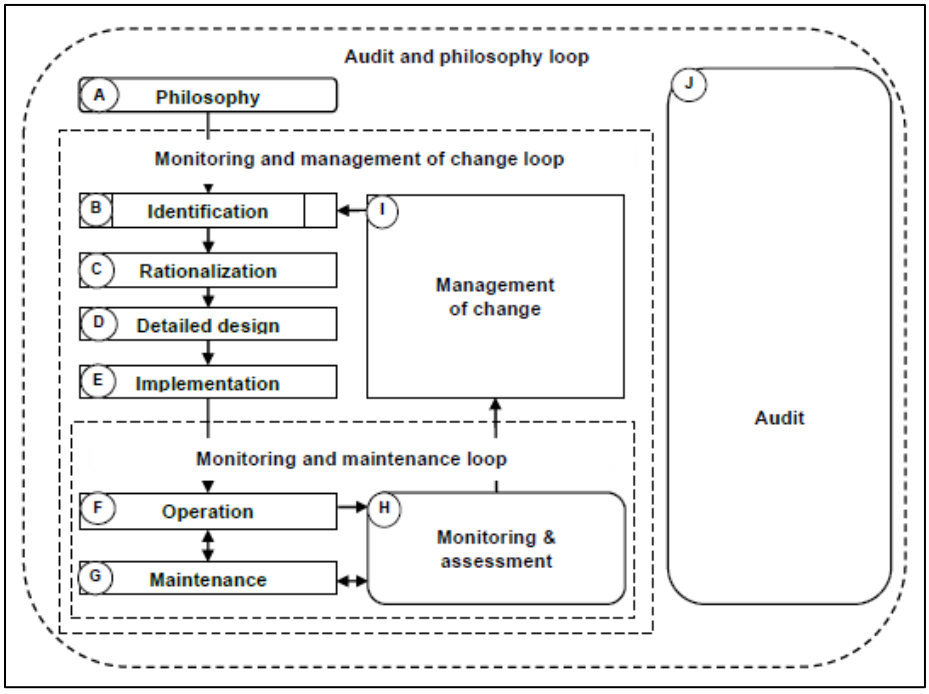

Figura 4: Ciclo de vida de la gestión de alarmas. [29]

1.5. Objetivo y Justificación del estándar ISA 18.2

Objetivo: La ISA 18.2 tiene como objetivo dirigir el diseño, desarrollo, instalación y gestión de los Sistemas de Alarmas en las industrias de procesos. A través de recomendaciones y pasos para dar como resultado la mejora continua en la gestión de alarmas.

Justificación: Este estándar surge tras la necesidad de recopilar toda la información sobre la gestión de alarmas conocida hasta el momento de su creación y crear una sola guía conocida por todas las empresas que cumpla y genere buenas prácticas para contribuir en solucionar los problemas que se observaban en ese momento. Era primordial crear este estándar debido a que tras diversas investigaciones en accidentes industriales se concluyó, que en su mayoría se produjeron tras una serie malas prácticas y por consiguiente se pudieron haber evitado con una buena gestión de alarmas. De esta manera las industrias pueden tener la capacidad de realizar un óptimo control de su proceso y de sus alarmas, evitando pérdidas económicas e incluso vidas humanas. [30]

1.6. Componentes del Estándar ISA 18.2

Este estándar está basado en un documento que está compuesto por dos partes. La primera, es la parte introductoria que inicia en el capítulo 1 y finaliza en el capítulo 5. Posteriormente, se encuentra el cuerpo del estándar desde el capítulo 6 hasta el capítulo 18 en donde se presentan entre otras cosas los requisitos obligatorios y los no obligatorios.

En la parte introductoria se encuentra la alcanzabilidad del estándar, los términos técnicos y sus definiciones, las abreviaciones, los sistemas de alarmas con sus estados, entre otras cosas.

El cuerpo del estándar está definido por las etapas del ciclo de vida de la gestión de alarmas observada en la figura 4. En este se explican los puntos clave a tener en cuenta para el diseño y desarrollo de cada etapa, como se debe realizar y los resultados que se deben obtener.

Para tener una visión de lo que se encuentra en cada etapa, en la tabla 1 se plasman las actividades, las entradas y las salidas de cada una. Debido a que en cada etapa se debe tener cierta información que puede venir de otra de etapa o directamente de la filosofía de la empresa y de la misma manera, cada etapa arroja resultados que son necesarios para otra etapa formando así el ciclo de vida para la gestión de alarmas.

Tabla 1: Etapas del ciclo de vida de la gestión de alarmas con sus entradas y salidas. [30]

Etapa del ciclo de vida de la gestión de alarmas		Actividades	Entradas	Salidas
Etapa	Título			
A	Filosofía	Documentar los objetivos, las directrices y los procesos de trabajo para la gestión de alarmas y las ASRS (Especificación de los requerimientos del sistema de alarmas).	Objetivos y estándares, recomendaciones de auditoria.	Filosofía de alarmas y las especificaciones de los requerimientos del sistema de alarmas (ASRS).

B	Identificación	Determinar el potencial de las alarmas.	Reportes de PHA(análisis de peligro de proceso), P&Ids, procedimientos de operaciones, etc.	Lista de alarmas posibles.
C	Racionalización	Racionalización, clasificación, priorización y documentación.	Filosofía de alarmas y listados de posibles alarmas.	Bases de datos de alarmas maestro y los requerimientos del diseño de alarmas.
D	Diseño detallado	Diseño básico de alarmas, diseño del HMI y el diseño alarmante avanzado.	Bases de datos de alarmas maestro y los requerimientos del diseño de alarmas.	Diseño de alarmas completo.
E	Implementación	Instalación de alarmas, pruebas y capacitación de la implementación.	Diseño de alarmas completo y la base de datos de alarmas maestro, ASRS especificaciones de los requerimientos del sistema de alarmas.	Alarmas de operación y procedimientos de respuesta a las alarmas.
F	Operación	Operador responsable de alarmas de capacita con respecto a la actualización.	Alarmas de operación y procedimientos de respuesta a alarmas.	Datos de alarmas.
G	Mantenimiento	Reparación de mantenimiento y reemplazo junto con	Reportes del monitoreo de alarmas y filosofía de alarmas.	Datos de alarmas.

		pruebas periódicas.		
H	Supervisión y evaluación	Datos del monitoreo de alarmas y reporte del desempeño.	Datos de alarma y filosofía de alarmas.	Reporte del monitoreo de alarmas y cambios propuestos.
I	Gestión de cambio	Proceso para autorizar adiciones, modificaciones y eliminaciones de alarmas.	Filosofía de alarmas y cambios propuestos.	Cambios de alarmas autorizados.
J	Auditoria	Auditoria periódica de los procesos de gestión de alarmas.	Estándares, filosofía de alarmas y protocolos de auditoria.	Recomendaciones para mejoras.

1.7. Técnicas del estándar ISA 18.2

Dentro del estándar ISA 18.2 hay diferentes técnicas que se utilizan para cumplir con las diferentes actividades listadas en la tabla 1.

En la identificación por ejemplo se utilizan diferentes técnicas para la detección de las necesidades de las alarmas. Estas pueden ser; las revisiones de procedimientos de operación, recomendaciones de investigaciones de incidentes, auditorías o de estudios especiales como Análisis de Procesos Peligrosos (PHA), Análisis de Protección por Capas (LOPA) y Análisis de modo falla y sus efectos (FMAE), entre otros.

En la etapa del diseño detallado se puede dividir esta etapa en tres partes. La primera, es el diseño básico de alarmas, la segunda es el diseño del HMI y la tercera es el diseño avanzado de alarmas. Para el diseño avanzado de alarmas se utilizan técnicas que ayuden a mejorar el rendimiento del sistema de alarmas y así garantizar que al operador se le van a presentar alarmas solo cuando estas sean relevantes. Estas técnicas mediante programación, modelamiento y uso de capas lógicas modifican dinámicamente los atributos de las alarmas para ocultarlas y mostrar las relevantes. Dentro de estos métodos avanzados de alarmas se puede indicar entre otros los siguientes: alarmas basadas en modelos, matriz de estado y en lógica, supresión de alarmas basado en agrupamiento, por limitación de tiempo, por conteo y por modificación lógica de atributos. [31]

En estas etapas se observan las técnicas más representativas. Entre las demás etapas se realizan diferentes actividades de manera ordenada en cada una para cumplir con una salida. Esta salida es la entrada de otra etapa formando un ciclo, es decir, el estándar ISA 18.2 es una técnica que conforma la mejora continua para optimizar la gestión de procesos.

1.7.1. Filosofía de alarmas

Objetivo

La filosofía de alarma sirve como marco para establecer los criterios, definiciones, principios y responsabilidades para todas las etapas del ciclo de vida de la gestión de alarmas. Esto se logra especificando elementos que incluyen los métodos para la identificación de alarmas, racionalización, monitoreo, gestión de cambios y auditoría a seguir.

Formato

La filosofía de alarma es un documento que debe incluir definiciones de términos que se encontrarán en el curso del diseño y mejora de un sistema de alarma. Entre estas se lista el objetivo del sistema de alarmas, las definiciones, las referencias, los roles y las responsabilidades, el diseño principal, la determinación del setpoint, los método de priorización, las definiciones de las clases de alarmas, las alarmas que más necesitan gestión, la racionalización, la documentación de las alarmas, la guía para el diseño de las alarmas, las consideraciones específicas para el diseño de alarmas, los principios para el diseño del HMI, técnicas de alarmas aprobadas mejoradas y avanzadas, guía para la implementación, procedimiento para la respuesta de alarmas, el entrenamiento, estantería de alarmas (cómo, cuándo y por quién se pueden manejar), mantenimiento del sistema de alarmas, pruebas del sistema de alarmas, monitoreo del desempeño del sistema de alarmas, la preservación de la historia de alarmas, la gestión de cambios, la auditoria de la gestión de alarmas y los procedimientos relacionados con el sitio.

1.7.2. Identificación

Objetivo

La identificación es un término general para los diferentes métodos que se pueden utilizar para determinar la posible necesidad de una alarma o un cambio a una alarma. La etapa de identificación es el punto de entrada del ciclo de vida de la gestión de alarmas para las alarmas o cambios de alarma recomendados. Las alarmas identificadas son un insumo para la racionalización. [32]

Métodos

Esta norma no define ni requiere ningún método específico para la identificación de alarmas. Las alarmas pueden identificarse mediante una variedad de buenas prácticas de ingeniería o requisitos reglamentarios. Se debe utilizar alguna combinación de métodos de identificación para determinar las posibles alarmas. El método de identificación de alarmas puede afectar la clasificación de una alarma. Cuando sea apropiado, la identificación de la alarma puede realizarse durante la racionalización de la alarma.

Algunos métodos comunes de identificación de alarmas son:

a) Asignación de capas de seguridad,

b) Análisis de peligros del proceso (PHA),

c) Estudio de peligrosidad y operabilidad (HAZOP),

d) Análisis de capa de protección (LOPA),

e) Investigaciones de incidentes,

f) Permisos ambientales,

g) Análisis de modos y efectos de falla (FMEA),

h) Buenas prácticas de fabricación actuales (cGMP),

i) Revisiones de calidad,

j) Revisiones de P&ID,

k) Revisiones de procedimientos operativos, y

l) Recomendaciones del fabricante de equipos empaquetados.

1.7.3. Documentación

La información relacionada con las posibles alarmas debe capturarse durante la identificación y usarse en la racionalización de alarmas si está disponible, incluyendo:

a) El umbral de consecuencia (por ejemplo, restricción).

b) La respuesta del operador.

c) La consecuencia de la inacción.

d) La causa probable.

e) La justificación del umbral de consecuencias.

1.7.4. Racionalización

Objetivo

Durante la racionalización, las alarmas existentes o potenciales se comparan sistemáticamente con los criterios para alarmas documentados en la filosofía de alarmas. Si la alarma propuesta cumple con los criterios, entonces se documentan el punto de ajuste de la alarma, la consecuencia y la acción del operador, y la alarma se prioriza y clasifica de acuerdo con la filosofía. La racionalización produce la información de diseño detallada, documentada en la base de datos maestra de alarmas, necesaria para la etapa de diseño del ciclo de vida de la gestión de alarmas.

Las actividades de racionalización son:

a) Justificación de la alarma.

b) Determinación del punto de ajuste de la alarma.

c) Priorización de alarmas.

d) Clasificación de alarmas.

e) Revisión de la racionalización.

Métodos

Se aplica la guía para la determinación de los puntos de ajuste de alarma establecidos en la filosofía de alarma. Los métodos efectivos utilizan información que incluye:

a) El tiempo de respuesta permitido.

b) La complejidad de la acción del operador.

c) El tiempo necesario para completar la acción del operador.

d) El rango de funcionamiento normal.

e) Otros límites operativos o de diseño.

f) Conocimiento del funcionamiento y la historia del proceso.

1.7.5. Documentación

Se debe documentar la racionalización para que se convierta en la base para garantizar la integridad del sistema de alarma. La documentación (por ejemplo, una base de datos maestra de alarmas) es el vínculo entre cada alarma y la filosofía de alarma y se puede utilizar para varios propósitos, que incluyen:

a) Entrada a la etapa de diseño detallado del ciclo de vida de la alarma.

b) Utilización como parte del MOC.

c) Procedimientos de respuesta a alarmas.

d) Formación y uso por parte de los operadores.

e) Auditoría periódica y conciliación de los ajustes de alarma del sistema de control.

f) Evaluación del monitoreo de alarmas y datos de efectividad.

1.7.6. Diseño detallado

Objetivo

El diseño de HMI para sistemas de alarma es parte de la etapa del ciclo de vida del diseño detallado. Esta describe la funcionalidad para proporcionar indicaciones de alarma y funciones relacionadas al operador y otros usuarios de HMI. La indicación y visualización de alarmas es solo un componente del diseño de la HMI y contribuye a una interacción eficaz entre el operador y el proceso.

Requerimientos

El diseño detallado de las alarmas comprende desde la documentación, las alarmas y el HMI del SCADA del proceso. Estos requerimientos se listan de manera:

Durante el proceso de diseño básico, los atributos de alarma predeterminados deben seleccionarse para cada alarma que se haya racionalizado y configurado según el criterio de ingeniería. Los atributos como el punto de ajuste y la banda muerta pueden ser diferentes según el tipo de alarma específico que se implementará. La definición de los atributos de alarma adecuados puede ayudar a minimizar la cantidad de alarmas molestas que se generan durante el funcionamiento. En las siguientes subcláusulas se proporcionan recomendaciones para el diseño de atributos de alarma específicos. Los atributos de alarma deben incluir:

a) Descripción de la alarma.

b) Punto de ajuste de alarma o condiciones lógicas.

c) Prioridad de alarma.

d) Banda muerta de alarma.

e) Retardo a la conexión o retardo a la desconexión.

f) Grupo de alarmas.

g) Mensaje de alarma.

El HMI debe tener todos los requerimientos para diseño final del HMI:

1. Requerimientos de la información.
2. Requerimientos funcionales.
3. Requerimientos del display.
4. Requerimientos del registro de alarmas.

Esto en consecuencia a las buenas prácticas bajo un conjunto de patrones que se listan en cada una.

Además se explica un poco acerca de las alarmas basadas en lógica las cuales se logran utilizando técnicas (por ejemplo, lógica booleana o árboles de decisión) para determinar las modificaciones que se realizarán en los sistemas de alarma. Esto puede implementarse en el sistema de control o externamente al sistema de control.

1.7.7. Implementación

Objetivo

La implementación es una etapa separada del ciclo de vida de la alarma, que es la transición del diseño a la operación. Este cubre los requisitos generales para implementar o modificar una alarma o un sistema de alarma.

Métodos

Los sistemas de alarma se deben probar durante la implementación para garantizar que se cumplan los elementos apropiados en la filosofía de alarma y ASRS. La prueba del sistema de alarma modificado debe ser apropiada para la naturaleza del cambio, según lo determinado por los procedimientos del MOC del sitio. Las pruebas de los nuevos sistemas de alarma incluirán:

a) Las indicaciones sonoras y visuales para cada prioridad de alarma.

b) Las características de la HMI, como mensajes de alarma en el resumen de alarma o equivalente.

c) Los métodos para retirar una alarma del servicio y volver a ponerla en servicio.

d) Los métodos de estantería.

e) Los métodos para la supresión de alarmas.

f) Cualquier función adicional de técnicas de alarma mejoradas o avanzadas.

g) Los métodos de filtrado de alarmas, clasificación, vinculación de alarmas a pantallas de proceso.

1.7.8. Documentación

Se proporcionará la siguiente documentación:

a) La información de racionalización documentada.

b) Información suficiente para realizar pruebas de alarmas.

c) Los procedimientos de respuesta a alarmas.

d) Cualquier supresión diseñada o documentación alarmante mejorada.

e) Documentación de prueba, si así lo requiere la filosofía de alarma.

Una vez completada la implementación del sistema de alarma, la información de racionalización se actualizará de acuerdo con el procedimiento MOC del sitio.

1.7.9. Operación

Objetivo

La operación es una etapa separada del ciclo de vida de la gestión de alarmas. Este cubre los requisitos para que las alarmas permanezcan y regresen al estado operativo. El estado operativo es cuando una alarma puede indicar una condición anormal al operador. También se describe el uso de herramientas para el manejo de alarmas dentro del estado operativo. La operación es la etapa del ciclo de vida posterior a la implementación y al regresar del mantenimiento.

Método

Se manejan los siguientes ítems como respuesta a las alarmas:

Procedimientos de respuesta a alarmas: Los procedimientos de respuesta de alarma deben ser fácilmente accesibles para el operador según se especifica en la filosofía de alarma.

Estantería de alarmas: Se permitirán las estanterías de alarma según se documente según se detalla en la filosofía de alarma. el nombre de la etiqueta para la alarma, la descripción de la etiqueta o la descripción de la alarma para la alarma, el tipo de alarma, el punto de ajuste de la alarma, las causas potenciales, la consecuencia de la inacción, la acción del operador, el tiempo de respuesta permitido y la clase de alarma.

Capacitación de actualización para operadores: Los requisitos de formación para las alarmas se determinarán mediante la clasificación de alarmas u otros métodos detallados en la filosofía de alarmas.

1.7.10. Mantenimiento

Objetivo

El mantenimiento es una etapa separada del ciclo de vida de la gestión de alarmas. La cláusula 15 cubre los requisitos para la prueba, el reemplazo y la reparación del sistema de alarma. Describe la transición de las alarmas al estado fuera de servicio y luego volver al servicio. El mantenimiento también requiere capacitación de actualización para el personal que mantiene el sistema de alarma.

Concepto:

Se manejan diferentes conceptos dentro de esta fase como:

Prueba de alarmas periódica: Los requisitos de las pruebas periódicas de alarma se determinarán mediante la clasificación de alarma u otros métodos detallados en la filosofía de alarma. El propósito de las pruebas periódicas es asegurar que la alarma continúe funcionando como fue diseñada.

Alarmas fuera de servicio: Los requisitos para el procedimiento fuera de servicio serán determinados por la clasificación de alarma u otros métodos como se detalla en la filosofía de alarma.

Reparación de equipos: La información relacionada con un mal funcionamiento de la alarma debe estar disponible para el operador. Las alarmas afectadas por equipos que no funcionan (por ejemplo, equipos que se ponen fuera de servicio para reparación o mantenimiento preventivo) deben ponerse fuera de servicio si la condición no se resuelve dentro de un tiempo razonable como se especifica en la filosofía de alarma.

Reemplazo de equipo: El procedimiento MOC debe abordar el equipo de reemplazo (por ejemplo, dispositivos de medición, válvulas, equipo de proceso) que cambiarán los atributos de la alarma. Si se realiza un reemplazo, es posible que se requiera la validación de la alarma según la clase de alarma, como se especifica en la filosofía de alarma.

Formación de actualización para el mantenimiento: Los requisitos de formación de repaso para el mantenimiento de alarmas serán determinados por los requisitos de clase como se detalla en la filosofía de alarma. Los requisitos de formación de repaso para el

mantenimiento de alarmas serán determinados por los requisitos de clase como se detalla en la filosofía de alarma.

1.7.11. Supervisión y evaluación

Objetivo

Una vez que se ha implementado el ciclo de vida de la gestión de alarmas y se han reducido las alarmas molestas (por ejemplo, alarmas con vibración), la tasa de alarma resultante refleja más fielmente la eficacia del control del proceso, las prácticas operativas y los sistemas de mantenimiento. El rendimiento del sistema de alarma se puede mejorar aún más mediante mejoras en el control, la operación o el mantenimiento del proceso. Las técnicas de alarma avanzadas a menudo son necesarias para cumplir con los objetivos de rendimiento de la filosofía de alarma.

Métodos

Son posibles varios tipos de análisis de sistemas de alarma, indicadores clave de rendimiento y métodos. Tanto la evaluación inicial del sistema de alarma como el monitoreo continuo deben incluir medidas como las que se muestran en la Tabla 2. La lista de análisis elegidos debe coincidir con la filosofía de la alarma.

a) Tasa de alarma promedio por consola de operador.

b) Tasa de alarma máxima por consola de operador.

c) Inundaciones de alarma.

d) Alarmas frecuentes.

e) Charlas y alarmas fugaces.

f) Alarmas obsoletas

g) Distribución de prioridad de alarma anunciada.

Tabla 2: Métricas para el rendimiento de alarmas. [30]

Métricas de rendimiento de alarmas basado en al menos 30 días de datos		
Métrico	**Valor objetivo**	
Alarmas anunciadas por hora	Valor objetivo: muy probablemente aceptable	Valor objetivo: máximo manejable
Alarmas anunciadas por hora por consola del operador	~ 6 (promedio)	~ 12 (promedio)
Alarmas anunciadas cada 10 minutos por consola del operador	~ 1 (promedio)	~ 2 (promedio)
Métrico	**Valor objetivo**	
Porcentaje de períodos de 10 minutos que contienen más de 10 alarmas	~ <1%	
Número máximo de alarmas en un período de 10 minutos	≤10	
Porcentaje de tiempo que el sistema de alarma está en condición de inundación	~ <1%	
Contribución porcentual de las 10 alarmas más frecuentes a la carga general de alarmas	~ <1% a 5% como máximo, con planes de acción para abordar las deficiencias.	
Cantidad de alarmas intermitentes y fugaces	Cero, planes de acción para corregir cualquiera que ocurra.	
Alarmas obsoletas	Menos de 5 presentes en cualquier día, con planes de acción para abordar.	
Distribución de prioridad anunciada	3 prioridades: ~ 80% bajo, ~ 15% medio, ~ 5% alto o 4 prioridades: ~ 80% bajo, ~ 15% medio, ~ 5% alto, ~ <1% más alto Otras prioridades de propósito especial) excluidas del cálculo	

1.7.12. Gestión de cambio

Objetivo

La gestión del cambio es una etapa separada del ciclo de vida. La cláusula 17 cubre los requisitos para cambios en el sistema de alarma relacionados con la adición de nuevas alarmas, eliminación de alarmas existentes, modificación de atributos de alarma, cambios en las funciones del sistema de alarma, autorización y documentación. El propósito de la gestión de cambios es asegurar que los cambios estén autorizados y sujetos a los criterios de evaluación descritos en la filosofía de alarma. El proceso MOC (management of change) asegura que se apliquen las actividades apropiadas del ciclo de vida a los cambios en el sistema de alarma.

Método

La gestión de cambio es un método en general que debe abordar los siguientes temas:

a) La base técnica del cambio propuesto.

b) El impacto del cambio de salud, la seguridad y el medio ambiente, las modifiaciones.

c) Están de acuerdo con la filosofía de alarma, las modificaciones para los procedimientos.

d) Operativos.

e) Periodo de tiempo para el que el cambio es válido

f) El grado de seguridad se mantiene si la alarma se implementa por razones de seguridad.

g) Disciplinas apropiadas se incluye en la revisión.

h) Cambios en el sistema de alarma, incluidas las actualizaciones del sistema, seguir todas las actividades posteriores apropiadas del ciclo de vida de la gestión de alarmas.

i) La implementación de todos los cambios se adhiere a los procedimientos especificados en la filosofía de alarma.

1.7.13. Auditoria

Objetivo

La auditoría es una etapa separada del ciclo de vida que se lleva a cabo periódicamente para mantener la integridad del sistema de alarma y los procesos de gestión de alarmas. La auditoría del rendimiento del sistema puede revelar brechas que no son evidentes en el monitoreo. La ejecución contra la filosofía de alarma se audita para identificar cualquier requisito de mejora del sistema, como modificaciones a la filosofía de alarma o al proceso de trabajo definido en el mismo.

Método

Se deben realizar entrevistas o cuestionarios al personal como parte de la auditoría para identificar problemas de rendimiento y usabilidad. Los temas de la entrevista pueden incluir:

a) Las alarmas ocurren solo en condiciones que requieren la acción del operador, la prioridad de alarma

b) Se aplica de manera consistente y significativa, los operadores tienen tiempo suficiente para responder alarmas

c) Se definen y se siguen las funciones y responsabilidades de los usuarios del sistema de alarmas.

La filosofía de alarma debe ser auditada según las pautas de la industria y los requisitos y recomendaciones de esta norma. Los procesos y procedimientos de trabajo que garantizan el cumplimiento de la filosofía de alarma deben evaluarse periódicamente para determinar su eficacia. La auditoría debe revisar toda la documentación relacionada, que puede incluir:

a) Verificación de que las alarmas requieren la acción del operador para evitar una consecuencia definida.

b) Documentación de los atributos de alarma y racionalización.

c) Documentación MOC de modificaciones a atributos de alarma en la base de datos de alarmas maestra.

d) Informes de monitoreo de desempeño de alarmas.

e) Documentación de reparaciones de alarmas averiadas.

f) Documentación de alarmas fueras de servicio.

1.8. Ejemplos de aplicación

Para observar los ejemplos de aplicación se deben observar ciertos problemas que necesitan ser resueltos por el estándar ISA 18.2. Este, fue idealmente creado para procesos industriales en donde las alarmas realizan el enfoque en las variables controladas. Sin embargo, actualmente es imperativo tener una óptima gestión de alarmas tanto en el campo industrial como en la seguridad de la información de la empresa y sus usuarios. Tal es el caso que actualmente se han disparado los ataques informáticos como lo describe la siguiente noticia:

"El 62% de las empresas afirma que recibe más ciberataques desde el comienzo la pandemia de la Covid-19, además de impactar notablemente en el ámbito sanitario, económico y social, ha supuesto un desafío para la ciberseguridad. Las restricciones de movilidad y las medidas adoptadas de confinamiento domiciliario han forzado a muchas organizaciones a implantar la digitalización con gran rapidez y a adoptar el trabajo en remoto como principal vía para la continuidad de negocio de la compañía. En este escenario, el 62% de las empresas afirma que su infraestructura tecnológica ha sufrido más ataques desde el comienzo de la pandemia." [33]

Tal es el caso que debido a este problema la automatización tiene un importante y amplio papel tal y como lo indica la siguiente nota:

"La automatización desempeñará un papel importante en la configuración de los ataques a la ciberseguridad y las actividades de defensa en 2021. Así lo predicen los investigadores del Threat Lab de WatchGuard Technologies. De igual manera también consideran que la automatización ayudará a los proveedores de cloud hosting, a tomar medidas enérgicas contra los grupos de ciberdelincuentes." [34]

Un caso de aplicación a modo de ejemplo en el sector industrial se encuentra en CENACE, siendo esta una importante energética en México. En este estudio se sacan las siguientes conclusiones:

No se ha dado el seguimiento adecuado al sistema de alarmas del EMS del CENACE, ya que no se cuanta con un documento actualizado del sistema de alarmas y los cambios solicitados no han sido implantados. Del análisis realizado se encontró que el sistema de alarmas del EMS del CENACE no está dentro de los índices recomendados por las normas EEMUA 191 y ANSI/ISA-18.2.Se recomienda generar un grupo permanente de trabajo que tenga bajo su responsabilidad la gestión del sistema de alarmas del EMS del CENACE. Se recomienda modificar los procedimientos para que en estos se considere los principios dotados por las normas EEMUA 191 o ANSI/ISA-18.2 para la gestión del sistema de alarmas. [31]

En este caso el estándar ISA 18.2 arroja resultados objetivos junto con recomendaciones para el uso óptimo se la gestión de alarmas desde el punto de vista ingenieril.

II. Capítulo 2: Norma ISA/IEC-62443 basado en el Estándar ISA 99

2.1. ISA 99

Objetivo

El objetivo de este estándar es mejorar la confidencialidad, integridad y disponibilidad de los componentes o sistemas utilizados para la fabricación o el control y proporcionar criterios para adquirir e implementar sistemas de control seguros. El cumplimiento de la orientación del Comité mejorará la seguridad electrónica de los sistemas de control y fabricación, y ayudará a identificar vulnerabilidades y abordarlas, reduciendo así el riesgo de comprometer la información confidencial o causar la degradación o falla de los sistemas de control de fabricación.

2.2. Elementos funcionales

El alcance de esta norma se puede expresar en términos de la gama de funciones abordadas. Esta funcionalidad suele describirse en forma de modelo. Uno de estos modelos se definió inicialmente en el "Modelo de referencia para la fabricación integrada por computadora"

También es importante comprender el alcance de esta norma con respecto a otras normas que abordan el tema de la seguridad de la tecnología de la información genérica. Uno de esos estándares es ISO 177993, que proporciona recomendaciones generales para la gestión de la seguridad de la información.

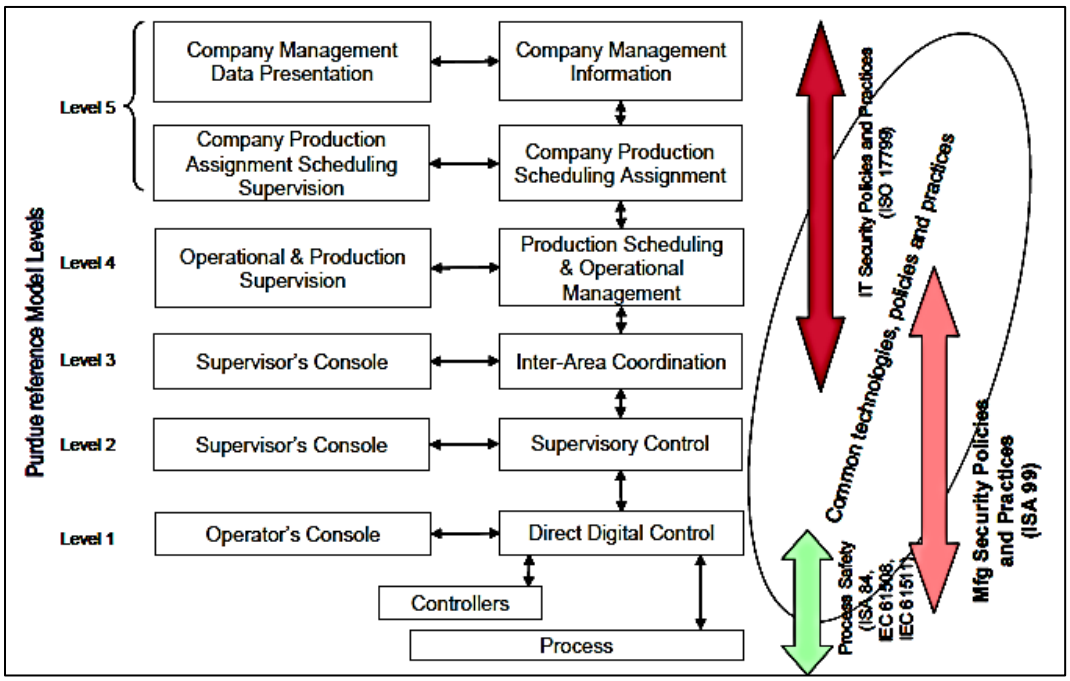

Figura 5: Objetivos funcionales. [35]

En términos de este modelo, el enfoque principal de este estándar está en los niveles 0 a 3 de esta jerarquía. Los sistemas de planificación comercial y logística (es decir, nivel 4) no se tratan explícitamente dentro del alcance de este estándar, aunque se considera la integridad de las comunicaciones de datos entre este y los otros niveles.

2.3. Elementos de seguridad

La seguridad de la información generalmente incluye tres propiedades (confidencialidad, integridad y disponibilidad) que a menudo se abrevian con el acrónimo "CIA". En una estrategia de seguridad de tecnología de la información típica, el enfoque principal está en la confidencialidad y los controles de acceso necesarios para lograrlo. La integridad cae en la segunda prioridad y la disponibilidad es la más baja.

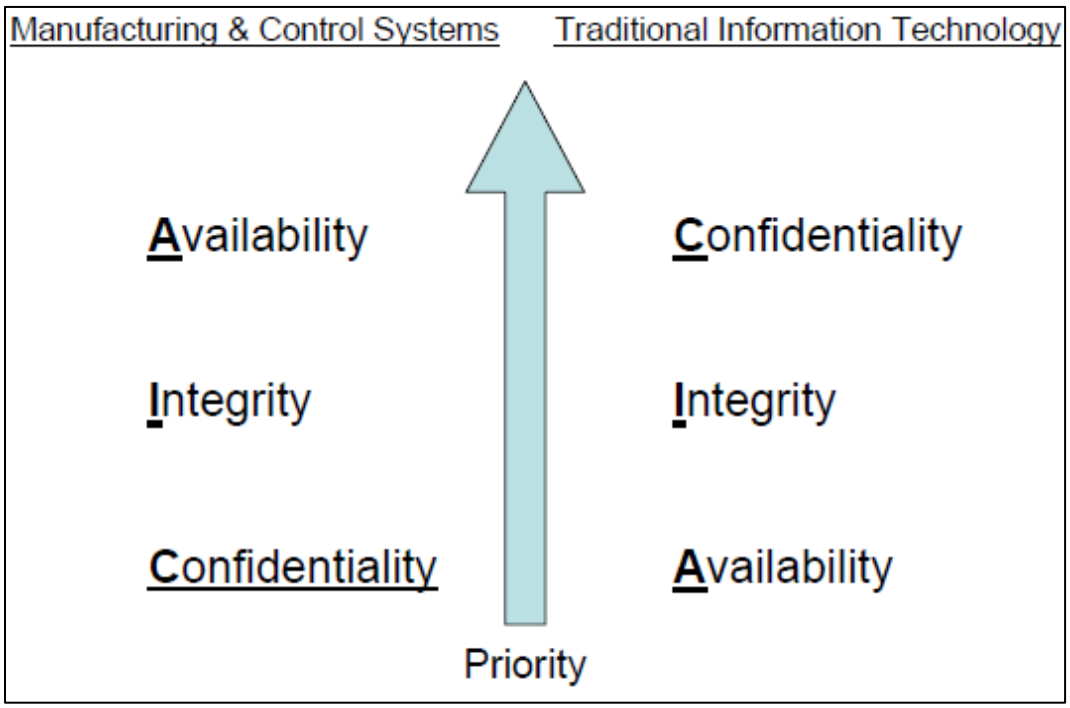

Figura 6: Comparación de objetivos. [35]

También es importante tener en cuenta que ciertos requisitos operativos darán como resultado que los componentes individuales o los sistemas en su conjunto tengan diferentes prioridades para estas propiedades (es decir, los problemas de integridad o disponibilidad pueden superar la confidencialidad, o viceversa). Esto, a su vez, puede conducir al despliegue de diferentes contramedidas para lograr estas propiedades de seguridad.

2.4. Niveles de seguridad

RFC 2828 define el nivel de seguridad como "La combinación de un nivel de clasificación jerárquica y un conjunto de designaciones de categorías no jerárquicas que representan cuán sensible es la información". La sensibilidad de la información se puede definir como baja, media y alta.

Los niveles de seguridad pueden verse como un enfoque análogo a los niveles de integridad de la seguridad (SIL). Se definen cinco niveles de seguridad, que son independientes de la técnica utilizada para realizar la evaluación de riesgos.

- Nivel 0: Sin seguridad: la información fluye libremente dentro y entre todas las zonas. El acceso y uso de los datos no están controlados. No hay garantía de integridad,

confidencialidad, restricción del flujo de datos, ni detección, reporte y respuesta a violaciones.

- Nivel 1: Control de acceso basado en roles (RBAC), basado en ANSI X9.69, para intercambio de información bidireccional. Este nivel garantiza que los atributos de los archivos del sistema se establezcan en los valores de publicación estándar. En este nivel, no se realiza ninguna acción y los servicios del sistema no se ven afectados.

- Nivel 2: RBAC para el intercambio de información unidireccional seleccionado. Este nivel proporciona un control de seguridad adecuado para la mayoría de los entornos. Algunas de las configuraciones de los archivos y parámetros del sistema se modifican, lo que restringe el acceso al sistema para reducir los riesgos de ataques a la seguridad. Se informan las debilidades de seguridad y cualquier modificación realizada para restringir el acceso. En este nivel, los servicios del sistema no se ven afectados.

- Nivel 3: Igual que el nivel 2, pero este nivel ofrece un sistema muy seguro. Los archivos y parámetros del sistema se ajustan para minimizar los permisos de acceso. La mayoría de las aplicaciones y comandos del sistema funcionan normalmente, pero en este nivel, las consideraciones de seguridad tienen prioridad sobre el comportamiento de otros sistemas.

- Nivel 4: No existen canales de comunicación entre ninguna zona. La seguridad de las comunicaciones y la seguridad de la información dentro de una zona es un asunto local.

Los niveles 0 y 4 son condiciones límite y no se tratan en este documento. Los niveles 1, 2 y 3 se utilizan para cuantificar los requisitos de seguridad en términos de niveles de seguridad.

Para el propósito de esta discusión, los requisitos de seguridad se cuantifican en términos de la “fuerza” de integridad, confidencialidad, autenticación, autorización, etc. que relaciona la evaluación de riesgos (y las políticas de seguridad) con la consecuencia. Por ejemplo, los requisitos de rendimiento de la comunicación (tiempo de respuesta) o las limitaciones de recursos (ancho de banda) significan que no se puede, dentro de estas limitaciones, hacer cumplir prácticamente la confidencialidad de la información que fluye por el conducto entre la red empresarial y la red de control. Pero, si la evaluación de riesgos coloca a la amenaza interna como la máxima prioridad, el fortalecimiento de la autenticación y autorización para el acceso y uso de dispositivos o información es la primera orden del día. Luego, dependiendo de las consecuencias percibidas de la amenaza interna, se requiere el nivel de seguridad 1 para controlar el acceso a algunos dispositivos o procesos, el nivel 2 para otros y el nivel 3 para aquellos que son de "misión crítica". Para este ejemplo, el conducto es el mismo para los tres niveles: entre la red empresarial y la red de control.

2.5. Modelos

Esta sección describe una serie de modelos que brindan diversas vistas del tema de la fabricación y la seguridad de los sistemas de control. El objetivo es identificar los requisitos y las características importantes del entorno con el nivel de detalle necesario para abordar los problemas de seguridad con una comprensión común del marco y el vocabulario.

Para abordar plenamente este objetivo, pueden ser necesarios varios tipos de modelos, cada uno de los cuales describe el alcance general desde una perspectiva lógica diferente. Ejemplos incluyen:

a) Modelos lógicos que muestran niveles de sistemas y dispositivos que van desde la empresa hasta el módulo de control, o cómo se aplican los diferentes requisitos y restricciones de seguridad para varias partes del entorno general.

b) Modelos físicos que describen la jerarquía desde la infraestructura física hasta las aplicaciones.

c) Modelos conceptuales que sirven para ilustrar un tema o concepto específico

En cada uno de los casos anteriores, los modelos ya se han definido en otras normas o publicaciones. Siempre que sea posible, estos modelos establecidos se utilizarán en esta norma.

2.6. Modelo de referencia general

El modelo de referencia general que forma la base de esta norma se muestra en el siguiente diagrama. Se basa en el modelo de referencia de Purdue (PRM) para fabricación integrada por computadora y en el modelo de jerarquía funcional de ANSI / ISA-95.00.01-2000. Además de la jerarquía de control de PRM e ISA-95, el Modelo de referencia general también muestra la separación entre los sistemas y redes de Control y Seguridad como se especifica en ANSI / ISA-84.01-1996. Este modelo jerárquico describe las funciones y actividades desde el Proceso (Nivel 0) hasta la Empresa (Nivel 5).

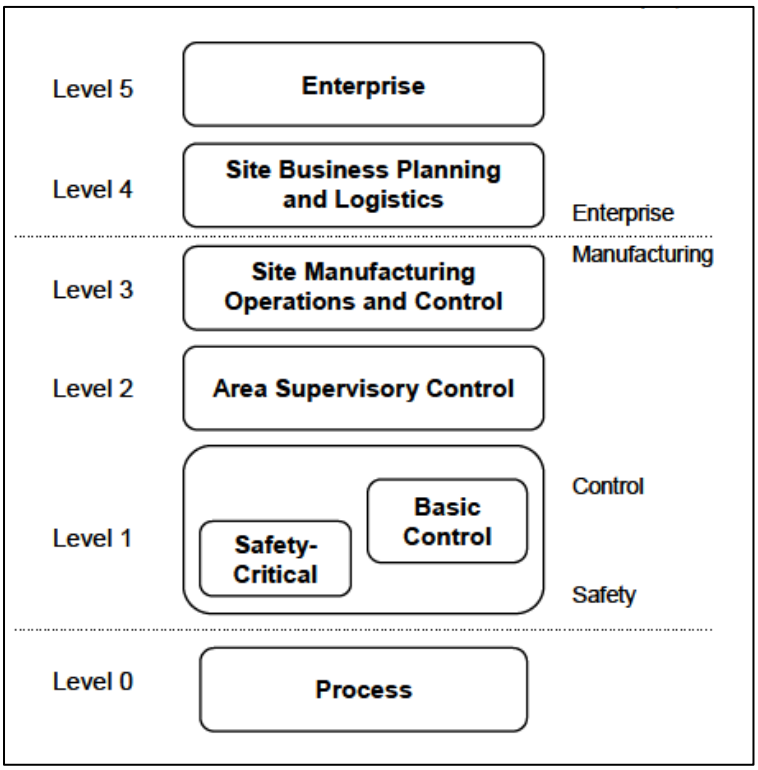

Figura 7: Modelo de referencia general. [35]

2.6.1. Nivel 5 – Empresa

Las funciones de nivel 5 incluyen sistemas financieros corporativos o regionales y otros componentes de infraestructura corporativa, como sistemas de correo electrónico. Las actividades de nivel 5 incluyen, pero no se limitan a:

a) Contabilidad empresarial.

b) Interacciones de empresa a empresa.

c) Interacciones de empresa a cliente.

d) Objetivos de producción de plantas individuales.

2.6.2. Nivel 4: Planificación comercial y logística del sitio

Las funciones de nivel 4 incluyen la programación de la producción, la gestión operativa y la gestión del mantenimiento para una planta o sitio individual en una empresa. Las actividades del nivel 4 incluyen, pero no se limitan a:

a) Uso de materias primas, repuestos e inventario disponible.

b) Uso total de energía e inventario disponible.

c) Inventario general de bienes en proceso y producción.

d) Información de control de calidad.

e) Uso e historia de vida de maquinaria y equipo.

f) Datos sobre el uso de la mano de obra.

g) Programa básico de producción de la planta.

h) Programas de mantenimiento preventivo.

i) Niveles óptimos de inventario de materias primas, fuentes de energía, repuestos y bienes en curso.

j) Planificación de la capacidad.

2.6.3. Nivel 3 - Operaciones y control de fabricación en el sitio

Las funciones de nivel 3 incluyen despacho de producción, programación de producción detallada, garantía de confiabilidad y optimización de control en todo el sitio. Las actividades de nivel 3 incluyen, pero no se limitan a:

a) Informar sobre la producción.

b) Datos sobre producción, inventario, mano de obra, materias primas, repuestos y uso de energía.

c) Recopilación de datos y análisis fuera de línea para respaldar las funciones de ingeniería.

d) Funciones del personal tales como estadísticas del período de trabajo.

e) Programa de producción detallado.

f) Optimizar los costos para áreas de producción individuales.

2.6.4. Nivel 2 - Control de supervisión de área

El nivel 2 incluye el equipo de operaciones de fabricación para un área de producción individual. Por lo general, hay varias áreas de producción en una planta, como destilación, conversión y mezcla en una refinería.

El nivel 2 generalmente incluye las siguientes funciones:

a) Interfaz hombre-máquina del operador.

b) Alarmas y alertas del operador.

c) Funciones de control de supervisión.

d) Recopilación del historial de procesos.

2.6.5. Nivel 1 - Control básico

El nivel 1 incluye equipos de control y monitoreo de procesos. El equipo de monitoreo de procesos lee los datos de los sensores, puede ejecutar un algoritmo y mantiene el historial del proceso. Los ejemplos de sistemas de monitoreo de procesos incluyen sistemas de medición de tanques, monitores de emisiones continuas y sistemas indicadores de temperatura. El equipo de control de procesos es similar. Lee datos de sensores, ejecuta un algoritmo de control y envía una salida a un elemento final (por ejemplo, válvula de control). Los controladores de nivel 1 están conectados directamente a los sensores y elementos finales del proceso.

El nivel 1 incluye control continuo, control de secuencia, control de lotes y control discreto. Muchos controladores modernos incluyen todos los tipos de control en un solo dispositivo.

Ejemplos de equipos de Nivel 1 incluyen:

a) Controladores del sistema de control distribuido (DCS).

b) Controladores lógicos programables (PLC).

c) Unidades terminales remotas (RTU).

2.6.6. Nivel 0 – Proceso

El proceso incluye varios tipos diferentes de instalaciones de fabricación en todos los sectores, que incluyen, entre otros: fabricación de piezas discretas, procesamiento de hidrocarburos, distribución de productos, productos farmacéuticos, pulpa y papel, energía eléctrica, etc.

El nivel 0 incluye los sensores y elementos finales que están directamente conectados al proceso y al equipo de proceso.

2.7. Sistemas críticos de seguridad

Los sistemas críticos para la seguridad incluyen sistemas de protección y sistemas instrumentados de seguridad que monitorean el proceso y toman acciones automáticas para devolver el proceso a un estado seguro si excede los límites de seguridad. Esta categoría también incluye sistemas que monitorean el proceso y alertan a un operador sobre condiciones inseguras inminentes.

Aunque el modelo de referencia muestra los sistemas críticos para la seguridad como un nivel separado, este no es necesariamente el caso en todas las situaciones. Es posible implementar sistemas críticos para la seguridad dentro del mismo nivel que el control básico, utilizando una separación lógica adecuada. La representación que se muestra en este modelo de referencia se eligió como un medio de enfatizar la necesidad de esta separación para garantizar la integridad de las funciones de seguridad.

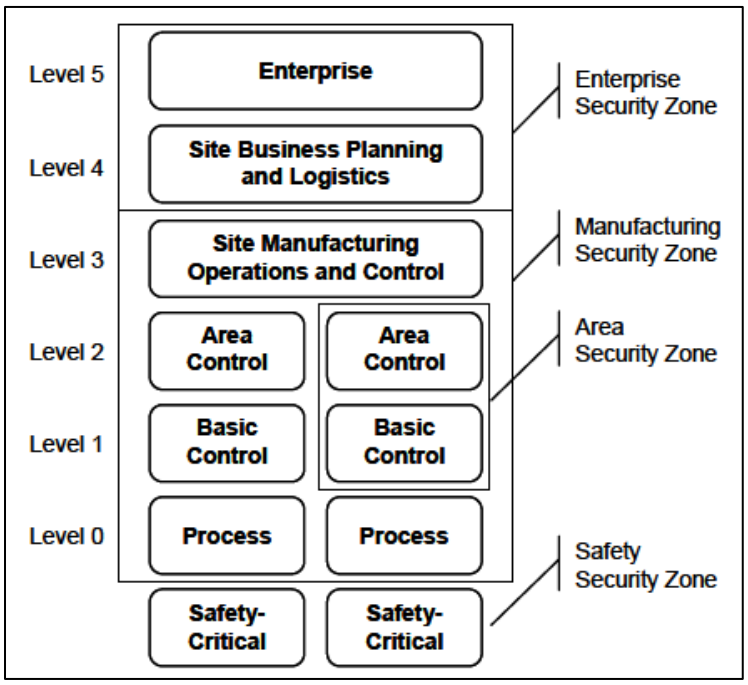

Figura 8: Ejemplo de modelo de referencia con zonas de seguridad. [36]

El enfoque principal de este estándar está en los niveles 0 a 3 del modelo ANSI / ISA-95. Planificación empresarial y los sistemas logísticos (es decir, nivel 4) no se incluyen dentro del alcance de este documento, aunque integridad de las comunicaciones de datos desde los dominios de los sistemas de control y fabricación en el deberían incluirse los sistemas empresariales de recursos empresariales.

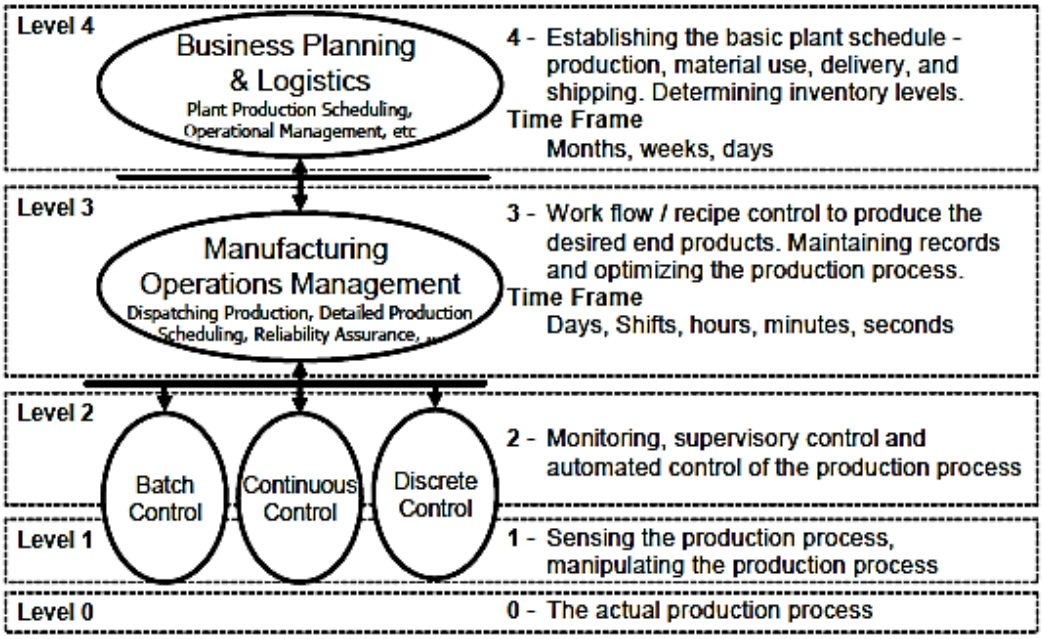

Figura 9: Jerarquía funcional del ISA 95. [36]

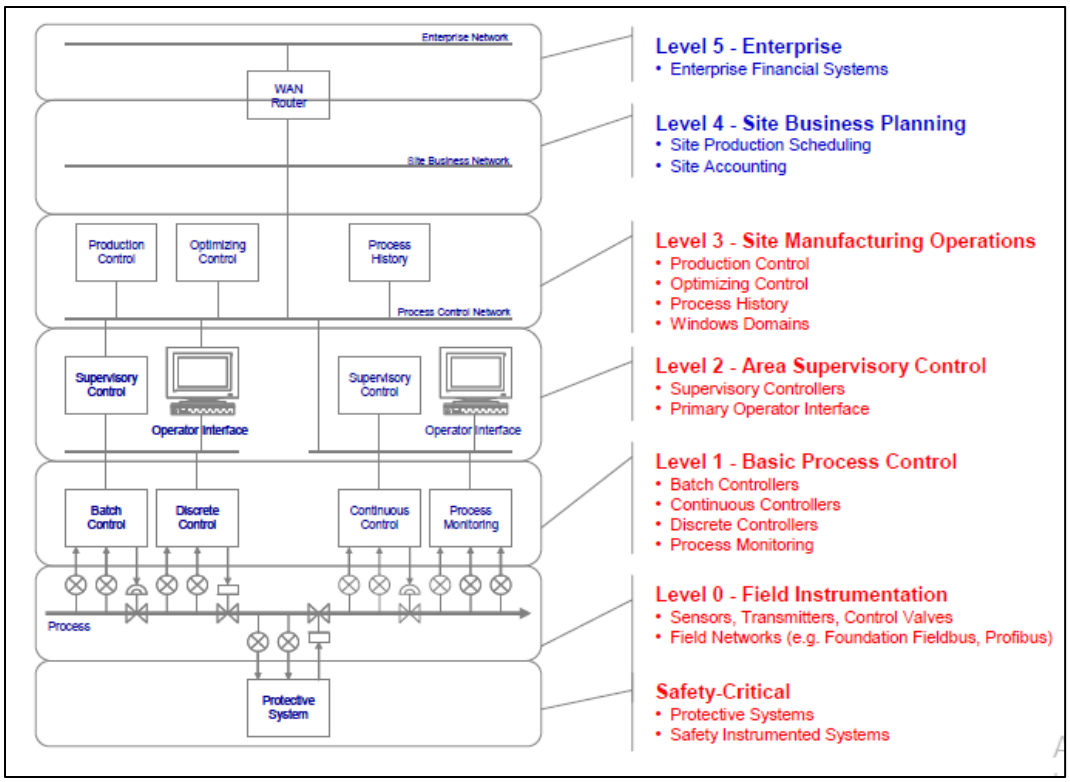

Figura 10: Ejemplo DCS usando la referencia del modelo general. [36]

El sistema de gestión de la seguridad cibernética es el conjunto general de políticas y procedimientos de seguridad que colectivamente se utilizan para impulsar la seguridad cibernética en toda la empresa. El sistema de gestión aborda la creación de políticas y procedimientos, actividades de mitigación para reducir vulnerabilidades, reevaluación del panorama cambiante de vulnerabilidades y la efectividad de las procedimientos y, finalmente, la eficacia general del programa general. La madurez de la empresa programa de seguridad cibernética aumenta a medida que los elementos del sistema de gestión de seguridad cibernética se implementado.

El sistema completo de gestión de la seguridad cibernética consta de (18) elementos clave que tienen lugar en el siguientes cuatro fases principales:

• Plan: establecer el alcance y la política del sistema de gestión de seguridad cibernética, identificar, clasificar, y evaluar los riesgos y desarrollar un plan de continuidad del negocio.

• Do: implementar y operar el sistema de gestión de seguridad y todos sus procesos.

• Check: monitorear, evaluar y medir el desempeño e informar los resultados a la gerencia para revisión.

• Act: tomar acciones correctivas y preventivas y mejorar continuamente el desempeño.

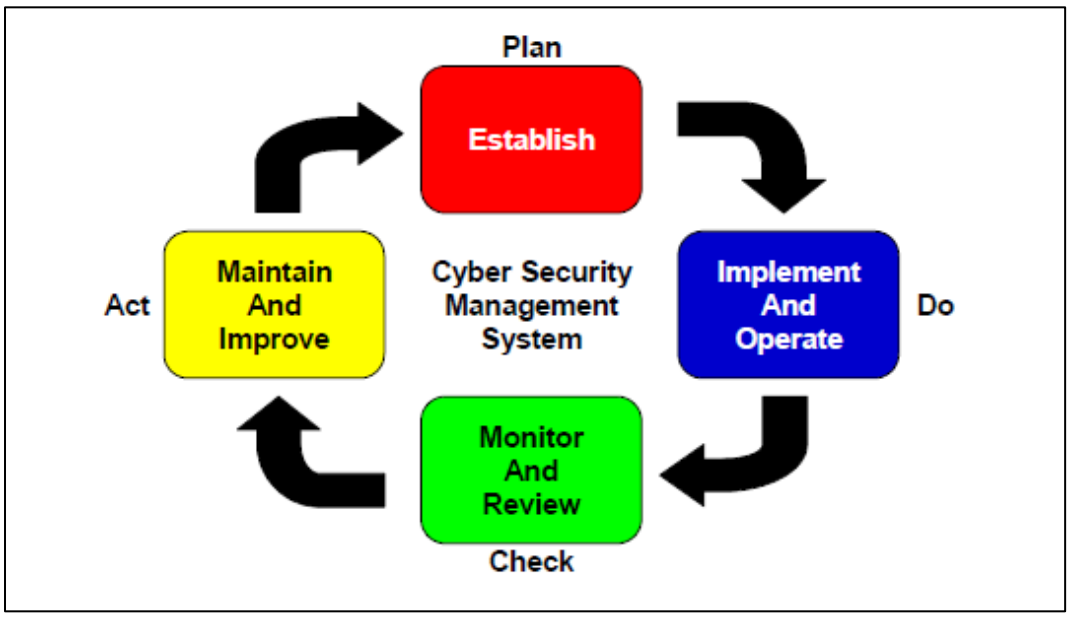

Figura 11: Actividad continúa en la gestión de un sistema de ciberseguridad. [36]

2.8. Norma ISA/IEC-62443

2.8.1. Situación actual de la ciberseguridad industrial

Actualmente se manejan los niveles de seguridad (SL) establecidos para las zonas previamente establecidas en los IACS (Sistemas de control y automatización industrial) entre los cuales se manejan tres escalas representadas en la siguiente Figura 12.

Nivel de seguridad	Descripción cuantitativa
1	Bajo
2	Medio
3	Alto

Figura 12: Niveles de seguridad. [36]

Así mismo se manejan diferentes tipos de nivel de seguridad (SL) entre los cuales se encuentran:

a) SL (Objetivo); Nivel de seguridad objetivo para una zona o conducto.

b) SL (Alcanzado); Nivel de seguridad alcanzado para una zona o conducto.

c) SL (Capacidad); Capacidad de nivel de seguridad de contramedidas asociadas con una zona o conducto o capacidad de nivel de seguridad inherente de dispositivos o sistemas dentro de una zona o conducto.

El ciclo de vida de la ciberseguridad industrial a través de la norma ISA/IEC-62443 en base al estándar ISA 99 presenta tres fases principales cuyos ciclos internos están representados por diagramas de flujos.

La figura 13 muestra el ciclo de vida general del nivel de seguridad. A una zona se le asigna un SL (Objetivo) durante la fase de evaluación del ciclo de vida de la seguridad. Las contramedidas se implementan durante la fase de implementación para cumplir con el SL (Objetivo) para la zona. El SL (Alcanzado) por una zona depende de varios factores. Para garantizar que el SL (logrado) sea mejor o igual que el SL (Objetivo) para la zona en todo momento, las contramedidas se auditan y/o prueban y actualizan, si es necesario, durante la fase de mantenimiento del ciclo de vida de la seguridad.

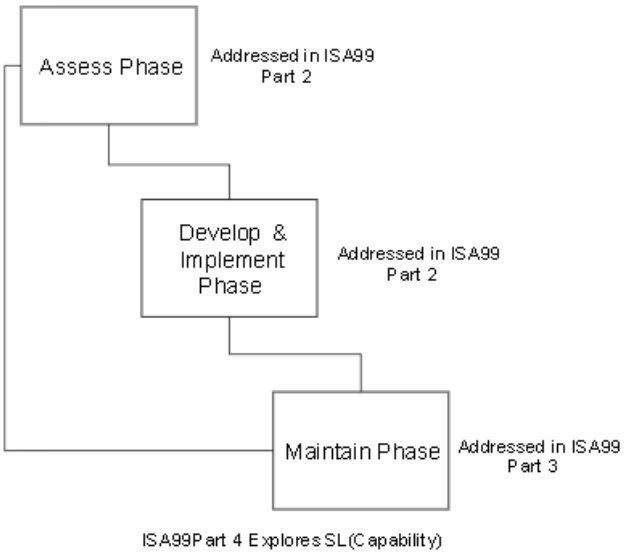

Figura 13: Ciclo de vida de la ciberseguridad industrial. [37]

La fase de evaluación del ciclo de vida de la ciberseguridad industrial incluye actividades vistas en la Figura 14. Una evaluación de riesgos por zona deberá ser desarrollado y el SL (Objetivo) asignado a la zona.

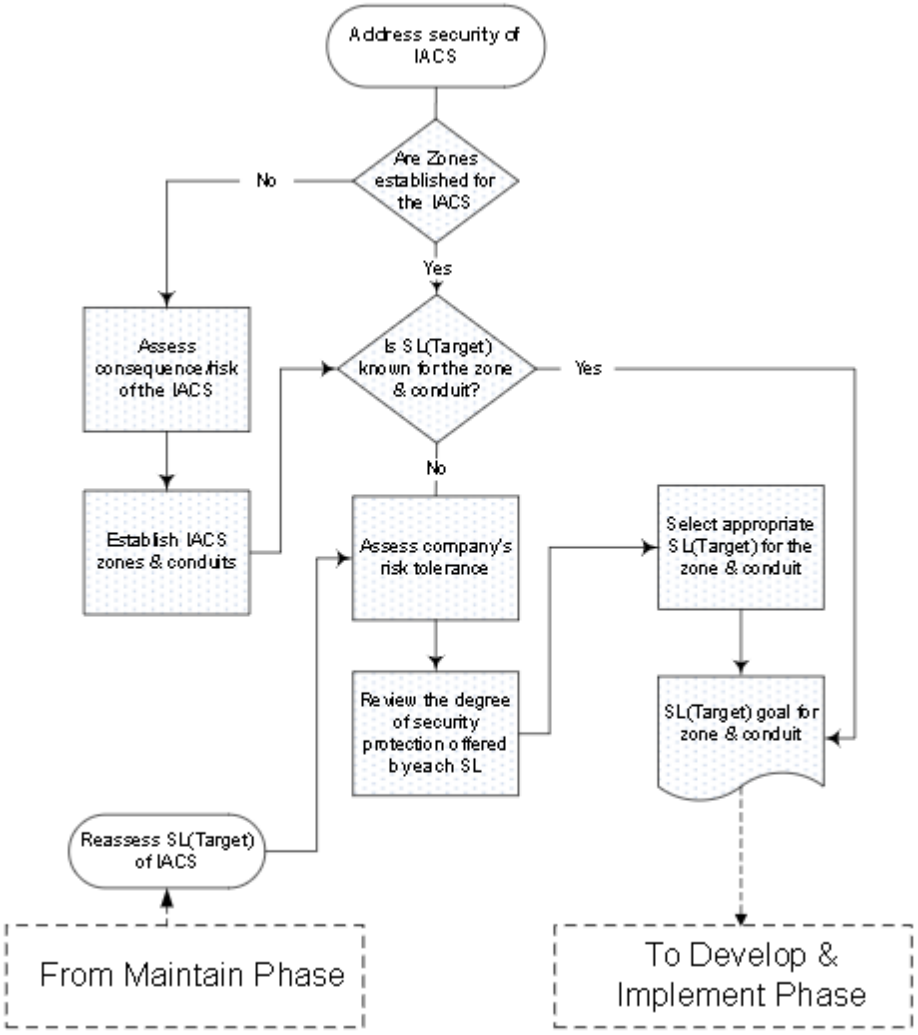

Figura 14: Ciclo de vida de la ciberseguridad industrial: Fase de evaluación. [37]

Una vez que se ha asignado un SL (Objetivo) a una zona en la fase de evaluación, se deben implementar contramedidas para alcanzar el SL (Logrado) mejor o igual que el SL (Objetivo) para la zona. La figura 15 muestra las actividades, para las zonas IACS nuevas y existentes en la fase de implementación del ciclo de vida del nivel de seguridad. El SL (Logrado) se determina después de que el sistema se haya validado con los requisitos de seguridad de la zona.

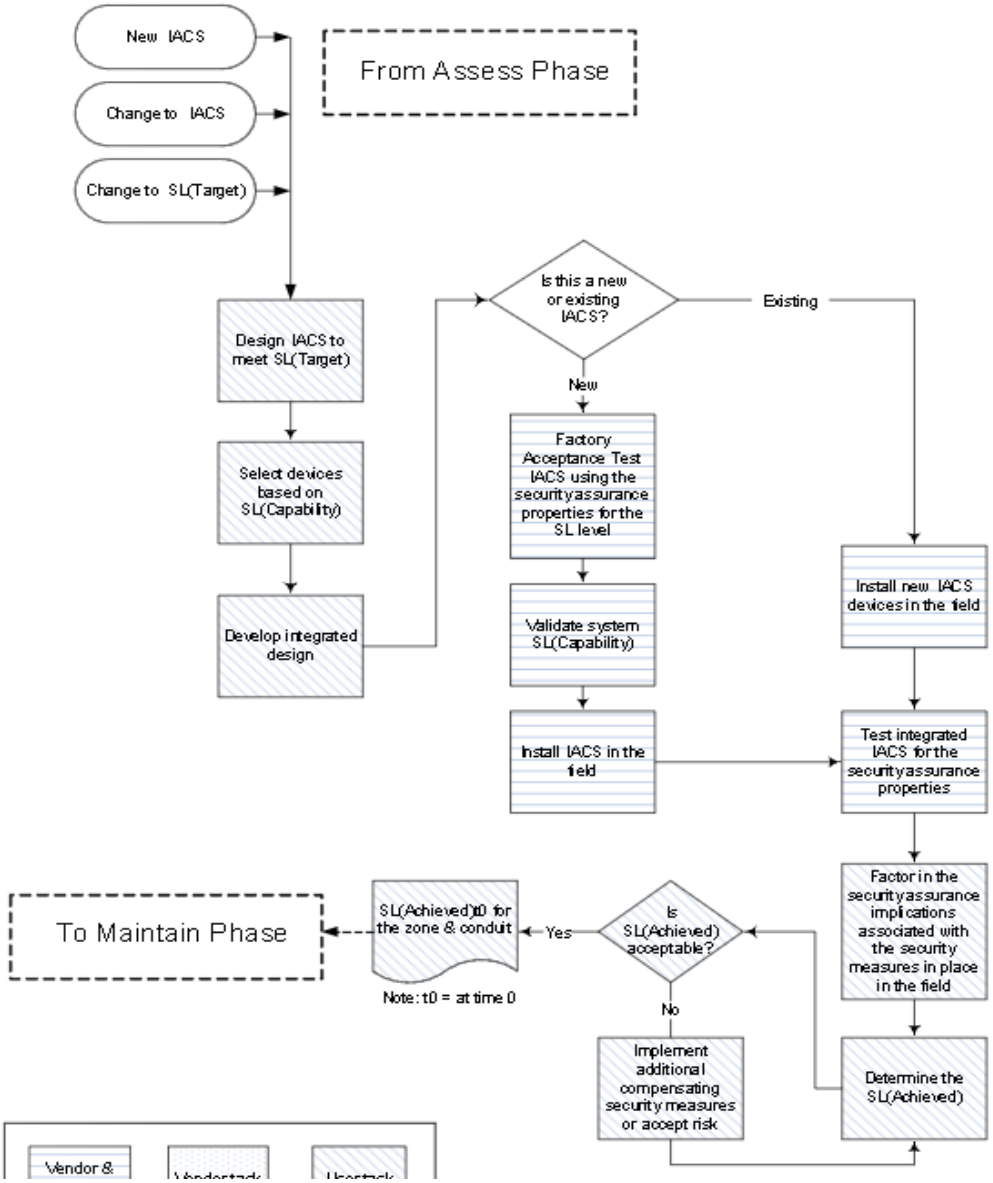

Figura 15: Ciclo de vida de la ciberseguridad industrial: Fase de implementación. [37]

Las contramedidas y las propiedades de seguridad inherentes de los dispositivos y sistemas se degradan con el tiempo. Las propiedades de seguridad relevantes para la zona, incluidos los conductos asociados, deben auditarse y/o probarse a intervalos regulares o cada vez que se descubra una nueva vulnerabilidad para garantizar que el SL (Logrado) sea mejor o igual que el SL (Objetivo) para el zona en cualquier momento. Las actividades asociadas con el mantenimiento del SL (Logrado) por una zona se muestran en la Figura 16.

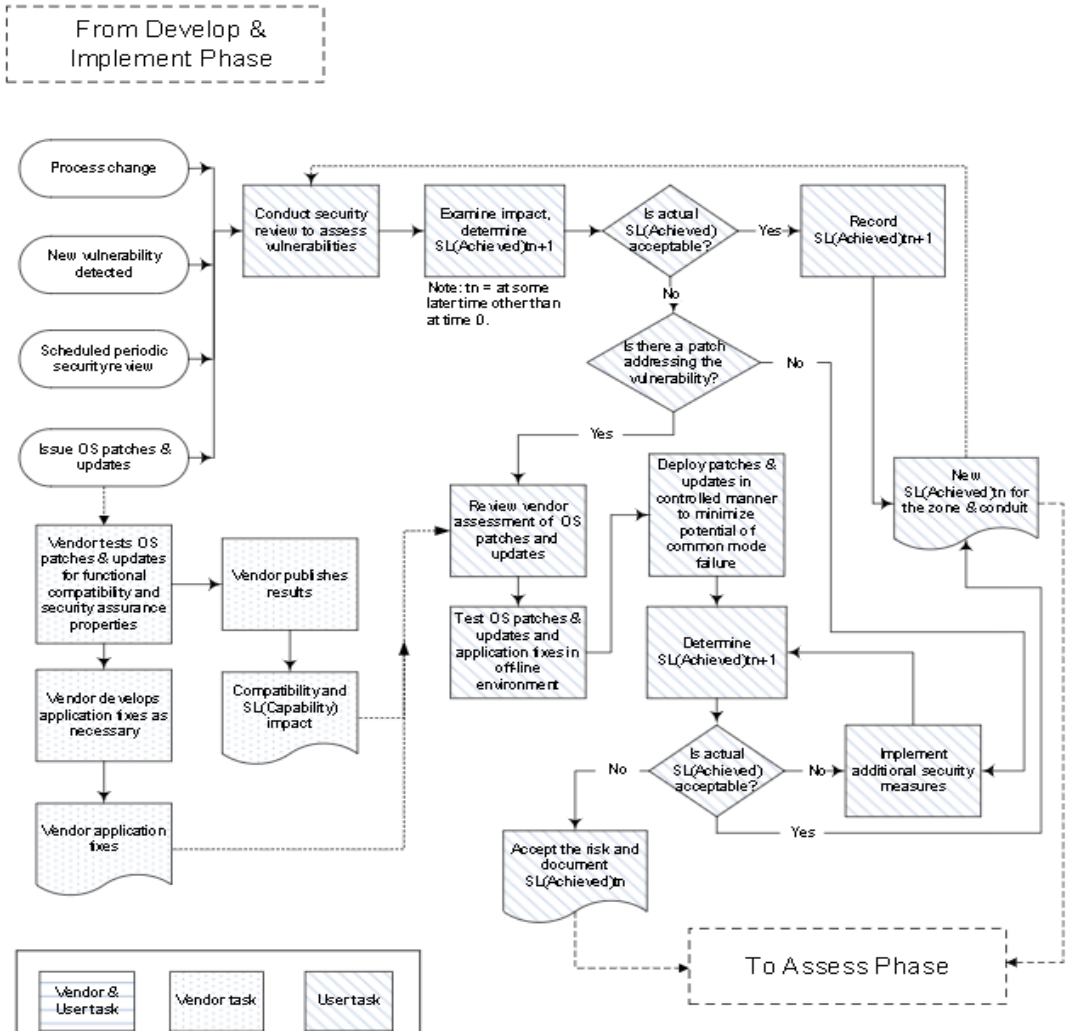

Figura 16: Ciclo de vida de la ciberseguridad industrial: Fase de mantenimiento. [37]

2.9. Objetivos y justificación de la norma ISA/IEC-62443

2.9.1. Objetivo del estándar ISA/IEC-62443

El objetivo de este estándar es mejorar la confidencialidad, integridad y disponibilidad de los componentes o sistemas utilizados para la fabricación o el control y proporcionar criterios para adquirir e implementar sistemas de control seguros. El cumplimiento de la orientación del Comité mejorará la seguridad electrónica de los sistemas de control y fabricación, y ayudará a identificar vulnerabilidades y abordarlas, reduciendo así el riesgo de comprometer la información confidencial o causar la degradación o falla de los sistemas de control de fabricación.

2.9.2. Elementos funcionales del estándar ISA/IEC-62443

El alcance de esta norma se puede expresar en términos de la gama de funciones abordadas. Esta funcionalidad suele describirse en forma de modelo. Uno de estos modelos se definió inicialmente en el "Modelo de referencia para la fabricación integrada por computadora"

También es importante comprender el alcance de esta norma con respecto a otras normas que abordan el tema de la seguridad de la tecnología de la información genérica. Uno de esos estándares es ISO 177993, que proporciona recomendaciones generales para la gestión de la seguridad de la información.

2.10. WISEPLANT y su división en la ciberseguridad industrial

WISEPLANT maneja una división y paquete de seguridad para empresas industriales y capacitaciones en los ingenieros encargados de esta área.

El nombre completo de la empresa es "WISEPLANT smart, safe & security" lo que indica que en esta organización es pilar la inteligencia, la seguridad y la protección. Por ejemplo, la empresa ofrece un paquete conocido como "Zones and Conduits Manager (ZCM)" traducido también como gestión de zonas y conductos.

ZCM provee una gestión de usuarios basada en roles con 2FA/MFA para ver, editar o comentar cualquier activo, activo cibernético, zona, conducto, planta, proceso, etc. Dentro de ZCM se encuentran todas las actividades de ciberseguridad requeridas por ISA/IEC-62443 y solo el usuario autorizado con el uso permitido puede tener acceso a funciones esenciales o información confidencial [38]. De esta manera los datos se mantienen seguros con cifrado nativo fuerte, copia de seguridad y procedimientos de restauración. Y el cliente puede evitar que cualquier información crítica salga de su instalación crítica sin un acceso formal rastreado.

Los servicios de WISEPLANT no solo se basan en proveer el software y hardware a las empresas, sino también en la capacitación del personal para que se realice un buen diseño en los sistemas de alarmas. Esto, debido a que muchos profesionales erróneamente creen que por medio del monitoreo, la detección de anomalías y eventualmente la incorporación de controles, es suficiente para proteger los activos industriales de las múltiples amenazas. Posteriormente a la capacitación del personal, se implementan las fases de la ISA/IEC-62443 correspondientes para que la empresa cumpla con todos los protocolos de seguridad en caso de enfrentar una alarma de alto nivel. Esto se debe realizar y reforzar debido a que saltar directamente al monitoreo sin antes incorporar la seguridad por diseño llevará a los usuarios a una elevada tasa de falsos positivos y a una falsa expectativa de seguridad. [39]

ISA/IEC-62443: Norma basada en el estándar ISA 99.

.

III. Capítulo 3: Articulación del estándar ISA 18.2 y la norma ISA/IEC-62443

3.1. Construcción del modelo unificado

Se tomaron como referencia el estándar ISA 18.2 y la norma ISA/IEC-62443 siendo estas utilizadas ampliamente en la actualidad por diversos sectores industriales.

Estas, presentan sus propios modelos y ciclos de vida previamente desarrollados y adaptados para su uso. En la Figura 17, por ejemplo se observa el ciclo de vida de la gestión de alarmas ampliamente utilizada y descrita en el estándar ISA 18.2. Y en la Figura 18, se observa el modelo de la metodología utilizada por Wiseplant para la aplicación y pedagogía de la norma ISA/IEC 62443. Estos modelos se observaron y se realizó el respectivo análisis para obtener las actividades más relevantes en pro de la gestión de alertas cibernéticas.

Como se observa en la Figura 17, el ciclo de vida de la gestión de alarmas tiene 10 actividades pero seis de estas (Identification, Rationalization, Detailed desing, Implementation, Operation, Maintenance) están en constante observación y auditoria. Esto con el fin mantener actualizado el ciclo de sistemas de alarmas y tomar las decisiones acertadas.

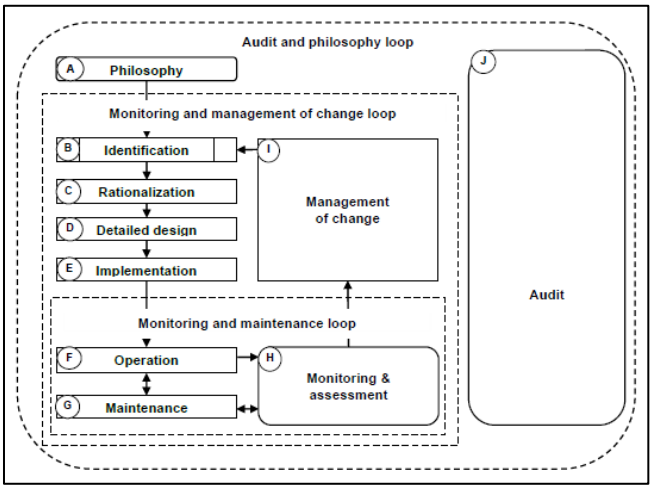

Figura 17: Ciclo de vida de la gestión de alarmas para la articulación con la norma ISA/IEC-62443. [30]

Por otro lado, en la Figura 18 se observa el ciclo de vida utilizado en Wiseplant para la metodología de la norma ISA/IEC 62443. Esta norma, se divide en tres fases y cada una presenta diferentes actividades internas. De la misma manera, a modo de ciclo se repiten consecutivamente las fases de evaluación, implementación y mantenimiento.

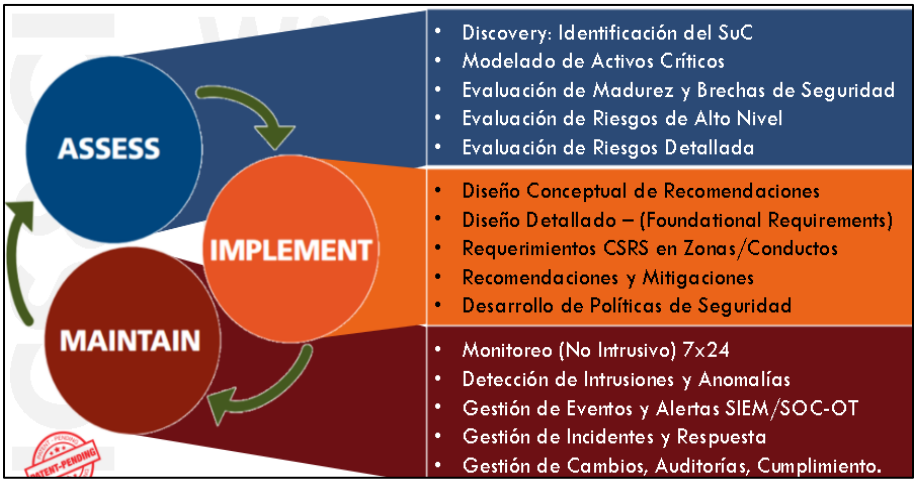

Figura 18: Ciclo de vida de la metodología de la norma ISA/IEC62443 utilizada por Wiseplant. [40]

Se destaca que coincidencialmente tienen una estructura muy similar lo que facilita su unificación y a su vez fortalece la creación de un modelo completo con lo mejor de ambas y cuyos ciclos internos promuevan la correcta racionalización de alertas cibernéticas.

Para iniciar se tomaron las tres fases descritas en la norma ISA/IEC-62443 y en ellas se implantaron las actividades que componen el nuevo modelo. En la Figura 19, se observa cómo se dividió el estándar ISA 18.2 en tres partes para este estudio, con el fin de tener un mejor entendimiento y una comparación más simple.

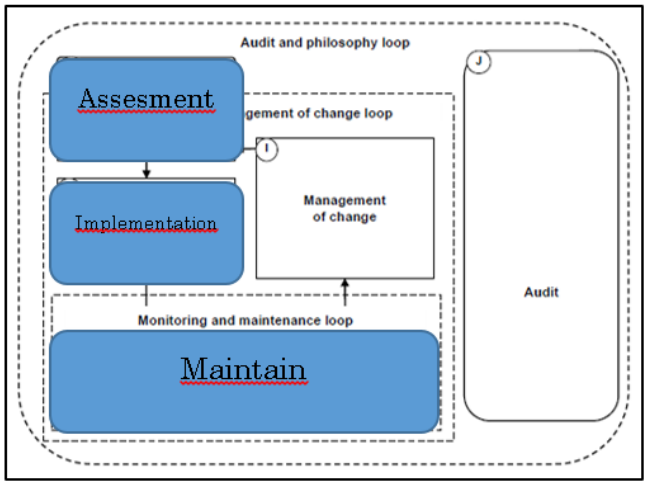

Figura 19: Ciclo de vida de la gestión de alarmas del estándar ISA 18.2 dividido en tres fases. [44]

Al encontrar la similitud y tener la información organizada se empiezan a definir las actividades que deben componer el modelo que se está desarrollando. El estudio del sistema en cuestión, es indispensable para en base a este, aplicar el modelo desarrollado.

Por lo anterior se implementó el GAP (Análisis de brecas de seguridad) y la identificación del SUC (Sistema bajo consideración) tomado de la norma ISA/IEC-62443.

En la figura 20 se observa la analogía en la fase de evaluación entre la norma ISA/IEC-62443 y el estándar ISA 18.2. De esta manera se empezaron a agrupar las diferentes actividades y fases y se inició la construcción del modelo gráfico.

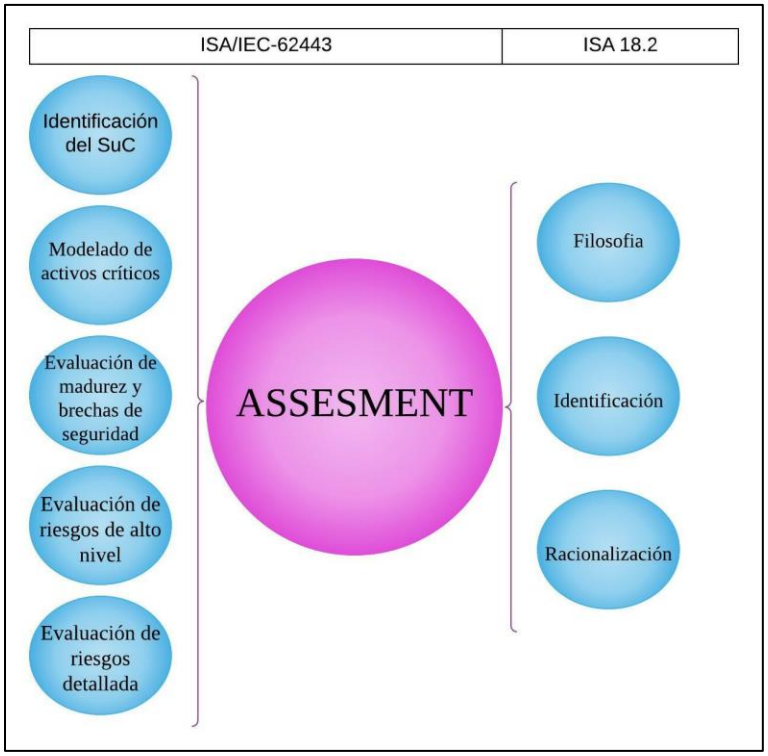

Figura 20: Paralelismo en la etapa de evaluación entre la norma ISA/IEC-2443 y el estándar ISA 18.2. [44]

En las figura 20 se observa las actividades y la fase perteneciente a la norma ISA/IEC-62443 y las actividades pertenecientes al estándar ISA 18.2.

Después de un posterior análisis, las actividades se organizaron de la manera más óptima y coherente posible de acuerdo al orden que tienen internamente en sus respectivos estándares.

En la figura 21 se observa la primera forma en la que se planeaban organizar y de la que partió la construcción del modelo final. Se inició planteando también un ciclo de vida para que el sistema de gestión de alertas cibernéticas a proponer se actualice constantemente.

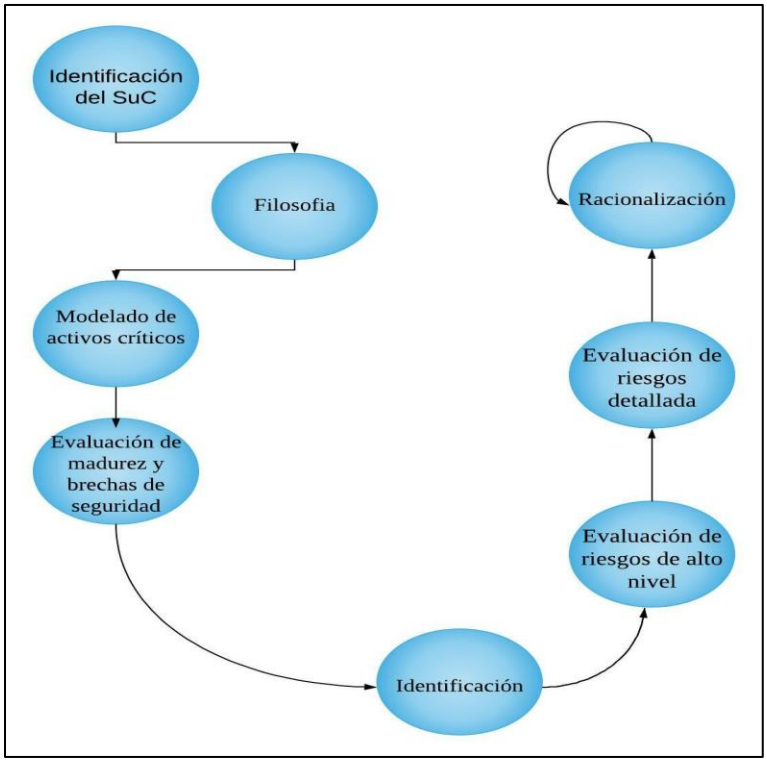

Figura 21: Bosquejo del primer modelo con las actividades organizadas. [44]

Aquí con el equipo de trabajo de Wiseplant, entendimos que era primordial y una excelente complementación implantar como entrada del SuC, la Filosofía de alarmas estudiada y desarrollada en el estándar ISA 18.2. Posteriormente se añadieron el análisis de riesgos en el orden en el que se implementan actualmente en la norma ISA/IEC-62443.

Con estas actividades se cerraría la primera fase omitiendo "la identificación" del estándar ISA 18.2 debido a que esta, está inmersa en las anteriores.

En la fase de implementación siendo bastantes similares los dos estándares, se toman las actividades principales del estándar ISA 18.2 (Rationalization, Detailed desing, Implementation) y se complementan, con forma de entrada, los datos que se obtienen en el análisis de riesgo detallado y de alto nivel tomado de la norma ISA/IEC-62443 junto con la implementación de contramedidas, una herramienta muy utilizada y bastante importante en la gestión de incidentes.

Consecutivamente en la fase de mantenimiento se dejan las mismas actividades que están presentes en la Figura 17 con el mismo ciclo interno. Todo el modelo debe tener la debida auditoria, sin embargo esta fase tendrá dos ciclos internos, permitiendo la robustez del mismo y la adaptación y corrección inmediata. En base a esto, el modelo estaría desarrollado de manera teórica y se procedería a organizarlo de manera gráfica. El modelo organizado gráfica y jerárquicamente desarrollado sujeto a cambios en cuanto a la modificación de actividades está expuesto en la figura 22.

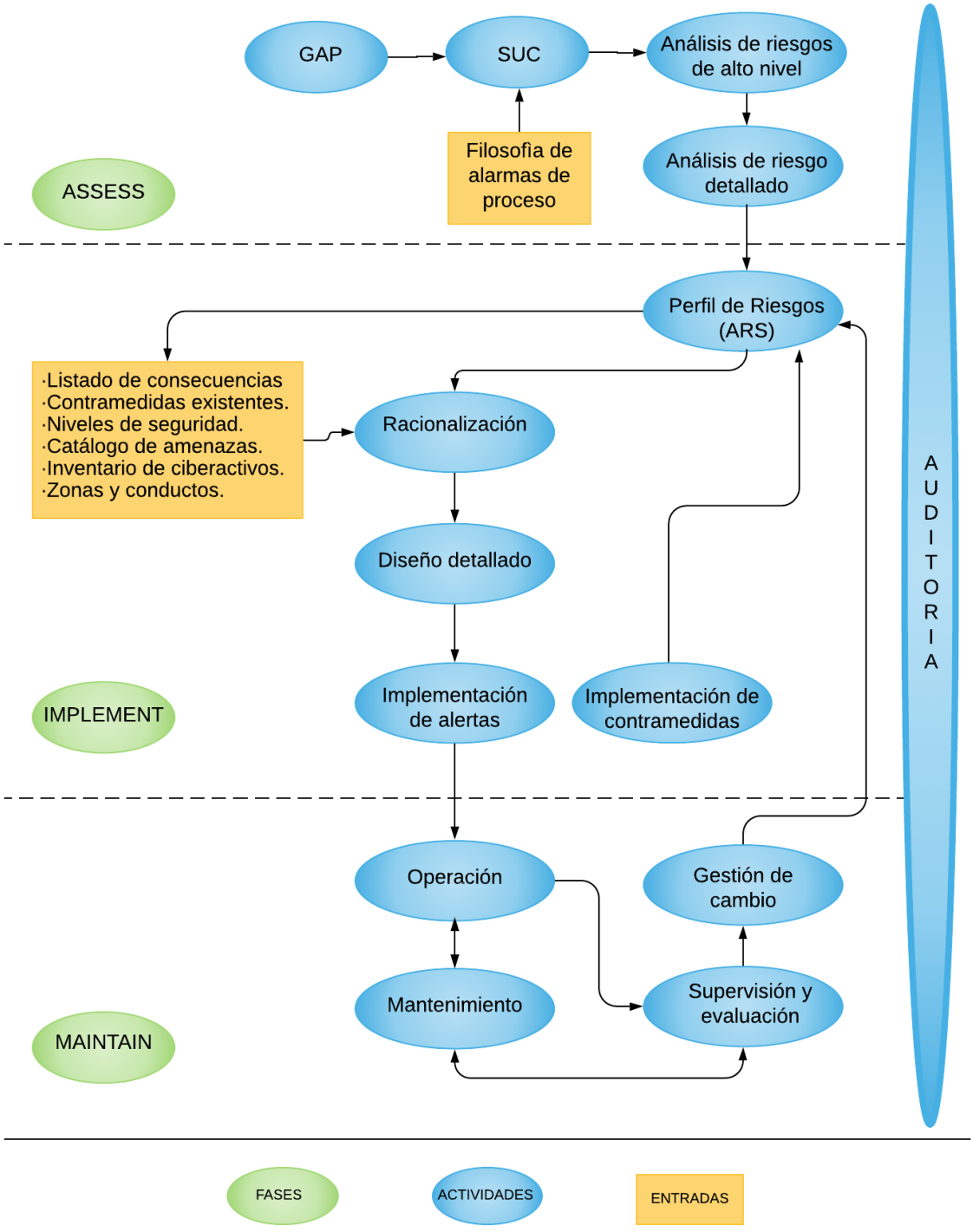

Figura 22: Modelo organizado sujeto a cambios y a la supresión de algunas actividades. [44]

En la Figura 22 se observa el modelo al cuál en conjunto con los asesores de Wiseplant, se decidió quitar el perfil de riesgos (ARS) debido a que está inmerso en el análisis de riesgos y de esta manera, dejar la racionalización como eje principal del modelo.

3.2. Modelo unificado entre el estándar ISA 18.2 y la norma ISA/IEC 62443

En base a los modelos ya establecidos correspondientes al estándar de gestión de alarmas ISA 18.2 y el modelo de la norma ISA/IEC 62443 observados en la figura 4 y en la figura 13 respectivamente. Se estableció un modelo con las cualidades de ambas normas en pro de la gestión de alertas cibernéticas. Este modelo está compuesto por tres fases descritas como: Evaluación, implementación y mantenimiento. A su vez está compuesto por 13 actividades y 2 entradas siendo estas necesarias y previamente definidas para el desarrollo de la actividad en la que se involucra.

Consecuentemente a la Figura 22 se suprimió el perfil de riesgos debido a que lo que se quiere es que la actividad principal sea la racionalización y además, en el análisis de riesgos está inmerso el perfil de riesgos. Por esto, se decidió que la salida de la fase de evaluación, la salida de la fase de mantenimiento y las entradas definidas sean las entradas de la racionalización, obteniendo así nuestro modelo gráfico. En conjunto forman un ciclo que identifica y racionaliza las alertas cibernéticas y suprime las amenazas con el propósito de salvaguardar los ciberactivos y prevenir los desastres. El modelo desarrollado se observa en la figura 17.

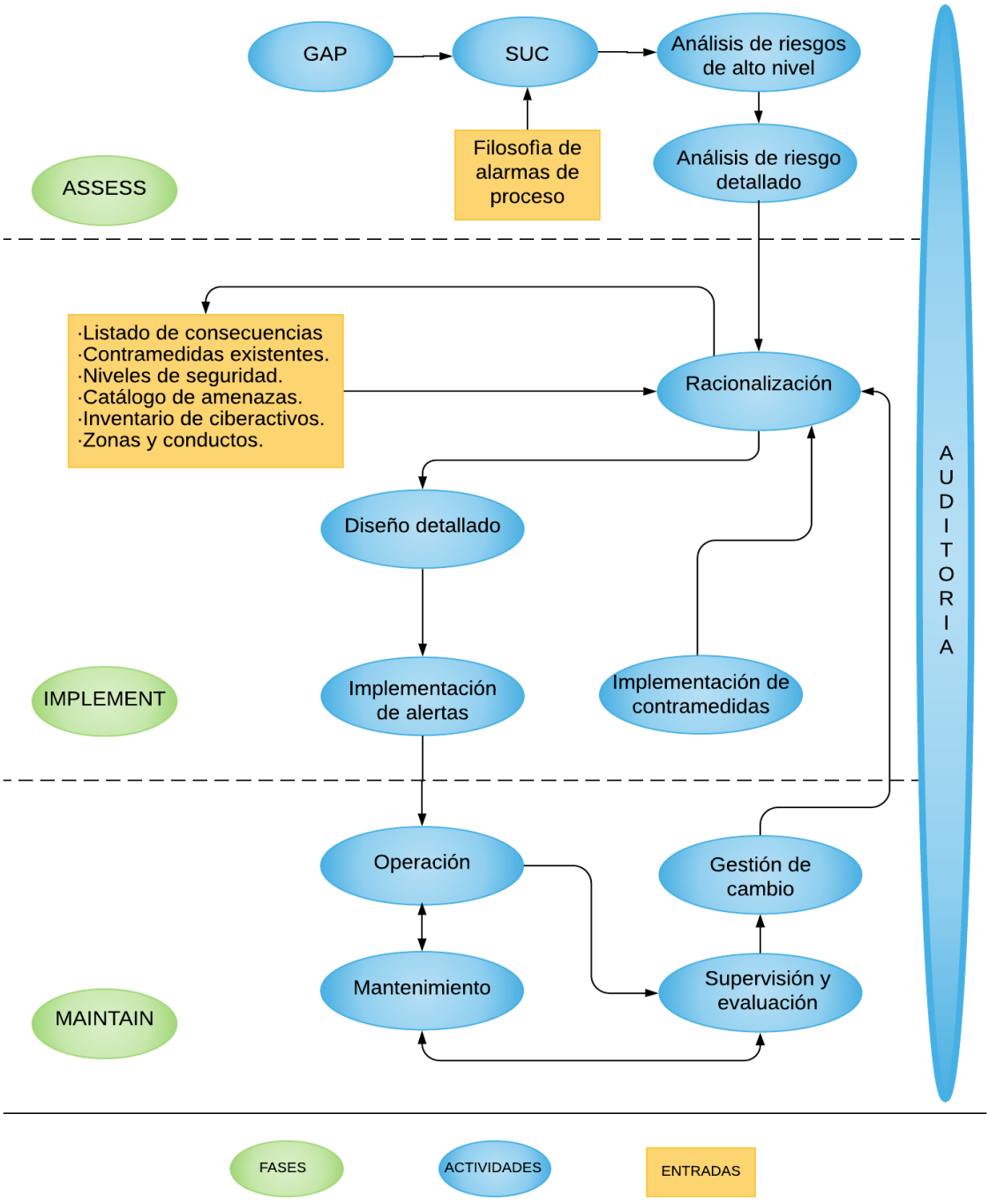

Figura 23: Modelo de la unificación entre el estándar ISA 18.2 y la norma ISA/IEC-62443. [44]

3.3. Entradas y salidas del modelo unificado

Para mayor claridad se describen con etiquetas (A, B,…) las actividades que componen el modelo unificado desarrollado previamente con el fin de describir cada una y listar sus entradas y salidas. Algunas entradas ya están definidas y dependen del contexto político, geográfico y cultural en el que se encuentra la industria. Otras simplemente se obtienen en el transcurso del desarrollo del modelo y por consiguiente las salidas de algunas actividades son las entradas de otras, de acuerdo con el modelo. Las entradas y salidas especificadas se observan en la tabla 3.

Tabla 3: Entradas y salidas del modelo unificado del estándar ISA 18.2 y la norma ISA/IEC-62443

Actividades del ciclo de vida de la gestión de alertas		Descripción	Entradas	Salidas
Act.	Título			
A	GAP	El principal objetivo de esta actividad es evaluar la gobernanza, las políticas, los procedimientos y las prácticas actuales de la organización para encontrar oportunidades de mejora mediante la comparación de las mejores prácticas en Ciberseguridad Industrial.	• Estándares internacionales. • Modelos de evaluación. • Estándares nacionales. • Regulaciones populares.	• Listado por fortalezas. 8. • Lista de vulnerabilidades de procedimiento.
B	SUC	La identificación del Sistema en Consideración (SuC), es una colección definida de Sistemas de Control de Automatización Industrial (IACS) y activos relacionados para realizar análisis de riesgos de seguridad.	• Evaluación documental. • Inspección visual. • Exploraciones pasivas (no intrusivas). • Métodos para identificar vulnerabilidades.	• Listado completo de activos cibernéticos (incluye contramedidas tecnológicas existentes). • Enumerado parcial de vulnerabilidades tecnológicas.

				• Definición inicial de zonas y conductos.
B.1	Filosofía de alarmas	Se documentan los objetivos, las directrices y los procesos de trabajo para la gestión de alarmas y las ASRS (Especificación de los requerimientos del sistema de alarmas).	• Objetivos. • Estándares. • Recomendaciones de auditoria.	• Filosofía de alarmas. • Las especificaciones de los requerimientos del sistema de alarmas (ASRS).
C	Análisis de riesgos de alto nivel (HLRA)	Esta actividad está destinada a evaluar la capa física de la planta, donde se encuentran todas las posibles consecuencias y sus impactos. Se identifican mediante la realización de un estudio de criticidad. Es una actividad multidisciplinar y se puede realizar de forma totalmente remota con todos los participantes que asisten en línea.	• Lista completa de activos cibernéticos. • P&ID (Diagramas de procesos). • Estudio HAZOP • Matriz de riesgos.	• Identificación de receptores de riesgo. • Listado completo de consecuencias e impactos.
D	Análisis de riesgos detallado	El análisis detallado de riesgos es la actividad principal dentro de la fase de evaluación. Este se realiza mediante metodologías que satisfagan los requisitos con el fin de clasificar riesgos de manera concisa y coherente. Los requisitos varían de	• Catálogo de amenazas. • Lista de vulnerabilidades. • Contramedidas existentes. • Lista de logros.	• Lista de vulnerabilidades. • Segmentación óptima de zonas y conductos. • Lista completa de recomendaciones. • Niveles de seguridad objetivo

		acuerdo al IACS implementado.	• Matriz de evaluación de riesgos. • Diagrama inicial de zonas y conductos.	para zonas y conductos. • Clasificación de amenazas (Perfil de riesgos).
E	Racionalización	La racionalización es la actividad más importante de este modelo debido a que es eje fundamental de la gestión de alertas cibernéticas. En esta se realiza la racionalización, clasificación, priorización y documentación de las alertas. En base a la filosofía de alarmas establecida en la organización y al análisis de riesgos realizado previamente.	• Filosofía de alertas. • Listado de posibles alertas. • Perfil de riesgos. • Listado de consecuencias. • Contramedidas existentes. • Niveles de seguridad. • Catálogo de amenazas. • Inventario de ciberactivos. • Zonas y conductos.	• Bases de datos de alertas maestro. • Requerimientos del diseño de alertas (ASRS).
F	Diseño detallado	Se realiza el diseño básico de alarmas, diseño del HMI y el diseño de respuesta a las alarmas.	• Bases de datos de alertas maestro. • Requerimientos del diseño de alertas.	• Diseño de alertas completo, incluye plan de respuesta a las alertas.
G	Implementación de alertas	Se desarrolla la Instalación de alertas debidamente racionalizadas y con su prioridad y plan de respuesta claro, posteriormente se prueba en la práctica y se realiza la capacitación a los agentes relacionados entorno a la implementación.	• Diseño de alertas completo. • La base de datos de alertas maestros. • ASRS especificaciones de los requerimientos del sistema de alertas.	• Alertas de operación. • Procedimientos de respuesta a las alertas.

H	Implementación de contramedidas	Se Implementan las recomendaciones de las contramedidas compensatorias como resultado del análisis del riesgo detallado.	• Lista de vulnerabilidades. • Segmentación óptima de zonas y conductos. • Lista completa de recomendaciones. • Niveles de seguridad objetivo para zonas y conductos. • Clasificación de amenazas (Perfil de riesgos).	• Actualización de las alertas y el plan de respuesta.
I	Operación	El Operador o los agentes responsables de las alertas se capacitan con respecto a la actualización como resultado del modelo aplicado.	• Alertas de operación. • Procedimientos de respuesta a alertas.	• Datos de alertas.
J	Mantenimiento	Se hacen las reparaciones necesarias según se observen afectaciones junto con pruebas periódicas.	• Reportes del monitoreo de alertas. • Filosofía de alarmas y alertas.	• Datos de alertas.
K	Supervisión y evaluación	Se toman los datos del monitoreo de alarmas y del reporte del desempeño.	• Datos de alertas. • Filosofía de alarmas y alertas.	• Reporte del monitoreo de alertas. • Cambios propuestos.

L	Gestión de cambio	Proceso para autorizar adiciones, modificaciones y eliminaciones de alertas.	• Filosofía de alertas. • Cambios propuestos.	• Cambios de alertas autorizados.
M	Auditoria	Auditoria periódica de los procesos de gestión de alertas.	• Estándares. • Filosofía de alarmas. • Protocolos de auditoria.	• Recomendaciones para mejoras.

3.4. Actividades del modelo unificado

Como resultado del análisis y de la integración realizada y teniendo en cuenta las definiciones del estándar ISA 18.2 y la norma ISA/IEC 62443 se describen las siguientes actividades y fases necesarias para el desarrollo del modelo unificado:

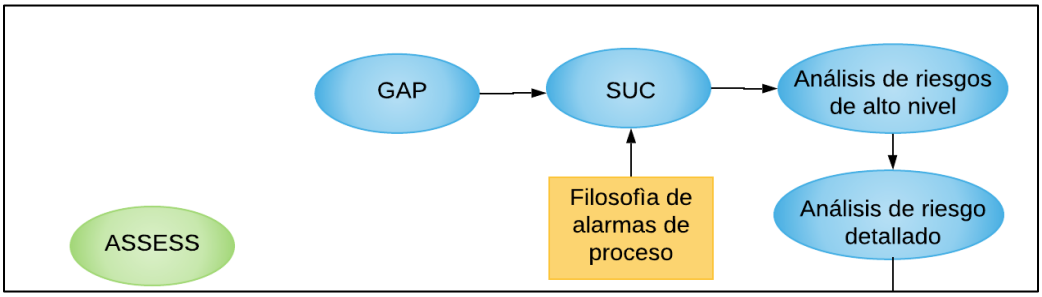

Figura 24: Fase de evaluación [44]

Se organizaron las actividades como se observa en la Figura 18 para la fase de evaluación como objetivo para un correcto reconocimiento de la industria, su posición y las amenazas y riesgos que esta tiene. Se puede mencionar que el GAP, SUC, análisis de riesgos de alto nivel y análisis de riesgo detallado se basan en la norma ISA/IEC-62443 mientras que la Filosofía de alarmas de proceso es la actividad principal del estándar ISA 18.2. En este caso se manejó como entrada del modelo, para que se maneje toda la información del proceso con respecto a las alarmas existentes. Este documento

se debe realizar si no se tiene, sin embargo en gran parte de los casos ya existe por lo que se puede reutilizar para este modelo de gestión de alertas cibernéticas.

3.5. GAP (Análisis de brechas de seguridad)

El principal objetivo de esta actividad es evaluar la gobernanza, las políticas, los procedimientos y las prácticas actuales de la organización para encontrar oportunidades de mejora mediante la comparación con las mejores prácticas en Ciberseguridad Industrial. Algunas prácticas son ISA/IEC-62443, NIST, NERC, C2M2 entre otras según sean necesarias. Evaluando las buenas prácticas por parte de la organización en comparación a información internacional certificada, posteriormente se analizan sus fortalezas y debilidades. La práctica en ciberseguridad industrial se elige en base a los requisitos del proceso u organización definidos de acuerdo a las leyes estatales, políticas, tipo de proceso, tipo de empresa, entre otros factores. De esta manera se inicia la evaluación de seguridad de la empresa y la recolección de información para una correcta toma de decisiones y desarrollar un buen modelo de gestión de alertas.

3.6. SUC (Análisis del sistema bajo consideración)

Se deben documentar los objetivos, las directrices y los procesos de trabajo para la gestión de alarmas y las ASRS (Especificación de los requerimientos del sistema de alarmas).

Requerimientos

La organización debe identificar claramente el SUC, incluida una clara delimitación del perímetro de seguridad y la identificación de todos los puntos de acceso al SUC.

Justificación y orientación complementaria

Con el fin de realizar un análisis de ciberseguridad, un SUC está destinado a incluir todos los activos de IACS que se necesitan para proporcionar una solución de automatización completa.

Los diagramas de arquitectura e historia del sistema se pueden utilizar para determinar e ilustrar los activos de IACS que se incluyen en la descripción de SUC.

Nota: El SUC puede incluir múltiples subsistemas como DCS, SIS, SCADA y paquetes de proveedores.

3.6.1. Filosofía de alarmas

Es necesaria una planificación básica antes de diseñar un nuevo sistema de alarma o modificar un sistema existente. Generalmente, el primer paso es el desarrollo de una filosofía de alarma que documente los objetivos del sistema de alarma y los procesos para cumplir con esos objetivos. La filosofía de alarma refleja los procesos de trabajo de operaciones y mantenimiento y puede hacer referencia a esos procesos en otros documentos. Para los sistemas nuevos, la filosofía de alarma sirve como base para el documento de especificación de requisitos del sistema de alarma (ASRS).

Los criterios para la priorización de alarmas y la definición de clases de alarmas, métricas de rendimiento, límites de rendimiento y requisitos de informes se basan en los objetivos y principios de los sistemas de alarma. Los esquemas para la presentación de las indicaciones de alarma en la HMI, incluido el uso de prioridades, también se establecen en el protocolo de alarma, que debe ser coherente con el diseño general del HMI. La filosofía especifica los procesos utilizados para cada una de las etapas del ciclo de vida de la gestión de alarmas, como el umbral y los requisitos para la gestión de cambios.

El desarrollo del ASRS se incluye en la etapa de filosofía del ciclo de vida. La especificación puede ser específica del plan, proporcionando detalles sobre restricciones u opciones y puede ser la base para seleccionar nuevos sistemas de control o modificar los existentes. La especificación generalmente entra en más detalles que la filosofía de alarma y puede proporcionar una guía específica para el diseño del sistema.

Teniendo en cuenta que el documento correspondiente a la filosofía de alarmas se debe tener en la mayoría de los casos. Este se utiliza en su totalidad para la gestión de alertas cibernéticas, sin embargo, se deben realizar enfoques en algunos ítems que tienen más correlación con el propósito. Entre los cuales se encuentran:

- Propósito del sistema de alarmas.
- Roles y responsabilidades en la gestión de alarmas.
- Principios del diseño de alarmas.
- La determinación del Setpoint en las alarmas.
- Los métodos de priorización.
- Definición de clases de alarmas.
- Alarmas altamente gestionadas.
- Racionalización.
- Guía en el diseño de alarmas.
- Consideraciones específicas para el diseño de alarmas.

- Mejoras aprobadas y técnicas de alarmas avanzadas.
- Procedimientos de respuesta para las alarmas.
- Estantería de alarmas.
- Prueba de alarmas.
- Gestión de cambios.

3.7. Análisis de riesgos de alto nivel

Requisito

La organización debe realizar una evaluación de riesgo de ciberseguridad de alto nivel a partir del SUC o verificar si una existente todavía es aplicable para identificar el riesgo de ciberseguridad no mitigado que en el peor de los casos podría causar la interferencia, interrupción o desactivación de operaciones de misión crítica en los IACS.

Sobre la base de la evaluación del riesgo, se asigna un nivel de objetivo de seguridad inicial para el SUC.

Justificación y orientación complementaria

El propósito del análisis de riesgos de ciberseguridad de alto nivel, es comprender el riesgo en el peor de los casos que presenta el SUC a la organización, en caso de que se vea comprometido. Esta evaluación ayuda a priorizar la evaluación de riesgos detallada y facilita la agrupación de activos en zonas y conductos dentro del SUC.

Para procesos potencialmente peligrosos, los resultados del análisis de peligros del proceso (PHA) y las evaluaciones de seguridad funcional como se define en IEC 61511-1 deben ser referenciados como parte de la evaluación de riesgo de ciberseguridad de alto nivel para identificar los impactos del peor de los casos. Las organizaciones también deben tener en cuenta la inteligencia sobre amenazas de los gobiernos, los centros de análisis e intercambio de información específicos del sector (ISAC) y otras fuentes relevantes.

La evaluación del riesgo de alto nivel a menudo se logra utilizando una matriz de riesgo que establece la relación entre probabilidad, impacto y riesgo (como una matriz de riesgo corporativo).

Una matriz de riesgo es utilizada en la gestión de riesgos para determinar cualitativamente el nivel de riesgo mediante la evaluación de la probabilidad de que ocurra un incidente y la gravedad de la consecuencia en caso de que ocurra el incidente.

Una matriz de riesgo presenta la probabilidad en uno de los ejes y la gravedad en el segundo eje. Las intersecciones entre probabilidad y severidad establecen el rango de riesgo. La intersección entre la probabilidad más baja y la gravedad más baja da como resultado el rango de riesgo más bajo. Mientras que la intersección entre la probabilidad más alta y la severidad más alta da como resultado el rango de riesgo más alto. Las intersecciones suelen estar codificadas por colores para indicar un rango de riesgo creciente, siendo el verde el más bajo y el rojo el más alto.

Aunque siempre son bidimensionales, las matrices de riesgo son de tamaño dependiendo del número de categorías en las escalas de probabilidad y gravedad.

La tabla 4 es un ejemplo de una matriz de riesgo 3 x 5.

Tabla 4: Ejemplo de la matriz de riesgo 3 x 5.

		Severidad		
		A	B	C
Probabilidad	5	Riesgo alto	Riesgo alto	Medio alto
	4	Riesgo alto	Medio alto	Medio
	3	Medio alto	Medio	Medio bajo
	2	Medio	Medio bajo	Riesgo bajo
	1	Medio bajo	Riesgo bajo	Riesgo bajo

Una escala de verosimilitud divide el rango completo de valores en categorías o datos discretos. La Tabla 4 es un ejemplo de una escala de probabilidad con cinco categorías. Este ejemplo demuestra cómo algunas escalas de probabilidad proporcionan múltiples formas de dividir los datos en categorías. En este ejemplo se proporciona una palabra guía, una descripción de probabilidad y una escala de frecuencia.

Tabla 5: Ejemplo para la escala de probabilidad.

Escala de probabilidad	Palabra guia	Descripción de prbabilidad	Guia basada en frecuencia
1	Cierto	Casi seguro	>10-1 por año (alta demanda)
2	Probable	Probable que ocurra	10-1 a 10-3 por año (baja demanda)
3	Posible	Bastante posible pero inusual que ocurra	10-3 a 10-4 por año
4	Improbable	Posiblemente posible, pero es poco probable que ocurra.	10-4 a 10-5 por año
5	Remoto	Tan improbable que se puede asumir que no ocurrirá.	<10-5 por año

De manera similar, una escala de consecuencia o gravedad divide todo el rango de valores de severidad en categorías discretas o bins. La Tabla 5 es un ejemplo de una escala de categorías con tres categorías. Este ejemplo demuestra cómo algunas escalas de probabilidad proporcionan múltiples formas de dividir los datos. En este ejemplo, se proporcionan una palabra guía, una descripción de la probabilidad y una escala de frecuencia.

Tabla 6: Ejemplo de consecuencia o escala de severidad.

	Operacional			Financiacional				HSE		
Categoria	Interrupción en un sitio	Interrupción en múltiples sitios	Infraestructura nacional y servicios	Costo (Millones de dolares)	Legal	Regulador	Confianza pública	Personas en el lugar	Personas fuera del lugar	Medio ambiente
A(Alto)	>7 Days	>1 Day	Afecta a múltiples sectores o interrumpe los servicios comunitarios de manera importante	>500	Delito criminal mayor		Pérdida de imagen de marca	Fatalidad	Fatalidad de incidente con alto impacto en la comunidad	Citación por agencia regional o daño significativo a largo plazo en un área grande.
B(Medio)	<2 Days	>1 Hour	Potencial para impactar en un sector a un nivel más allá de la empresa	>5	Delito menor		Perdida de la confianza del cliente	Péridad de jornada laboral o lesión grave	Complicaciones o impacto en la comunidad local	Citación por agencia local
C(Bajo)	<1 Day	<1 Hour	Poco o ningún impacto para sectores más allá de la	<5	Ninguno		Ninguno	Primeros auilios o	Sin complicaciones	Liberación pequeña y contenida por debajo

			compañía individual. Poco o ningún impacto en la comunidad					lesión grave		de los límites notificables.

Aunque existen algunas matrices de riesgo estándar en diferentes contextos, los proyectos individuales y las organizaciones suelen crear su propio camino o una matriz de riesgo existente. Este anexo informativo proporciona varios ejemplos de matrices de riesgo adicionales para enfatizar al lector que las matrices de riesgo pueden variar en categorías de escala de dimensiones, codificación de colores, clasificación de riesgo, etc. Es fundamental que la entidad que facilita la evaluación de riesgo obtenga la matriz de riesgo correcta que se ha aprobado por el propietario del activo para la instalación que se está evaluando.

Tabla 7: Ejemplo de la matriz de riesgo 3 x 3.

Probabilidad	Altamente probable	Medio	Alto	Alto
	Posible	Bajo	Medio	Alto
	Improbable	Bajo	Bajo	Medio
		Despreciable	Moderado	Severo
		Impacto		

Tabla 8: Ejemplo de una matriz de riesgos 5x5

		Consecuencias				
		Problema menor fácilmente manejado por los procesos normales del dia a dia.	Alguna interrupción posible (daños entre $500K y $1 millon)	Tiempo y recursos significativos requeridos (daños entre $1 millon y $10 millones)	Operaciones severamente dañadas (daños entre $10 millon y $25 millones)	La supervivencia empresarial está en riesgo (daño mayor a $25 millones)
Probabilidad	Casi cierto (más del 90%)	Alto	Alto	Extremo	Extremo	Extremo
	Probable (entre 50% - 90%)	Moderado	Alto	Alto	Extremo	Extremo
	Moderado (entre el 10% y 50%)	Bajo	Moderado	Alto	Extremo	Extremo

	Improbable(entre el 3% y el 10%)	Bajo	Bajo	Moderado	Alto	Extremo
	Raro (menos del 3%)	Bajo	Bajo	Moderado	Alto	Alto

Tabla 9: Ejemplo de una matriz de riesgos 4x3

			Severidad			
			Aceptable Poco o ningún efecto sobre evento	**Tolerable** Los efectos se reducen, pero no son críticos para el resultado	**Indeseable** Impacto grave en la sección o el resultado.	**Intolerable** Podria resultar en un desastre.
Likelihood	**Improbable** El riesgo es improbable que ocurra.		Bajo	Medio	Medio	Alto
	Posible El riesgo probablemente ocurrirá		Bajo	Medio	Alto	Extremo
	Probable El riesgo ocurrirá		Medio	Alto	Alto	Extremo

La actividad de evaluación de riesgos de alto nivel implica la selección y ejecución de metodologías para la identificación y priorización de riesgos .Es importante definir las metodologías desde el principio para que proporcionen una estructura para el resto de evaluación de riesgos. La figura muestra que es importante involucrar a la partes interesadas identificadas durante la actividad inicial del programa CSMS en el proceso

de identificación y evaluación de la prioridad de los riesgos. El paso final para documentar los resultados y la justificación es importante porque este registro se considerará invaluable cuando la evaluación de riesgos deba ser confirmada o actualizada en el futuro.

Entre las actividades y las dependencias relacionadas con el análisis de riesgos se encuentran las siguientes en la figura 19.

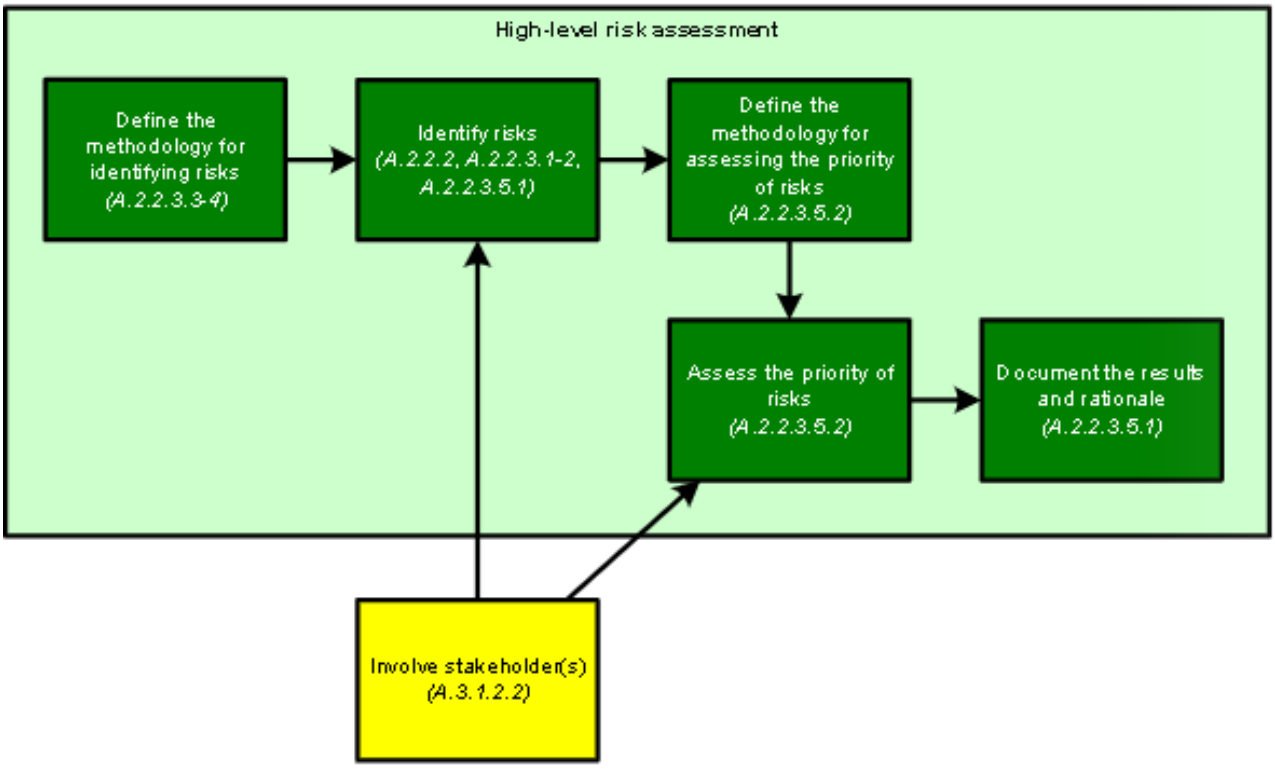

Figura 25: Actividades y dependencia para la actividad: Análisis de riesgos de alto nivel. [42]

3.8. Análisis de riesgos detallados

Se analizan los requisitos de evaluación de riesgos detallados para un IACS y proporciona la justificación y la orientación complementaria sobre cada requisito. Los requisitos se aplican a todas las zonas y conductos. Está permitido utilizar los resultados existentes si la zona está estandarizada (por ejemplo, la reproducción de múltiples instancias de un diseño de referencia).

Se puede seguir cualquier metodología de evaluación de riesgos detallada (como, por ejemplo, ISO 31000, NIST SP800-39 e ISO / IEC27005) siempre que la metodología seleccionada satisfaga los requisitos. Las metodologías de evaluación de riesgos detalladas y de alto nivel deben derivarse del mismo marco, estándar o fuente y deben utilizar una escala de clasificación de riesgos consistente para producir resultados consistentes y coherentes.

El diagrama de flujo correspondiente al análisis de riesgo detallado se observa en la figura 20 donde se encuentran las subactividades con sus respectivas entradas y salidas. Estas en conjunto tienen el fin de realizar una evaluación de riesgos completa y coherente cuyo resultado es de suma importancia para el modelo de gestión de alertas desarrollado en este proyecto.

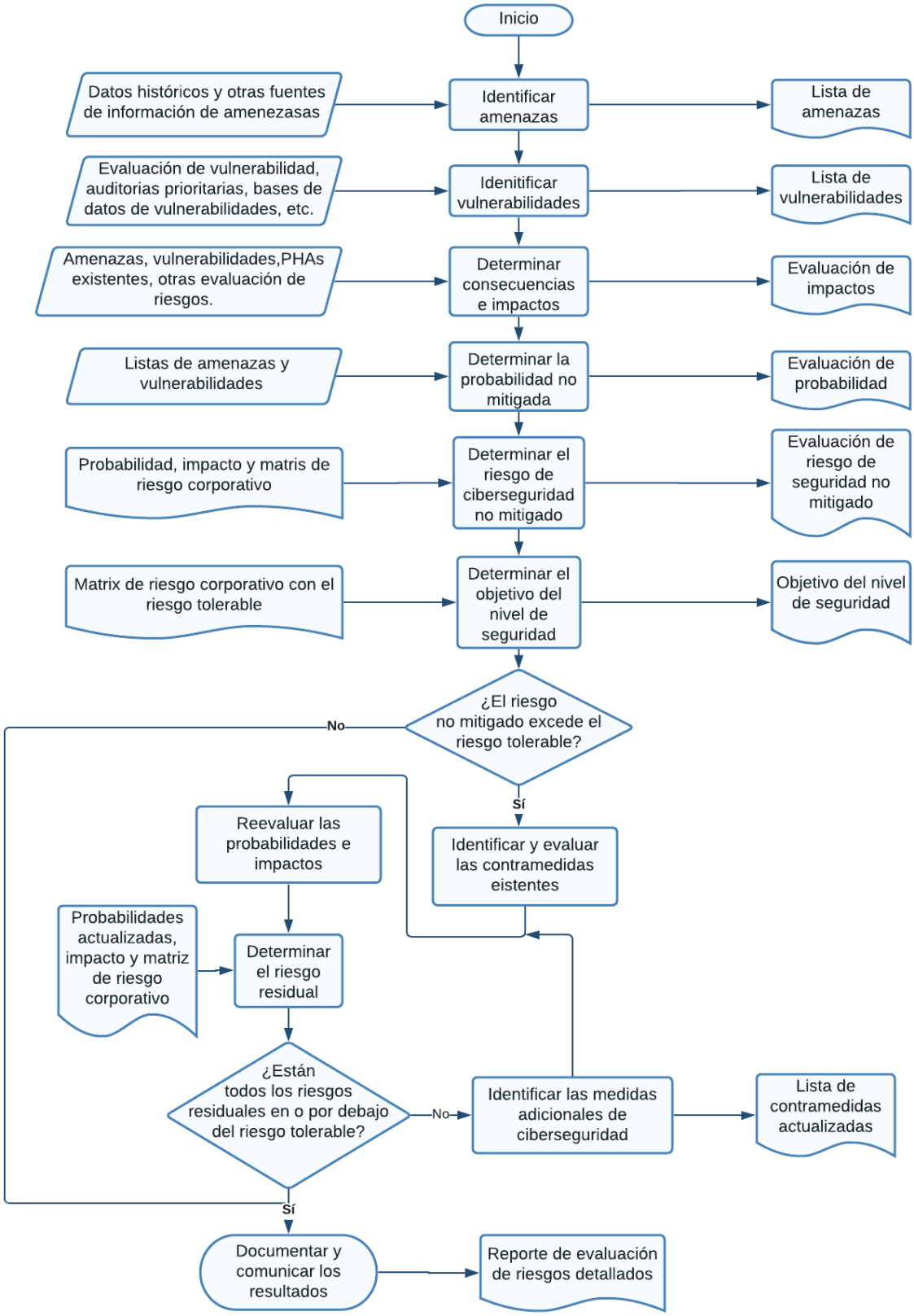

Figura 26: Diagrama de flujo de le evaluación de riesgos detallados. [42] [44]

Las subactividades presentan requerimientos y guías con métodos de desarrollo, las cuales se describen como:

3.8.1. Identificar amenazas.

Requerimientos

Se desarrollará una lista de las amenazas que podrían afectar los activos contenidos dentro de la zona o conducto.

Justificación y orientación complementaria

Es importante preparar una lista completa y realista de amenazas para realizar una evaluación de seguridad. La descripción de una amenaza debe incluir, entre otros, lo siguiente:

a) Descripción de la fuente de la amenaza.

b) Descripción de la capacidad o nivel de habilidad de la fuente de amenaza.

c) Descripción de posibles vectores de amenaza.

d) Identificación de los activos potencialmente afectados.

Algunos ejemplos de descripción de amenazas son:

- Un empleado no malintencionado accede físicamente a la zona de control de procesos y conecta una memoria USB en una de las computadoras.
- Un personal de soporte autorizado accede lógicamente a la zona de proceso utilizando una computadora portátil infectada.
- Un empleado que no es malicioso abre un correo electrónico que compromete sus credenciales de acceso.

Dado el potencial de una gran cantidad de posibles amenazas, es aceptable resumir agrupando fuentes, activos, puntos de entrada, etc.

3.8.2. Identificar vulnerabilidades.

Requerimientos

La zona o conducto se analizará en profundidad para identificar y documentar las vulnerabilidades conocidas en los activos contenidos dentro de la zona o conducto, incluidos los puntos de acceso.

Justificación y orientación complementaria

Para que una amenaza tenga éxito, es necesario explotar una o más vulnerabilidades en un activo. Por lo tanto, es necesario identificar las vulnerabilidades conocidas en los activos para comprender mejor los vectores de amenazas.

Un enfoque generalmente aceptado para identificar vulnerabilidades en un IACS es realizar una evaluación de vulnerabilidades. Consulte ISA TR84.00.09 para obtener información adicional sobre las evaluaciones de vulnerabilidad de seguridad cibernética de IACS.

Además, existen numerosas fuentes de información sobre vulnerabilidades conocidas y comunes en IACS, como ICS-CERT, proveedores de IACS, etc.

3.8.3. Determinar consecuencias e impactos.

Requerimientos

Se evaluará cada escenario de amenaza para determinar la consecuencia y el impacto en caso de que se materialice la amenaza. Las consecuencias deben documentarse en forma de impacto en el caso mayoritario en áreas de riesgo tales como seguridad del personal, pérdidas financieras, interrupción del negocio y medio ambiente.

Justificación y orientación complementaria

Estimar el impacto en el peor de los casos de una amenaza cibernética es un aporte importante para realizar el análisis de costo / beneficio de los controles de seguridad. Si el impacto del peor de los casos es bajo. El equipo de evaluación de riesgos puede decidir avanzar a la siguiente amenaza.

3.8.4. Determinar la probabilidad absoluta.

Requerimientos

Cada amenaza debe evaluarse para determinar la probabilidad absoluta de que el tratamiento se realice.

Justificación y orientación complementaria

Las contramedidas de ciberseguridad existentes no deben tenerse en cuenta al determinar la probabilidad absoluta. Sin embargo, la determinación de probabilidad reconoce cualquier capa de protección que no sea ciberindependiente, como la seguridad

física o las salvaguardias mecánicas (como las válvulas de seguridad de presión) que se hayan implementado para reducir la probabilidad.

La probabilidad se evalúa dos veces durante el proceso detallado de evaluación de riesgos. Inicialmente se determina sin tener en cuenta las contramedidas existentes para establecer el riesgo no mitigado. Además, la medida de probabilidad puede ser cualitativa y un método consiste en utilizar una escala de probabilidad definida por la organización como parte de su sistema de gestión de riesgos.

3.8.5. Determinar el riesgo de seguridad cibernética no mitigado.

Requerimientos

El riesgo de ciberseguridad no mitigado para cada amenaza se determinará combinando la medida de impacto determinada en la subactividad 3.8.3 y la medida de probabilidad absoluta determinada en la subactividad 3.8.4.

Justificación y Guía

La determinación del riesgo de ciberseguridad no mitigado a menudo se logra utilizando una matriz de riesgo que establece la relación entre el impacto de la probabilidad y el riesgo, como una matriz de riesgo corporativo.

3.8.6. Determinar el objetivo del nivel de seguridad.

Requerimiento

Se establecerá un SL-T para cada zona o conducto de seguridad.

Justificación y Guía

SL-T es el nivel de seguridad deseado para una zona o conducto IACS en particular. Se establece comunicar claramente esta información a los responsables de diseñar, implementar, operar y mantener la ciberseguridad.

SL-T puede expresarse como un valor único o un vector.

No existe un método prescrito para establecer SL-T. Algunas organizaciones optaron por establecer SL-T basándose en la diferencia entre el riesgo de ciberseguridad absoluto y el riesgo tolerable. Mientras que otros optan por establecer SL-T basado en las definiciones de SL proporcionadas en la norma ISA/IEC-62443.

3.8.7. Comparación del riesgo no mitigado con el riesgo tolerable.

Requerimientos

El riesgo absoluto determinado para cada amenaza identificada en la subactividad 5 se comparará con el riesgo tolerable de la organización. Si el riesgo no mitigado supera el riesgo tolerable, la organización continuará evaluando la amenaza completando subactividad 8 a través de la subactividad 3.8.12. De lo contrario, la organización puede documentar los resultados en la subactividad 3.8.13 y pasar a la siguiente amenaza.

Justificación y Guía

El propósito de este paso es determinar si el riesgo no mitigado es tolerable o requiere una evaluación adicional.

3.8.8. Identificar y evaluar las medidas existentes.

Requerimiento

Las contramedidas existentes en el SUC se identificarán y evaluarán para determinar la efectividad de las contramedidas para reducir la probabilidad o el impacto.

Justificación y Guía

Para determinar el riesgo residual, la probabilidad de que se produzca y el impacto deben evaluarse teniendo en cuenta la presencia y la eficacia de las contramedidas existentes. Este paso en el proceso se centra en identificar y evaluar las contramedidas existentes.

3.8.9. Reevaluar la probabilidad y el impacto.

Requerimientos

La probabilidad y el impacto se reevaluarán considerando las contramedidas y su efectividad.

Justificación y Guía

La probabilidad ilimitada determinada en la subactividad 3.8.4 no tuvo en cuenta las contramedidas existentes. En este paso, se consideran y utilizan contramedidas para determinar la probabilidad mitigada. Asimismo, las consecuencias e impacto

determinados en la subactividad 3.8.3 también deben ser reevaluadas considerando las contramedidas identificadas.

3.8.10. Determinar los riesgos residuales.

Requerimientos

El riesgo residual para cada amenaza identificada en 3.8.1 se determinará combinando la medida de probabilidad de riesgo mitigada y los valores de impacto mitigado determinados en la subactividad 3.8.9.

Justificación y Guía

La determinación del riesgo residual proporciona una medida del nivel actual de riesgo, así como una medida de la efectividad de las contramedidas existentes. Es un paso esencial para determinar si el nivel actual de riesgo excede las pautas de riesgo.

3.8.11. Están todos los riesgos residuales en o por debajo del riesgo tolerable.

Requerimientos

El riesgo residual determinado para cada amenaza identificada en 3.8.1 se comparará con el riesgo tolerable de la organización. Si el riesgo residual excede el riesgo tolerable, la organización debe determinar si se aceptará el riesgo residual. Transferido o mitigado según la política de la organización.

Justificación y Guía

El propósito de este paso es determinar si el riesgo residual es tolerable o requiere una mayor mitigación.

3.8.12. Identificar las contramedidas de ciberseguridad adicionales.

Requisitos

Las contramedidas existentes en el SUC se identificarán y evaluarán para determinar la efectividad de las contramedidas para reducir la probabilidad o el impacto.

Justificación y orientación complementaria.

Para determinar el riesgo residual, la probabilidad y el impacto deben evaluarse teniendo en cuenta la presencia y eficacia de las contramedidas existentes. Este paso del proceso se centra en identificar y evaluar las contramedidas existentes.

Proporciona orientación sobre los tipos de contramedidas y su eficacia al asignar una capacidad de nivel de seguridad a cada requisito del sistema.

3.8.13. Documentar y comunicar los resultados.

Requerimientos

Los resultados de la evaluación detallada del riesgo cibernético se documentarán, se informarán y se pondrán a disposición de las partes interesadas adecuadas en la organización. Se asignará una clasificación de seguridad de la información adecuada para proteger la confidencialidad de la documentación. La documentación incluirá la fecha en que se llevó a cabo cada sesión, así como los nombres y títulos de los participantes. La documentación que fue fundamental para realizar la evaluación del riesgo cibernético (como, diagramas de arquitectura del sistema, PHA, evaluaciones de vulnerabilidades, evaluaciones de brechas y fuentes de información sobre amenazas) se registrará y archivará junto con la evaluación del riesgo cibernético.

Justificación y Guía

Las evaluaciones de riesgos de seguridad cibernética deben documentarse y ponerse a disposición del personal adecuado de la organización. Las evaluaciones de riesgos de ciberseguridad son documentos vivos que pueden usarse para múltiples propósitos, incluidas pruebas, auditorías y evaluaciones de riesgos futuras. Sin embargo, también es importante proteger la propiedad de esta información, ya que a menudo contiene detalles confidenciales sobre los sistemas, vulnerabilidades conocidas y salvaguardas existentes.

Entre las actividades y las dependencias relacionadas con el análisis de riesgos se encuentran las siguientes en la Figura 27.

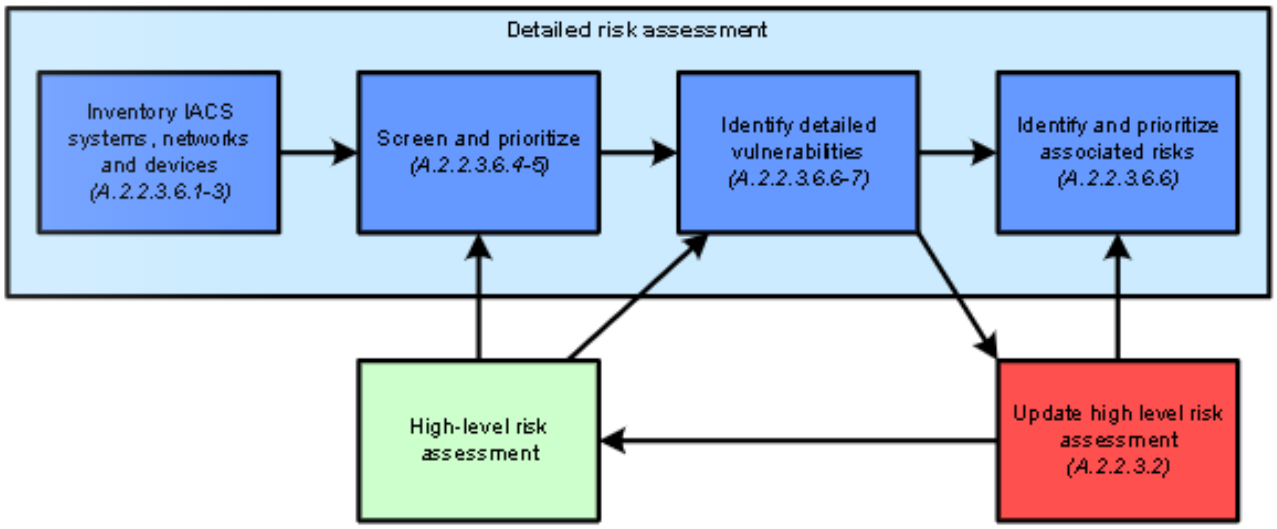

Figura 27: Actividades y dependencias para la actividad: Evaluación de riesgos detallados. [42]

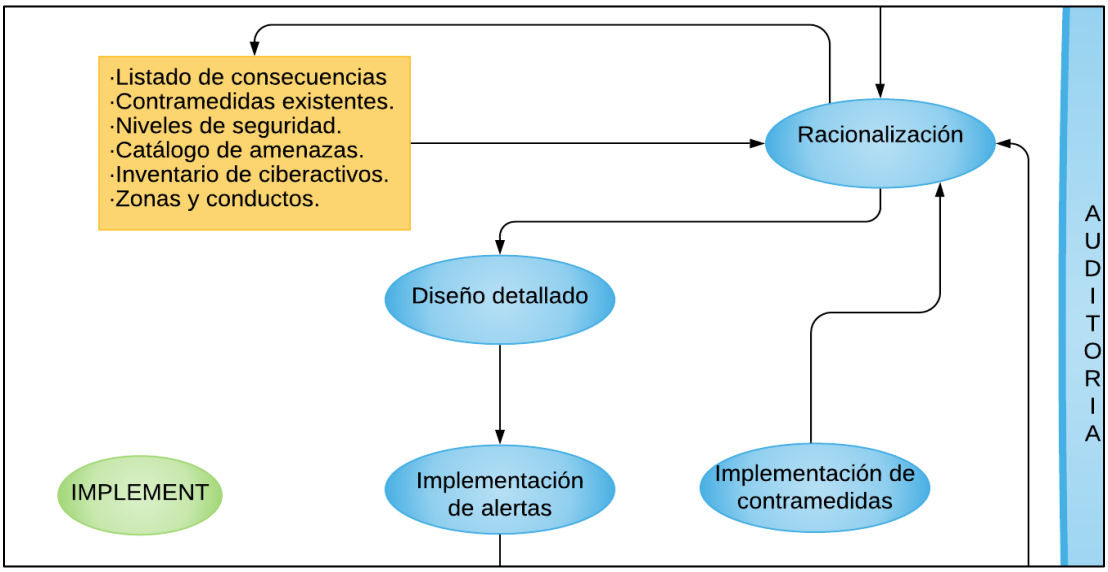

Figura 28: Fase de implementación. [44]

Para este modelo se maneja como **eje principal** la actividad que tomamos del estándar ISA 18.2 llamada **Racionalización**, a esta actividad llega el resultado de la fase de evaluación vista en la Figura 18 con toda la información concreta, correcta y actualizada de la industria con el fin de que en esta actividad se realice la justificación, determinación, priorización y clasificación de las alertas cibernéticas. Además, como complementación de la norma ISA/IEC-62443, de esta actividad se desprende un listado de entradas como se observa en la Figura 28 en el cuadro de color café claro. Este listado

se vuelve una entrada de la misma con el fin de tener una retroalimentación y un ciclo que tenga como resultado una correcta gestión de las alertas cibernéticas.

Posteriormente se realiza el diseño detallado de las alertas cibernéticas y la implementación de las alertas racionalizadas. A la par de la implementación de las alertas se realiza la implementación de contramedidas en base a las amenazas que se hayan identificado a lo largo del modelo.

3.9. Racionalización.

Objetivo

Durante la racionalización, las alertas existentes o potenciales se comparan sistemáticamente con los criterios para alarmas documentados en la filosofía de alarmas y se establecen las especificaciones y criterios de acuerdo con el análisis de criticidad realizado en la evaluación de riesgos. Si la alerta propuesta cumple con los criterios en general, entonces se documentan el punto de ajuste, la consecuencia, la acción del operador y la alerta se prioriza y clasifica de acuerdo con la filosofía. La racionalización produce la información de diseño detallado, documentado en la base de datos maestra de alertas, necesaria para la etapa de diseño del ciclo de vida de la gestión de alertas cibernéticas. Esta actividad se realiza a la par que en el estándar ISA 18.2 con información más profunda en el análisis de criticidad de la evaluación de riesgos.

Las actividades de racionalización son:

a) Justificación de la alerta.

b) Determinación del punto de ajuste de la alerta.

c) Priorización de alertas.

d) Clasificación de alertas.

e) Revisión de la racionalización.

Documentación de la racionalización

- Requerimientos de la racionalización de la documentación

La racionalización deberá determinar y documentar, como mínimo lo siguiente para cada alerta racionalizada según la filosofía de alarmas de la empresa para cada estado de la planta:

a) Tipo de alerta.

b) Prioridad de alerta.

c) Clase de alerta.

d) SetPoint de la alerta o condición lógica.

e) Acción del operador.

f) Consecuencias de la inacción.

Atributos adicionales de la alerta pueden ser determinados durante la racionalización de alarmas acorde a la filosofía de alarmas.

- Recomendaciones para la documentación de la racionalización.

La racionalización debería determinar y documentar lo siguiente para cada alerta racionalizada según la filosofía de alarma para cada estado de la planta:

a) El máximo tiempo de respuesta permitible.

b) La causa probable.

c) La razón fundamental para el SetPoint de la alerta.

d) El método de identificación.

e) La necesidad para técnicas avanzadas de alertas. Si es necesario.

- Estados de la planta.

Los estados de la planta pueden incluir:

a) Puesta en marcha.

b) Operación normal.

c) Operación, paso o fase en procesos batch.

d) Apagar o parar.

Justificación de la alerta

- Proceso de la justificación de la alerta.

Cada alerta que requiere racionalización es comparada con los criterios en la filosofía de alarmas y con el análisis de criticidad de la evaluación de riesgos, para justificar que es una alerta debe:

a) La alerta es dirigida al operador.

b) La alerta indica una desviación del proceso, una condición anormal o un mal funcionamiento del equipo.

c) La alerta requiere una respuesta oportuna.

- Enfoque de justificación.

La justificación de alerta de proceso debe:

a) Utilizar un equipo de enfoque, incluido el conocimiento del proceso y del sistema de control.

b) Dependen en gran medida de la información del operador.

- Justificación de la alerta individual.

Todas las alertas para ser racionalizadas son sistemáticamente revisadas. Esto generalmente se hace por progresión a través de dibujos de ingeniería, bases de datos o pantallas HMI. La información que se debe capturar para cada alerta racionalizada debe especificarse en la filosofía de alarma y normalmente incluye:

a) Verificación de que la alerta propuesta cumple los criterios para una alerta establecidos en la filosofía.

b) Las acciones que el operador puede tomar en respuesta a la alerta.

c) La consecuencia que ocurrirá si no se toman medidas.

d) El tiempo de respuesta permitido.

Aquellas alertas para las cuales la acción del operador es simplemente transmitir la información a la persona o grupo apropiado para la acción (por ejemplo, alertas de diagnóstico de la industria) deben revisarse para determinar si existe un método alternativo para transferir la información sin sobrecargar al operador o al sistema de alertas.

- Rendimiento del sistema de impacto de alarma.

La justificación de la alerta debería justificar que:

a) La alerta no se convertirá en una molestia.

b) La alerta no duplica otra alarma.

Se pueden especificar técnicas de alertas avanzadas (por ejemplo, alertas basadas en estado o alertas basadas en lógica) para evitar un impacto negativo en el rendimiento del sistema de alertas debido a las condiciones enumeradas anteriormente

Determinación del SetPoint de la alerta

Se aplica la guía para la determinación de los puntos de ajuste de alerta establecidos en la filosofía de alarma. Los métodos efectivos utilizan información que incluye:

a) El tiempo de respuesta permitido.

b) La complejidad de la acción del operador.

c) El tiempo necesario para completar la acción del operador.

d) El rango de operación normal.

e) Otros límites operativos o de diseño.

f) Conocimiento del proceso operativo e histórico.

Priorización

La prioridad de alerta se utiliza para ayudar al operador a determinar el orden en el que se deben responder. El método de asignación de prioridad definido en la filosofía de alarma se aplica a la alerta racionalizada y se le asigna una priorización. La priorización efectiva generalmente da como resultado que las prioridades más altas se elijan con menos frecuencia que las prioridades más bajas. La mayor parte de las alertas deben asignarse a la prioridad de alerta más baja (la menos importante) y la menor a la prioridad de alerta más alta (la más importante) con la consecuencia y el tiempo de respuesta permitido, de modo que las alarmas de prioridad más baja tienen las consecuencias menos graves y el tiempo más largo permitido. Los tiempos de respuesta y las alertas de máxima prioridad tienen las consecuencias más graves (por ejemplo, alertas de incendio y de gas) y los tiempos de respuesta más cortos permitidos.

La priorización puede incluir la consideración de clases de alerta (por ejemplo, clases de HMA) o métodos de identificación (por ejemplo, LOPA) para establecer la prioridad de la alerta.

Clasificación

Las alertas se asignarán a una o más clases según se define en la filosofía de alarma. La clasificación puede ocurrir antes, durante o después de la justificación y priorización de la alerta.

No es necesario que las alertas de la misma clase tengan la misma prioridad.

Revisión

Una vez completada la priorización de la justificación inicial y la clasificación de todas las alertas requeridas, los resultados deben revisarse para garantizar la aplicación coherente de los criterios a lo largo del proceso. Los resultados deben compararse con la filosofía de alarma y el análisis de criticidad.

Eliminación de alertas rechazadas

Las alertas existentes que son rechazadas por no cumplir con los criterios para una alerta deben documentarse junto con la base (es decir, el criterio que no cumplió) que justifica la eliminación. Las alertas rechazadas pueden ser candidatas a otras formas de notificaciones (por ejemplo, alarmas). Luego, esas alertas deben estar sujetas a una revisión adicional mediante el procedimiento MOC para eliminar la alarma del sistema.

Documentación

Se debe documentar la racionalización para que se convierta en la base para garantizar la integridad del sistema de alertas. La documentación (por ejemplo, una base de datos maestra de alertas) es el vínculo entre cada alerta y la filosofía de alarma y se puede utilizar para varios propósitos, que incluyen:

a) Entrada a la etapa de diseño detallado del ciclo de vida de la alerta.

b) Utilización como parte del MOC.

c) Procedimientos de respuesta a alertas.

d) Formación y uso por parte de los operadores.

e) Auditoría periódica y conciliación de los ajustes de alerta del sistema de control.

f) Evaluación del monitoreo de alertas y datos de efectividad.

3.10. Diseño detallado.

Objetivo

El diseño de HMI para sistemas de alertas es parte de la etapa del ciclo de vida del diseño detallado. Esta describe la funcionalidad para proporcionar indicaciones de alerta y funciones relacionadas al operador y otros usuarios de HMI. La indicación y visualización de alertas es solo un componente del diseño de la HMI y contribuye a una interacción eficaz entre el operador y el proceso. (Panel de visualización de alarmas y alertas)

Requerimientos

El diseño detallado de las alertas comprende desde la documentación, las alertas y el HMI del SCADA del proceso. Estos requerimientos se listan de manera:

Durante el proceso de diseño básico, los atributos de alerta predeterminados deben seleccionarse para cada alerta que se haya racionalizado y configurado según el criterio de ingeniería. Los atributos como el punto de ajuste y la banda muerta pueden ser diferentes según el tipo de alerta específico que se implementará. La definición de los atributos de alerta adecuados puede ayudar a minimizar la cantidad de alertas molestas que se generan durante el funcionamiento. En las siguientes subcláusulas se proporcionan recomendaciones para el diseño de atributos de alarma específicos. Los atributos de alarma deben incluir:

a) Descripción de la alerta.

b) Punto de ajuste de alerta o condiciones lógicas.

c) Prioridad de alerta.

d) Banda muerta de alerta.

e) Retardo a la conexión o retardo a la desconexión.

f) Grupo de alerta.

g) Mensaje de alerta.

El HMI debe tener todos los requerimientos para diseño final del HMI:

1. Requerimientos de la información

2. Requerimientos funcionales.

3. Requerimientos del Display.

4. Requerimientos del registro de alarmas.

Esto en consecuencia a las buenas prácticas bajo un conjunto de patrones que se listan en cada una.

Además se explica un poco acerca de las alertas basadas en lógica las cuales se logran utilizando técnicas (por ejemplo, lógica booleana o árboles de decisión) para determinar las modificaciones que se realizarán en los sistemas de alerta. Esto puede implementarse en el sistema de control o externamente al sistema de control.

3.11. Implementación de alertas.

Objetivo

La implementación es una etapa separada del ciclo de vida de la alerta, que es la transición del diseño a la operación. Este cubre los requisitos generales para implementar o modificar una alerta o un sistema de alerta.

Métodos

Los sistemas de alerta se deben probar durante la implementación para garantizar que se cumplan los elementos apropiados en la filosofía de alarma y ASRS. La prueba del sistema de alerta modificado debe ser apropiada para la naturaleza del cambio, según lo determinado por los procedimientos del MOC del sitio. Las pruebas de los nuevos sistemas de alerta incluirán:

a) Las indicaciones sonoras y visuales para cada prioridad de alerta.

b) Las características de la HMI, como mensajes de alerta en el resumen de alerta o equivalente.

c) Los métodos para retirar una alerta del servicio y volver a ponerla en servicio.

d) Los métodos de estantería.

e) Los métodos para la supresión de alerta.

f) Cualquier función adicional de técnicas de alerta mejoradas o avanzadas.

g) Los métodos de filtrado de alerta, clasificación, vinculación de alarmas a pantallas de proceso.

Documentación

Se proporcionará la siguiente documentación:

a) La información de racionalización documentada.

b) Información suficiente para realizar pruebas de alertas.

c) Los procedimientos de respuesta a alertas.

d) Cualquier supresión diseñada o documentación alarmante mejorada.

e) Documentación de prueba, si así lo requiere la filosofía de alarma.

Una vez completada la implementación del sistema de alerta, la información de racionalización se actualizará de acuerdo con el procedimiento MOC del sitio.

3.12. Implementación de contramedidas

La selección de contramedidas es el proceso técnico de gestión de riesgos. La organización tiene contramedidas comunes preseleccionadas de tolerancia al riesgo y los resultados de la evaluación de riesgos de alto nivel y nivel detallado impulsan el enfoque de gestión de riesgos para la selección de contramedidas. Si la organización está implementando un nuevo sistema o modificando un sistema existente, esto impulsa una actualización de la evaluación de riesgos detallada y de alto nivel para el escenario en el que se implementa este nuevo sistema. La selección de las contramedidas relacionadas con el sistema nuevo o modificado procede a partir de esta información de riesgo actualizada. El desarrollo o modificación de sistemas requiere una actualización de los planes de respuesta a incidentes y continuidad del negocio.

Contramedidas de seguridad seleccionadas.

Se analizan muchas las cuestiones de políticas, procedimientos y prácticas relacionadas con estas contramedidas de seguridad en particular. Principalmente alrededor de estos seis elementos:

- Personal de Seguridad.
- Seguridad física y ambiental.
- Segmentación de la red.
- Control de acceso: administración de cuentas.
- Control de acceso: Autenticación.
- Control de acceso: Autorización.

Estas contramedidas particulares se seleccionaron para su inclusión porque su impacto central en la política y la arquitectura hacen que sea esencial considerarlas desde el principio al construir cualquier CSMS. No es la intención de esta actividad especificar una lista completa y suficiente de contramedidas, ya que la integridad se determina mediante la racionalización y el proceso de evaluación y gestión de riesgos descritos en el modelo desarrollado.

En el análisis de riesgo detallado se realiza una puntual identificación de contramedidas, sin embargo es de suma importancia para este modelo establecer una actividad que se realice a la par con la implementación de alertas, debido a que se tiene información más detallada, racionalizada y clara de estas y se puede establecer un plan de respuesta más óptimo y seguro. No obstante, la información del análisis de riesgo detallado se reutiliza y se le añaden optimizaciones en base al conocimiento que se tiene de las alertas obteniendo así un lazo cerrado de riesgos y reduciendo al mínimo las probabilidades y por consecuencia sus impactos.

Esta implementación se debe realizar según la norma ISA/IEC-62443 y junto con las contramedidas existentes ya especificadas se toman las decisiones correctas alrededor de las alertas definidas e implementadas.

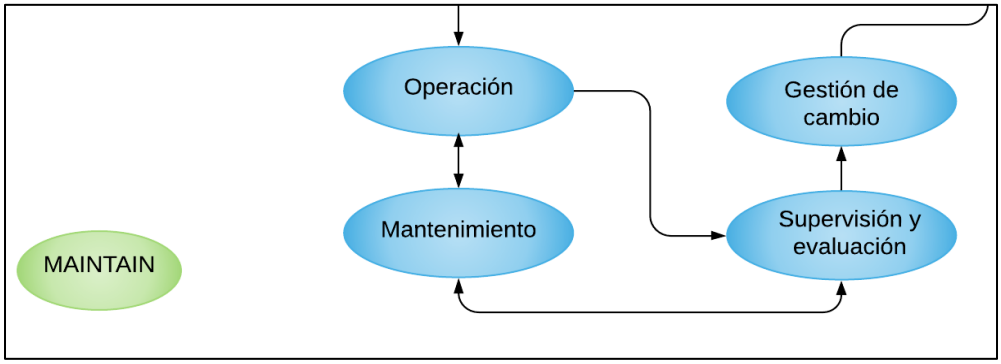

Figura 29: Fase de mantenimiento. [44]

Como fase final se obtiene la de fase de mantenimiento descrita en la Figura 29. En este, se realizó un ciclo interno tomado del estándar ISA 18.2 cuyo propósito es realizar supervisión y mantenimiento constante del sistema implementado, en este caso de la gestión de alertas cibernéticas. Las cuatro actividades observadas se realizan por expertos en el área y deben tener inducción correcta como resultado del modelo implementado.

3.13. Operación.

Objetivo

La operación es una etapa separada del ciclo de vida de la gestión de alertas. Este cubre los requisitos para que las alertas permanezcan y regresen al estado operativo. El estado operativo es cuando una alerta puede indicar una condición anormal al operador. También se describe el uso de herramientas para el manejo de alertas dentro del estado operativo. La operación es la etapa del ciclo de vida posterior a la implementación y al regresar del mantenimiento.

Método

Se manejan los siguientes ítems como respuesta a las alertas:

Procedimientos de respuesta a alertas: Los procedimientos de respuesta de alerta deben ser fácilmente accesibles para el operador según se especifica en la filosofía de alarma.

Estantería de alertas: Se permitirán las estanterías de alerta según se documente según se detalla en la filosofía de alarma. el nombre de la etiqueta para la alerta, la descripción de la etiqueta o la descripción de la alerta, el tipo de alerta, el punto de ajuste de la

alerta, las causas potenciales, la consecuencia de la inacción, la acción del operador, el tiempo de respuesta permitido y la clase de alerta.

Capacitación de actualización para operadores: Los requisitos de formación para las alertas se determinarán mediante la clasificación de alertas u otros métodos detallados en la filosofía de alarmas.

3.14. Mantenimiento.

Objetivo

El mantenimiento es una etapa separada del ciclo de vida de la gestión de alertas. La cláusula 15 cubre los requisitos para la prueba, el reemplazo y la reparación del sistema de alerta. Describe la transición de las alertas al estado fuera de servicio y luego volver al servicio. El mantenimiento también requiere capacitación de actualización para el personal que mantiene el sistema de alarma.

Concepto:

Se manejan diferentes conceptos dentro de esta fase como:

Prueba de alertas periódica: Los requisitos de las pruebas periódicas de alerta se determinarán mediante la clasificación de alerta u otros métodos detallados en la filosofía de alarma. El propósito de las pruebas periódicas es asegurar que la alerta continúe funcionando como fue diseñada.
Alertas fuera de servicio: Los requisitos para el procedimiento fuera de servicio serán determinados por la clasificación de alerta u otros métodos como se detalla en la filosofía de alarma.

Reparación de equipos: La información relacionada con un mal funcionamiento de la alerta debe estar disponible para el operador. Las alertas afectadas por equipos que no funcionan (por ejemplo, equipos que se ponen fuera de servicio para reparación o mantenimiento preventivo) deben ponerse fuera de servicio si la condición no se resuelve dentro de un tiempo razonable como se especifica en la filosofía de alarma.

Reemplazo de equipo: El procedimiento MOC debe abordar el equipo de reemplazo (por ejemplo, dispositivos de medición, válvulas, equipo de proceso) que cambiarán los atributos de la alerta. Si se realiza un reemplazo, es posible que se requiera la validación de la alerta según la clase de alerta, como se especifica en la filosofía de alarma.

Formación de actualización para el mantenimiento: Los requisitos de formación de repaso para el mantenimiento de alertas serán determinados por los requisitos de clase como se detalla en la filosofía de alarma. Los requisitos de formación de repaso para el mantenimiento de alertas serán determinados por los requisitos de clase como se detalla en la filosofía de alarma.

3.15. Supervisión y evaluación.

Objetivo

Una vez que se ha implementado el ciclo de vida de la gestión de alertas y se han reducido las alertas molestas (por ejemplo, alertas con vibración), la tasa de alerta resultante refleja más fielmente la eficacia del control del proceso, las prácticas operativas y los sistemas de mantenimiento. El rendimiento del sistema de alerta se puede mejorar aún más mediante mejoras en el control, la operación o el mantenimiento del proceso. Las técnicas de alerta avanzadas a menudo son necesarias para cumplir con los objetivos de rendimiento de la filosofía de alarma.

Métodos

Son posibles varios tipos de análisis de sistemas de alerta, indicadores clave de rendimiento y métodos. Tanto la evaluación inicial del sistema de alerta como el monitoreo continuo deben incluir medidas como las que se muestran en la Tabla 2. La lista de análisis elegidos debe coincidir con la filosofía de la alarma.

1. Tasa de alerta promedio por consola de operador.
2. Tasa de alerta máxima por consola de operador.
3. Inundaciones de alerta.
4. alertas frecuentes.
5. Charlas y alertas fugaces.
6. Alertas obsoletas
7. Distribución de prioridad de alerta anunciada.

3.16. Gestión de cambios.

Objetivo

La gestión del cambio es una etapa separada del ciclo de vida. Cubre los requisitos para cambios en el sistema de alarma relacionados con la adición de nuevas alarmas, eliminación de alarmas existentes, modificación de atributos de alarma, cambios en las funciones del sistema de alarma, autorización y documentación. El propósito de la gestión de cambios es asegurar que los cambios estén autorizados y sujetos a los criterios de evaluación descritos en la filosofía de alarma. El proceso MOC (management of change) asegura que se apliquen las actividades apropiadas del ciclo de vida a los cambios en el sistema de alertas.

Método

La gestión de cambio es un método en general que debe abordar los siguientes temas:

1. La base técnica del cambio propuesto.
2. El impacto del cambio de salud, la seguridad y el medio ambiente.
3. Están de acuerdo con la filosofía de alarma, las modificaciones para los procedimientos.
4. Operativos.
5. Periodo de tiempo para el que el cambio es válido
6. El grado de seguridad se mantiene si la alerta se implementa por razones de seguridad.
7. Disciplinas apropiadas se incluye en la revisión.
8. Cambios en el sistema de alerta, incluidas las actualizaciones del sistema, seguir todas las actividades posteriores apropiadas del ciclo de vida de la gestión de alertas.
9. La implementación de todos los cambios se adhiere a los procedimientos especificados en la filosofía de alarma.

3.17. Auditoria

Objetivo

La auditoría es una etapa separada del ciclo de vida que se lleva a cabo periódicamente para mantener la integridad del sistema de alerta y los procesos de gestión de alertas. La auditoría del rendimiento del sistema puede revelar brechas que no son evidentes en el monitoreo. La ejecución contra la filosofía de alarma se audita para identificar cualquier requisito de mejora del sistema, como modificaciones a la filosofía de alarma o al proceso de trabajo definido en el mismo.

Método

Se deben realizar entrevistas o cuestionarios al personal como parte de la auditoría para identificar problemas de rendimiento y usabilidad. Los temas de la entrevista pueden incluir:

- Las alertas ocurren solo en condiciones que requieren la acción del operador, la prioridad de alerta
- Se aplica de manera consistente y significativa, los operadores tienen tiempo suficiente para responder alertas
- Se definen y se siguen las funciones y responsabilidades de los usuarios del sistema de alertas.

La filosofía de alarma debe ser auditada según las pautas de la industria y los requisitos y recomendaciones de esta norma. Los procesos y procedimientos de trabajo que garantizan el cumplimiento de la filosofía de alarma deben evaluarse periódicamente para determinar su eficacia. La auditoría debe revisar toda la documentación relacionada, que puede incluir:

- Verificación de que las alertas requieren la acción del operador para evitar una consecuencia definida.
- Documentación de los atributos de alerta y racionalización
- Documentación MOC de modificaciones a atributos de alerta en la base de datos de alertas maestra.
- Informes de monitoreo de desempeño de alertas.
- Documentación de reparaciones de alertas averiadas.
- Documentación de alertas fueras de servicio.

IV. Conclusiones y trabajos futuros

La gestión de alarmas, incidentes y alertas cibernéticas son ciclos repetitivos debido a que se basan en la mejora continua y deben ser actualizados constantemente para tener información real de la empresa, proceso o industria. En este trabajo se realizó la propuesta de un modelo cuyo eje o actividad principal es la racionalización, debido a que actualmente no se está realizando correctamente en el campo de las alertas cibernéticas y además del número de alarmas industriales, también están creciendo los ataques informáticos a todo tipo de entidades privadas y públicas. Se espera que con este modelo se logren identificar las alertas cuyas amenazas son potencialmente más peligrosas que otras y se logren controlar en el momento correcto para realizar la principal razón por lo que se realizó este proyecto, la prevención de desastres.

La gestión de alertas cibernéticas, permite obtener un diagnóstico en tiempo real de la industria y si bien la actividad principal de este modelo es la racionalización, no se debe desconocer la importancia de todas las demás, debido a que es de suprema importancia realizar un análisis completo al sistema o industria en cuestión y también, tener un ciclo final como el que se observa en la fase de "Mantenimiento" para la optimización constante del sistema de gestión de alertas. Este ciclo de vida en conjunto, tiene lo más relevante de dos estándares y normas que han sido guías en la seguridad de la industria, por lo que se espera que una futura aplicación llegase a tener resultados beneficiosos para los receptores de riesgo y de realizarse futuras modificaciones, se moldee acorde a las alertas cibernéticas con respecto a su crecimiento. Se espera que con el modelo gráfico y las especificaciones basadas en los modelos originales, se solucionen parte de las malas prácticas actuales en múltiples compañías, o por lo menos tener el primer pilar con relación a la gestión de alertas cibernéticas. Se espera también, realizar los cambios que se consideren necesarios y proponer ante el comité de ISA la formalización de un apartado que incluya este modelo como base para el contexto actual de la gestión de alertas cibernéticas en las tecnologías de operaciones (OT).

La empresa Wiseplant, ha desarrollado prácticas en diferentes organizaciones las cuales están protegidas bajo el principio de confidencialidad de la empresa. Sin embargo, en caso de avanzar con el proceso ante el comité de ISA, han expuesto se podría compartir la información con el permiso correspondiente. Para este trabajo no se pudieron exponer las prácticas de acuerdo al principio de confidencialidad pactado con cada una de las empresas usuarias.

La información utilizada para el desarrollo de la propuesta fue obtenida de los estándares ISA 18.2 y la norma ISA/IEC-62443 brindada y utilizada bajo el concepto de confidencialidad correspondiente.

V. Referencias

[1] S. Atanasova, «https://repositori.urv.cat/estatic/TFG0011/en_TFG3376.html,» 12 07 2021. [En línea]. Available: https://repositori.urv.cat/estatic/TFG0011/en_TFG3376.html.

[2] C. B. Y. Cortés, «Conciencia tecnológica,» 26 11 2017. [En línea]. Available: https://www.redalyc.org/jatsRepo/944/94454631006/html/index.html.

[3] I. E. D. Villanueva, «predictiva21,» 2021. [En línea]. Available: https://predictiva21.com/revoluciones-industriales-mundo-i-parte/.

[4] M. F. Vega, «Ministerio de trabajo y asuntos internacionales de España,» 1999. [En línea]. Available: https://www.insst.es/documents/94886/326827/ntp_390.pdf/967860c0-87f3-4cb8-8421-6e3a8583a941.

[5] I. Queirolo, «sistemamid,» 02 2011. [En línea]. Available: https://sistemamid.com/panel/uploads/biblioteca/2015-03-21_09-16-53117532.pdf.

[6] Huellas verdes, «INNOVA,» 10 01 2018. [En línea]. Available: www.innovaambiental.com.co/los-9-peores-desastres-de-la-industria-quimica/.

[7] N. Yañez, «pdfcoffee,» [En línea]. Available: https://pdfcoffee.com/6-isa-182-gestion-de-alarmas-3-pdf-free.html.

[8] H. Gutierrez, «El país,» 2021. [En línea]. Available: https://elpais.com/noticias/ataques-informaticos/. [Último acceso: 4 4 2022].

[9] Logitek, «industrial cybersecurity,» 17 01 2019. [En línea]. Available: https://www.ciberseguridadlogitek.com/norma-iec-62443-integrara-common-regulatory-framework-cybersecurity-crf/#:~:text=La%20norma%20IEC%2062443%20es,industrial%20frente%20a%20amenazas%20cibern%C3%A9ticas%20(.

[10] mintic, «mintic,» 2016. [En línea]. Available: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

[11] I. 27001, «https://normaiso27001.es/,» 2016. [En línea]. Available: https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/.

[12] oasys-sw, «oasys-sw,» 2021. [En línea]. Available: https://oasys-sw.com/diferencias-entre-it-y-ot/#:~:text=En%20el%20caso%20de%20OT,IT%20y%20OT%3A%20la%20seguridad.. [Último acceso: 04 04 2022].

[13] snhu, «southern new hampshire university,» 29 10 2019. [En línea]. Available: https://www.snhu.edu/about-us/newsroom/2018/07/what-is-information-technology.

[14] I. N. J. R. -. I. J. A. I. Ramírez, «ISAmex,» 15 12 2012. [En línea]. Available: https://www.isamex.org/intechmx/index.php/2020/12/15/diferencia-entre-it-y-ot/. [Último acceso: 28 06 2021].

[15] smctraining, «smctraining,» 2021. [En línea]. Available: https://www.smctraining.com/es/webpage/indexpage/311.

[16] G. M. Vela, «core,» 09 2014. [En línea]. Available: https://core.ac.uk/download/pdf/41814524.pdf.

[17] EEMUA, «EEMUA,» 2021. [En línea]. Available: https://www.eemua.org/home.aspx. [Último acceso: 04 04 2022].

[18] I. Queirolo, Congreso Latinoamericano y 3° Nacional de Seguridad, Salud Ocupacional y Medio Ambiente en la industria del Petróleo y del, [En línea]. Available: https://www.iapg.org.ar/congresos/2010/seguridad/PublicarWEB/GestionDeAlarmasEnSeguridadIntegrada.pdf.

[19] OSHA, «Occupational Safety and Healt Administration,» 2002. [En línea]. Available: https://www.osha.gov/sites/default/files/publications/highly-hazardous-chemicals-factsheet-spanish.pdf. [Último acceso: 2022].

[20] J. C. P. Pérez, «La importancia de prevenir los riesgos laborales en una Oranización,» 2015.

[21] D. Rapini, «Rockwellautomation,» [En línea]. Available: https://www.rockwellautomation.com/es-co/company/news/blogs/successful-alarm-management-with-your-distributed-control-system.html.

[22] library, «library,» 2014. [En línea]. Available: https://1library.co/document/qv89pgrz-filosofia-alarmas-central-termica-combinado-eficiencia-sistema-alarmas.html.

[23] S. Moya, «ISAMex,» 2017, [En línea]. Available: https://www.isamex.org/intechmx/index.php/2017/03/20/mejora-la-seguridad-de-tu-planta-la-implementacion-de-un-sistema-de-administracion-de-alarmas/.

[24] ISA, «ISAMex,» 2022. [En línea]. Available: https://www.isamex.org/intechmx/index.php/manejo-y-gestion-de-alarmas-utilizando-el-estandar-ansi-isa-18-2/#:~:text=El%20est%C3%A1ndar%20ANSI%20%2F%20ISA%2D18.2%20por%20lo%20tanto%2C%20intenta,seguridad%20de%20los%20procesos%20industriales..

[25] M. Á. Antoñanzas, «CNN en español,» CNN en español, 09 02 2021. [En línea]. Available: https://cnnespanol.cnn.com/video/ataque-informatico-aguas-florida-hacker-hidroxido-envenenamiento-seg-pkg-miguel-angel-antonanzas/. [Último acceso: 09 04 2021].

[26] Portafolio, «Portafolio.co,» [En línea]. Available: https://www.portafolio.co/economia/finanzas/reduccion-costos-causo-explosion-refineria-bp-354552.

[27] B. Mundo, «BBC,» 2010. [En línea]. Available: https://www.bbc.com/mundo/internacional/2010/06/100602_derrame_petroleo_bp_cifras_golfo_mexico_amab. [Último acceso: 2021].

[28] G. M. Vela, GESTIÓN DE ALARMAS EN SISTEMAS DE CONTROL DISTRIBUIDO, 2014.

[29] J. Paredes, «Va de Barcos,» 2017. [En línea]. Available: https://vadebarcos.net/2017/09/16/desastres-maritimos-plataforma-piper-alpha/.

[30] HSE, «HSE,» 194. [En línea]. Available: https://www.hse.gov.uk/comah/sragtech/casetexaco94.htm.

[31] gettyimages, «Gettyimages,» 1994. [En línea]. Available: https://www.gettyimages.co.uk/detail/video/buncefield-fuel-depot-explosion-possible-causes-itn-lib-news-footage/679984236.

[32] ISA, «ANSI/ISA-18.2-2016,» North Carolina.

[33] I. 18.2, Management of Alarm Systems, 2016.

[34] W. G. -. C. Erazo, «Análisis del sistema de alarmas del EMS del CENACE,» p. 9.

[35] ISA, «ISA 18.2,» *ISA,* p. 82, 2016.

[36] G. G. Juanes, «El 62% de las empresas afirma que recibe más ciberataques desde el comienzo de la Covid-19,» *Cuadernos de seguridad,* 13 01 2021.

[37] G. G. Juanes, «La automatización dará forma a la ciberseguridad en 2021,» *cuadernosdeseguridad.com,* 18 12 2020.

[38] I. 99, Manufacturing and Control Systems Security, DRAFT dISA-99.00.01.

[39] I. 99, Part 2: Establishing a Manufacturing and Control, dISA-99.00.02.

[40] ISA/IEC–62443-1-1, «ANSI/ISA–62443-1-1 (99.01.01)–2007,» de *Security for Industrial Automationand Control SystemsPart 1-1: Terminology, Concepts, and Models*, AMERICAN NATIONAL STANDARD, 2007, pp. 65-68 .

[41] Z. S. SERVER, «Wiseplant,» [En línea]. Available: https://wiseplant.com/catalog/zcm-srvr/.

[42] s. a. s. Wiseplant smart, «Wiseplant,» [En línea]. Available: https://wiseplant.com/cybersecurity/.

[43] Wiseplant, «Curso 2160,» 2021.

[44] C. Muñoz, «(Realización propia)Propuesta armonizada del estándar ISA 18.2 e ISA/IEC-62443 bajo un enfoque integral para la empresa WISEPLANT.,» Popayán, 2021.

[45] ISA/IEC–62443-3-3, «Security for industrial automation and control systems,» 2017.

[46] I. Queirolo, «Petrotecnia,» Febrero 2011. [En línea]. Available: http://www.petrotecnia.com.ar/febrero2011/sin/Alarmas.pdf. [Último acceso: Febrero 2021].

[47] A. n. standard, management of alarm systems for the process industries, 2016.

[48] L. institute, «Lisainstute,» 29 10 2019. [En línea]. Available: https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas#:~:text=Investigaci%C3%B3n%3A%20laboratorios%20que%20por%20su,(sector%20e%20infraestructura%20sanitaria).&text=Transportes%20(aeropuertos%2C%20puertos%2C%20instalaciones,sistemas%20de%20co.

[49] I. cibersegurity, «ciberseguridadlogitek,» [En línea]. Available: https://www.ciberseguridadlogitek.com/wp-content/uploads/ciberseguridadlogitek_ley-_PIC_PSO_PPE_wp.pdf.

[50] A. industrial, «InfoPLC,» 3 2 2019. [En línea]. Available: https://www.infoplc.net/actualidad-industrial/item/106194-estado-ciberseguridad-industrial-2018-espana. [Último acceso: 2021].

[51] J. Paredes, «va de barcos,» 17 09 2017. [En línea]. Available: https://vadebarcos.net/2017/09/16/desastres-maritimos-plataforma-piper-alpha/. [Último acceso: 22 03 2021].