UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ZARAGOZA

LA IMPORTANCIA DE LA CIBERSEGURIDAD; ESTUDIO SPR DESARROLLADO PARA UNA PLANTA HIDRODESULFURADORA DE NAFTAS TÍPICA.

T E S I S

QUE PRESENTA:

VARGAS FLORES MARCOS

PARA OBTENER EL TÍTULO DE

INGENIERO QUÍMICO

DIRECTOR DE TESIS

M.I. MARIO PEREZ MARÍN

ASESORES

M. C. VICTOR HUGO VILLAR MARÍN

I.Q. DELFINO GALICIA RAMIREZ

Ciudad de México, año 2021

Agradecimientos y Dedicatorias

A mi madre Roció, por tantos sacrificios en mi niñez, y su amor incondicional hacia mi maltrecha persona. Tu hijo te ama mucho, mamá. Por favor vive mucho más tiempo.

A mi abuela Elena, por sus cuidados, su cariño y su apoyo sin igual que siendo sincero no sentí merecer, pero siempre estuvo ahí. Te amo mucho Abue, te pude dar tu libro al fin.

A mi familia en general, todos y cada uno de ellos, por confiar en mí, por todo su apoyo, sus ánimos y los regaños oportunos, los consejos y todo lo demás que me sería imposible poner en palabras. Los adoro familia, no sé qué sería de mí sin ustedes.

A mi novia Rosalinda, gracias por estar a mi lado y por dejarme estar junto a ti, tu amor y apoyo han sido fundamentales en mi vida este tiempo, espero siga siendo asi por muchos más años. El futuro nos pinta bien. Te amo.

A mis amigos, dicen que el que es amigo de muchos no es amigo de nadie, yo con todo respeto discrepo, he tenido la fortuna de conocer a mucha gente maravillosa y dentro de ella a bastantes personas muy especiales que considero amigos, gente que para bien o para mal ha influido en mí.

Amigos míos. Steve, Francisco, Salvador, Israel, Carlos, todos los "Luises", todos los "Fernando", Por nombrar a algunos. A todos, nombrados y omitidos los estimo y les agradezco el buen trato, así como las palabras de aliento, sepan que los admiro y les deseo lo mejor.

A mi director y asesores de tesis y Sinodales. Para ustedes no tengo más que agradecimiento ilimitado, admiración, respeto y buenos deseos.

Profesor Mario, le agradezco infinitamente su tutela, su apoyo y sus jalones de orejas, sé que muchas veces no fui muy disciplinado, como sea no se rindió conmigo, muchas gracias.

Profesor Víctor, si no fuera por su confianza en mí, no se me habrían presentado las oportunidades a las que he tenido acceso. Infinitas gracias.

Profesores Delfino, Alejandro y Rodolfo. Gracias por darme parte de su tiempo para pulir este trabajo, valoro mucho el esfuerzo que hicieron y siempre les estaré en deuda.

A todos mis profesores. Gracias al cumplimiento de su labor es que al igual que mis compañeros egresados he logrado alcanzar una meta más. Ustedes son fuentes invaluables de conocimiento y experiencia. Espero para ustedes solamente bienestar y buenas nuevas. Mil gracias.

Agradezco a la institución académica por ser el medio para cumplir esta meta, por proveer los recursos y el espacio para mi formación, Universidad Nacional Autónoma de México, FES Zaragoza, mi querida alma mater, seré siempre orgulloso de haber pertenecido a ti. A donde quiera que vaya juro que daré lo mejor de mí para poner en alto y traer prestigio a tu nombre. Invaluable para mi es poder decir desde el fondo de mi pecho que. Por mi raza hablará el espíritu.

“Por hoy ya acabamos, pero acabar es nunca”

I.Q. Jose Luis Macías Pérez

Índice.

Lista de figuras.

Lista de tablas.

Lista de acrónimos.

ANSI: *American National Standards Institute. / Instituto Americano Nacional de Estándares.*
BPSD: *Barriles de Petroleo Estándar por Día.*
CHazOp: *Control Hazard and Operability Study. / Análisis Funcional de Operabilidad y Control.*
CVA: *Cyber Vulnerability Assessment. / Evaluación de Vulnerabilidad Cibernética.*
DCS: *Distributed Control System. / Sistema de Control Distribuido.*
DFP: *Diagrama de Flujo de Proceso.*
DTI: *Diagrama de Tubería e Instrumentación.*
FMEA: *Failure Modes and Effect Analysis. / Análisis Modular de Fallos y Efectos.*
HazOp: *Hazard and Operability Study. / Análisis Funcional de Operabilidad.*
HDN: *Hidrodesulfuradora de Nafta.*
HDT: *Hydrotreating. / Hidrotratamiento.*
IACS: *Industrial Automation Control System. / Sistema de Control y Automatización Industrial.*
ICS: *Industrial Control System. / Sistema de Control Industrial.*
IEC: *International Electrotechnical Commision. / Comisión Electrotécnica Internacional.*
ISA: *International Society of Automation. / Sociedad Internacional de Automatización.*
LOPA: *Layer of Protection Analysis. / Análisis de Capas de Protección.*
PES: *Programmable Electronic System. / Sistema Electrónico Programable.*
PHA: *Process Hazard Analysis. / Análisis de Peligros del Proceso.*
PLC: *Programable Logic Controller. / Control Lógico Programable.*
PSV: *Pressure Safety Valve. / Válvula de Seguridad o alivio de Presión.*
SCD: *Sistema de Control Distribuido*
SHU: *Selective Hydrogenation Unit. / Unidad de hidrogenación selectiva.*
SIF: *Safety Instrumented Function. / Función Instrumentada de Seguridad.*
SIL: *Safety Integrity Level. / Nivel de Seguridad.*
SIS: *Safety Instrumented System. / Sistema Instrumentado de Seguridad.*
SL: *Security Level. / Nivel de Seguridad.*
SPR: *Security PHA Review. / Revisión de Seguridad PHA.*
TMEL: *Target Maximum Event Likelihoods / Objetivo de máxima probabilidad de evento.*
Malware: *Malicious Software /Software malicioso.*

FR: *Foundational requirements/ Requisitos fundamentales*

I Resumen

Este trabajo busca corroborar el impacto positivo de los métodos de análisis de peligros a la ciberseguridad[1] en plantas de proceso, más específicamente el método SPR (Security PHA Review) aplicado en una planta hidrodesulfuradoras de naftas típica.

Las plantas de proceso son intrínsecamente peligrosas debido a sus condiciones elevadas de presión y temperatura, estos peligros se mantienen bajo control gracias a los dispositivos de control de proceso, los cuales en los últimos años se han vuelto totalmente digitales, añadiendo de este modo más vulnerabilidades a las ya presentes en el diseño y operación del proceso. Estas vulnerabilidades no han sido pasadas por alto por aquellos grupos o individuos, desde gobiernos con intereses contrarios o grupos terroristas hasta pequeños grupos de atacantes sin intereses definidos, que desean sabotear intencionalmente algún proceso industrial, explotando estas vulnerabilidades en diversas ocasiones y generando, incidentes, accidentes y desastres que pudieron haberse evitado la mayoría de los casos si se hubiese hecho un análisis más profundo de salvaguardas intrínsecamente seguras o un análisis como el Security PHA Review.

Después de haber realizado un estudio HazOp de la planta HDN (Hidrodesulfuradora de Naftas) conceptual y detectar los escenarios ciber-vulnerables se asignó un SL objetivo para cada uno, obteniendo de este modo una razonable idea/estimación de los requisitos que se debe cubrir para proteger dicho escenario con base en los estándares de la ISA/IEC 62443, el cuál es un estándar global de ciberseguridad para la automatización industrial. Implementando los requerimientos establecidos para cada SL según lo indica el estándar ISA/IEC 62443 se persigue evitar un sobre-diseño o peor aún un sub-desempeño de los sistemas ya que si se sobre diseñan serán excesivamente costosos y el dinero invertido estará desaprovechado, y si se incurre en un sub-desempeño, muy probablemente las medidas establecidas no serán suficientes para mitigar los riesgos de un ciberataque.

[1] Conjunto de elementos, medidas y equipos destinados a controlar la seguridad informática de una entidad o espacio virtual. (Cambridge Dictionary, 2021)

II Introducción

El estudio SPR desarrollado para una planta hidrodesulfuradora de Naftas típica, desde su concepción como idea se encuentra relacionado en diversos niveles con los conocimientos que se adquieren en la carrera de ingeniería química de la FES Zaragoza.
El enfoque principal se inclina hacia, la seguridad en procesos industriales, el desarrollo de métodos de identificación de peligros y la gestion de recursos humanos y económicos empleados en la seguridad de procesos, Sin perder de vista que el estudio de un proceso industrial del giro energético tal como la hidrodesulfuración de Nafta se relaciona a su vez con tantos conceptos de la rama de la ingeniería tales como; transferencia de energía, termodinámica, hidráulica, diseño de equipo, reacción química, métodos de separación y un largo etcétera. Los cuales, si bien no son tocados a profundidad en este trabajo, su comprensión y conocimiento previo fueron de importancia capital para el desarrollo de los capítulos de esta tesis.
Una motivación para decantar a esta rama de la investigación fue el ciberataque con un ransomware[2] ocurrido a PEMEX en noviembre del 2019, el cual sirvió como ejemplo de lo sensibles que son las plantas mexicanas a los ciberataques. Sumando esto la presencia y disposición del Maestro Mario Pérez Marín para dirigir este trabajo, así como la certeza de la capacidad del profesorado de la facultad para apoyar, y enriquecer este trabajo.

La metodología para el desarrollo de la presente tesis se concibió para solo desarrollar la metodología SPR sobre un HazOp preexistente, sin embargo, la ausencia de este desembocó en uno de los retos más grandes de este trabajo. Elaborar una emulación de HazOp implementada en solitario, con la validación de un experto en la materia como el Mtro. Pérez Marín. Para después sobre ese producto iniciar el tema medular de la Tesis, es decir, la metodología SPR, la asignación de niveles de seguridad (SL´s) y con base en ellos definir los requerimientos de ciberseguridad necesarios para cada escenario según el estándar de la ISA/IEC 62443, persiguiendo siempre el uso suficiente pero eficiente de medidas para solventar las ciber-vulnerabilidades de los sistemas expuestos a ciberataques.

La presentación del primer capítulo en este trabajo busca plantear un contexto general al lector sobre los métodos tradicionales de identificación de peligros, su impacto positivo y parte de su historia, pero también sus limitaciones. Una vez bien asentada esta parte, en el capítulo dos se da un contexto general de la ciberseguridad, los métodos existentes que la abordan, su contraste con los métodos tradicionales y obviamente la metodología SPR que es la espina dorsal de esta tesis, introduciendo también al estándar ISA/IEC 62443 el cual sirve de apoyo para identificar SL y asignar requerimientos de ciberseguridad. Para completar el marco de referencia del tema, el capítulo tres describe brevemente de manera ilustrativa y general el funcionamiento de una planta hidrodesulfuradora de nafta, su papel dentro de una refinería y las condiciones de proceso bajo las que opera. Se trata a menor profundidad que los temas anteriores, ya que es la planta en la cual se desarrolla el trabajo

[2] Tipo de Malware que al entrar a un sistema secuestra funciones importantes o información sensible cifrándola y negando el acceso al propietario original. (AVAST, 2021)

de este caso de estudio, pero el HazOp mismo, el SPR y las demás etapas de la metodología de esta tesis son aplicables y escalables prácticamente a cualquier proceso industrial.
Por último, en el capítulo 4 se da lugar al caso de estudio, es decir la presentación detallada de la metodología, los resultados, su discusión e interpretación.

Como fin de la introducción se puede afirmar que: La finalidad del presente trabajo es resaltar la importancia de la ciberseguridad, desde la perspectiva de un ingeniero, más específicamente de un I.Q. de ahí la otra parte del título. Su intención es tomar un caso general y típico pero vigente a la fecha, y aplicar sobre él un método para identificar ciber-vulnerabilidades, que se clasifican y subsanan con medidas estandarizadas.

III Marco Teórico

III.I Breve historia y contexto de la ciberseguridad

> A lo largo de la historia de las plantas de proceso, específicamente de las plantas de refinación de hidrocarburos se ha implementado el uso de dispositivos para mantener las condiciones de proceso, para reaccionar ante desviaciones de estas mismas condiciones y para mitigar las consecuencias de un incidente, en un inicio todos y cada uno de estos dispositivos era análogo, operado por señales eléctricas de 4 a 20 mA o neumáticas de 62 a 103 kPa (9 a 15 psi), o dispositivos mecánicos como fuelles o resortes**.** (Hughes, 2002)**.**

Con estos dispositivos se llegó a establecer durante mucho tiempo un control aceptable de los procesos, con el surgimiento de la ciencia informática se comenzó a pensar en implementar dispositivos digitales que pudieran controlar los procesos industriales, no tardó mucho tiempo en nacer el control digital de proceso. En el inicio de este movimiento se desconocían (o no se conocían a profundidad), los peligros y vulnerabilidades que eran intrínsecos a estos dispositivos, debido a que su funcionamiento y arquitectura no se conocían, salvo por los fabricantes.

> Una vez que se dispersaron los conocimientos informáticos, la comunidad a la que llegaron dichos conocimientos incluía sectores que se percataron que podrían sacar algún beneficio de explotar las vulnerabilidades presentes en los dispositivos digitales de control de proceso, o los gobiernos contrarios se daban cuenta de que podían sacar ventaja de sabotear las plantas de proceso de los gobiernos con los que tenían diferencias. A raíz de todos estos sucesos surgió por necesidad la disciplina de la ciberseguridad, sustentando sus bases y adquiriendo experiencia de todos los eventos de ciberataques a plantas de proceso (M. Marszal & McGlone, 2019).

En el idioma inglés existen dos términos bien diferenciados entre sí, el primero *Safety* para referirse a la prevención de condiciones que son peligrosas, accidentes, incidentes o siniestros dentro de la industria de los procesos; dicha industria es delimitada por el estándar (IEC 61511, 2016) de la siguiente manera: “Se aplica para una amplia variedad de industrias dentro del sector de procesos, por ejemplo, química, petróleo y gas, pulpa y papel, farmacéutica, alimentos y bebidas, y generación no nuclear de energía.” (IEC 61511, 2016)

Una definición más común es dada por el diccionario de Cambridge. “Un estado en el que o un lugar donde está seguro y no está en peligro o en riesgo” (Cambridge Dictionary, 2021). El segundo término *Security* es para referirse a la prevención de actos de naturaleza intencional, intrusiones, robos, vandalismo, “Protección de una persona, edificio, organización o país contra amenazas como delitos o ataques de países extranjeros” (Cambridge Dictionary, 2021). Mientras que en el idioma español ambos conceptos se ven englobados en una sola palabra, *Seguridad “Cualidad de seguro”* y a su vez *Seguro* “Libre o exento de riesgos”. (RAE Real Academia Española, 2021)

El hecho de que se hable de *cibersecurity* y no de *cibersafety* hace latente este factor de la intencionalidad, es importante tener esto en mente al tratar conceptos relacionados con ciberseguridad.

III.II SL Security Level

> Un concepto importante empleado en el ámbito de la seguridad es el SL (Security Level). Como se define en la serie ISA/IEC-62443, son categorías que definen un conjunto de políticas, procedimientos y prácticas que deben implementarse para asegurar una zona de ICS. A diferencia del "SIL" cuantitativo definido en los estándares IEC-61511 y la ISA-84, que es una banda de probabilidad promedio de fallas bajo demanda, el SL es un conjunto de requisitos cualitativos para explicar cómo se debe diseñar y operar un sistema en función de las capacidades y la motivación del atacante (M. Marszal & McGlone, 2019).

Se podría argumentar que el enfoque debería estar en la capacidad empresarial para defenderse o ser resiliente a un ataque, pero ese no es el enfoque que selecciona este estándar. La serie ISA/IEC 62443 define cuatro niveles de seguridad, SL 1 a SL 4, siendo SL 1 el menos seguro y SL4 el más seguro. Los niveles se definen (en abstracto) de la siguiente manera:

- **SL1** – Personal que comete errores no intencionales.
- **SL2** – Ataques no dirigidos, ataques comerciales basados en internet que se propagan al ICS.
- **SL3** – Ataques de ICS dirigidos, que podrían ser realizados por un miembro de confianza, un empleado descontento, un contratista externo, personal bien intencionado que viole las prácticas de seguridad, etc.
- **SL4** – Administradores de sistemas, ataques dirigidos de una nación a otra.

Las definiciones de SL anteriores son de naturaleza cualitativa, y proporcionan poco en cuanto a especificaciones de diseño concretas.

Para ubicar las vulnerabilidades e implementar salvaguardas en los procesos industriales de forma tradicional se emplean métodos PHA (Process Hazard Analysis), con base en los buenos resultados obtenidos por estos métodos la comunidad de la Seguridad de Procesos (en particular, las áreas de Análisis de Riesgos) optó por adaptarlos para ser usados en el área de la ciberseguridad, asi surgió un conjunto de métodos basados en los PHA, ciber-HazOp, CHazOp, SPR. Etc.

La mayoría de estos métodos más enfocados a ciberseguridad toman la estructura de los métodos tradicionales de análisis de peligros, HazOp, Árbol de fallas, What If, aunque principalmente de HazOp, pero adaptando partes del método para evaluar vulnerabilidades y recomendar salvaguardas referentes a la ciberseguridad.

III.III Estudio (Security PHA Review) SPR.

El estudio SPR es una variación de los estudios PHA enfocándose en la seguridad de los sistemas, y se basa en evaluar la ciber-vulnerabilidad de las salvaguardas que cubren un evento con causa ciber-vulnerable.

La realización de estudios SPR para identificar y mitigar adecuadamente los vectores de amenaza de ciberataque contra las instalaciones de proceso tiene varios beneficios.

- Menor riesgo.
- Mejor comprensión de los vectores de ciberataques.
- Tomar las decisiones correctas para el diseño en cuestión.
- Mayor eficiencia.
- Cumplimiento de estándares

Lo anterior lo afirma (M. Marszal & McGlone, 2019), aunque quizá caiga en un sesgo afirmar que; se corre un menor riesgo, que se obtiene una mayor eficiencia, o que se toman las decisiones correctas para el diseño en cuestión. Ya que todo lo anterior enlistado depende de la calidad de la información con la que se alimente al SPR o incluso de la calidad de los estudios de riesgo anteriormente realizados. Sin embargo, es un hecho que cumple con los estándares establecidos y reconocidos, más específicamente el estándar ISA/IEC 62443. Como se verá más adelante en este trabajo

III.IV Método HazOp.

> El método HazOp surgió en 1963 en la compañía Imperial Chemical Industries (ICI), que utilizaba técnicas de análisis crítico en otras áreas. Posteriormente se generalizó y formalizó, y actualmente es una de las herramientas más utilizadas internacionalmente en la identificación de peligros en una identificación industrial. (Romero Faz, 2017).

Un estudio HAZOP es un análisis estructurado de un sistema, proceso u operación para el cual se dispone de información detallada de diseño, realizado por un equipo multidisciplinario. El equipo procede con un examen línea por línea o etapa por etapa de un diseño firme para el proceso u operación. Si bien es sistemático y riguroso, el análisis también pretende ser abierto y creativo. Esto se hace utilizando un conjunto de palabras guía en combinación con los parámetros del sistema para buscar desviaciones significativas de la intención del diseño. Una desviación significativa es aquella que es físicamente posible, por ejemplo, sin flujo, alta presión o reacción inversa.

Las desviaciones como la ausencia de temperatura o la viscosidad inversa no tienen un significado físico sensible y no se tienen en cuenta. El equipo se concentra sobre aquellas desviaciones que podrían conducir a peligros potenciales para la seguridad, la salud o el medio ambiente.

> Además de la identificación de peligros, es una práctica común para identificar posibles problemas operativos; éstos pueden estar relacionados con la seguridad, los factores

humanos, la calidad, la pérdida financiera o los defectos de diseño. Cuando se encuentran las causas de una desviación, el equipo evalúa las consecuencias utilizando la experiencia y el juicio. Si las salvaguardas existentes se consideran inadecuadas, el equipo recomienda una acción de cambio o pide una mayor investigación del problema. Las consecuencias y las acciones relacionadas pueden clasificarse según el riesgo. El análisis se registra y se presenta como un informe escrito que se utiliza en la implementación de las acciones Derivadas del estudio realizado por el grupo multidisciplinario. (Crawley & Tyler, 2015).

IV Planteamiento del problema.

Las plantas hidrodesulfuradoras de Naftas presentes en el país que procesan crudo amargo (rico en azufre), son intrínsecamente peligrosas debido a las condiciones de presión, temperatura y substancias que manejan, y los componentes digitales del sistema de control de estas plantas aportan vulnerabilidades que podrían ser objeto de un ciberataque, dirigido o no, y desencadenar incidentes o accidentes. Mediante la metodología HazOp en conjunto con la metodología SPR se plantea una opción que podría ayudar a mitigar las consecuencias de los ciberataques en las plantas hidrodesulfuradoras.

V Hipótesis.

Si se analiza con un método SPR las ciber-vulnerabilidades dentro de una planta de hidrotratamiento de Naftas, entonces, se podrán identificar los escenarios ciber-vulnerables y seleccionar un SL para cada uno que permita evitar sobre diseño y sub-desempeño del sistema de ciberseguridad, y también se logrará que la planta esté protegida contra las ciber-amenazas que corresponden a las coberturas del nivel de SL seleccionado para cada escenario.

VI Objetivos.

VI.I Objetivo general.

Realizar un análisis de peligros de proceso (PHA) y aplicar la metodología "SPR" para detectar los escenarios que pueden sufrir un ciberataque y con esta información asignar un SL a cada escenario y fijar los requerimientos de ciberseguridad para el caso de una planta hidrotratadora de Naftas. Bajo el estándar ISA/IEC-62443.

VI.II Objetivos específicos.

- Revisar aspectos básicos de los temas; Análisis HazOp, ciberseguridad e hidrodesulfuración de naftas. Que son los temas que dan soporte conceptual al presente trabajo.

- Analizar la planta dividida en Nodos[3], y mostrar estos nodos en los diagramas de flujo de proceso (DFP´s), así como en los diagramas de tubería e instrumentación (DTI´s).

- Aplicar un análisis análogo de HazOp, pero sin la participación de un equipo multidisciplinario. Y con las hojas de trabajo resultantes alimentar al método SPR, para generar recomendaciones de salvaguardas intrínsecamente seguras, así como requerimientos indicados en la ISA/IEC-62443 basados en el nivel de seguridad SL.

- Asignar a cada escenario detectado como ciber-vulnerable un SL basado cualitativamente en sus potenciales consecuencias tal como indica la tabla 2 obtenida de la fuente. (M. Marszal & McGlone, 2019).

[3]El nodo es la unidad básica de análisis conformada por tuberías y/o equipos que puede ser tan simple o compleja como se deseé, y se delimita la mayoría de las veces en función de la funcionalidad de los equipos.

Capítulo 1. Estudios PHA (Análisis HazOp)

1. Estudios PHA.

El término PHA se corresponde con las siglas en inglés de *Proccess Hazard Analysis*, y engloba una serie de técnicas que permiten la adecuada detección de peligros, así como la posterior valoración cualitativa y/o cuantitativa de los peligros presentes en cualquier proceso, a fin de minimizarlos o, en su defecto controlarlos.

Los estudios PHA representan un eslabón muy importante dentro de la cadena de la seguridad y son parte fundamental de los sistemas de gestión de la seguridad. (REPSOL YPF, 2007)

Dentro de las técnicas más utilizadas para la conducción de estudios PHA, se encuentran (por orden aproximado creciente de complejidad):

- HAZID (Hazard Identification)
- CHECKLIST (Lista de control)
- WHAT IF (¿Qué pasa sí?)
- HazOp (Hazard Operability Analysis)

La industria de los procesos presta bastante atención al desarrollo de sistemas integrales de gestión de seguridad con el objetivo de proteger a los trabajadores y al medio ambiente. También existen requisitos dentro de la legislación, como la directiva Seveso II, la directiva 96/82 de la unión europea, o el Sistema para la administración del trabajo-Seguridad en los procesos y equipos críticos que manejen sustancias químicas peligrosas establecido en la NOM-028-STPS 2012, y cada legislación en cada país especifica que las empresas que manejan materiales peligrosos cuenten con un Sistema integral de gestión de riesgos adecuado y cumplan con obligaciones específicas. Estos requisitos van desde la preparación de políticas de prevención de accidentes graves hasta la presentación de informes de seguridad detallados a una autoridad competente. Un elemento integral de los sistemas de gestión de seguridad es el uso de técnicas sistemáticas para la identificación de peligros.

Además de cumplir con los requisitos legales, se pueden obtener considerables beneficios comerciales mediante el uso de un enfoque sistemático y completo para la identificación de peligros. Estos beneficios incluyen, la mejora de la calidad, una puesta en marcha más rápida y una reducción de los problemas de operatividad posteriores.

1.1 Metodología de estudios de peligro o Hazard Study (HS).

Para un nuevo proyecto, el mayor beneficio se obtiene al realizar una serie de estudios a lo largo del proceso de diseño. Una de esas secuencias es la metodología del estudio de peligros que consta de seis etapas (HS por Hazard Study) desarrollada por ICI y que detalla (Crawley & Tyler, 2015). Cada etapa o estudio verifica las acciones de estudios previos.

- ***HS-1 Revisión de peligros en la etapa conceptual.***

En este primer estudio, se identifican los peligros básicos de los materiales y la operación y se establecen los criterios SHE (Safety, Healt, Enviroment). Identifica qué información se

necesita y el programa de estudios requerido para asegurar que todos los temas de SHE se aborden adecuadamente. Los aspectos cubiertos pueden incluir cinética de reacción, datos de toxicidad, impacto ambiental y cualquier característica especial del proceso que necesite una evaluación adicional. Además, se identifican las limitaciones impuestas por la legislación pertinente. Esto tiene como objetivo escalar, evitar o reducir los peligros potenciales en el proceso.

- ***HS-2 HAZID en la fase de diseño de ingeniería (feed) o definición del proyecto.***

Este estudio generalmente cubre la identificación de peligros y la evaluación de riesgos, la operabilidad y las características de control que deben integrarse en el diseño detallado y cualquier característica ambiental especial que deba cubrirse. Es importante que los niveles de integridad de seguridad (SILS)de cualquier sistema instrumentado de seguridad (SIS) se aborden durante este estudio, ya que el diseño seguirá siendo flexible y se pueden aplicar cambios de diseño simples que reducirán los SILS y así simplificarán el diseño. Al final del HS-2, el nivel de desarrollo del diseño y los diagramas de tuberías e instrumentación (P &ID) sería "aprobado para el diseño" (AFD). Se deberían haber agregado todas las características principales. Es útil examinar los diagramas AFD en busca de errores más evidentes utilizando lista de verificación.

- ***HS-3 Estudio de riesgos con base en el diseño detallado.***

Normalmente, esto implica una revisión posterior de un diseño ya avanzado destinado a la identificación de peligros y problemas de operatividad. En esta etapa se pueden incluir, si corresponde, estudios de alivio y purga, clasificación de áreas, protección personal y manipulación manual. Los estudios HAZOP normalmente se llevan a cabo en esta etapa.

- ***HS-4 Verificación de Construcción/Diseño.***

Esta revisión se realiza al final de la etapa de construcción. El equipo se verifica para asegurarse de que se haya construido según lo previsto y de que no haya violaciones de la intención del diseñador. También confirma que se hayan incorporándolas acciones del estudio de riesgos de diseño detallado y se verifican los procedimientos operativos y de emergencia.

- ***HS-5 Revisión de seguridad previa al arranque de la planta.***

Esto examina la preparación del grupo de operaciones para la puesta en marcha y generalmente cubre la capacitación, los procedimientos operativos finales, los procedimientos de preparación y la preparación para la puesta en marcha, incluidas las pruebas de funcionamiento, limpieza y purga. La confirmación del cumplimiento de las normas legislativas y de la empresa se realiza en esta etapa.

- ***HS-6 Cierre del proyecto/ revisión posterior al arranque de la planta.***

Este estudio, llevado a cabo unos meses después de la puesta en operación y el inicio de producción, confirma que todos los problemas sobresalientes de los cinco estudios anteriores están completos y busca cualquier situación que pueda brindar comentarios

útiles. Además de estos seis estudios, se pueden incluir dos más. Por lo general, estos se denominan estudio cero y estudio siete, para que se ajusten al esquema de numeración utilizado anteriormente.

- ***HS-0 Consideración de sistemas inherentemente más seguros o menos contaminantes.***

El estudio cero se lleva a cabo entre los departamentos de investigación y departamento técnico antes de la etapa de concepto. Intenta identificar e incorporar las ideas inherentemente más seguras y ecológicas lo antes posible para que formen parte del diseño final.

- ***HS-7 Consideraciones y revisión de demolición o abandono.***

Este estudio puede tener lugar antes del cierre definitivo, pero el objetivo del estudio es identificar los problemas que deben abordarse durante el proceso de demolición. Debe considerar cuestiones tales como métodos y normas de limpieza, reducción de tamaño, recuperación y reciclaje de inventarios de trabajo, reciclaje de equipos, eliminación segura de materiales, equipos no reciclables y ubicación de materiales tóxicos potencialmente nocivos. Además, debe evaluar la integridad de los dispositivos, soportes de elevación, las rutas de acceso y la secuencia de extracción.

La figura 1 (Crawley & Tyler, 2015) representa la relación entre las fases de un proyecto de construcción de un proceso industrial y las etapas de estudio propuestas por el ICI (Imperial Chemical Industries)

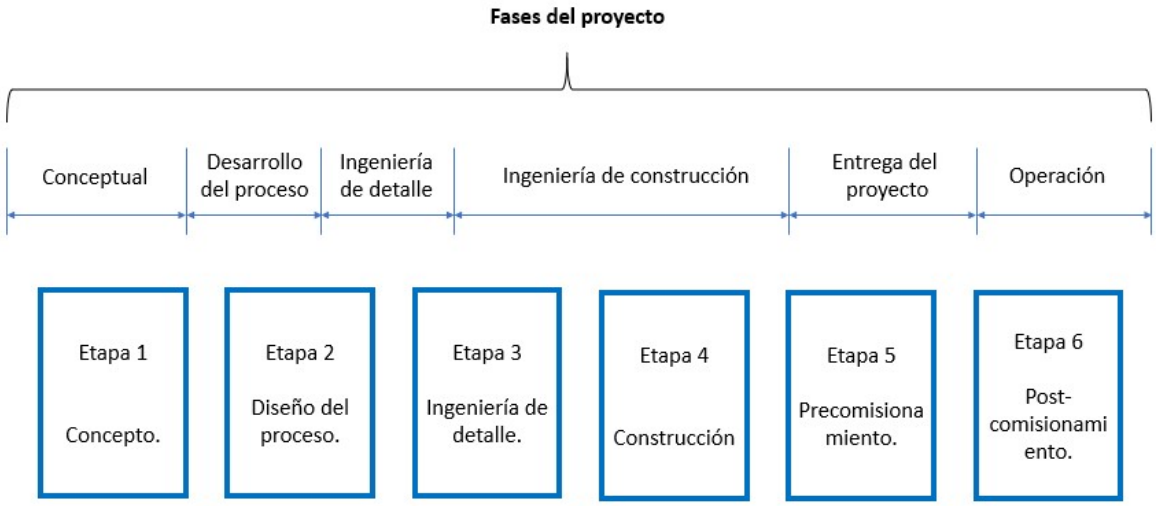


Figura 1 Relación entre las seis etapas del estudio de peligro y el ciclo de vida del proceso. Obtenida de (Crawley & Tyler Cap. 1, 2015).

1.2 Análisis de peligros HazOp.

Un estudio HAZOP es un examen estructurado y sistemático de un proceso u operación planificado o existente. Previo a comenzar con el análisis se debe formar un equipo multidisciplinario con personal técnico especializado en cada área del proceso, todos dirigidos por un especialista en análisis de riesgos. Al comienzo del estudio, el equipo crea un modelo conceptual del sistema u operación. Esto utiliza todo el material relevante disponible, como un diseño firme y detallado, un esquema de los procedimientos operativos, hojas de datos de materiales y los informes de estudios de peligros anteriores. Luego, se buscan los peligros y los problemas operativos potenciales considerando las posibles desviaciones de la intención del diseño de la sección o etapa bajo revisión. La intención del diseño es una imagen verbal de lo que debería estar sucediendo y debería contener todos los parámetros clave que se explorarán durante el estudio. También debe incluir una declaración del rango operativo previsto. Esto suele ser más limitante que las condiciones físicas de diseño. Para aquellas desviaciones donde el equipo puede sugerir una causa, las consecuencias se estiman utilizando la experiencia del equipo y se toman en cuenta las salvaguardas existentes.

> Cuando el equipo considera que el riesgo no es trivial o cuando un aspecto requiere más investigación, se genera un registro formal para permitir el seguimiento del problema fuera de la reunión. Luego, el equipo continúa con el análisis. (A. Crowl & F. Louvar, 2002).

La validez del análisis depende obviamente de contar con las personas adecuadas en el equipo, la precisión de la información utilizada y la calidad del diseño. Normalmente se asume que el trabajo de diseño se ha realizado de manera competente para que las operaciones dentro de las condiciones de diseño sean seguras. Incluso cuando este sea el caso, las últimas etapas del proyecto también deben llevarse a cabo correctamente, es decir, se siguen los estándares de ingeniería y existen estándares adecuados de construcción, puesta en servicio, operación, mantenimiento y gestión. Un buen estudio HAZOP intenta tener en cuenta estos aspectos y los cambios que se pueden esperar razonablemente durante la vida útil de la operación. A veces, un estudio identificará problemas que están dentro de los límites del diseño, así como problemas que se desarrollan a medida que la planta envejece o que son causados por errores humanos.

1.3 Información requerida.

Para llevar a cabo de manera correcta un estudio HazOp se requiere disponer de información fiable del proceso, mínimamente documentos del nivel aprobados para diseño (AFD), si bien el resultado final del estudio HazOp depende de muchos factores, como el equipo multidisciplinario que lo lleve a cabo, o el expertis del líder HazOp, el acceso a información precisa y certera contribuye en gran parte a la calidad del resultado final.

Un listado de los documentos imprescindibles para un HazOp se muestra a continuación:

- DFP´s de proceso.
- DTI´s de proceso.
- Balances de materia y energía.
- Descripción del proceso.
- DTI´s de servicios auxiliares.
- Hojas de datos de equipos estáticos y dinámicos.
- Hojas de datos de materiales.
- Plano de localización de la planta.
- Hojas de datos de válvulas de seguridad y PSV´s

1.4 Nodos, etapas o etapas del proceso.

Es fundamental que el equipo comience con un conocimiento completo del apartado, nodo o etapa a analizar, ya sea conociendo la situación existente o teniendo suficiente información para poder conformar un modelo conceptual adecuado. Se debe desarrollar una descripción completa, incluidos todos los parámetros clave, y el informe HAZOP debe incluir la descripción del diseño. A continuación, se formula y registra una intención de diseño para el nodo. Esto debe incluir una declaración del rango operativo previsto para que el equipo de análisis HazOp pueda reconocer cualquier situación que se encuentre fuera de este rango como desviaciones. La intención del diseño puede estar relacionada con la descripción del nodo y, por tanto, con los parámetros de diseño del equipo y líneas del proceso incluidas en el nodo.

> Es una buena práctica desarrollar una intención de diseño integral, claramente vinculada a los diagramas que se están utilizando, a los que se puede hacer referencia durante la búsqueda de desviaciones. Una intención de diseño puede referirse a elementos de equipamiento en la sección, a materiales, condiciones, fuentes y destino, a cambios o transferencias, así como a los medios de control del nodo. No solo se refiere a los equipos de la planta, sino que cubre lo que se pretende hacer dentro de la sección que se analiza. (PEMEX, 2011)

1.5 Desviaciones, Palabras clave y variables de proceso.

El siguiente paso es generar una desviación significativa acoplando una palabra guía y un parámetro. Se puede generar una desviación tomando un parámetro y combinándolo con cada palabra guía para ver si se produce una desviación significativa. El conjunto estándar de palabras guía para plantas de proceso se enumera en la tabla 1, junto con sus significados generales. Algunas empresas han desarrollado su propio conjunto de palabras guía para tecnologías particulares. Si bien se pueden hacer recomendaciones claras en cuanto a qué palabras guía deben tenerse en cuenta, no es posible brindar un asesoramiento tan firme con respecto a los parámetros. La selección de parámetros es una tarea que cada equipo debe abordar para cada sistema estudiado. Se debe enfatizar que muchos de los

parámetros enumerados no se aplicarán a todos los problemas o procesos, ya que los parámetros se relacionan con el sistema individual.

Tabla 1 Lista de palabras guía estándar Obtenida de: Elaboración propia.

Palabras guía más comunes.	
Palabra guía	Significado
No/Ninguno	No se logra ningún propósito de diseño.
Más/Mayor	Aumento cuantitativo de un parámetro.
Menos/Menor	Disminución cuantitativa de un parámetro.
Reverso	Ocurre el opuesto lógico de la intención de diseño.
Otro/Otra	Se produce una actividad inusual.

A continuación, se presenta una lista enunciativa mas no limitativa de parámetros: Flujo, presión, temperatura, mezcla, nivel, transferencia, viscosidad, reacción, composición, separación, fase, tamaño de partícula y potencial hidrógeno.

La combinación de los parámetros de proceso anteriores con las palabras guía dan como resultado una amplia gama de desviaciones, por ejemplo, “Menor Flujo” o “Mayor Presión” sin embargo, dependiendo de las características del nodo que se esté analizando algunas de las desviaciones resultantes podrían carecer de sentido, por ejemplo, si se supone que el nodo analizado es una sección de tuberías que conectan con un calentador a fuego directo, si bien es posible formar la desviación “Menor Nivel”, ésta no tiene sentido físico o implicación alguna dentro del nodo analizado. Por lo anterior es importante prestar atención siempre a las características del nodo y a su intención de diseño al momento de plantear las desviaciones, Figura 2.

Figura 2 Formación de una desviación de proceso. Obtenida de: Elaboración propia

1.6 Metodología de Análisis HazOp.

En la figura 3 (Crawley & Tyler, 2015) se muestra el ciclo de análisis que debe llevarse a cabo para cada nodo que es sometido a un análisis HazOp.

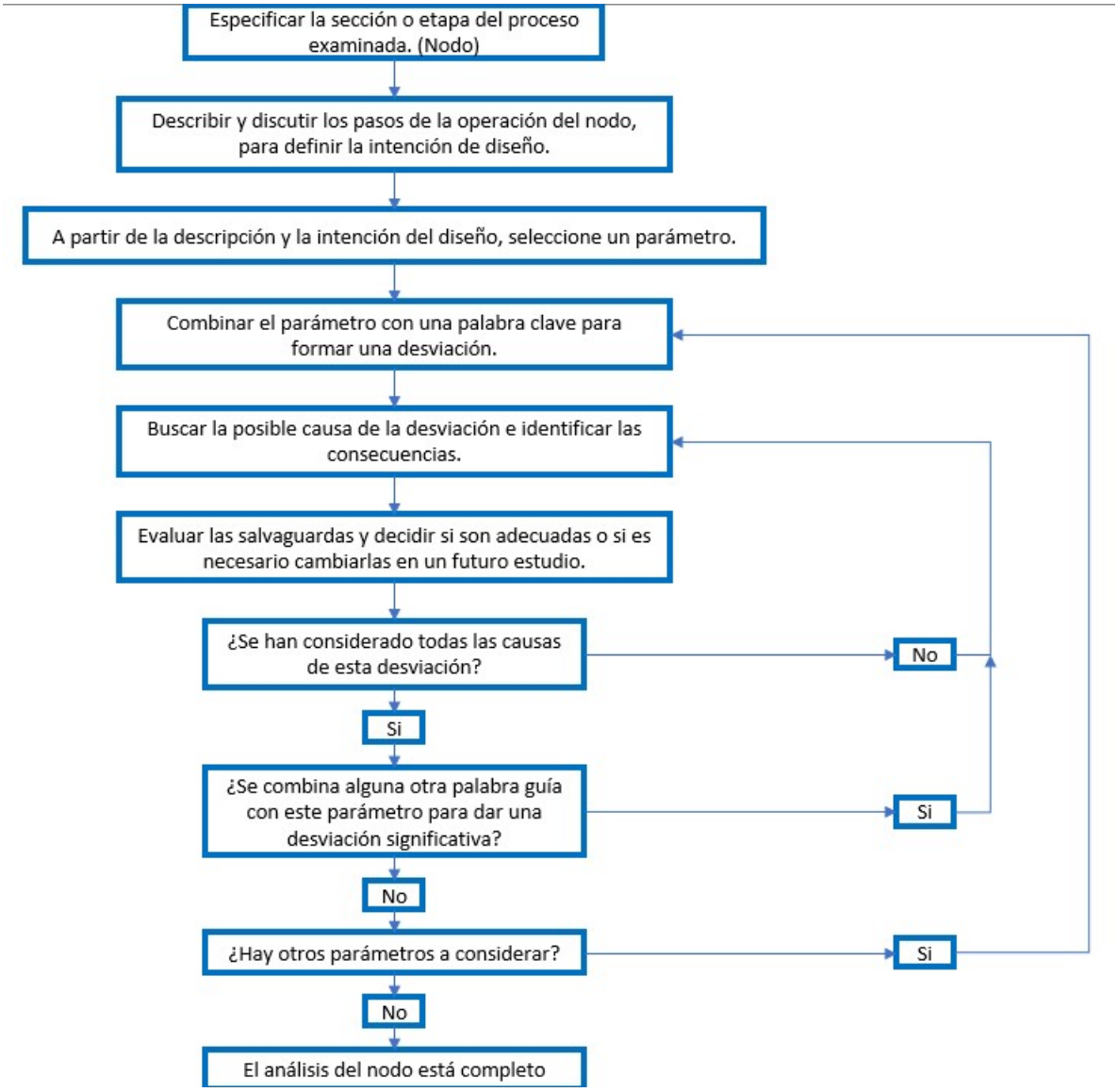


Figura 3 Ciclo del análisis HazOp para un nodo del proceso. Obtenida de: (Crawley & Tyler Cap. 3, 2015)

Capítulo 2. Ciberseguridad.

2.1 Introducción a la ciberseguridad.

El término "ciberseguridad" ha sido objeto de literatura académica y popular que en gran medida ha visto el tema desde una perspectiva particular. El término se usa ampliamente y sus definiciones son muy variables, están ligadas al contexto, a menudo subjetivas y, en ocasiones, poco informativas. Una definición propuesta por (Craigen, Diakun-Thibault, & Purse, 2014) en su artículo *Defining cybersecurity* es:
"La ciberseguridad es la organización y colección de recursos, procesos y estructuras que se utilizan para proteger el ciberespacio y los sistemas habilitados por el ciberespacio de sucesos que atentan contra la integridad del sistema". (Craigen, Diakun-Thibault, & Purse, 2014)

Como se menciona anteriormente, es importante realizar una buena contextualización cuando se trata el tema de ciberseguridad.
Las plantas de proceso son intrínsecamente peligrosas, y abatir los riesgos inherentes hasta un límite tolerable es una actividad compleja y multidisciplinaria, que implica consumo de recursos humanos y materiales de manera intensiva. A medida que la tecnología evoluciona las plantas de proceso comienzan a emplear nuevos equipos y técnicas que reducen costos y elevan la productividad. Estos nuevos sistemas y técnicas empleadas generan a su vez nuevos y diferentes peligros que deben ser considerados durante el diseño y abordados con la protección adecuada.

> Con el paso de las décadas la presencia de sistemas de control neumático o eléctrico (análogo) se ha visto desplazado casi en su totalidad por sistemas electrónicos programables. (PES´s). Los PES´s incluyen sistemas de control distribuido (DCS´s) y controladores lógicos programables (PLC´s). Estos sistemas tienen una base computacional, una de las ventajas de los sistemas de base computacional es que permiten realizar cálculos más complejos y con mayor velocidad el control del proceso. Además de almacenar la información acerca de la operación del proceso y facilitar su acceso. Estos sistemas son englobados en los llamados sistemas de control industrial (ICS´s) (M. Marszal & McGlone, 2019).

“Durante estos años, los ciberataques contra infraestructuras críticas han ido en aumento, y los medios empleados han sido cada vez más sofisticados y avanzados.”
(Instituto Nacional de ciberseguridad (INCIBE), 2018)**.**

El motivo por el cual no se aprecia un gran impacto en los ciberataques hacia los sistemas de control industrial, es la forma en que los ingenieros de Seguridad Funcional, Seguridad Industrial y de Proceso han diseñado sus plantas para que estén resguardadas contra las fallas que puedan causar daños físicos considerables, tanto si la falla ocurre orgánicamente a través de fallas de hardware aleatorio o deliberadamente por causa de ataques cibernéticos. Las salvaguardas empleadas por estos ingenieros pueden ser comunes o innovadoras, económicas y con frecuencia intrínsecamente muy seguras contra el

ciberataque, debido a que estos dispositivos se inventaron mucho antes de la llegada de la computadora. (PSV´s, Discos de ruptura, bobinas o Reley´s, etc.).

Si bien las ventajas de este poder computacional y la comunicación abierta son obvias, desafortunadamente también introducen nuevos potenciales escenarios de peligro que no existían cuando los sistemas eran análogos en su totalidad. Los nuevos escenarios de peligro que son inherentes a las fallas propias de los sistemas se ven adecuadamente contempladas por los métodos de análisis de peligros ya existentes (PHA). Otros escenarios pudieran no ser identificados por estos PHA existentes, tal es el caso de los ciber ataques. Estas nuevas amenazas no se generan por una falla aleatoria de hardware o un componente mecánico, si no por actos deliberados de las personas y las organizaciones que lo planifican y ejecutan.

2.2 Brevísima historia de los ciberataques.

Por años, las industrias expertas han intentado prevenir los daños físicos masivos a las plantas de proceso y las pérdidas de vidas humanas que podrían ocurrir como resultado de los ciberataques. En Estados Unidos agencias gubernamentales han preparado casos de estudio como el caso "Aurora", realizado por el departamento de seguridad nacional, lo resultados fueron ampliamente difundidos por medios internacionales de comunicación como la CNN.

Además de las advertencias del gobierno de Estados Unidos y el mundo académico sobre la vulnerabilidad a ciberataques, existe evidencia que sugiere que un puñado de ciberataques exitosos causaron daño físico. Es muy difícil comprender completamente estos ataques porque la información relacionada con ellos a menudo se suprime. Los informes sobre los ataques suelen ser contradictorios e incompletos, e incluyen muchos rumores de fuentes no identificadas. Es importante recordar esto al considerar los siguientes casos:

El más ampliamente conocido de estos ataques es el ataque Stuxnet a las centrifugadoras de uranio iraníes.

> En el ataque Stuxnet un "gusano informático" fue introducido al sistema de ICS que controlaba las centrifugadoras de purificación de uranio. Este gusano informático tomó el control del equipo de proceso llevando a las centrifugadoras a operar a una mayor velocidad, incrementando la presión del sistema sin el conocimiento de los operadores, resultando esto en un daño o afectación física del equipo. Lo que no es tan conocido o publicitado es que el ataque Stuxnet podría haberse evitado fácilmente y solo tuvo éxito porque el diseño del equipo de proceso carecía de salvaguardas que son absolutamente seguras contra ciberataques (Gómez Llinás, 2017).

Otro ciber ataque, cuya veracidad ha sido cuestionada incluso en los primeros informes de este hecho, es el presunto ataque al oleoducto Bakú-Tiflis-Ceyhan (BTC).

> Los reportes indican que actores maliciosos a nivel internacional presurizaron el oleoducto, resultado en una ruptura y una explosión, de acuerdo con los reportes, el ataque suprimió las alarmas e impidió que los operadores del proceso se enteraran del estado operativo del ducto. Si el ataque procedió de acuerdo con el reporte, es casi seguro que si se hubiese utilizado un simple arreglo de relay´s simples en el motor para detener la bomba por una sobre corriente o si hubiese tenido un sistema de alivio de presión por válvulas mecánicas se habrían evitado las consecuencias del ataque. Ninguno de estos factores se reportó en el informe del evento (Lee, 2015).

La oficina federal alemana de información de seguridad (BSI) realizó un reporte sobre un ciberataque a un alto horno en Alemania, pero no dio nombre de la empresa operadora ni cuando tuvo lugar el ataque.

> Los atacantes obtuvieron acceso a los sistemas de la fábrica aplicando la técnica de spear-phishing, lo que les permitió penetrar la red corporativa. A partir de allí comenzaron su "ascenso", explorando la estructura hasta llegar a la red de producción, donde afectaron una "multitud" de sistemas. Lo más grave fue que la planta se vio imposibilitada de apagar el alto horno correctamente, causando un daño masivo al sistema, aunque el reporte no brinda detalles adicionales. Las organizaciones de ciberseguridad alrededor del mundo, los gobiernos, la comunidad académica y comercial han invertido una gran cantidad de esfuerzo a comunicar que infraestructura crítica es vulnerable a los ciberataques, que continúan creciendo en frecuencia.

En un caso más cercano y reciente (Badillo, 2020), según información obtenida a través de la plataforma nacional de transparencia, Pemex identificó más de 176.3 millones de intentos de agresiones a sus sistemas de enero de 2015 a agosto de 2020, esto quiere decir que sufrió en promedio 85,176 intentos de ataque al día. "Las deficiencias en las configuraciones de seguridad en los dispositivos de comunicación, la falta de análisis de vulnerabilidades previo a la puesta en marcha de los sistemas, la carencia de alertas para prevenir la fuga de información por parte de los prestadores de servicios y la falta de análisis de impacto al negocio desde la perspectiva de alta dirección de Pemex, representan un probable riesgo para la operación de los procesos y servicios aunado a que comprometen la integridad, confiabilidad y disponibilidad de los activos de la empresa", expuso un reporte de la ONEA México.

Aunado a esto, la ASF confirmó que existen en la red más de 180,000 archivos sustraídos mediante ataques cibernéticos a Pemex tan solo en 2019, el volumen aproximado de esta documentación es de 6 Gigabytes, dichos documentos presuntamente fueron sustraídos por la banda de hackers Doppel Paymer y se exigió un rescate de 565 bitcoins equivalente a 4.9 millones de dólares.

2.3 Métodos de análisis de riesgos a la ciberseguridad.

Los estándares de ciberseguridad requieren un análisis de riesgos para establecer el nivel de desempeño requerido. Cuando se revisa la ISA/IEC 62243 respecto a los análisis de riesgo, los profesionales de la seguridad de procesos pueden confundirse fácilmente, ya que la norma a menudo combina y confunde el análisis de riesgo, el análisis de vulnerabilidades y la revisión general del diseño de quipos. Como tal, para un profesional de la ciberseguridad, un servidor con paquetes de software desactualizados se considera un riesgo (o en ocasiones una vulnerabilidad), mientras que en las industrias de proceso cuando se habla de riesgo, generalmente se refiere a escenarios completos. Estos escenarios comienzan con la falla de un equipo o un error humano, incluyen salvaguardas que podrían evitar el evento iniciador si funcionan correctamente y se definen las consecuencias en términos de daño físico si ocurre el evento final.

La norma ANSI/ISA-62443-2-1 (99.02.01)-2009 *Security for Industrial Automation and Control Systems – Parte 2-1: "Establecimiento de programas de seguridad de sistemas de control y automatización industrial."* Define dos tipos de evaluación de riesgos que pueden ser aplicados a un ICS considerando la ciberseguridad: La evaluación de High-level y la de detalle. La evaluación de riesgo *High-Level*, de acuerdo con el estándar, considera los tipos generales de vulnerabilidades del sistema ICS con respecto a la ciberseguridad y cuáles serían las consecuencias de proceso que se darían debido a estas vulnerabilidades presentes en el sistema. La evaluación de riesgo detallada es similar, pero en lugar de categorías generales de vulnerabilidades, se utilizan vulnerabilidades específicas que están directamente relacionadas con las marcas, modelos y revisiones de software de los componentes específicos del ICS.

Varios grupos han intentado promulgar metodologías para realizar la evaluación de riesgos como se presenta en la serie ISA / IEC 62443. Algunos métodos que se han propuesto incluyen:

- Cyber PHA
- Cyber Hazard Operability study (cyber HAZOP)
- Control hazards and operability study (CHAZOP)

Estos métodos siguen un marco de referencia similar el cuál es:

1. Identificar los activos o dispositivos del ICS
2. Identificar una amenaza potencial para estos activos.
3. Identificar una vulnerabilidad que permita que la amenaza tenga éxito.
4. Determinar las probabilidades del ataque.
5. Determinar las consecuencias.
6. Calcular el riesgo.

Estos procesos no identifican los escenarios peligrosos, en lugar de ello, identifican las vulnerabilidades de diseño de los equipos. Si bien estos enfoques utilizan nombres que se

relacionan con las técnicas de identificación de peligros, no lo son. De hecho, son simplemente variaciones de "análisis de modos de falla y efectos" (FMEA). Si bien FMEA es una buena herramienta para analizar el diseño de equipos e identificar los puntos débiles, es una mala herramienta para identificar escenarios de peligrosidad en el proceso.

La mayoría de los métodos de evaluación de riesgos cibernéticos adolecen del problema de identificar debilidades en el diseño de equipos de ICS sin poder generar eventos iniciadores que impulsen escenarios de riesgo. Sin estos escenarios de riesgo, no se puede determinar el riesgo general de la planta. Se debe utilizar otro enfoque para identificar los escenarios de riesgo en los que las vulnerabilidades cibernéticas puedan afectar el perfil de riesgo general de una planta.

2.4 Estudio SPR (Security PHA Review).

Este estudio SPR es una es una evolución de PHA para asignar objetivos de rendimiento a la ciberseguridad ICS y hacer recomendaciones para implementar salvaguardas que son inherentemente seguras contra ciberataques en lugar de sólo establecer objetivos SL altos. El proceso SPR fue desarrollado por profesionales de la seguridad técnica que tenían una sólida experiencia no solo en seguridad de procesos sino también en el diseño e implementación de ICSS. El enfoque SPR se desarrolló específicamente para encajar de forma natural con el ciclo de vida normal del proyecto de diseño, implementación y operación de plantas de la industria de procesos, al tiempo que aprovecha las tareas de ingeniería existentes y los informes generados para la seguridad general del proceso. De esta forma, las limitaciones de los enfoques de análisis de riesgo cibernético existentes podrían eliminarse al tiempo que se maximiza el uso de la información y la documentación generada en otras etapas del ciclo de vida de la ingeniería.

El estudio SPR está diseñado específicamente para seleccionar el SL requerido utilizando el estudio PHA existente como base y punto de partida. El proceso SPR asigna un SL a una zona ICS de una manera análoga a la capa de análisis de protección (LOPA) que asigna un SIL objetivo (SIL_{obj}) para cada Función Instrumentada de Seguridad (FIS).

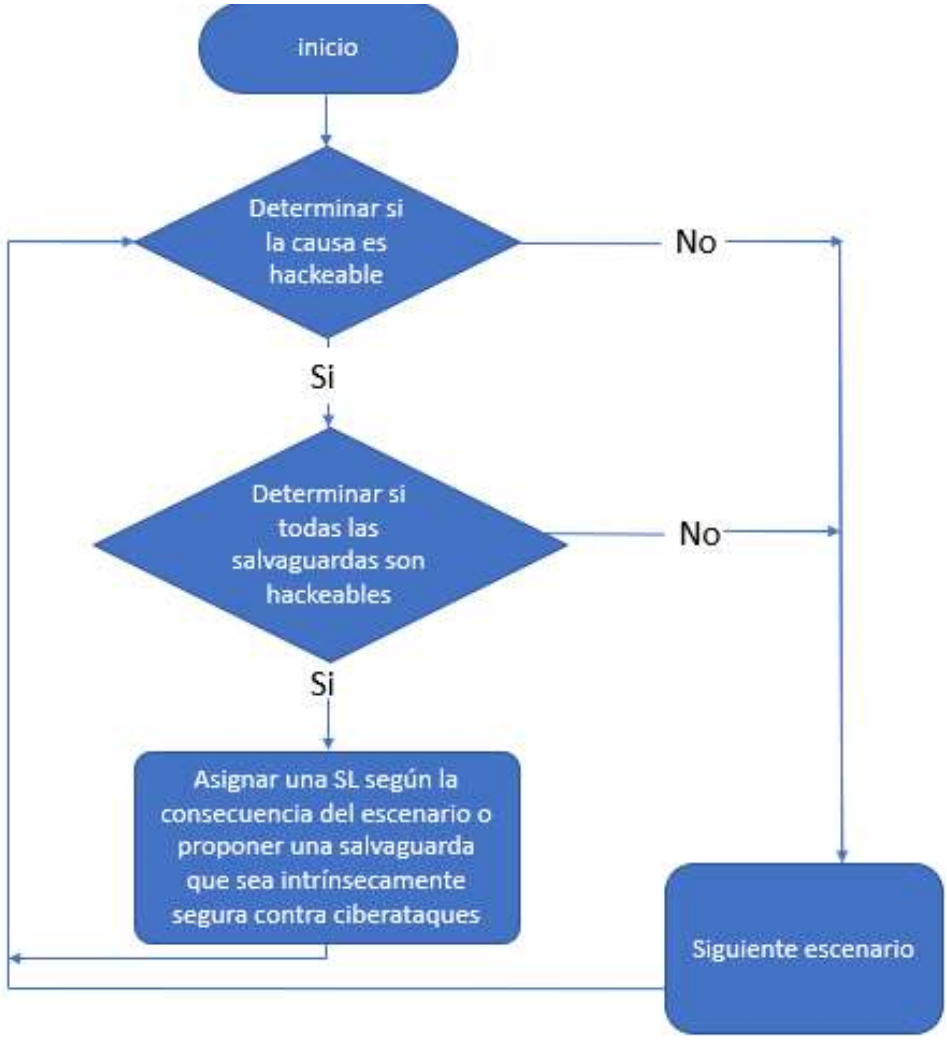


Figura 4 Modelo simplificado del proceso SPR. Adaptada de: (M. Marszal & McGlone, Cap. 1. 2019)

El proceso de SPR, que se muestra en la Figura 4, comienza con la recopilación de los resultados de la PHA. Esto se puede hacer con el informe de una PHA existente o como un paso adicional durante un estudio de PHA mientras el estudio está en progreso. Luego, se revisa cada escenario de la PHA para determinar si es vulnerable a un ciberataque (hackeable), lo que significa que un actor malévolo podría tomar el control del ICS y con ello, podría ocasionar un evento destructivo. Acto seguido, se revisa cada causa o cada evento iniciador para determinar si se puede hackear. Generalmente, esto sería cierto para cualquier falla del lazo de control del Sistema de Control (DCS o cualquier otro sistema de control basado en tecnología electrónica) o los controles propios de equipos "paquete, que se suministran con todo y su control propio". No sería así para las interacciones humanas con equipos de procesos mecánicos que no están conectados a una computadora. Si la causa no es hackeable, el analista pasa al siguiente escenario.

A continuación, se revisan las salvaguardas para determinar si se pueden hackear. En general, todos los circuitos de control, funciones SIS y respuestas del operador a las alarmas puedes ser ciber-vulneradas, pero los dispositivos mecánicos, como las válvulas de alivio, no lo son. Si alguna de las salvaguardas no se puede sabotear, el analista pasa al siguiente escenario.

Si la causa de un escenario, así como todas las salvaguardas pueden ser hackeadas, entonces se determina que el escenario general es hackeable, lo que significa que, si un actor malévolo tomara el control del ICS y capas tipo SIS, esa persona podría generar el escenario a propósito y propiciar las consecuencias asociada a ese escenario. Para cada escenario hackeable, se debe determinar la categoría de consecuencia de la PHA. Basado en los criterios de tolerancia al riesgo del proceso, entonces se asignaría una SL de ISA / IEC a ese escenario. Por supuesto, si la consecuencia es severa y da como resultado una SL que no es deseable, el equipo de análisis tendría la opción de recomendar una salvaguarda que sea inherentemente segura contra el ciberataque y, de este modo, eliminar el escenario como un posible impulsor del problema. Después de que todos los escenarios hayan sido revisados de esta manera, el SL asignado a una zona será el más alto de todos los SL asignados a los escenarios asociados con el equipo ICS de esa zona.

2.4.1 Beneficios del estudio SPR.

La realización de estudios SPR para identificar y mitigar adecuadamente los vectores de amenaza de ciberataque contra las instalaciones de proceso tiene varios beneficios según (M. Marszal & McGlone, 2019).

- **Menor riesgo:** el estudio SPR permite reducir el riesgo a un nivel tolerable al garantizar que todos los escenarios de peligro del proceso que pueden sufrir ciberataque se revisan para determinar la consecuencia máxima, que luego se utiliza para asignar un SL. A diferencia de otros métodos de evaluación de riesgos, el proceso SPR considera el uso de salvaguardas que son inherentemente seguras contra ataques cibernéticos para reducir el riesgo en lugar de depender de una protección basada en computadora cada vez más compleja, eliminando así las debilidades y aumentando la confiabilidad y resistencia de la solución.

- **Mejor comprensión de los vectores de ciberataques:** debido a que el proceso del estudio SPR se centra en el equipo de proceso en lugar del equipo ICS, permite comprender mejor qué acciones se pueden tomar en el proceso para generar una consecuencia. El proceso crea un mapa de los pasos que puede tomar un atacante para provocar una condición peligrosa, lo que permite centrarse más en el diseño del ICS para prevenir esos escenarios específicos.

- **Tomar las decisiones correctas para el diseño en cuestión:** la selección de las salvaguardas de ciberseguridad adecuadas depende de la situación en cuestión. Los

aumentos en la ciber seguridad a menudo se compensan con costos más altos y sistemas más complejos y difíciles de usar. El equilibrio óptimo se logra aplicando el grado de protección que se requiere para mitigar los riesgos identificados a un nivel tolerable. Un SPR ayuda a tomar estas decisiones al proporcionar una base completa y precisa para determinar cuáles son realmente los riesgos y la reducción necesaria para cada escenario. Esto se logra enfocándose en el proceso que se está protegiendo, no en el equipo del sistema de control.

- **Mayor eficiencia:** debido a que los estudios SPR son extensiones de los procedimientos de trabajo de seguridad de procesos existentes, son más eficientes que realizar estudios nuevos y separados de riesgo de ciberseguridad que esencialmente comienzan desde cero, en cuyo caso muchas actividades de análisis de riesgo se reharían. Un SPR se acopla a los análisis previamente realizados, lo que resulta en una reducción del tiempo de ingeniería y una mayor aceptación de las partes interesadas que ya están familiarizadas con las prácticas de trabajo de seguridad de procesos existentes.

- **Cumplimiento de estándares:** el cumplimiento de estándares es siempre un factor importante para el diseño de plantas de proceso, especialmente en industrias altamente reguladas. El proceso SPR aprovecha las buenas prácticas de ingeniería reconocidas y generalmente aceptadas como punto de partida para el análisis. Luego, el proceso continúa para agregar pasos que garantizarán el cumplimiento de estándares y regulaciones adicionales que son específicos de la ciberseguridad. En general, el enfoque de SPR garantiza el cumplimiento de estándares de ciberseguridad y procesos, al tiempo que minimiza la cantidad de trabajo adicional y la repetición.

Las aplicaciones del método SPR en plantas de proceso mexicanas no son de conocimiento público, al menos no existe un registro al que se tenga acceso al momento de escribir este trabajo, debido entro otras cosas que las autoridades nacionales no exigen un registro público riguroso y por la naturaleza sensible de la información, las empresas que si lo realizan resguardan celosamente este tipo de archivos. Por lo anterior es difícil obtener un contexto global y más aún nacional de la implementación de este método.

2.5 Nivel de seguridad o Security Level (SL)

Como se define en la serie ISA/IEC-62443, son categorías que definen un conjunto de políticas, procedimientos y prácticas que deben implementarse para asegurar una zona de ICS. A diferencia del "SIL" cuantitativo definido en los estándares IEC-61511 y la ISA84, que es una banda de probabilidad promedio de fallas bajo demanda, el SL es un conjunto de requisitos cualitativos para explicar cómo se debe diseñar y operar un sistema en función de las capacidades y la motivación del atacante. La serie ISA/IEC 62443 define cuatro niveles de seguridad, SL 1 a SL 4, siendo SL 1 el menos seguro y SL4 el más seguro. Los niveles se definen (en abstracto) de la siguiente manera:

- **SL1** – Personal que comete errores no intencionales.

- **SL2** – Ataques no dirigidos, ataques comerciales basados en internet que se propagan al ICS.
- **SL3** – Ataques de ICS dirigidos, que podrían ser realizados por un miembro de confianza, un empleado descontento, un contratista externo, personal bien intencionado que viole las prácticas de seguridad, etc.
- **SL4** – Administradores de sistemas, ataques dirigidos de una nación a otra.

Las definiciones de SL anteriores son de naturaleza cualitativa, y proporcionan poco en cuanto a especificaciones de diseño concretas. Además, los diseñadores de sistemas de control pueden interpretar fácilmente estos requisitos de manera diferente cuando están escritos de esta manera abstracta. Se requiere mucha más información para comprender completamente las diferencias en las prácticas de diseño entre los distintos SL.

Evaluando los criterios de riesgo, basados en las afectaciones a la seguridad, al ambiente y a los activos, de este modo se fija el SL objetivo. A continuación, se muestran estos criterios en la tabla 2 (M. Marszal & McGlone, 2019).

Tabla 2 SL Objetivo. Obtenida de: (M. Marszal & McGlone, 2019).

Categoría	Daños			TMEL	SL
	Seguridad	*Ambiental*	*Comercial*		
Nula	Sin daños significantes para la seguridad.	Ninguno	Ninguno	N/A	1
Muy baja	Heridas menores que requieren atención de primeros auxilios.	Pequeñas fugas con mínimos requerimientos de limpieza.	$50,000 USD $1,000,000 MNX	1.00E-02	1
Baja	Tiempo perdido y heridas que no requieren hospitalización prolongada.	Fugas moderadas limitadas a daños en el sitio con un esfuerzo de limpieza moderado.	$500,000 USD $10,000,000 MNX	1.00E-03	2
Moderada	Heridas severas, hospitalización prolongada o desmembramiento.	Fugas grandes con impacto limitado a fuera del sitio, con requerimientos significativos de limpieza en el sitio	$5,000,000 USD $100,000,000 MNX	1.00E-04	2
Alta	Una fatalidad	Fugas grandes fuera del sitio que requieren limpieza extensa y provocan daño en varias áreas sensibles	$50,000,000 USD $1000,000,000 MNX	1.00E-05	2
Muy alta	Múltiples fatalidades	Fugas muy grandes fuera del sitio que requieren limpieza extensa y provocan daño permanente en varias áreas sensibles	$500,000,000 USD $10,000,000,000 MNX	1.00E-06	3
Muy muy alta	Múltiples muertes fuera de sitio	Fugas muy muy grandes fuera del sitio que requieren limpieza exhaustiva y reaparición continua durante muchos años junto con daños permanentes en muchas áreas sensibles	$5,000,000,000 USD $100,000,000,000 MNX	1.00E-07	4

2.6 Zonas de seguridad y capas de protección o conduits.

El concepto de SL se aplica a un subconjunto del equipo ICS en una planta de proceso. Este subconjunto de equipos se denomina zona de seguridad, que a menudo se abrevia simplemente a zona. el estándar define una zona de seguridad de la siguiente manera:

Zona de seguridad: Una agrupación de activos lógicos o físicos que comparten requisitos de seguridad comunes. Una zona tiene un límite claro con otras zonas. La política de seguridad de una zona normalmente se aplica mediante una combinación de mecanismos tanto en la frontera como en el centro de la zona. Las zonas pueden ser jerárquicas en el sentido de que pueden estar compuestas por una colección de subzonas.

Debido a que aplican diferentes niveles de seguridad para diferentes operaciones, el concepto de zona permite implementar diferentes componentes de un ICS con diferentes niveles de seguridad. Cada zona debe estar creada de tal manera que se encuentre claramente delimitada para diferenciar entre los componentes que se encuentren dentro de ésta y los que no, las zonas son comúnmente delimitadas por barreras físicas, pero también pueden definirse de manera lógica (es decir una zona virtual) basándose en las diferentes funcionalidades que pueden existir dentro de un solo equipo físico.

Un conduit es una colección de equipos que contienen datos que mueven de una zona a otra. Las normativas definen un conduit de la siguiente manera:

Conduit o capa de protección: Una agrupación lógica de activos de comunicación que protege la seguridad de los canales que contiene. (Esto es análogo a la forma en que un conducto físico protege los cables de daños físicos).

En un sistema de control moderno, es deseable que la información fluya por toda la organización, y con este propósito esta debe salir y entrar de ciertas zonas. Para que esta comunicación se realice de forma segura, se emplea un tipo diferente de zona de seguridad denominada conduit. Al igual que el resto de las zonas el conduit o capa se conforma de componentes físicos y lógicos. El conduit o capa de protección debe diseñarse de acuerdo con el SL más alto de las zonas a las que comunica. Un diagrama conceptual muy simple de muestra a continuación en la figura 5.

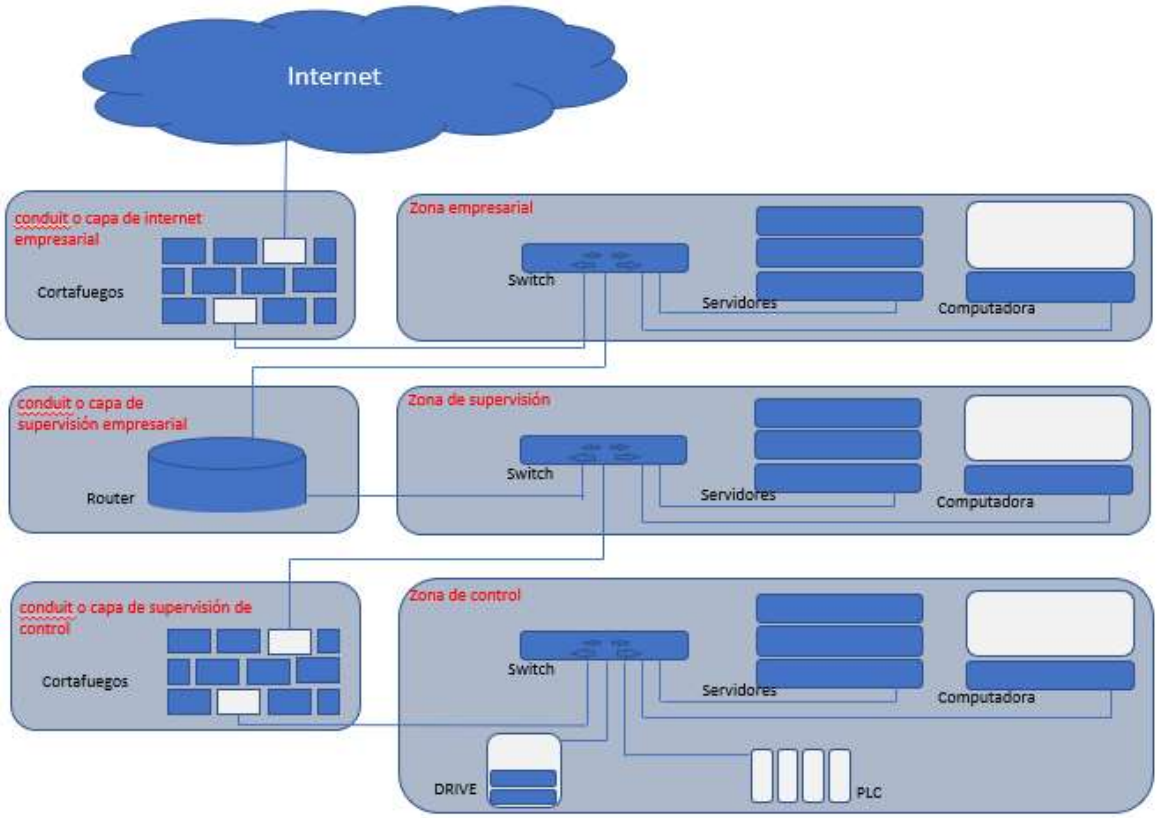


Figura 5 Modelo simple de zonas y conduits Adaptada de: (M. Marszal & McGlone. 2019, Cap. 1)

2.7 Descripción general de la ISA/IEC 62443.

La ISA / IEC 62443 es una colección de estándares e informes técnicos. Estos documentos están interrelacionados en el sentido de que establecen requisitos de seguridad para los sistemas de control y automatización industrial.

2.7.1 Estructura de la serie ISA / IEC 62443.

La serie ISA / IEC 62443, *Security for industrial Automation and Control Systems*, es una colección de estándares que proporciona requisitos de ciberseguridad para sistemas de control de automatización industrial (IACS). Debido a que el tema es tan amplio, un solo documento que discuta todas las facetas del análisis, diseño, operación y mantenimiento no sería práctico. En su lugar, se crearon varios documentos que estaban dirigidos a un interés específico la ciberseguridad en el proceso. La Figura 5 presenta una descripción general de los documentos que componen la serie ISA / IEC 62443 y cómo se relacionan.

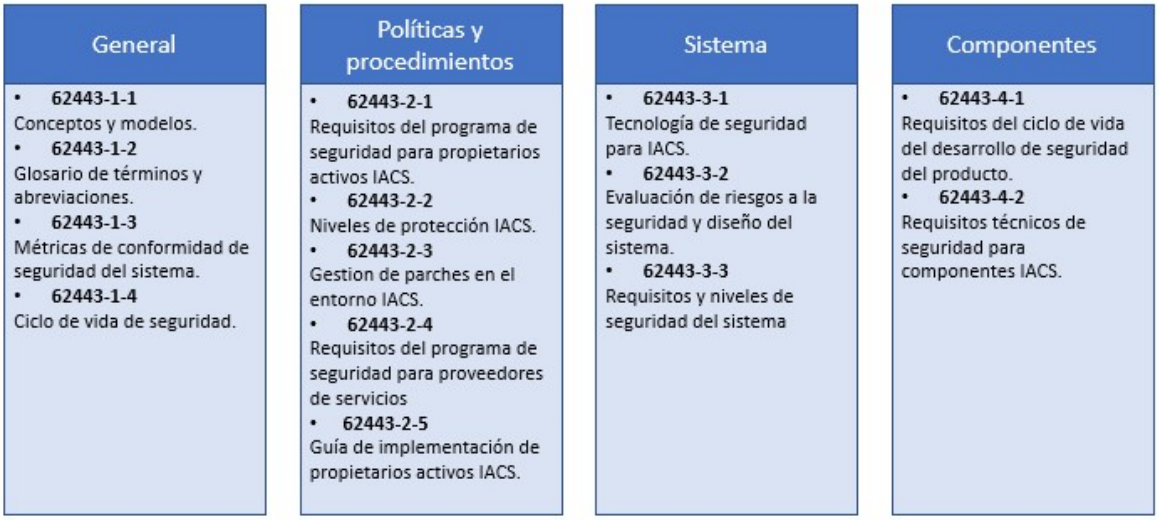


Figura 6 Colección de documentos que conforman la ISA/IEC 62443. Obtenida de: (M. Marszal & McGlone. 2019, Cap. 2)

Como se muestra en la Figura 6, la serie ISA / IEC 62443 (M. Marszal & McGlone, 2019) es una colección de 14 documentos que están separados en cuatro categorías separadas.

Primero, está la categoría general. Contiene cuatro documentos que están destinados a ser de interés general para todas las partes interesadas y disciplinas. El primer documento;

Parte 1-1 Terminología, Conceptos y Modelos, contiene una descripción general de por qué se debe implementar la ciberseguridad, una definición del ciclo de vida del nivel de ciberseguridad, incluidos los requisitos para cada paso del ciclo de vida y una descripción general del riesgo.

Parte 1-2: Glosario maestro de términos y abreviaturas, desempeña eficazmente el papel que su título implica.

Parte 1-3 Métricas que conforman el sistema de seguridad contiene un conjunto de parámetros que pueden medirse para determinar la efectividad del ICS.

Parte 1-4: Casos de uso y ciclo de vida de seguridad de IACS, amplía las definiciones originales de los pasos y requisitos del ciclo de vida que se presentaron en la Parte 1-1 con más detalle.

La segunda categoría, políticas y procedimientos, tiene cinco documentos y está destinada a ser de interés principal para las personas que trabajan para empresas que emplean un ICS para controlar las operaciones de sus procesos. Este grupo de documentos ayuda a estas partes interesadas a desarrollar políticas y procedimientos internos o corporativos sobre cómo una empresa implementará específicamente la ciberseguridad.

Parte 2-1: Requisitos del programa de seguridad para los propietarios de activos de IACS, proporciona una descripción general del contenido que debe incluirse en los documentos de las directrices corporativas, junto con algunas opciones para la implementación.

Parte 2-2: Niveles de protección IACS.

Parte 2-3: Gestión de parches en el entorno IACS. proporciona información detallada a quienes mantienen el ICS sobre cómo realizar la gestión de parches en un entorno operativo, destacando las diferencias entre ese proceso y cómo se realiza habitualmente en un entorno de oficina. y por qué esos métodos no serían eficaces para el ICS.

Parte 2-4: Requisitos del programa de seguridad para proveedores de servicios, define los requisitos normativos relacionados con la instalación y el mantenimiento.

Parte 2-5: Guía de implementación para propietarios de activos IACS, define los requisitos asociados con la operación de un sistema de gestión de seguridad.

En tercer lugar, está la categoría del sistema que contiene tres documentos que describen los detalles del diseño del sistema implícitos o mencionados en otros documentos.

Parte 3-1: Tecnología de seguridad para IACS., proporciona detalles sobre los tipos de equipos, parámetros operativos y procedimientos que se pueden utilizar para la ciberseguridad en un ICS.

Parte 3-2: Diseño del sistema de evaluación de riesgos de seguridad, proporciona información relacionada con la realización de evaluaciones de riesgos y analiza cómo los resultados del proceso de evaluación de riesgos se relacionan con los parámetros de diseño.

Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad, es el documento que define lo que significan los distintos SL´s en términos de equipos y los requisitos operativos necesarios para lograr los distintos SL´s.

La cuarta es la categoría de componentes. Se compone de dos documentos que se dedican a definir los requisitos de ciberseguridad a nivel de componente, a diferencia del nivel general del sistema que es el enfoque principal de los documentos en las otras categorías. Debido a que estos documentos discuten el nivel de componente, son principalmente de interés para los proveedores de equipos que suministran componentes 1CS a los usuarios finales.

Parte 4-1: Requisitos del ciclo de vida de la implementación de seguridad del producto, establece los requisitos para los proveedores de equipos con respecto a los procedimientos que deben usarse al desarrollar sus productos.

Parte 4-2: Requisitos de seguridad técnica para componentes IACS, proporciona un conjunto más detallado de características técnicas que deben implementarse en los componentes proporcionados por los proveedores de equipos de ICS para mejorar la ciberseguridad. Mientras que la Parte 4-1 se centra realmente en el proceso de diseño, la Parte 4-2 se centra más en los atributos de los componentes.

2.7.2 Ciclo de vida y requisitos de acuerdo con la ISA / IEC 62443.

Como muchos otros estándares sobre instrumentación y sistemas de control implementados en aplicaciones de plantas de proceso, la ISA / IEC 62443 emplea un enfoque de ciclo de vida para estructurar las tareas que deben realizarse, las entradas y salidas de cada fase, así como los requisitos que esas tareas deben cumplir, como se muestra en la figura 6.

La siguiente fase del ciclo de vida del nivel de seguridad es la fase de implementación. En la fase de implementación, los requisitos de SL identificados en la fase de evaluación se convierten en atributos de diseño del sistema específicos que se documentan en un documento de especificación de requisitos de seguridad. Esta especificación se utiliza luego como base para el diseño detallado, la compra, la configuración y la instalación del ICS. Una vez instalado el sistema completo, se prueba para garantizar que todos los requisitos especificados de ciberseguridad se hayan implementado.

En resumen, la 1SA / IEC 62443 no es un documento único conciso, sino que es una colección de múltiples documentos que aborden diversos pasadores y disciplinas que participan en la ciberseguridad para un ICS.

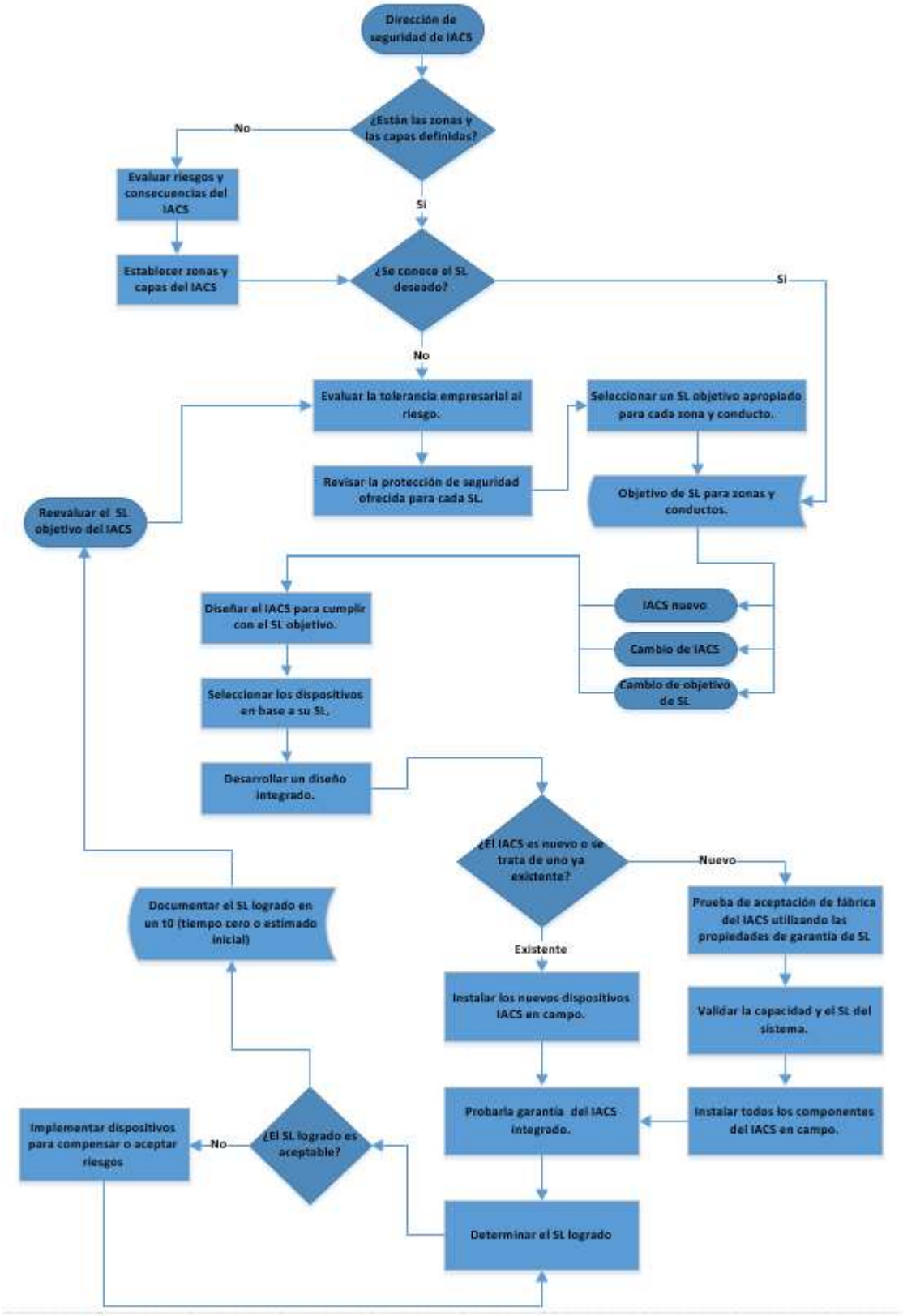


Figura 7 Ciclo de vida del proceso según la ISA/IEC 62443. Adaptada de: (M. Marszal & McGlone. 2019, Cap. 2)

2.8 Limitaciones de los métodos de análisis de riesgo a la ciberseguridad.

Muchos de los métodos desarrollados para definir las prácticas de ciberseguridad establecen que el punto de partida para la ciberseguridad es un análisis de riesgo que definirá el grado requerido de ciber protección del ICS. Desafortunadamente, estos métodos confunden y combinan términos de forma imprecisa, lo que da como resultado recomendaciones para realizar tareas que no identifican adecuadamente los peligros a salvaguardar. Gran parte de la confusión proviene del uso del término evaluación de riesgos para describir los pasos del ciclo de vida que incluyen la identificación de peligros, la evaluación del modo de falla de las salvaguardas y la verificación y validación del diseño de ICS. Los otros tipos de análisis son apropiados cuando se usan para determinar otros riesgos que ocurren en diferentes momentos del ciclo de vida, este análisis proporciona resultados apropiados que se pueden usar para predecir fallas de equipos y otros problemas potenciales. Para aliviar la confusión que rodea a la evaluación de riesgos, este capítulo y el siguiente definirán claramente la terminología precisa y los métodos específicos utilizados en la evaluación de riesgos. Los profesionales de la industria de procesos que están familiarizados con las metodologías exitosas y bien establecidas para el análisis de peligros de procesos se pudieran preguntar por qué se requiere una nueva metodología para evaluar el riesgo de ciberataques de las plantas de proceso. Algunos profesionales de la seguridad social en el gobierno, el mundo académico y la industria han desarrollado, o sugerido, métodos adicionales para abordar este problema. El problema principal con estos métodos adicionales es que complican el problema en las industrias de procesos que ya realizan análisis de riesgo diseñados para identificar el riesgo del proceso en sí. Al centrarse en el proceso bajo control, los demás procesos industriales, incluida la fabricación por lotes y discreta, también pueden protegerse. Además, el análisis de riesgos de los procesos industriales controlados por tecnología electrónica requiere una comprensión del proceso industrial y cómo reacciona a una falla. El análisis del equipo ICS por sí solo proporciona poco conocimiento del riesgo real que plantea el proceso industrial.

2.9 Requisitos de la ISA / IEC 62443 para la evaluación de riesgos.

Los requisitos de la serie ISA / IEC 62443 para la evaluación de riesgos requiere que se realice una evaluación de riesgos para determinar el nivel apropiado de salvaguarda de la ciberseguridad. Desafortunadamente los estándares usan el término libremente y en diferentes sentidos. Como resultado, incluso definir lo que se supone que la evaluación de riesgos se convierte en confusa y varía según la situación y el contexto. El estándar ANSI / ISA-62443-2-1 define dos tipos de evaluación de riesgos que deben realizarse en un ICS con respecto a la ciberseguridad: alto nivel o Hig-Level y detallado. Lo que se refiere el estándar como evaluación de riesgos de alto nivel considera los tipos generales de vulnerabilidades de los ICS con respecto a la ciberseguridad y las consecuencias al proceso que se pueden esperar si esas vulnerabilidades están presentes en el sistema. La evaluación de riesgos detallada es similar, pero en lugar de categorías generales de vulnerabilidades, se analizan directamente las vulnerabilidades específicas que están relacionadas con las marcas, modelos y versiones de software de los componentes ICS específicos. Para aclarar

la terminología. El diagrama de flujo que se muestra en la Figura 7, es consistente con las técnicas de identificación de peligros tradicionales y la aplicación de la gama completa de salvaguardas de proceso (de las cuales la ciberseguridad es solo una). La terminología y las técnicas en el flujo de trabajo son de la serie ISA / IEC 62443.

La Figura 8 presenta el diagrama de flujo simplificado para la aplicación de protección de ciberseguridad, la malla verde, indica los puntos que se cubren en la tesis. La primera tarea es la identificación de escenarios de procesos en los que el riesgo es intolerable. En la terminología de la ISA / IEC 62443, este es el análisis de riesgo de alto nivel. La palabra más crítica aquí es: "proceso". Sin comprender el proceso industrial que se está controlando y sin saber en qué circunstancias se puede perder el control, junto con las consecuencias, las causas y las salvaguardas relacionadas con ese escenario: el riesgo simplemente no se puede conocer. Los métodos tradicionales de evaluación de riesgos promulgados por la comunidad de ciberseguridad simplemente no son capaces de realizar esta tarea, razón por la cual se desarrolló el método SPR. Esta tarea de identificación inicial implica analizar el proceso y no el ICS.

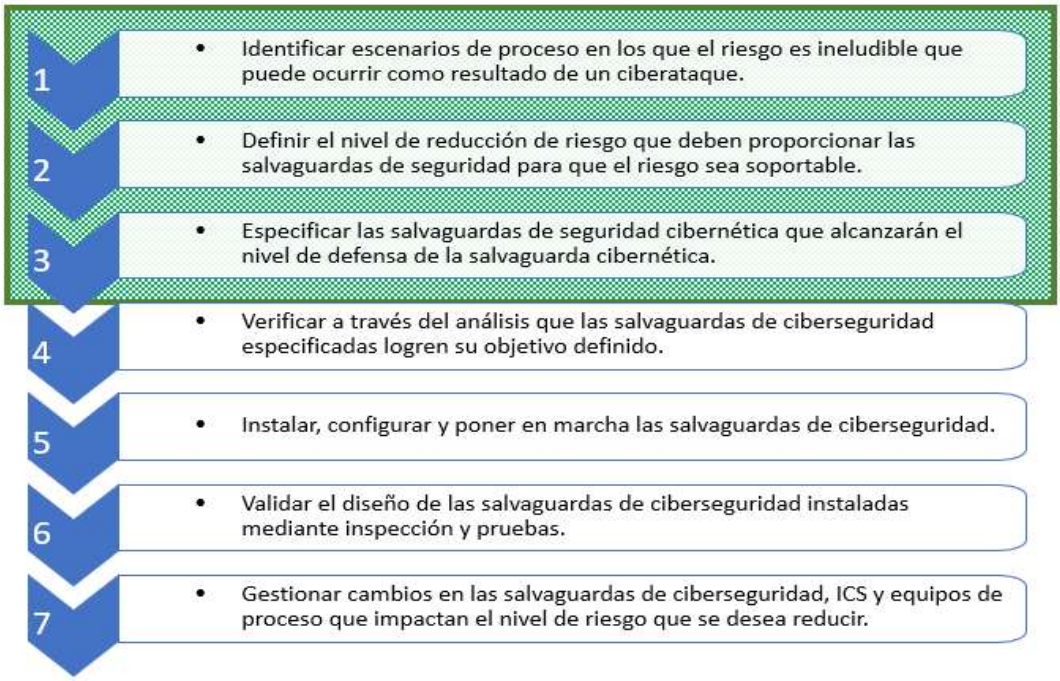


Figura 8 Diagrama de flujo de un proceso de ciberseguridad. Adaptada de: (M. Marszal & McGlone, 2019).

Una vez que se identifican los escenarios vulnerables a un ciberataque, se puede determinar hasta qué punto se debe utilizar la ciberseguridad para reducir el riesgo. De acuerdo con la serie ISA / IEC 62443, se asignaría una SL para lograrlo. Después de que se define el SL, se puede desarrollar una especificación de requisitos de ciberseguridad que enumerará y definirá el equipo ICS y los atributos necesarios para lograr el SL asignado. En este punto del ciclo de vida del nivel de seguridad, se puede realizar una tarea de verificación que analiza el diseño del ICS para garantizar que se cumplan todos los requisitos de SL. En esta etapa, se puede utilizar una técnica para evaluar la efectividad del diseño. En la

terminología de la ISA / IEC 62443, esto se consideraría una evaluación de riesgos detallada. El uso del término evaluación de riesgos aquí es confuso, sin embargo, está contenido en la norma y se debe estudiar su uso. De hecho, en esta etapa el equipo del proyecto está realizando una revisión del diseño. A modo de analogía, no es raro que un equipo de proyecto que diseña una bomba considere todos los modos de falla y los efectos de su diseño para una aplicación específica (por ejemplo, sus metalurgias seleccionadas, espesores de pared y materiales de juntas y sellos) para asegurarse de que sea apropiada para la aplicación específica. Sin embargo, nadie llamaría a esto un análisis de riesgo. Entonces, lo que la comunidad de ciberseguridad llama una evaluación de riesgos detallada, cualquier otra disciplina de ingeniería lo llamaría erróneamente, una revisión de diseño.

En las etapas posteriores del ciclo de vida de ciberseguridad, el diseño verificado se instala y prueba para garantizar que el diseño coincida con la especificación y que no se introdujeron vulnerabilidades durante el proceso de instalación. Este paso de validación se conoce comúnmente como una evaluación de la vulnerabilidad cibernética (CVA), que se realiza después de la instalación inicial del equipo, así como de forma continua durante la fase de operaciones del proceso de gestión del cambio.

2.10 Métodos de evaluación de riesgos, propuestos por la comunidad de ciberseguridad.

Varios equipos de profesionales han propuesto diversas metodologías para realizar evaluaciones de riesgos como se presenta en la serie ISA / IEC 62443. Si bien las técnicas presentadas son de poco beneficio para la identificación de peligros y la posterior selección de objetivos de SL, tienen algún beneficio para la parte de revisión del diseño de las actividades de ciberseguridad. Algunos métodos que han sido propuestos por la comunidad de ciberseguridad incluyen:

- Ciber PHA / ciber HAZOP
- CHAZOP

A continuación, se presenta el proceso simplificado en la figura 9 en forma de diagrama.

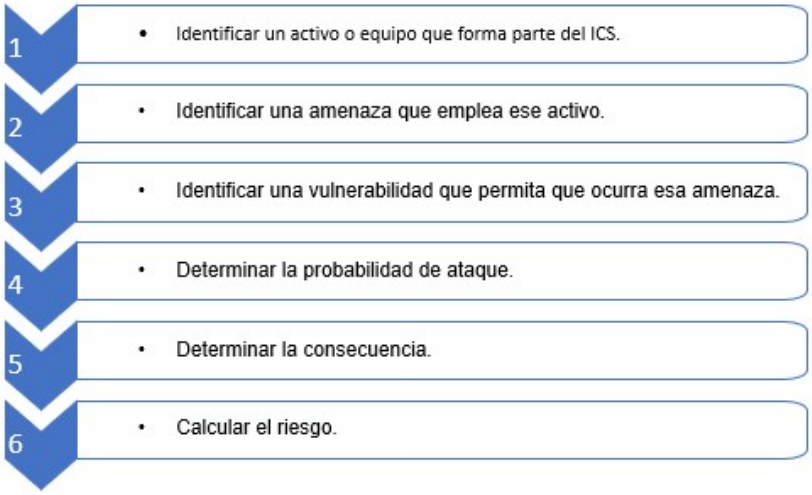


Figura 9 Proceso típico de una evaluación de riesgos a la ciberseguridad. Obtenida de: Elaboración propia.

El proceso mostrado en el diagrama no identifica los escenarios de peligro del proceso, sino que identifica vulnerabilidades en el diseño del equipo (o modos de falla, en la terminología común a PHA). Aunque estos enfoques utilizan nombres que implican que son como técnicas de identificación de peligros, no lo son. Las técnicas de la comunidad de seguridad cibernética presentadas en la Figura 6 son simplemente variaciones de FMEA que se aplican exclusivamente al ICS, no al proceso industrial controlado al que pertenece el análisis. Si bien FMEA es una buena herramienta para analizar el diseño del equipo e identificar cualquier punto débil, es una mala herramienta para identificar escenarios que hacen que el proceso se vuelva inmanejable y potencialmente pierda la contención de materiales y energía peligrosos.

Debido a que la mayoría de los métodos de evaluación de riesgos cibernéticos adolecen del problema de identificar debilidades en el diseño de equipos de red, no se puede determinar el riesgo general de la planta. Se debe utilizar otro enfoque para identificar los escenarios de riesgo en los que las vulnerabilidades cibernéticas pueden afectar el perfil de riesgo general de la planta de proceso. Aquí es donde un SPR encaja en un programa de ciberseguridad bien diseñado.

2.10.1 Ciber PHA / Ciber HAZOP

Ciber PHA, o ciber HAZOP, fue uno de los primeros métodos desarrollados por la comunidad general de ciberseguridad (no específicamente por ingenieros de seguridad de procesos) para evaluar el riesgo asociado con los accidentes de control industrial causados por ciberataques. Los nombres se eligieron para imitar las técnicas de la industria de procesos probadas y establecidas de PHA y HAZOP. Si bien los nombres son similares, las técnicas son sustancialmente diferentes. Mientras que las técnicas PHA y HAZOP analizan equipos en el proceso industrial y postulan desviaciones de la intención del diseño, la técnica ciber PHA / ciber HAZOP identifica equipos ICS y luego postula vulnerabilidades (es decir, modos de falla) de esos elementos. El proceso comienza con una lista de todos los equipos ICS en el alcance del estudio. Esto incluiría cualquier equipo de control que

pueda comunicarse a través de una conexión de red, incluidos controladores, estaciones de operador, estaciones de ingeniería, registradores, y equipo de campo con acceso a Internet. Una vez enumerados los equipos, se identifican todas las vulnerabilidades conocidas del equipo. A su vez, se discute cada vulnerabilidad. Esta discusión considera las consecuencias y la probabilidad de que ocurran si se explota la vulnerabilidad. Las consecuencias y probabilidades se clasifican de acuerdo con el riesgo que generan, y su tolerancia se evalúa en función de los criterios tolerables de riesgo corporativos. Si se determina que el riesgo es inaceptable para cualquiera de las vulnerabilidades, se hace una recomendación para reducir el riesgo.

2.10.2 CHAZOP

A fines de la década de 1980 y principios de la de 1990, la mayoría de los sistemas de control analógicos fueron reemplazados por sistemas de control por computadora más potentes. Esto resultó en una serie de fallas nuevas asociadas con los sistemas de control por computadora que no estaban presentes en los sistemas de control analógico. Para abordar estos nuevos peligros, en 1991 Peter Andow propuso y documentó un nuevo enfoque de identificación y análisis de peligros que aplicaba los conceptos de HAZOP a los sistemas de control computarizados. La nueva técnica se denominó estudio de control de riesgos y operabilidad, o (Control Hazard and Operability) CHAZOP. CHAZOP es una metodología desarrollada en industrias de procesos para ayudar a evaluar cómo las fallas en los sistemas de control computacional, como PLC´S y DCS´s, afectan el proceso. Esto asegura que se aplique una cantidad adecuada de redundancia y protecciones de diseño al diseño de estos sistemas de control. CHAZOP fue diseñado originalmente para extender el HAZOP de una planta para generar escenarios en los que la causa de un incidente es una falla de un componente del sistema de control. En un CHAZOP, la intención del diseño de cada componente del ICS se determina y sigue una discusión sobre cómo aplicar las palabras guía y la intención del diseño para crear una desviación. En le Figura 10 se muestran las principales características de las metodologías Ciber-PHA y Chazop.

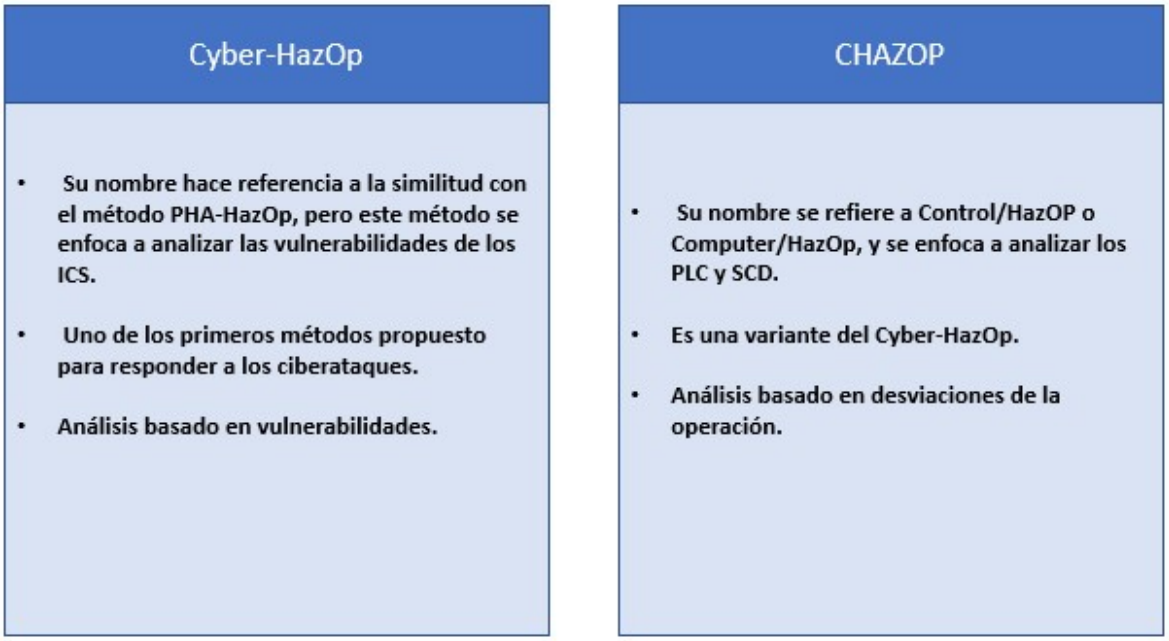


Figura 10 Cuadro comparativo entre ciber-HazOp y CHAZOP. Obtenida de: Elaboración propia.

2.11 Problemas inherentes a los análisis de riesgo cibernético.

Los PHA cibernéticos y otras técnicas de análisis de riesgo cibernético que se aplican con frecuencia, tienen múltiples deficiencias que impiden que se utilicen eficazmente como técnicas de identificación de peligros. El resultado de estas deficiencias es a menudo una falla en la identificación de escenarios críticos y una dependencia e implementación excesivas de la protección cibernética en situaciones en las que no es efectiva, o incluso no es necesaria. El fracaso de las técnicas de análisis de riesgo cibernético para la identificación de peligros es el resultado de las siguientes deficiencias que están presentes en prácticamente todas las técnicas de análisis de riesgo cibernético:

- Ausencia de evento iniciador.
- Resultados potenciales infinitos.
- Frecuencia de ataque incognoscible.
- No considerar la seguridad inherente.
- Frecuencia de ataques deliberados.

Si bien estas deficiencias generalmente impiden que las técnicas de análisis de riesgo cibernético sean efectivas para realizar la identificación de peligros, estas técnicas todavía son bastante capaces de ayudar en la revisión del diseño durante las etapas de validación y verificación del ciclo de vida del nivel de seguridad.

2.11.1 Ausencia de evento iniciador.

Para que un proceso de análisis de riesgo funcione, debe comenzar con algún tipo de evento iniciador. Un evento iniciador es una acción que hace que comience una cadena de eventos que culmina en un accidente. La mayoría de los métodos que se han propuesto para

analizar los riesgos de seguridad cibernética no dan como resultado un evento inicial porque las indicaciones para comenzar la discusión son las vulnerabilidades cibernéticas de los dispositivos de red (incluidos los protocolos de comunicación) y el equipo ICS. Cuando una vulnerabilidad está presente en un dispositivo de conexión de red o una pieza de equipo ICS, ese equipo se encuentra en un estado fallido que permite que sea explotado por un atacante malintencionado, *pero la única respuesta adecuada a lo que sucede es nada*. En realidad, la vulnerabilidad no provoca que ocurra nada, simplemente reside inactiva en el equipo ICS. A modo de analogía, considere usar un análisis similar en otra salvaguarda industrial común, la válvula de alivio. Un estudio podría postular que una válvula de alivio tiene una "vulnerabilidad" como el caso de su disco podría estar desalineado y atascado, impidiendo que pueda abrirse cuando se expone a alta presión. Si se le pregunta al equipo, "¿Cuál es la consecuencia de que la válvula de alivio se atasque?" la única respuesta sería "nada". El hecho de que una salvaguarda no funcione cuando se le pide que lo haga no es un evento inicial que cause un accidente de proceso. En cambio, el modo de falla residirá en la válvula en un estado inactivo hasta que haya una situación que haga que la presión aumente y la válvula de alivio no responderá. De manera similar, las vulnerabilidades del ICS o del dispositivo de red no causan nada: son modos de falla inactivos que esperan a que un evento de inicio real haga que la planta entre en un estado inseguro.

2.11.2 Resultados potenciales infinitos.

Una limitación principal de todos los procedimientos de análisis de riesgo cibernético es que están identificando vectores de ataque, pero no consecuencias. Las vulnerabilidades cibernéticas del sistema de control, en sí mismas, no son las causas iniciales de la pérdida de control de la planta de proceso y los accidentes potenciales subsiguientes de pérdida de contención primaria. Cuando una técnica de análisis de riesgo cibernético postula una vulnerabilidad, como un ataque de intermediario de una estación de operador, los resultados que pueden resultar de ese ataque son infinitos. Si un ataque de intermediario tiene éxito y un actor malintencionado obtiene el control de una planta de proceso de manera discreta, entonces el atacante puede crear cualquier escenario que pueda imaginar con el equipo en cuestión.

Debido a que no se está considerando un escenario de proceso específico en este caso, no es posible comprender realmente cuál es la consecuencia. Como tal, no hay una forma sistemática de pasar de la vulnerabilidad de ICS a la gravedad de la consecuencia porque hay infinitas posibilidades que deben considerarse. Como resultado, los equipos de análisis a menudo recurren a enfoques del "peor escenario" que exagerarán el riesgo y darán como resultado una protección cibernética excesiva y a menudo innecesaria.

2.11.3 No se considera la seguridad inherente contra los ataques cibernéticos.

Debido a los resultados potencialmente infinitos de los métodos de análisis de riesgo cibernético y la consideración del peor caso, las técnicas de evaluación del riesgo cibernético generalmente sobrestiman el riesgo en gran medida. Los métodos existentes solo analizan los dispositivos de red (incluida la red en sí) y el equipo ICS.

Un análisis de riesgos adecuado consideraría cada evento iniciador (o causa) que resulte en esa consecuencia dada. Luego, se evaluaría para cada una de las causas todas las salvaguardas que podrían evitar que la causa se convierta en una consecuencia. Estas salvaguardas podrían incluir elementos ciber-vulnerables como SIS, pero también podrían incluir salvaguardas que son inherentemente seguras contra ataques cibernéticos, como válvulas de alivio. Solo si un escenario puede generarse en su totalidad a través de un ciberataque malicioso, que incluye generar la causa y deshabilitar todas las salvaguardas, se deben considerar sus consecuencias al tomar una decisión sobre el nivel requerido de ciber-protección. Los métodos de evaluación del riesgo cibernético no son capaces de este nivel de detalle debido a la naturaleza del enfoque utilizado.

2.11.4 Frecuencia de ataques deliberados.

La mayoría de las técnicas de análisis de riesgo cibernético consideran la frecuencia como un parámetro cuando se habla de riesgo. Esto se hace para que los métodos de evaluación de riesgos cibernéticos sean análogos a otros métodos de evaluación de riesgos. Si bien la evaluación de riesgos tradicional puede utilizar eficazmente la probabilidad como parámetro, el análisis de riesgo cibernético no puede ni debe hacerlo. La probabilidad en los PHA tradicionales es el resultado de fallas humanas y de hardware aleatorias para realizar correctamente las tareas. Estos fallos son aleatorios y siguen las leyes de la estadística y la probabilidad. Este no es el caso de los ciberataques maliciosos. Los ciberataques son acciones deliberadas. Las leyes de la probabilidad no se aplican a acciones deliberadas. La probabilidad de un ciberataque no solo es desconocida, es incognoscible. Las técnicas que intentan emplear frecuencias de ataque utilizan un juicio deficiente al asignar las características de un fallo aleatorio a un ataque deliberado. En su lugar, es más apropiado aplicar la gravedad de las consecuencias, ya que es más probable que se intenten los ataques que generan altas consecuencias que los ataques que solo darán como resultado efectos pequeños.

Capítulo 3. Planta Hidrodesulfuradora de Naftas.

3 Planta hidro desulfuradora de Naftas.

La intención de este apartado es dar un contexto al funcionamiento de una planta Hidrodesulfuradora de nafta (HDN) dentro del esquema de una refinería.

El petróleo crudo que se obtiene del proceso de extracción se compone principalmente de aglomerados de hidrocarburos, llamados fracciones, que poseen diferentes puntos de ebullición, cuan más larga es la cadena de los compuestos de hidrocarburo mayor es su punto de ebullición.

> El primer tratamiento al que se somete la carga de crudo que ingresa a una refinería es una destilación a presión atmosférica, de la cual se obtienen diversos productos o "cortes", separándose en los platos de la columna fraccionadora gracias a la diferencia entre sus puntos de ebullición. Las diversas fracciones de líquidos son colectadas en los platos de la columna y posteriormente se transfieren a los condensadores para su enfriamiento adicional antes de ser enviadas a los tanques de almacenamiento (Oiltanking GmbH, 2016).

Las fracciones de hidrocarburos más pesados presentes en la destilación atmosférica son enviados a una destilación al vacío, para obtener una mayor cantidad de productos intermedios con mayor valor comercial. En la figura 8 se muestra un esquema ilustrativo del proceso de una refinería.

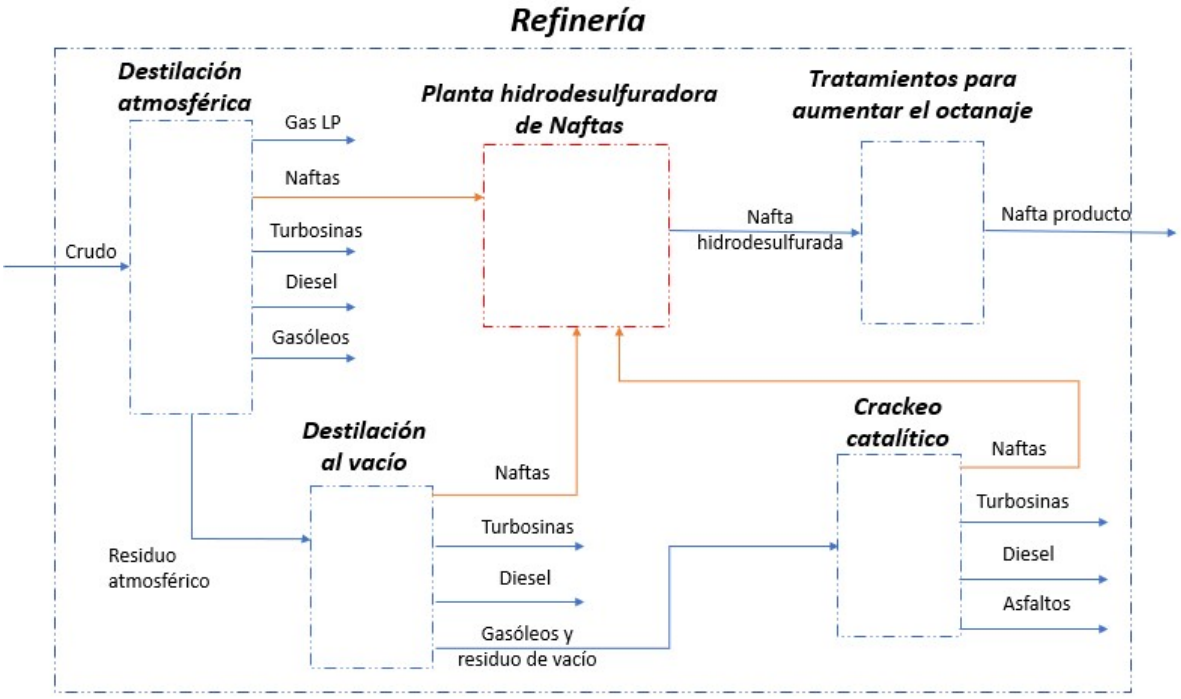


Figura 11 Esquema ilustrativo de la ubicación de una HDN en una refinería. Obtenido de: Elaboración propia.

Como se aprecia en la Figura 11, la planta Hidrodesulfuradora de naftas recibe carga de ambas columnas de destilación, atmosférica y de vacío, así como de la planta de crackeo catalítico, se llevan a cabo una destilación al vació y un crackeo catalítico con la finalidad

de aumentar la cantidad de productos de alto valor comercial como la Nafta, y reducir la cantidad de residuos pesados proveniente del petróleo que poseen un valor de mercado más bajo y menor utilidad.

Muy pocos componentes que salen de la columna fraccionadora están listos para el mercado. Muchos de ellos requieren un mayor procesamiento químico (por ejemplo, la reformación, combinación) dentro de otras fracciones. Las fracciones destiladas y químicamente procesadas son luego tratadas para remover las impurezas, tales como compuestos orgánicos que contienen azufre, nitrógeno, oxígeno, agua, metales disueltos y sales inorgánicas. Luego de ser tratadas, las fracciones son enfriadas y luego mezcladas para elaborar diversos productos. Eventualmente, algunos de estos productos son traídos por barco, ducto, ferrocarril o camión hasta uno de los terminales.

Las plantas hidrotratadoras de Nafta son parte importante de las refinerías de todo el mundo. Una vez que el crudo que ingresa a la refinería entra a la primera etapa de destilación, que es una destilación atmosférica, y se separa en varios cortes desde gas butano, hasta residuo atmosférico, pasando por turbosina, diésel, y Naftas. Cada uno de estos cortes contiene entre sus componentes al azufre en forma de ácido sulfhídrico H_2S, la presencia de ácido sulfhídrico en los cortes de petroleo dificulta su manejo debido a que los vuelve corrosivos y aumenta el riesgo de intoxicación del personal de la planta.

La intención de diseño de una planta hidrodesulfuradora de naftas es separar el ácido sulfhídrico de la nafta amarga (con H_2S), para convertirla en nafta endulzada (sin H_2S). Esto se logra gracias a una serie de reacciones químicas que se encargan de, saturar los dobles enlaces de las diolefinas, retirar la sílice y eliminar el ácido sulfhídrico.

3.1Descripción y generalidades.

La lectura de la siguiente descripción debe hacerse junto con la apreciación de los DFP´s presentes en el anexo A de esta tesis. La siguiente descripción está basada en **(Meyers, 2004, págs. 11.56-11.78 Cap 11.6**).

La finalidad de la planta HDN es eliminar compuestos indeseables presentes en la nafta de carga, principalmente diolefinas, sílice, olefinas, azufre y nitrógeno, mediante procesos de hidroconversión catalítica, separación y tratamiento para obtener como productos principales nafta ligera y nafta pesada.

El proceso inicia con la recepción en límite de batería de la nafta amarga, una vez dentro de la planta se filtra con ayuda del filtro FG-101 antes de pasar al tanque de carga FA-101, en donde se realiza una primera separación del agua amarga mientras que el hidrocarburo es transportado aguas abajo con ayuda de las bombas GA-101 A/B con destino al tren de precalentamiento formado por el lado tubos de los cambiadores de calor EA-101 y EA-102 donde incrementan su temperatura debido al efluente de reacción y al vapor sobrecalentado.

Pero antes de llegar al primer equipo de intercambio térmico se inyecta hidrógeno de reposición a la corriente principal, el cual proviene del sistema de reposición de hidrógeno conformado por; el compresor reciprocante BC-101 A/B, el enfriador inter-etapa EA-114 A/B, el tanque de succión FA-111, y el tanque inter-etapa FA-112 A/B.

Después de haber incrementado su temperatura la nafta amarga es llevada al primer reactor, el reactor de saturación de diolefinas DC-101, donde gracias a la presencia hidrógeno se rompen los dobles enlaces de las cadenas de hidrocarburos ayudando a evitar la formación de gomas y espumas más adelante en el proceso.

A pesar de que la reacción de saturación de diolefinas es exotérmica, es necesario calentar aún más el efluente del reactor DC-101 para que pueda llevarse a cabo la siguiente reacción, con este fin aguas abajo del reactor DC-1001 se encuentra el tren de calentamiento conformado por el lado tubos de los cambiadores de calor EA-103 A/B y EA-104, además del lado proceso del calentador a fuego directo BA-101. Entre los cambiadores y el calentador se encuentra el mezclador estático EZ-101 A/B. Para lograr controlar la temperatura del sistema se implementa un bypass de todos estos equipos.

Una vez se encuentra la corriente de proceso a la temperatura necesaria, ingresa a los reactores de guarda de sílice DC-102 A/B donde se elimina la sílice del sistema por medio de una reacción exotérmica y posteriormente el efluente del reactor DC-102 A/B se utiliza para precalentar la alimentación al mismo reactor mediante el lado coraza del cambiador EA-104.

Después de haber cedido parte de su energía térmica el efluente del reactor DC-102 A/B se convierte en la alimentación del reactor de hidrotratamiento DC-103 el cual es el “corazón de la planta HDT, ya que, en él se lleva a cabo la reacción hace posible posteriormente remover el azufre presente de la nafta producto.

El efluente del reactor DC-103 se encuentra a una temperatura relativamente alta si se compara con el resto del proceso, debido a esto se emplea para precalentar la alimentación del tren de reacción, cediendo su energía al pasar por el lado coraza de los cambiadores EA-103 A/B y EA-101 A/B.

Una vez se ha aprovechado al máximo la energía del efluente proveniente del tren de reacción se inyecta agua de lavado proveniente del tanque FA-107 con ayuda de la bomba BD-102 A/B. Posteriormente se baja aún más su temperatura para lograr una condensación mayor y una separación más eficiente, con el aereoenfriador EC-101 y con el cambiador EA-105 A/B que funciona con agua de enfriamiento.

Al bajar la temperatura de la corriente de proceso, esta ingresa al tanque separador FA-102 y se dividen en tres salidas, la salida superior de gas amargo que desemboca en el tanque FA-103, la corriente de agua amarga que se divide entre la inyección de agua de lavado y un envío de agua amarga hacia FA-113, y la corriente de hidrocarburo con destino al tanque FA-110.

El gas que entra al tanque FA-103 dentro de este tanque separador es separado del poco líquido que pueda contener y es enviado al sistema de absorción de H_2S a base de Amina, conformado por los siguientes equipos, Torre absorbedora DA-101, Tanque de amina rica FA-109, Tanque de amina pobre FA-108, cambiador EA-106 y tanque de gas recuperado FA-104. Una vez el gas principalmente conformado por hidrógeno pasa por este proceso se reduce drásticamente su cantidad de H_2S, este gas "recuperado" se envía al compresor centrífugo de recirculación GB-101 propulsado por la turbina de vapor MV-101, desde donde es distribuido hacia el tren de reacción para surtir del H_2 necesario a las reacciones de saturación de diolefinas e hidrotratamiento.

Por otro lado, la corriente de hidrocarburo que sale del tanque FA-103 se une con la proveniente del tanque FA-102 y ambas se dirigen al tanque FA-110, donde una vez más se lleva a cabo una separación, en esta ocasión se busca separar el poco gas hidrógeno de la corriente principal de hidrocarburo líquido.

La siguiente etapa del proceso consiste en separar los componentes más ligeros en forma de LPG producto de la mezcla de hidrocarburos, previo a la "estabilización" de la nafta se acondiciona la corriente a la temperatura necesaria con ayuda del lado tubos de los cambiadores EA-110 A/B y EA-107 A/B.

Una vez a las condiciones adecuadas ingresan al sistema de la torre estabi1izadora, el cual se compone de los siguientes equipos; torre estabilizadora DS-101, Calentador a fuego directo BA-102, bomba de reboileo GA-108 A/B, aerocondensador parcial EC-104, condensador total EA-108 A/B, tanque de reflujo FA-105, bombas de reflujo GA-104 A/B y bomba de LPG producto GA-110 A/B. Posteriormente la nafta estabilizada se enfría al pasar a través del lado coraza del cambiador EA-110 A/B antes de ingresar al reactor de guarda de azufre DC-104.

La nafta estabilizada debe separarse en nafta ligera y nafta pesada antes de ser enviada fuera de límite de batería. El sistema de separación de nafta está formado por los siguientes equipos; torre separadora DS-102, calentador a fuego directo BA-103, bomba de fondos GA-106 A/B, aerocondensador total EC-102, tanque de reflujo FA-106 y bomba de reflujo GA-105 A/B.

La nafta pesada se obtiene de los fondos de la torre, siendo bombeada por la bomba de fondos GA-106 A/B hacia un tren de enfriamiento conformado por, el lado coraza del cambiador EA-107 A/B, el aereoenfriador EC-103 y el enfriador con agua de enfriamiento EA-113.
La nafta ligera, por otro lado, se obtiene de los domos de la torre y es bombeada desde el tanque de reflujo FA-106 con ayuda de la bomba GA-109 A/B, en este caso también se enfría a través del paso por el enfriador con agua de enfriamiento EA-111.

Ambas corrientes se transportan por líneas separadas hacia sus respectivos límites de batería, en donde recibirán distintos tratamientos, sin embargo, una pequeña parte de ambas puede combinarse y regresar al inicio del proceso, aguas abajo del tanque de carga FA-101, por una línea de tubería especialmente dispuesta con el fin de recircular un flujo de nafta.

Capítulo 4. Caso de estudio y metodología.

4 Caso de estudio.

Se realizó un análisis HazOp como base para realizar el análisis SPR sobre las hojas de trabajo HazOp y de este modo encontrar los escenarios ciber-vulnerables enlistando las causas hackeables y las salvaguardas hackeables.

4.1 Nodos.

Los nodos son unidades de análisis que constan de conjuntos de equipos de la planta que comparten una intención de diseño, es decir los nodos se han propuesto bajo el criterio de funcionalidad, ejemplo: se integraron en un solo nodo los dos tanques separadores FA-102 y FA-103, porque ambos forman parte de un tren de separación

A continuación, se presenta una tabla donde se encuentran los nodos resultantes del ejercicio HazOp. En el Anexo C se muestra un extracto adoptado y adaptado de un proceso de Hidrodesulfuración de Naftas, en particular el Nodo 1, la intención es mostrar parte del estudio HazOp y su utilización para aplicar el método SPR y no es intención de esta tesis mostrar todo el estudio HazOp para evitar implicaciones de derechos de autor o de licenciamiento de la tecnología.

Tabla 3 Nodos resultantes del HazOp de la planta hidrodesulfuradora de Naftas.

Número de Nodo	Color	Intención de diseño	DTI's
1		El circuito de carga que comprende desde los límites de batería de nafta olefinica y parafínica a (6 kg/cm^2 y 38°C ambos) hasta el recipiente de separador trifásico FA-101 (2.5kg/cm^2 y 38°C) así como sus líneas asociadas.	1001 y 1002
2		La bomba del tanque de carga GA-101 (que aumenta la presión hasta 81.6 kg/cm^2) y líneas asociadas hasta las entradas al tren de calentamiento previo a la reacción.	1002 y 1003
3		El tren de calentamiento previo a la reacción que consta de los Cambiadores EA-101 (81.6 kg/cm^2 y 193°C) y EA-102 (81 kg/cm^2 216°C) ambos equipos procesan el fluido del lado tubos. Desde la entrada de EA-101 hasta la entrada del reactor DC-101	1003 y 1004
4		Reactor DC-101 de saturación de diolefinas y líneas asociadas que operan a 71kg/cm^2 y 216°C.	1004
5		Tren de calentamiento compuesto por EA-103 lado tubos (67.7 kg/cm^2, 267°C), EA-104 lado tubos (66.2 kg/cm^2, 331°C) y BA-101(61.1 kg/cm^2, 360°C), desde la salida del reactor de saturación de diolefinas DC-101 hasta la entrada del reactor de guarda de sílice DC-102.	1004, 1005, 1006 y 1007
6		Ambos reactores de guarda de sílice, DC-102A y DC-102B y líneas asociadas que operan a 63.4 kg/cm^2 y 364°C.	1007
7		Engloba al intercambiador EA-104 (58.5 kg/cm^2, 335°C) lado envolvente, al reactor de hidrotratamiento DC-103(58 kg/cm^2, 340°C) y sus líneas asociadas, desde la salida del DC-102B hasta la salida del DC-103.	1007 y 1008

Número de Nodo	Color	Intención de diseño	DTI's
8		Tren de enfriamiento del efluente que incluye EA-103 (55.5 kg/cm^2, 333°C) lado envolvente, EA-101 AB (54.8 kg/cm^2, 217°C) lado envolvente, EC-101(53.9 kg/cm^2, 125°C), EA-105 (53.4 kg/cm^2, 55°C) lado envolvente, que comprende desde la salida del reactor DC-103 hasta la entrada del tanque FA-102.	1003, 1005, 1008, 1009, 1010
9		Tren de separación conformado por los tanques FA-102 y FA-103 y líneas asociadas, que operan a 53 kg/cm^2 y 38°C. Este nodo se delimita desde la boquilla de entrada del tanque FA-102 hasta las salidas de líquido de los tanques y la entrada de la torre DA-101.	1010, 1011
10		Sección de absorción de aminas que incluye la torre DA-101(52 kg/cm^2, 43°C) y el tanque FA-104 (52 kg/cm^2, 43°C), delimitado desde la entrada de la torre absorbedora DA-101 hasta la entrada al compresor centrifugo GB-101X.	1011, 1013, 1014
11		Tanque de amina rica FA-109 que opera a 11.7 kg/cm^2 y 41°C y lineas asociadas, comprendido desde la salida inferior de la torre DA-101 hasta límite de batería de amina rica.	1011, 1013
12		Sistema de amina pobre que incluye EA-106 (2.8 kg/cm^2, 70°C) lado envolvente, FA-108 (1 kg/cm^2, 43°C) y GA-103A (56.5 kg/cm^2) que engloba desde el límite de batería de amina pobre hasta la entrada de la torre absorbedora DA-101.	1011, 1012
13		Compresor centrifugo GB-101X cuya presión de salida se requiere en 69.2 kg/cm^2 y una temperatura de descarga aproximada de 75°C y líneas asociadas	1014,1004, 1007, 1008, 1009
14		Compresor reciprocante del hidrógeno de reposición ambas etapas y ambos trenes BC-101AB (40 kg/cm^2, 109°C) enfriadores Inter etapa EA-114AB (sin datos) y líneas asociadas	1015, 1015A, 1003, 1005
15		Tanque esponja FA-110 que opera a 11.3 kg/cm^2 y 46°C y líneas asociadas.	1010, 1011, 1016, 1017
16		Incluye bomba GA-107 AB (17.5 kg/cm^2), cambiador de calor EA-107 AB (15.5 kg/cm^2, 98°C) lado tubos y EA-110AB (14.6 kg/cm^2 171°C) lado tubos, comprende desde la salida del tanque esponja FA-110 hasta la salida lado tubos del cambiador de calor EA-110AB.	1016, 1020
17		Sistema de estabilización que consta de la torre DS-101 (12.4kg/cm^2, 208°C), el aereoenfriador EC-104 (12.3 kg/cm^2, 71°C), EA-108AB (11.8 kg/cm^2, 55°C) lado envolvente, tanque de reflujo FA-105 (11.5 kg/cm^2, 36°C), bombas de reflujo GA-104AB (15.8 kg/cm^2), bombas de reboileo GA-108AB () y calentador BA-102(17.3 kg/cm^2).	1017, 1018, 1019
18		Bombas de LPG producto GA-110 AB que elevan la presión hasta 23.5 kg/cm^2, y líneas asociadas, desde la salida del tanque dé reflujo FA-105 hasta el límite de batería de LPG producto.	1017
19		Comprende al cambiador EA-110 AB (12.4 kg/cm^2, 208°C) lado envolvente y el reactor DC-104(11kg/cm^2, 135°C), va desde la entrada al cambiador EA-110 hasta la entrada de la torre fraccionadora DS-102.	1018, 1021

Número de Nodo	Color	Intención de diseño	DTI's
20		Comprende a la torre fraccionadora DS-102(1.8 kg/cm^2, 85°C), el aereoenfriador EC-102(1.6 kg/cm^2, 85°C), el tanque de reflujo FA-106(1.3 kg/cm^2, 60°C), la bomba de reflujo GA-105AB (5 kg/cm^2), bomba de reboileo GA-106AB (17.1 kg/cm^2) y el calentador BA-103(2.3 kg/cm^2, 168°C).	1020, 1021, 1022, 1023
21		Incluye la bomba GA-109 AB (25.6 kg/cm^2) y el cambiador EA-111(24.5 kg/cm^2, 60°C) lado envolvente, que se extiende desde la entrada a la bomba GA-109 AB hasta el límite de batería de nafta ligera.	1001, 1016,1020, 1023
22		Sistema de aguas amargas, conformado por el tanque separador FA-113(0.6 kg/cm^2, 35°C), y las bombas BD-103/R (5.72 kg/cm^2), BD-104/R (4.5 kg/cm^2). Engloba líneas de salida de gua provenientes de los tanques FA-102, FA-105 y FA-101 hasta el límite de batería de aguas amargas y slop.	1002, 1010, 1017, 1024
23		Carcasa y hogar del calentador a fuego directo BA-101 que opera quemando gas de refinería.	1006
24		Líneas de gas combustible y de gas natural asociadas al calentador BA-101 que operan a 3.5 kg/cm^2	1006
25		Sistema de agua de lavado, conformado por el tanque FA-107 (2.5 kg/cm^2, 40°C) y las bombas BD-102 AB (5.7 kg/cm^2) el nodo se extiende desde el límite de batería de agua de lavado hasta la inyección de agua a la entrada EC-104.	1009
26		Comprende únicamente a la bomba GA-102 AB que eleva la presión hasta 57 kg/cm^2 líneas asociadas que se extienden desde la salida de la pierna del tanque FA-102 hasta la entrada al tanque FA-107.	1003, 1009, 1010
27		Carcasa y hogar del calentador a fuego directo BA-102 que opera quemando gas de refinería.	1019
28		Líneas de gas combustible y de gas natural asociadas al calentador BA-102 que operan a 3.5 kg/cm^2.	1019
29		Comprende al cambiador EA-107 AB (16 kg/cm^2, 166 °C) lado envolvente, al aereoenfriador EC-103 (12 kg/cm^2, 71°C), y el cambiador EA-113 (14 kg/cm^2, 55°C) lado envolvente, se extiende desde la entrada del EA-107 AB hasta el límite de batería de nafta pesada.	1020
30		Carcasa y hogar del calentador a fuego directo BA-103 que opera quemando gas de refinería.	1022
31		Líneas de gas combustible y de gas natural asociadas al calentador BA-102 que operan a 3.5 kg/cm^2.	1022

Es preciso mencionar que algunos de los nodos se consideraron como equipos paquete cuyo diseño específico depende del fabricante, así como sus salvaguardas, por lo que se omitieron del análisis HazOp.

4.2 Hojas de trabajo HazOp.

Las hojas de trabajo HazOp son el producto del proceso de análisis realizado sobre cada Nodo, por lo tanto, se generó una hoja por cada nodo. Las hojas de trabajo se presentan en forma de tabla, Contienen un listado de todas las posibles desviaciones de la intención de diseño del nodo. Señalan también las consecuencias a las que puede orillar cada desviación y las salvaguardas presentes en el nodo que podrían actuar y evitar que la desviación generar un incidente o accidente. Finalmente se emitieron recomendaciones en los puntos donde se encontró que las salvaguardas no son las adecuadas o no son suficientes.

Las hojas de trabajo se generaron en el software OPEN PHA y se estructuraron en forma de tabla donde se contiene una columna para las desviaciones, otra para las consecuencias y una más para las salvaguardas.

Además de lo anterior, se agregó la opción de indicar si la causa y las salvaguardas son o no ciber-vulnerables. Esto como parte del análisis SPR que se llevó a cabo.

Ver anexo C

4.3 Recomendaciones.

Las recomendaciones que se obtuvieron como resultado el análisis SPR, fueron en su mayoría el verificar la presencia de salvaguardas intrínsecamente seguras a ciberataques, tales como PSV´s, alarmas, válvulas dobles check, equipos relevo, entre otras. Sin embargo, en los escenarios hackeables en donde no era posible anexar una de estas salvaguardas se debe evaluar cualitativamente los riesgos de acuerdo con los criterios de riego del operador de la instalación (en este caso los criterios de la tabla 3), para posteriormente implementar los requerimientos del SL obtenido, véase anexo D,

4.4 Metodología.

1.- **Estudio HazOp**.

Se inició realizando el estudio HazOp (ver Figura 2) para una planta HDN típica, lo cual se aprecia en las hojas de trabajo HazOp presentes Anexo A, a continuación, se muestra un ejemplo.

Nodo 4. Reactor de saturación de diolefinas y lineas asociadas.			Reactor DC-101 de saturación de diolefinas y lineas asociadas que operan a [redacted]kg/cm^2 y [redacted]°C				
Desviación	Causas						
	Causa	Causa Hackeable	Consecuencias				
			Consecuencia	Salvaguardas			PHA Recommendation
				Salvaguarda	Tipo salvaguarda	Salvaguarda Hackeable	
4.1 Mayor Presión	4.1.1 Fuego externo	No	4.1.1.1 Sobrepresionamiento del reactor DC-101	48 Válvula de seguridad PSV-61042 AB	Mecánica	No	
				49 indicador local de presión local PG-61113	Análoga local	No	
				63 Sitema de fuego y gas	SFG	No	
4.2 Menor Presión	4.2.1 Sin causas apartentes en el Nodo						

Figura 12 Ejemplo de hoja de trabajo HazOp. Obtenida de: Elaboración propia.

2.- **Causas y consecuencias hackeables.**

Después se analizó cada causa posible de una desviación y se hizo la pregunta ¿la causa es hackeable?, en caso de que la respuesta haya sido NO, se pasó a la siguiente causa, en caso de que la respuesta haya sido SI, se procedió a hacer la pregunta ¿todas las salvaguardas

que mitigan las consecuencias de este escenario son hackeables?, en caso de que la respuesta a ambas preguntas haya sido SI, se considera que el escenario es hackeable o ciber-vulnerable. Procedimiento que se describe gráficamente en la Figura 4, a continuación, se muestra un ejemplo de escenario hackeable.

Tabla 4 Ejemplo de escenario ciber-vulnerable

Evento iniciador	Localización	Hack?	Salvaguarda	Localización	Hack?	¿Todas las salvaguardas hackeables?	¿Escenario hackeable?
Falla de la válvula de quench FIC-202	DCS	Si	Intervención del operador basada en alarmas por alta temperatura TAH-204, TAH-205 y TAH-206	DCS	Si	Si	Si
			Intervención del operador basada en la alarma por bajo flujo de enfriamiento FAH-201	DCS	Si		
			Función instrumentada de seguridad UZC que detiene el flujo de entrada al detectar muy alta temperatura.	DCS	Si		

3.-**Asignación de SL.**

Una vez se obtuvo una lista de todos los escenarios ciber-vulnerables (Tabla 5), se procedió a asignar un SL cualitativo a cada uno de ellos con base a los criterios propuestos por (M. Marszal & McGlone, 2019) presentados en la Tabla 4.

4.- identificación de requerimientos en base a SL

Para finalizar, se indicó que requerimientos de ciber-seguridad se deben aplicar a cada escenario ciber-vulnerable de acuerdo con la ISA / IEC 62443 (Anexo D), para no sobredimensionar o generar sub-desempeño en los sistemas de ciberseguridad.

VII Resultados.

Se dividió la planta del caso de estudio (Planta hidrotratadora de Naftas típica) en un total en 31 nodos con base a su intención de diseño, en total al realizar el método HazOp para cada uno de los nodos se contabilizaron 146 escenarios, cada escenario desencadenado por una causa y protegido por una o más salvaguardas.

El uso del software gratuito Open PHA de Kenexis[4], fue de gran ayuda para gestionar los nodos, las salvaguardas y las desviaciones, al ser un software enfocado a los estudios HazOp y otros estudios de riesgo, fue muy útil para generar las hojas de trabajo HazOp y a

[4] Obtenido de forma gratuita desde el linkhttps://www.kenexis.com/software/openpha/# por recomendación del director de tesis.

su vez permitió indicar dentro del propio software si las salvaguardas presentes eran hackeables o no.

Como se ha mencionado con anterioridad a cerca del método SPR, para que un escenario se considere hackeable o ciber-vulnerable es necesario que la causa o las causas sea hackeables y todas las salvaguardas que podrían evitar que se desencadene el evento también, después de realizar este análisis para cada uno de los 146 escenarios resultó que 31 escenarios eran hackeables o ciber-vulnerables, es decir el 21.23%. Los escenarios hackeables obtenidos se presentan a continuación en la tabla 5.

Tabla 5 Escenarios hackeables o ciber-vulnerables.

Desviación	Causa	hackeable	Consecuencia	Salvaguarda	hackeable	Categoría	SL cualitativo
1.5 Mayor Nivel (Nafta)	1.5.1 Falla del lazo de control de nivel LIC-61100	Yes	1.5.1.1 Presionamiento del tanque de carga FA-101	21 Indicador controlador de presión PIC-61109 con alarma de alta presión, en el tanque FA-101	Yes	Muy baja	1
1.6 Mayor Nivel (agua amarga)	1.6.1 Falla de lazo de control de nivel-flujo LIC-61100 cerrando FV-61115	Yes	1.6.1.1 Arrastre de agua a sección de reacción con daño a catalizador	28 Indicador de nivel de interfase LIC-61101 con alarma por alto nivel.	Yes	Moderado	2
2.3 Mayor Flujo	2.3.1 Operación simultánea de las bombas de carga GA-101 A/B	Yes	2.3.1.1 Pérdida de nivel en el tanque de carga FA-101	40 Luces de estado EL-61001 AB de bombas GA-101 A/B	Yes	Muy baja	1
7.1 Mayor Presión	7.1.2 Falla de lazo de control FIC-61123	Yes	7.1.2.1 Menor temperatura en el reactor.	65 Indicadores de temperatura TI-61278 al TI-61283	Yes	Muy baja	1
7.6 Mayor temperatura	7.6.2 Falla en el lazo de control FIC-61123 cerrando la válvula FV-61123	Yes	7.6.2.1 Mayor temperatura con posible coquización en el reactor de hidrodesulfuración.	66 FIS por alta temperatura en el reactor DC-103 IS-6102	Yes	Baja	2
8.5 Mayor Temperatura	8.5.1 Falla de los motores del aereoenfriador EC-61001	Yes	8.5.1.1 Incremento de temperatura en el sistema aguas abajo del aereoenfriador.	70 Indicador de temperatura con alarma por alta temperatura TI-61159	Yes	muy baja	1
				71 Indicador de temperatura TI-61161	Yes		
10.8 Mayor nivel en el tanque FA-104	10.8.1 Falla de lazo de control LIC-61113 cerrando la válvula de control de nivel asociada.	Yes	10.8.1.1 Arrastre de líquido hacia la succión del compresor centrifugo GB-61001 lo que generaría daños en el mismo	104 FIS por alto alto nivel en el tanque FA-104 LSHH-61914 activa IS-6106A que manda el compresor a paro y aislamiento.	Yes	Alto	2
				105 Alarma por alto nivel en los indicadores LIC-61113 y LIC-61114	Yes		
				106 Indicador magnético local de nivel LG-61114	No		
11.1 Mayor Presión	11.1.1 Ver causas de menor nivel del nodo 10	Yes	11.1.1.1 Daños al tanque FA-109 y posible explosión	112 FIS por alta presión PSHH-61919 que activa IS-6105 voteo 1oo2 el cual cierra la EBV-61917 y la XV-61916	Yes	Muy alto	3
12.2 Menor Presión	12.2.1 Falla en el lazo de control de presión PIC-61138 Abriendo la	Yes	12.2.1.1 Posible cavitación de la bomba GA-103 AB	123 Lazo de control de recirculación FIC-61141 y FIC-61142	Yes	Muy baja	1

Desviación	Causa	hackeable	Consecuencia	Salvaguarda	hackeable	Categoría	SL cualitativo
	válvula PV-61138B y cerrando la válvula PV-6118A			124 Indicadores locales de presión PG-61139 AB	No		
				125 Alarma por alta vibración en las bombas GA-103 AB en el indicador VIT-61003	Yes		
				126 FIS por alta alta vibración VSHH-661XX que manda a paro de las bobas GA-103 AB	Yes		
12.7 Menor Nivel	12.7.1 Falla en el lazo de control de nivel LIC-61112 cerrando la válvula LV-61112	Yes	12.7.1.1 Posible cavitación de la bomba GA-103 AB	123 Lazo de control de recirculación FIC-61141 y FIC-61142	Yes	Muy baja	1
				124 Indicadores locales de presión PG-61139 AB	No		
				125 Alarma por alta vibración en las bombas GA-103 AB en el indicador VIT-61003	Yes		
				126 FIS por alta alta vibración VSHH-661XX que manda a paro de las bobas GA-103 AB	Yes		
12.8 Mayor Temperatura	12.8.1 Falla de agua de enfriamiento	Yes	12.8.1.1 Posible cavitación de la bomba GA-103 AB	123 Lazo de control de recirculación FIC-61141 y FIC-61142	Yes	Muy baja	1
				124 Indicadores locales de presión PG-61139 AB	No		
				125 Alarma por alta vibración en las bombas GA-103 AB en el indicador VIT-61003	Yes		
				126 FIS por alta vibración VSHH-661XX que manda a paro de las bombas GA-103 AB	Yes		
15.6 Menor Nivel	15.6.1 Falla en el lazo de control de nivel-flujo LIC-61119, abriendo la válvula FV-61146	Yes	15.6.1.1 Posible cavitación y daños al equipo de bombeo GA-107AB	146 FIS por muy bajo nivel IS-6113 que manda a paro de la bomba GA-107 AB y cierra la EBV-61911.	Yes	Muy baja	1
17.3 Mayor Flujo	17.3.1 Operación de ambas bombas GA-104A y GA-104B	Yes	17.3.1.1 Incremento del reflujo y disminución de nivel del tanque FA-105	161 Indicadores luminosos EL-61005 AB	Yes	Muy baja	1
				162 Lazo de control de flujo FIC-61161	Yes		
18.2 Menor presión	18.2.1 Fallo de la bomba GA-1010A	Yes	18.2.1.1 Interrupción del envio de LPG a límite de batería	167 Bomba de relevo GA-110 B	Yes	Muy baja	1
18.3 Mayor Flujo	18.3.1 Operación simultánea de la bomba GA-110A y la GA-110B.	Yes	18.3.1.1 Aumento del flujo que se envía a LB	168 Indicadores luminosos EL-61010 AB	Yes	Muy baja	1
20.3 Mayor Flujo	20.3.1 Operación de ambas bombas GA-105A y GA-105B	Yes	20.3.1.1 Incremento del reflujo y disminución de nivel del tanque FA-106	161 Indicadores luminosos EL-61005 AB	Yes	Muy baja	1
				162 Lazo de control de flujo FIC-61161	Yes		
22.5 Mayor Nivel de hidrocarburo	22.5.1 Falla de la bomba BD-104	Yes	22.5.1.1 Mezcla de hidrocarburo con agua amarga.	183 Bomba de relevo BD-104 R	Yes	Muy baja	1

Desviación	Causa	hackeable	Consecuencia	Salvaguarda	hackeable	Categoría	SL cualitativo
22.7 Mayor Nivel de agua amarga	22.7.1 Falla de la bomba BD-103	Yes	22.7.1.1 Mezcla de agua amarga con hidrocarburo	185 Bomba de relevo BD-103 R	Yes	Muy baja	1
22.8 Menor Nivel de aguas amarga	22.8.1 Falla de lazo de control de nivel LIC-61126	Yes	22.8.1.1 Cavitación de la bomba BD-103	186 FIS por muy bajo nivel en el tanque FA-113 que activa la IS-6119 y esta para la bomba BD-103	Yes	Muy baja	1
23.1 Mayor presión	23.1.1 Incremento del combustible alimentado al calentador BA-101.	Yes	23.1.1.1 Posible daño y explosión en el calentador BA-101	187 FIS por muy alta presión PSHH-61921 que activa la IS-6102 la cual para el calentador	Yes	Muy alto	3
				188 Indicador local de presión PI-61117	Yes		
23.3 Mayor Temperatura	23.3.1 Incremento del combustible alimentado al calentador BA-101.	Yes	23.3.1.1 posible daño a los tubos del equipo del calentador BA-101	189 Indicadores de temperatura TI-61131	Yes	Baja	2
25.3 Mayor Flujo	25.3.1 operación simultánea de ambas bombas BD-102 A y BD-102 B	Yes	25.3.1.1 Disminución del nivel en el tanque FA-107	192 Indicadores luminosos EL-61011A y EL-61011B de las bombas BD-102AB	Yes	Muy baja	1
25.6 Menor Nivel	25.6.1 Falla en el lazo de control de flujo FIC-61125 o FIC-61124 cerrando la válvula asociada	Yes	25.6.1.1 Cavitación de la bomba BD-102A	194 FIS por muy bajo nivel LSLL-61902 que activa la IS-6108 la cual para la bomba BD-102AB	Yes	Muy baja	1
27.1 Mayor presión	27.1.1 Incremento del combustible alimentado al calentador BA-102.	Yes	27.1.1.1 Posible daño y explosión en el calentador BA-102	196 FIS por muy alta presión PSHH-61907 que activa la IS-6115 la cual para el calentador	Yes	Muy alto	3
				197 Indicadores de presión PI-61236, PI-61166, PI-61907	Yes		
27.3 Mayor Temperatura	27.3.1 Incremento del combustible alimentado al calentador BA-102.	Yes	27.3.1.1 posible daño a los tubos del equipo del calentador BA-102	198 Indicadores de temperatura TI-61193, TI-61194, TI-61195, TI-61227	Yes	Baja	2
29.5 Mayor temperatura	29.5.1 Falla en el lazo de control TIC-61201 abriendo totalmente la válvula TV-61201.	Yes	29.5.1.1 Se entrega la nafta en LB a una temperatura mayor.	202 Indicador de temperatura TI-61229 en LB	Yes	Muy baja	1
				205 Indicador local de temperatura TG-61150	No		
	29.5.2 Falla de motores del aereoenfriadores EC-61003.	Yes	29.5.2.1 Se entrega la nafta en LB a una temperatura mayor.	203 Indicador de temperatura TI-61202	Yes	Muy baja	1
				206 Indicador local de temperatura TG-61103 AB	No		
	29.5.3 Falla en el agua de enfriamiento	No	29.5.3.1 Se entrega la nafta en LB y en la recirculación larga a una temperatura mayor.	207 Indicador de temperatura TI-61204	Yes	Muy baja	1
				208 Indicador local de temperatura TG-61153	No		
30.1 Mayor presión	30.1.1 Incremento del combustible alimentado al BA-103	Yes	30.1.1.1 Posible daño y explosión en el calentador BA-103	199 FIS por muy alta presión PSHH-61910 que activa la IS-6118 la cual para el calentador	Yes	Muy alto	3
				200 Indicadores de presión PI-61181, PI-61217, PI-61910	Yes		

Desviación	Causa	hackeable	Consecuencia	Salvaguarda	hackeable	Categoría	SL cualitativo
30.3 Mayor Temperatura	30.3.1 Incremento del combustible alimentado al BA-103	Yes	30.3.1.1 Posible daño a los tubos del equipo del calentador BA-103	201 Indicadores de temperatura TI-61237, TI-61217, TI-61218, TI-61219	Yes	Baja	2

VIII Discusión.

Se analizaron los peligros de un proceso de HDN con el método PHA y se aplicó la metodología SPR y gracias a ellos se detectaron los escenarios propensos a sufrir un ciberataque, también llamados "hackeables" o "ciber-vulnerables". Dando como resultado un total de 30 escenarios hackeables para la planta hidrodesulfuradora de naftas teórica. Al realizar la separación de la planta en Nodos se facilitó su análisis, estos nodos se plasmaron en diagramas DFP y DTI. Los cuales se incluyen en los anexos A y B de este trabajo. Es preciso mencionar en este punto que los DFP´s se recrearon y modificaron para no revelar información sensible propiedad del Instituto Mexicano del Petroleo.

Figura 13 Distribución de escenarios totales.

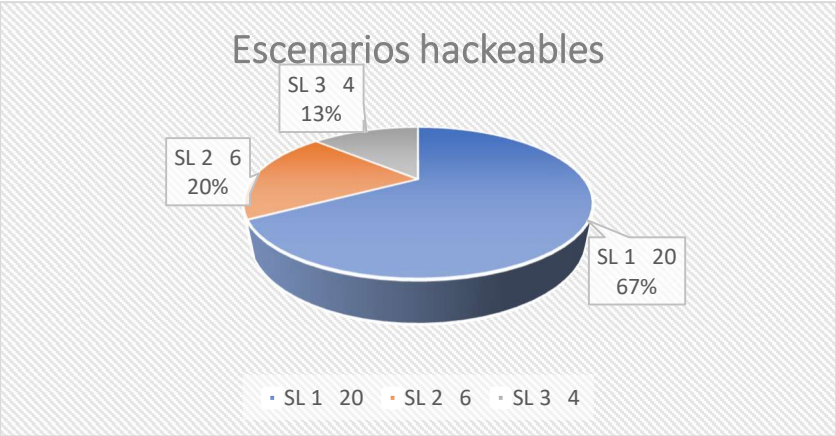


Figura 14 Distribución de SL en escenarios hackeables.

De los 30 escenarios hackeables de 4 de ellos requieren un SL 3 de, uno de estos, la desviación 11.1 se da por un bajo nivel en un tanque de alta presión que conecta este sistema a uno de baja presión, el llamado "Gas Blow-by", lo que genera daño y una explosión en el sistema de baja presión, los otros tres se dan por un descontrol en el sistema inyección de gas combustible a los calentadores a fuego directo BA-101, BA-102, BA-103. Del resto de los escenarios se obtuvieron seis escenarios con un SL 2 los cuales pueden generar consecuencias moderadas tales como cambios en la calidad del producto final, descontrol de temperatura en las reacciones químicas y posible desfogue., los otros 20 escenarios se encasillaron dentro del SL 1 ya que presentaban consecuencias tales como fugas pequeñas o incremento en algunos flujos del proceso. Mientras mayor sea el SL mayores serán los requisitos que deben cubrirse para asegurar que el proceso logre un nivel de seguridad aceptable a pesar de su ciber-vulnerabilidad.

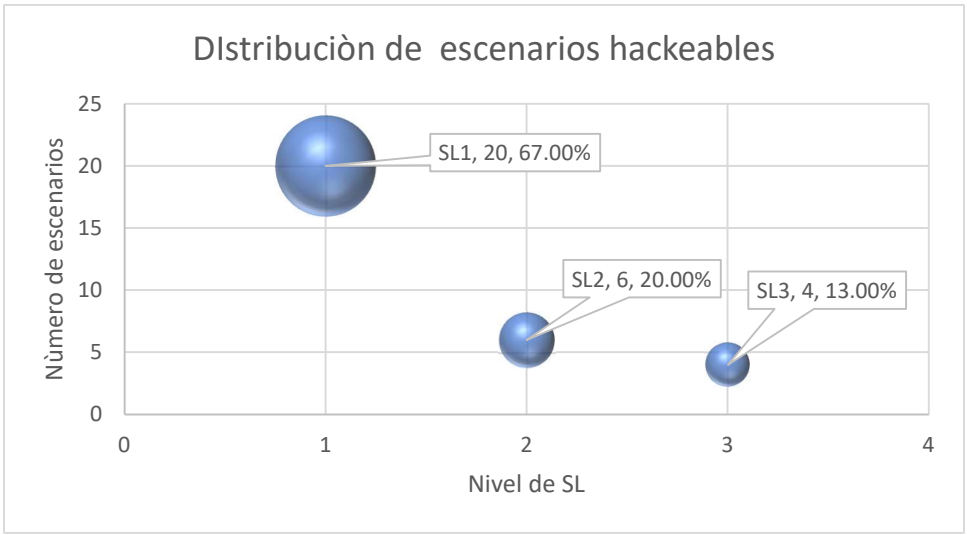


Figura 15 distribución de escenarios hackeables (gráfico burbuja)

Tabla 6 Comparación de requerimientos funcionales ANSI/ ISA-62443-3-3 según su SL

Requerimientos funcionales	SL1	SL2	SL3	SL4
FR 1 Autentificación e identificación de control.	10	15	22	24
FR 2 Control de uso (UC)	8	12	21	24
FR 3 Integridad del sistema (SI)	5	10	16	19
FR 4 Confidencialidad de datos (DC)	2	4	5	6
FR 5 Flujo de datos restringido (RDF)	4	6	10	11
FR 6 Respuesta oportuna a eventos (TRE)	1	2	3	3
FR 7 Disponibilidad de recursos (RA)	7	10	13	13
TOTALES	37	59	90	100

Como se observa en la tabla 6 los requerimientos funcionales para un escenario ciber-vulnerable son proporcionales a su nivel de SL asignado. En resumen, ascienden a un total de 37 requerimientos para SL1, 59 para SL2, 90 para SL3 y 100 para SL4. Variado también la cantidad de requerimientos de cada tipo. Para más detalles al respecto se recomienda analizar el anexo D del presente trabajo, donde se desglosa la tabla obtenida de (M. Marszal & McGlone, 2019) la cual a su vez es un extracto del estándar ISA-IEC-62443 (ISA/IEC)

VIII.I Ejemplo del caso de estudio.

Para ejemplificar el trabajo realizado sobre las hojas de trabajo HazOp generadas, se ejemplifica el desarrollo de la metodología SPR aplicada sobre la desviación 1.5 *"Mayor nivel de nafta en el tanque FA-101"*, causa 1.5.1 *"Falla del lazo de control de nivel LIC-61100"* Dicho escenario es primero de todo el análisis en ser detectado como ciber-vulnerable o hackeable.

Como podemos observar en la tabla 7, extraída del anexo C, página C2 del presente trabajo. La causa que genera la desviación de mayor nivel es la falla de un elemento del SCD (sistema de control distribuido), más específicamente la falla o manipulación de un instrumento perteneciente al lazo de control que incluye al controlador indicador de nivel LIC-61100. Este instrumento puede ser un indicador, un transmisor o el propio controlador. Una falla del SCD se puede generar por la intrusión de un atacante que se apodere del ICS. Para mayor comprensión ver anexo B. y figura 16 y 17.

La salvaguarda con la que cuenta el sistema para abatir las consecuencias de un evento generado por un ataque es un lazo de control de Presión, (lazo de control del PIC-61109) y alarmas por alta presión en el tanque FA-101. Que también pertenecen al SCD y son ciber-vulnerables.

Tabla 7 Desviación 1.5 "Mayor nivel de nafta", Causa 1.5.1. del nodo 1. Extracto del anexo C

Nodo1. Sección de Alimentación de Carga			**El circuito de carga que comprende desde los límites de batería de nafta olefinica y parafínica a (6 kg/cm2 y 38°C ambos) hasta el recipiente de separador trifásico FA-101 (2.5kg/cm2 y 38°C) así como sus lineas asociadas.**				
Desviación	**Causas**						
	Causa	**Causa Hackeable**	**Consecuencias**				
			Consecuencia	**Salvaguardas**			**PHA Recomendación**
				Salvaguarda	**Tipo salvaguarda**	**Salvaguarda Hackeable**	
1.5 Mayor Nivel (Nafta)	1.5.1 Falla del lazo de control de nivel LIC-61100	Yes	1.5.1.1 Presionamiento del tanque de carga FA-101	21 Indicador controlador de presión PIC-61109 con alarma de alta presión, en el tanque FA-101	SCD	Yes	1 Verificar que los sistemas de control distribuido, sistema instrumentado de seguridad y sistema de gas y fuego sean seleccionados con las medidas adecuadas de ciberseguridad, con la finalidad de proteger la integridad cibernética de estos sistemas contra posibles ciberataques. La selección debe basarse en un estudio de selección de "Security Level" (SL) de acuerdo con el IEC-62443.

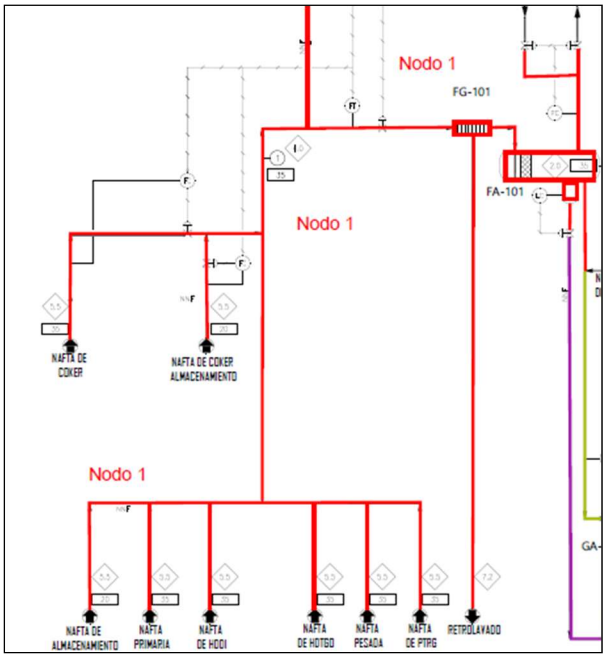


Figura 16 Representación del nodo 1 en DFP. Extracto del anexo A, pág. A2

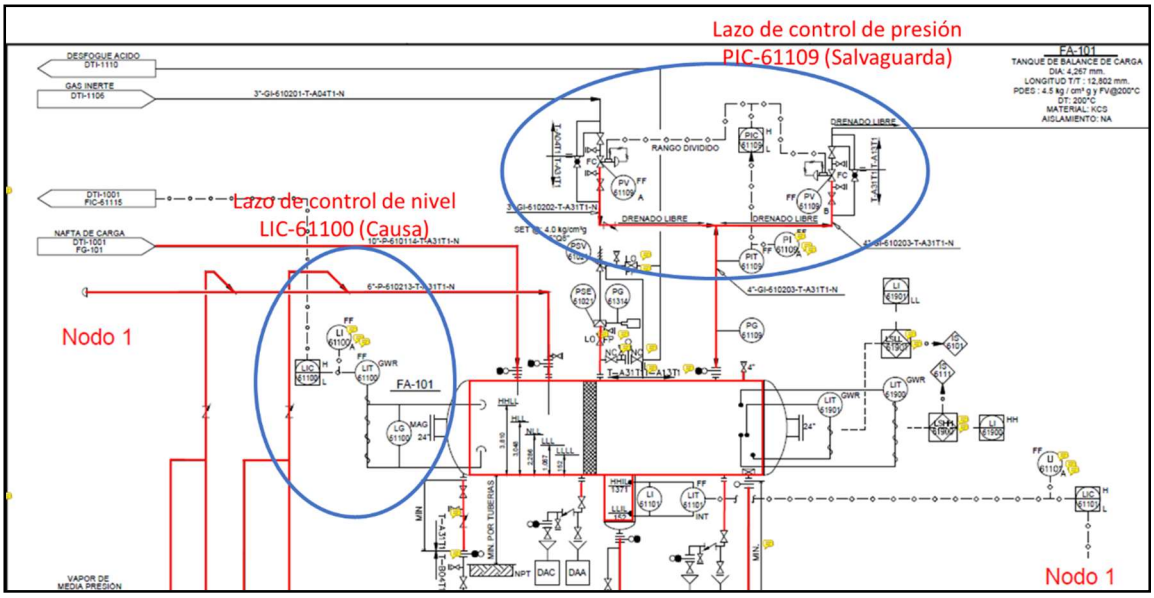


Figura 17 Elementos de control de la desviación 1.5 en DTI, Extracto del anexo B.

Una vez identificado que el escenario ciber-vulnerable se procede a asignar un SL. Comparando el escenario y sus posibles consecuencias con los criterios de la tabla 2.1, El análisis se efectúa bajo la siguiente lógica: Si el lazo de control de nivel es manipulado por un atacante que haya tomado control del SCD y que también inhabilita la salvaguarda (ver figura 17), lo que ocurriría sería que el nivel de nafta subiría hasta ocupar la totalidad del tanque FA-101, lo que ocasionaría una condición de sobrepresión en el equipo, y esto, a su vez provocaría una posible ruptura del equipo y fuga ya que la presión máxima alcanzable sería la presión en de llegada al límite de batería de nafta. Es decir 5 kg/cm^2 que es superior a la presión de diseño del tanque FA-101, es decir 4.5 kg/cm^2.

Cabe la posibilidad de que, gracias a los instrumentos locales, manómetros e indicadores de nivel, el personal operativo pueda darse cuenta de la desviación en el proceso y hacer algo al respecto cortando el flujo de alimentación por medio de válvulas manuales, pero sería cuanto menos irresponsable darle crédito a estos indicadores y válvulas como salvaguardas, ya que su posible resguardo del sistema depende de si son o no monitoreados mientras se lleva a cabo el ataque.

La sobrepresión podría dar origen a una fuga, pero difícilmente sería causante de lesiones en el personal. Al no tener un método eficiente para estimar el costo económico de las consecuencias este factor no es tomado en cuenta para este caso de estudio.

Por lo anterior se cataloga el escenario como de categoría *"Muy Baja"*, y se llega a la conclusión de que al escenario se le debe asignar un SL de l, con base en la tabla 5.1.

Tabla 2.1 Características del SL1 extracto de tabla 2.

Categoría	Daños			TMEL	SL
	Seguridad	*Ambiental*	*Comercial*		
Nula	Sin daños significantes para la seguridad.	Ninguno	Ninguno	N/A	1
Muy baja	Heridas menores que requieren atención de primeros auxilios.	Pequeñas fugas con mínimos requerimientos de limpieza.	$50,000 USD $1,000,000 MNX	1.00E-02	1

Tabla 5.1 Desviación 1.5 "Mayor nivel de nafta", Causa 1.5.1. del nodo 1. Extracto de Tabla 5

Desviación	Causa	hackeable	Consecuencia	Salvaguarda	hackeable	Categoría	SL cualitativo
1.5 Mayor Nivel (Nafta)	1.5.1 Falla del lazo de control de nivel LIC-61100	Yes	1.5.1.1 Presionamiento del tanque de carga FA-101	21 Indicador controlador de presión PIC-61109 con alarma de alta presión, en el tanque FA-101	Yes	Muy baja	1

Una vez identificado el nivel de seguridad como SL1 se procede a enlistar los 37 requerimientos de ciberseguridad necesarios para ese nivel de seguridad. Los cuales se desglosan en el anexo D. pero aquí se enlistan en forma de la tabla 8.

Tabla 8 Requerimientos fundamentales de ciberseguridad para un SL1 Adaptado del anexo D.

Descripción	***Nivel de seguridad***
FR 1. Autentificación e identificación de control.	***SL 1***
Identificar y autenticar a todos los usuarios humanos.	X
Administrar todas las cuentas de acuerdo con los usuarios autorizados, lo que incluye añadir, activar, modificar, deshabilitar y eliminar cuentas.	X
Administrar identificadores por usuario, grupo, rol o interfaz del sistema de control.	X
Inicializar el contenido autenticador, cambiar todos los autenticadores predeterminados en la instalación del sistema de control, cambiar/actualizar todos los autenticadores, y proteger los autenticadores de la divulgación o modificación no autorizada.	X
Identificar y autenticar de forma única a todos los usuarios involucrados en la comunicación inalámbrica.	X
Hacer cumplir la seguridad de la contraseña configurable, según la longitud mínima y la variedad de tipo de caracteres.	X
Retroalimentación oculta de la información de autenticación durante el proceso de autenticación.	X
Aplicar un límite configurable de número de intentos de acceso no validos consecutivos por parte de cualquier usuario (humano, proceso de software o dispositivo).	X
Mostrar un mensaje de notificación de uso del sistema antes del proceso de autentificación.	X
Supervisar y controlar todos los métodos de acceso al sistema de control a través de redes no confiables.	X
FR 2. Control de uso (UC)	***SL 1***
Hacer cumplir las autorizaciones asignadas a todos los usuarios humanos para controlar el uso del sistema de control para respaldar la segregación de funciones y el privilegio mínimo.	X

Descripción	*Nivel de seguridad*
Autorizar, monitorear y hacer cumplir las restricciones de uso para la conectividad inalámbrica al sistema de control.	X
Aplicar automáticamente restricciones de uso configurables.	X
Hacer cumplir las restricciones de uso para las tecnologías de códigos móviles según la posibilidad de causar daños al sistema de control.	X
Evitar más accesos iniciando un bloqueo de sesión después de un tiempo configurable de inactividad o por inicio manual.	X
Generar requisitos de auditoría relevantes para la seguridad para las siguientes categorías: control de acceso, errores de solicitud, eventos del sistema operativo, eventos del sistema de control, eventos de respaldo y restauración, cambios de configuración, actividad de reconocimiento potencial y eventos de registro de auditoría. Los registros individuales de la auditoría deben incluir el sello de tiempo, la fuente (dispositivo de origen, proceso de software o cuenta de usuario humano), categoría, tipo, ID de evento y resultado del evento.	X
Asignar suficiente capacidad de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la administración de registros y la configuración de registros y la configuración del sistema	X
Alertar al personal y prevenir la pérdida de servicios y funciones esenciales en caso de una falla en el procesamiento de auditoría	X
FR 3. Integridad del sistema (SI)	***SL 1***
Proteger la integridad de la información transmitida.	X
Emplear mecanismos de protección para prevenir, detectar, informar y mitigar los efectos de códigos maliciosos o software no autorizado.	X
Verificar el funcionamiento previsto de las funciones de seguridad e informar cuando se descubran anomalías durante, las pruebas de aceptación de fábrica (FAT), las pruebas de aceptación del sitio (SAT) y el mantenimiento programado.	X
Validar la sintaxis y el contenido de cualquier entrada que se utilice como entrada de control de procesos industriales o entrada que impacte directamente la acción del sistema de control.	X
Establecer las salidas en un estado predeterminado si el funcionamiento normal no se puede mantener debido a un ataque	X
FR 4. Confidencialidad de datos (DC)	***SL 1***
Proteger la confidencialidad de la información para la que se admite una autorización de lectura explícita, ya sea en reposo o en tránsito	X
Utilizar algoritmos criptográficos, tamaños adecuados de clave y mecanismos para el establecimiento y la administración de claves.	X
FR 5. Flujo de datos restringido (RDF)	***SL 1***
Segmentar lógicamente las redes de sistemas de control de redes de sistemas sin control y segmentar lógicamente las redes de sistemas de control críticos de otras redes de sistemas de control.	X
Monitorear y controlar las comunicaciones en los límites de las zonas para hacer cumplir la compartimentación definida en el modelo de conduits y zonas basado en riesgos.	X
Evitar que se reciban mensajes de persona a persona de propósito general de usuarios o sistemas externos al sistema de control.	X
Admitir la partición de datos, aplicaciones y servicios según la criticidad para facilitar la implementación de un modelo de zonificación.	X
FR 6. Respuesta oportuna a eventos (TRE)	***SL 1***
Permitir que los humanos autorizados y/o las herramientas accedan a los registros de auditoría en una base de solo lectura.	X
FR 7. Disponibilidad de recursos (RA)	***SL 1***

Descripción	*Nivel de seguridad*
Operar en un modo graduado durante un evento de denegación de servicio (DoS)	X
Limitar el uso de recursos por las funciones de seguridad para evitar el agotamiento de los recursos.	X
Admitir la identificación y localización de archivos críticos y tener la capacidad de realizar copias de seguridad de la información a nivel de usuario y de sistema (incluida la información de estado del sistema) sin afectar las operaciones normales de la planta	X
Recuperar y reconstruir a un estado seguro conocido después de una interrupción o falla.	X
Cambiar hacia y desde una fuente de alimentación de emergencia sin afectar el estado de seguridad existente.	X
Configurar de acuerdo con las configuraciones de red y seguridad recomendadas como se describe en las pautas proporcionadas por el proveedor. El sistema de control debe proporcionar una interfaz para la red actualmente implementada y los ajustes de configuración de seguridad.	X
Prohibir específicamente y/o restringir el uso de funciones, puertos, protocolos y/o servicios innecesarios.	X

Aunque puedan parecer bastantes requerimientos de ciberseguridad, es importante recordar que un escenario SL1 es el que posee el menor número de requerimientos fundamentales de ciberseguridad, solo 37. Eso quiere decir poco más de la mitad de un SL2 y aproximadamente una tercera parte de un SL3. También es oportuno hacer mención que no es el objetivo de este trabajo el analizar cada uno de los requerimientos fundamentales, así como su aplicación sobre la infraestructura de la planta HDN típica.

El expertis acumulado en el estándar ISA-IEC-62443 sirve como aval de que los requerimientos en ella enlistados para cada SL garantizan que no habrá sub-desempeño del sistema de protección, es decir que no serán menos que los necesarios, y su desempeño será suficiente para proteger al sistema frente a las amenazas que representa un SL1. En contraparte, la correcta aplicación del método SPR y asignación de SL, evitan el sobre-diseño de un sistema, es decir la imposición de requerimientos “sobrados” que no serán aprovechados y solo generarán mayores gastos operativos y de instalación.

IX Conclusiones.

En esta tesis se realizó un análisis PHA HazOp y con base en sus hojas de trabajo resultantes se generó un estudio SPR, que incluyó entre otras actividades la identificación de los escenarios hackeables. Se hizo posible llevar el análisis a una situación diferenciada y con ventajas respecto a una en la cual sin ninguna base de identificación de ciber-vulnerabilidades se impongan medidas mitigantes o preventivas de ciberataques.

Otro punto que resaltar es la importancia de la diferencia entre los términos *Safety* y *Security* Si bien en español ambos son englobados en la palabra Seguridad, tienen connotaciones distintas siendo el enfoque de *Safety* el enfoque bajo el cual se pensó esta tesis. (Ver marco teórico)

Por otra parte, se concluye también que el uso de software libre y especializado en el análisis de riesgo, como Kenexis Open PHA funciona bien para la aplicación de este método, ya que dentro de su propia interfaz permite llevar a cabo la identificación de salvaguardas y causas hackeables. Incluso puede generar las hojas de datos HazOp, aunque se exportaron a Excel para su mejor manejo y presentación, el tratar las hojas HazOp dentro del software también es una opción viable.

Los ciberataques son acciones deliberadas. Las leyes de la probabilidad no se aplican a acciones deliberadas. Una forma de solventar esta cuestión que tiene el análisis SPR es asumiendo un nivel de integridad, SL predeterminado, dependiendo de las intenciones y magnitud de un ciberataque y con base en este realizar las recomendaciones de software, hardware y protocolos necesarias. Si bien se mantiene la visión de una identificación de peligros físicos y de proceso, una vez que el método se adentra en terrenos de la ciberseguridad se comienzan a aplicar las reglas del SPR.

Si bien el método SPR, puede parecer sencillo (ver figura 4), Depende mucho de la calidad del estudio HazOp del que se parta para elaborarlo. Ya que si no se es claro al identificar correctamente causas y todos los conjuntos de salvaguardas, los resultados del SPR no serán fiables y por lo tanto de poca utilidad. El caso ideal es que el especialista que trabaja el método SPR, sepa identificar los estudios HazOp que están hechos de forma correcta, y mejor aún que sepa elaborar estudios HazOp con calidad.

El uso del nivel se seguridad o SL *(Security level)* en este trabajo se abordó evaluando consecuencias, es decir, los daños que podría causar un evento, siendo esta la forma en la que cualitativamente se asignó un valor del uno al tres para cada escenario ciber-vulnerable, posteriormente este valor sirvió para cuantificar la magnitud de medidas de software y hardware que se deben desplegar, se despliegan 37 medidas para un SL1 mientras que para un SL3 las medidas desplegadas ascienden a 100. De estos datos se puede concluir que la correcta asignación del valor SL es de importancia capital para evitar el sobre-diseño de escenarios que no son tan críticos, en los cuales implementar medidas en exceso solo haría que se desaprovecharan recursos económicos y operativos. Es decir, incremento de costos de operación y mantenimiento. también se busca evitar el sub-desempeño apoyándose del

expertis contenido en el estándar ISA/IEC-62443, expresado en su listado de requerimientos para cada nivel de seguridad SL.

Se concluye finalmente que el método SPR aplicado sobre un análisis HazOp, para una planta industrial es útil y factible solo si y solo sí; Las entradas de información son confiables y de calidad.

Esta utilidad se ve reflejada en evitar sobre-diseño y con ellos costos innecesarios generados por la compra hardware y software desaprovechado. Asi como también evitar incurrir en sub-desempeño, que a su vez dan pauta a que el sistema no sea capaz de proteger las vidas humanas, el medio ambiente, y los equipos e infraestructura de un ciberataque.

X Referencias.

A. Crowl, D., & F. Louvar, J. (2002). *Chemical Process Safety, Fundamentals with Applications.* United States of America: Prentice Hall PTR.

AVAST. (2021). Guía esencial sobre el ransomware. Obtenido de https://www.avast.com/es-es/c-what-is-ransomware

Badillo, D. (16 de Febrero de 2020). *"Flotan"en internet 180,000 archivos de Pemex sustraidos por hackers*. Obtenido de EL Economista: https://www.eleconomista.com.mx/empresas/Flota-en-internet-informacion-sensible-de-Pemex-sustraida-por-hackers-20210216.html

Cambridge Dictionary. (6 de 03 de 2021). *Safety Definition.* Obtenido de https://dictionary.cambridge.org/es-LA/dictionary/english/safety

Cambridge Dictionary. (06 de 03 de 2021). *Security Definition.* Obtenido de https://dictionary.cambridge.org/es-LA/dictionary/english/security

Craigen, D., Diakun-Thibault, N., & Purse, R. (Octubre de 2014). Defining Cybersecurity. *Technology Innovation Management Review*. Obtenido de https://www.timreview.ca/article/835

Crawley, F., & Tyler, B. (2015). *HAZOP: Guide to Best Practice Guidelines to Best Practice for the Process and Chemical Industries. Third Edition.* Amsterdam, UK: Elsevier.

Gómez Llinás, D. A. (2017). STUXNET EL VIRUS INFORMÁTICO: Análisis del ciberataque para la seguridad de los estados y su incidencia en la transformación del status quo. Bogotá: Universidad Colegio Mayor de Nuestra Señora del Rosaio.

Hughes, T. A. (2002). *Measurement and control basics.* USA.: ISA The Instrumentation Systems and Automation Society.

IEC 61511. (2016). Functional Safety – Safety instrumented systems for the process industry sector.

Instituto Nacional de ciberseguridad (INCIBE). (2018). Las claves de los útimos ataques en sistemas de control industrial. Obtenido de https://www.incibe-cert.es/blog/las-claves-los-ultimos-ataques-sistemas-control-industrial

ISA/IEC. (s.f.). ISA/IEC 62443 Series. *Security for Industrial Atomation and Control Systems*.

Lee, R. M. (15 de 06 de 2015). Closing the Case on the Reported 2008 Russian Cyber Attack on the BTC Pipeline. *SANS*. USA. Obtenido de

https://www.sans.org/blog/closing-the-case-on-the-reported-2008-russian-cyber-attack-on-the-btc-pipeline/

M. Marszal, E., & McGlone, J. (2019). *Security PHA Review for Consequence-Based Cybersecurity.* United States of America: International Society of Automation (ISA).

Meyers, R. (2004). *Handbook of petroleum refining processes.* Nueva York: Mc Graww-Hill Handbooks.

Oiltanking GmbH. (Diciembre de 2016). *Oiltanking*. Obtenido de https://www.oiltanking.com/es/publicaciones/glosario/detalles/term/el-proceso-de-refinacion-de-petroleo.html#:~:text=El%20Proceso%20de%20Refinación%20de%20Petróleo&text=Los%20cinco%20procesos%20básicos%20de,redisposición%20de%20la%20estructura%20molecular

PEMEX. (Marzo de 2011). DG-SASIPA-SI-02741. *Guía para realizar análisis de riesgos*. Subdirección de auditoría en seguridad industrial y protección ambiental.

PEMEX. (26 de 11 de 2020). *Nafta (Ligera y Pesada)*. Obtenido de https://www.pemex.com/comercializacion/productos/Paginas/gas/nafta.aspx

RAE Real Academia Española. (06 de 03 de 2021). *Definición de seguridad.* Obtenido de https://dle.rae.es/seguridad

REPSOL YPF. (24 de Septiembre de 2007). GUÍA PARA LA REALIZACIÓN DE ESTUDIOS PHA (Process Hazard Analysis). Obtenido de https://docplayer.es/20356386-Guia-para-la-realizacion-de-estudios-pha-process-hazard-analysis.html

Romero Faz, D. (Noviembre de 2017). Tesis Doctoral; Metodología para la evaluación del riesgo en instalaciones portuarias. Madrid, España.: Universidad Politécnica de Madrid, Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos.

Secretaría de medio ambiente y recursos naturales. (Julio de 2020). Guía para la elaboración del análisis de riesgo para el sector hidrocarburos. México: Gobierno de México.

Anexo A
Diagramas de d r Nodeados

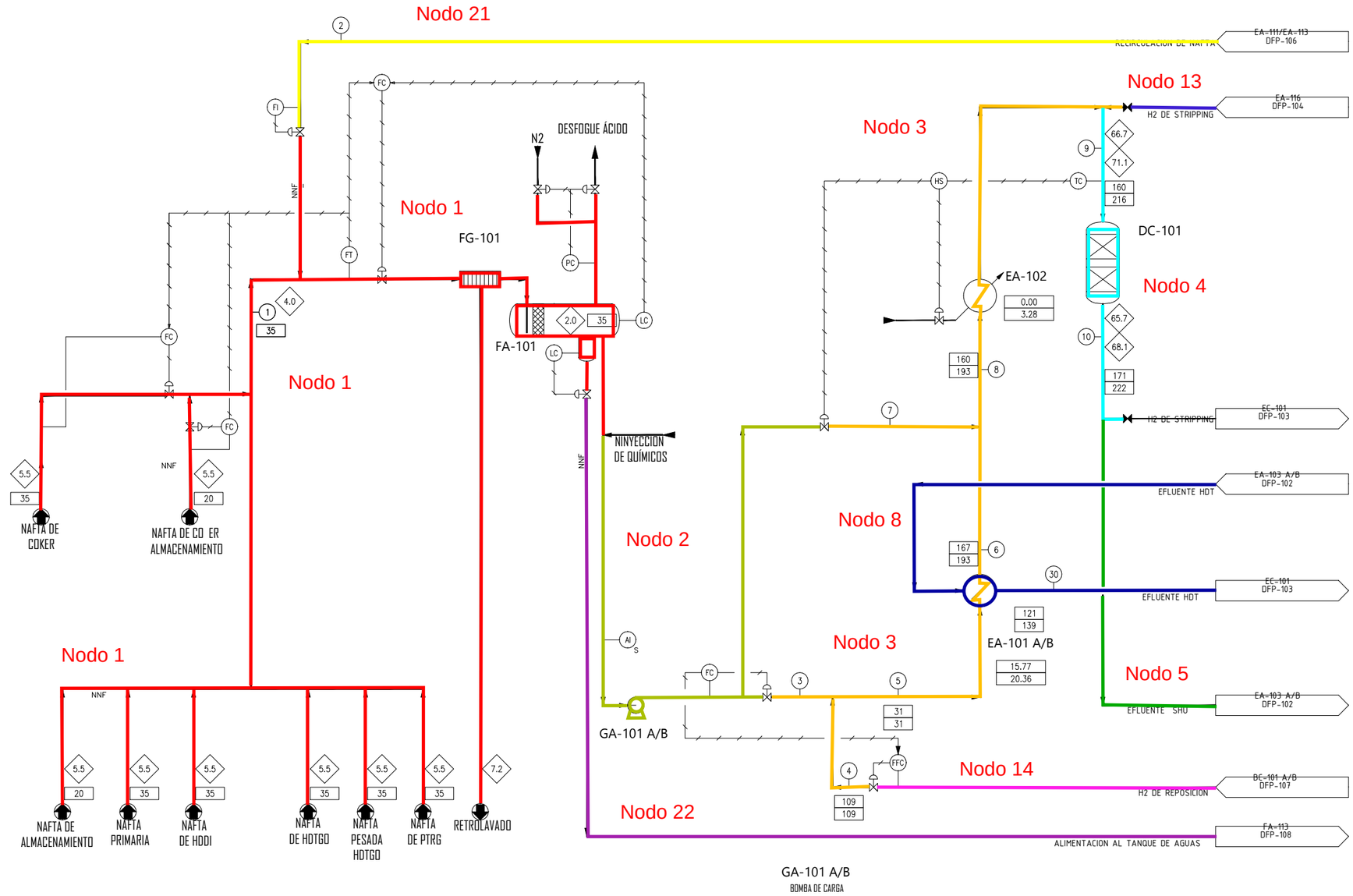
FG-101
FILTRO DE CARGA

FA-101
TANQUE DE ALMACENAMIENTO

EA-101 A/B
CAMBIADOR ENTRADA SHU/EFLUENTE HDT

EA-102
CALENTADOR ENTRADA SHU

DC-101
REACTOR SHU



GA-101 A/B
BOMBA DE CARGA

NUMERO DE CORRIENTE
TEMPERATURA °C
PRESION kg/cm 2
CARGA TERMICA Mkcal/h

INICIO DE CORRIDA EOR (END OF RUN)
FIN DE CORRIDA SOR (START OF RUN)
TEMPERATURA
PRESION
CARGA TERMICA

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-101

A2

EZ-101 A/B
MEZCLADOR ESTATICO

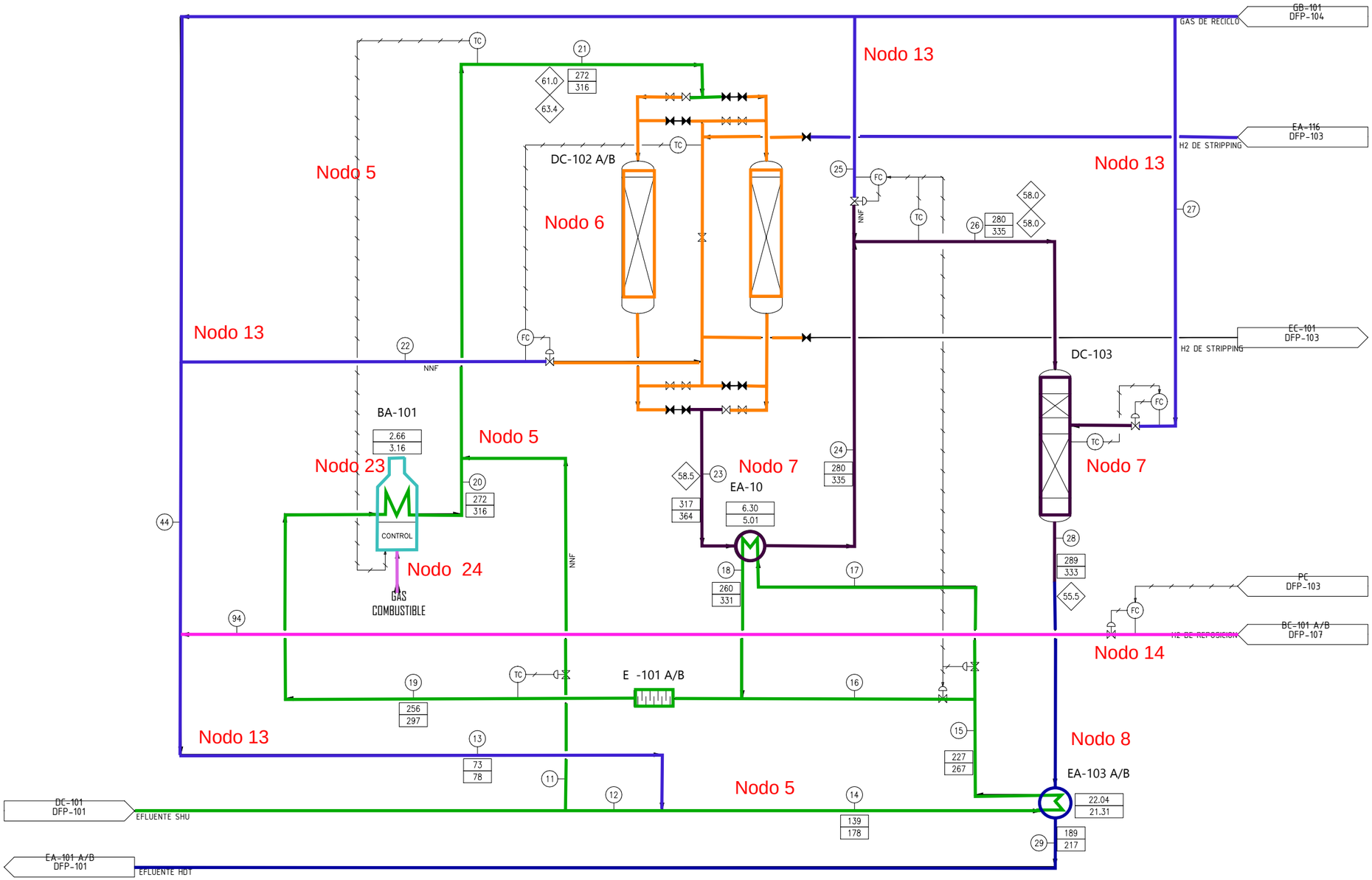
BA-101
CALENTADOR DE LA ALIMENTACIÓN AL REACTOR DE GUARDA

DC-102 A/B
REACTOR DE GUARDA DE SÍLICE

EA-104
CAMBIADOR ALIMENTACIÓN HDT/ALIMENTACIÓN GUARDA

DC-103
REACTOR DE HIDROTRATAMIENTO (HDT)

EA-103 A/B
CAMBIADOR EFLUENTE HDT/ALIMENTACI N GUARDA



NAMERO DE CORRIENTE
TEMPERATURA °C
PRESION kg/cm 2
CARGA TERMICA Mkcal/h

INICIO DE CORRIDA EOR (END OF RUN)
FIN DE CORRIDA SOR (START OF RUN)

TEMPERATURA	
SOR	
EOR	

PRESION	
SOR	
EOR	

CARGA TERMICA
SOR
EOR

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-102

A3

FA-107
TANQUE DE AGUA PARA LAVADO

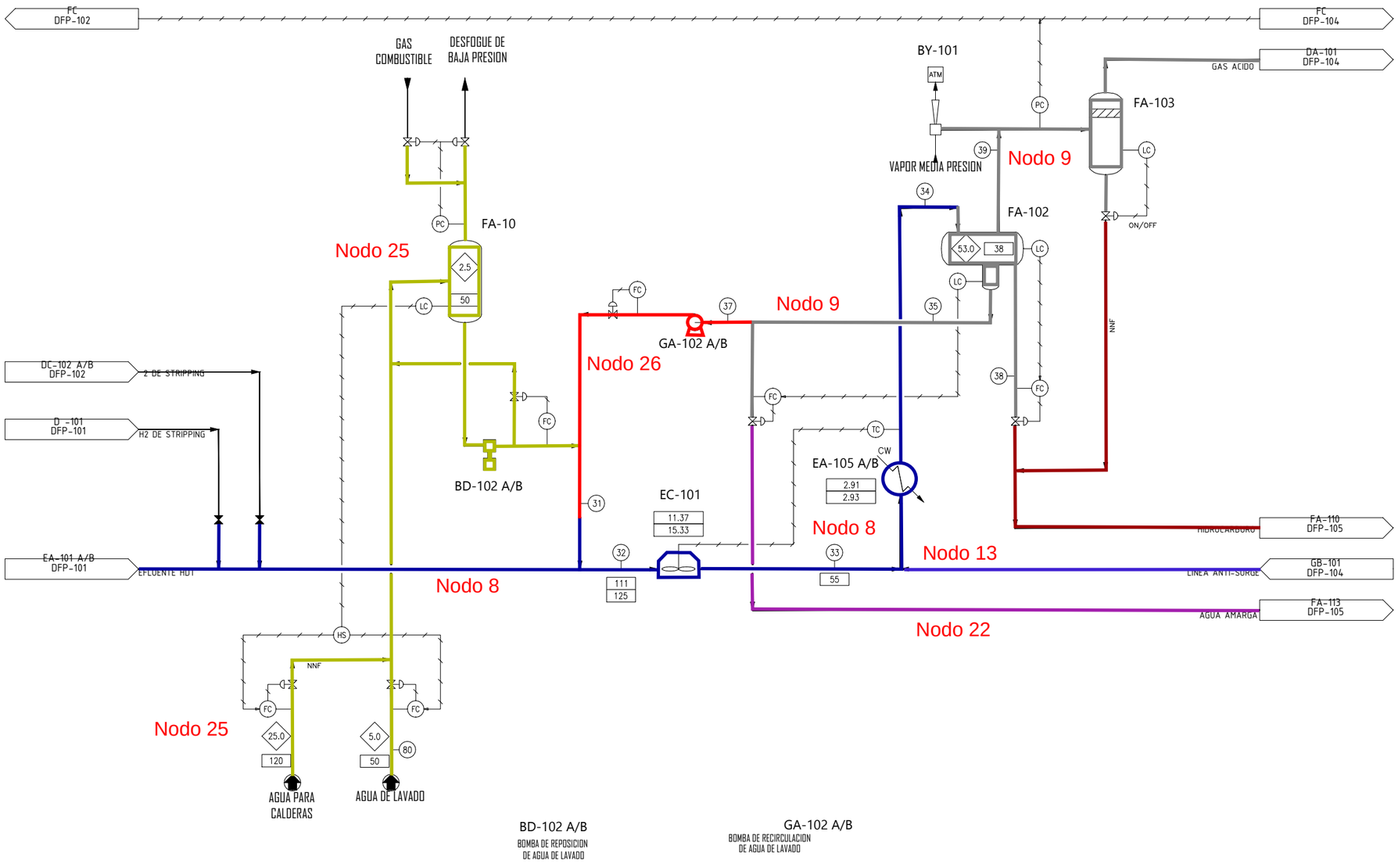
EC-101
AEREOENFRIADOR DEL EFLUENTE HDT

EA-105 A/B
ENFRIADOR CON AGUA DEL EFLUENTE HDT

FA-102
TANQUE SEPARADOR DE EFLUENTES

FA-103
K.O. DRUM DE AMINA

BY-101
EYECTOR



BD-102 A/B
BOMBA DE REPOSICION DE AGUA DE LAVADO

GA-102 A/B
BOMBA DE RECIRCULACION DE AGUA DE LAVADO

NUMERO DE CORRIENTE
TEMPERATURA °C
PRESION kg/cm 2
CARGA TERMICA Mkcal/h

INICIO DE CORRIDA EOR (END OF RUN)
FIN DE CORRIDA SOR (START OF RUN)
TEMPERATURA
SOR
EOR
PRESION
SOR
EOR
CARGA TERMICA
SOR
EOR

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-103

A4

EA-116
CALENTADOR DE STRIPPING

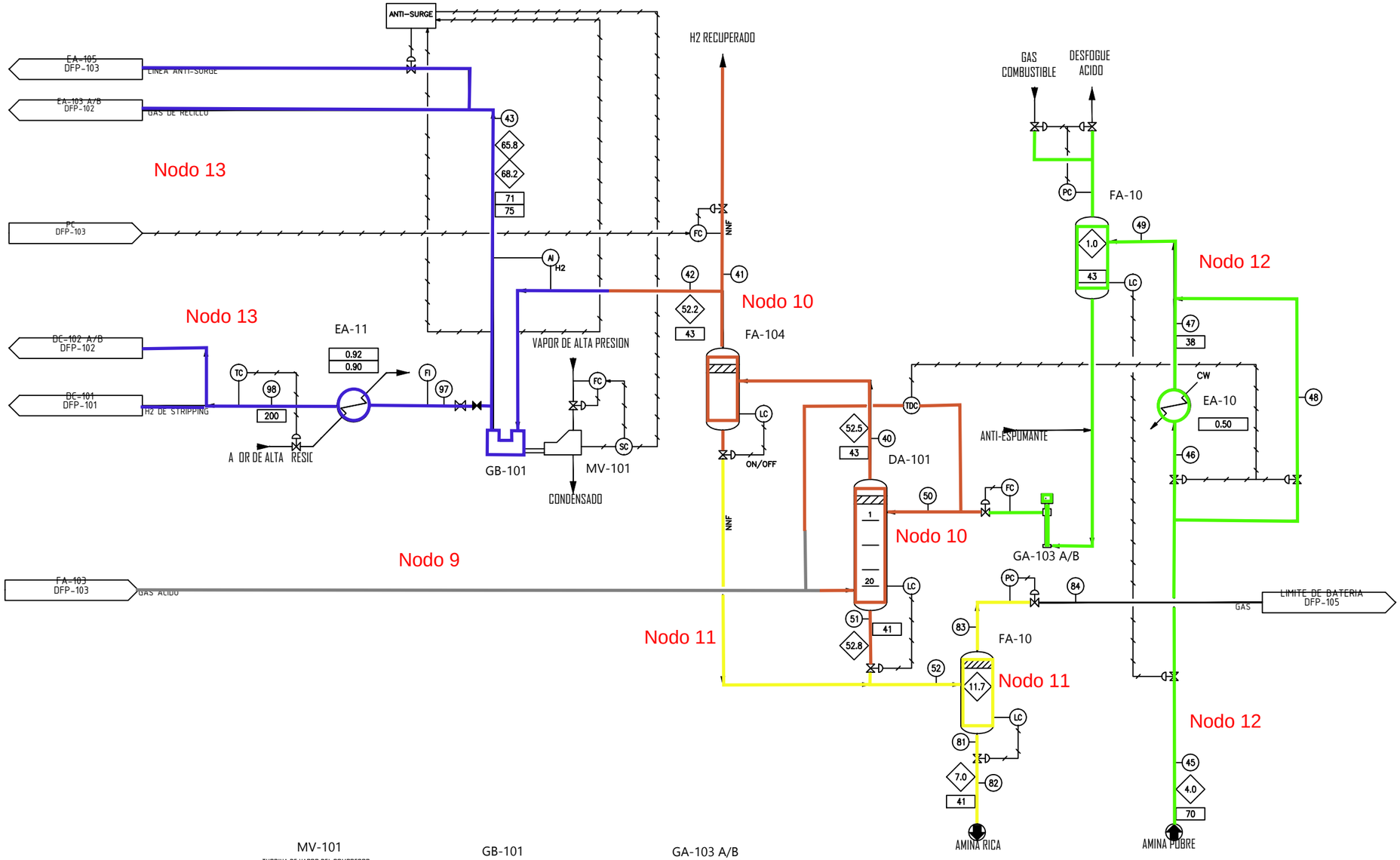
FA-104
K.O. DRUM DEL COMPRESOR DE RECIRCULACIÓN

DA-101
COLUMNA ABSORBEDORA DE AMINA

FA-109
SEPARADOR FLASH DE AMINA RICA

FA-108
TANQUE DE AMINA POBRE

EA-106
ENFRIADOR DE AMINA POBRE



MV-101
TURBINA DE VAPOR DEL COMPRESOR DE RECIRCULACION

GB-101
COMPRESOR DE RECIRCULACION

GA-103 A/B
BOMBA DE AMINA POBRE

NUMERO DE CORRIENTE
TEMPERATURA °C
PRESION kg/cm 2
CARGA TERMICA Mkcal/h

INICIO DE CORRIDA EOR (END OF RUN)
FIN DE CORRIDA SOR (START OF RUN)
TEMPERATURA
PRESION
SOR
EOR
CARGA TERMICA
SOR
EOR
SOR
EOR

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-10

FA-110
TANQUE ESPONJA

FA-105
TANQUE DE REFLUJO DE TORRE ESTABILIZADORA

GAS AMARGO

EA-108 A/B
CONDENSADOR DE DOMOS

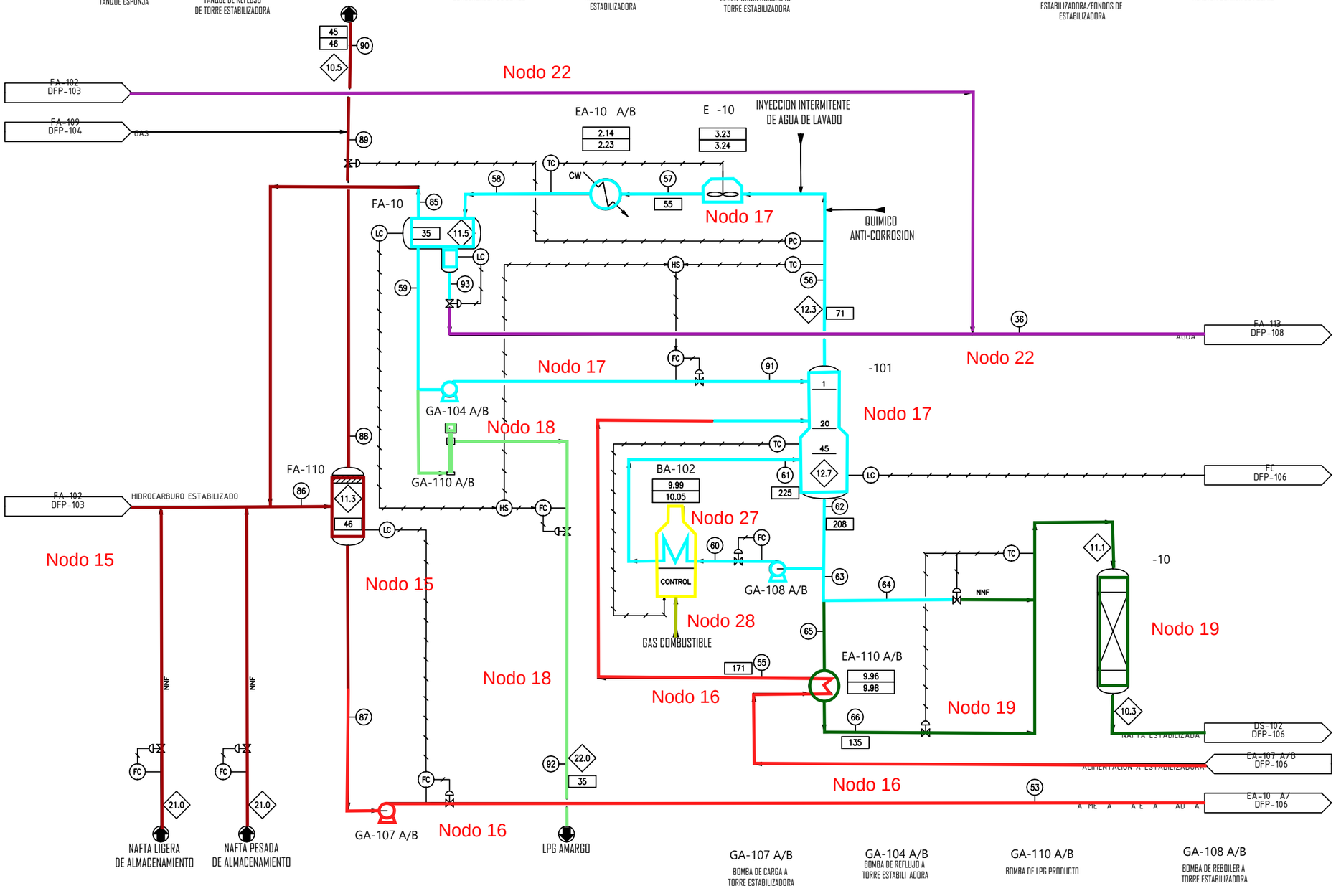
BA-102
REBOILER DE TORRE ESTABILIZADORA

EC-104
AEREO-CONDENSADOR DE TORRE ESTABILIZADORA

DS-101
TORRE ESTABILIZADORA

EA-110 A/B
CAMBIADOR ALIMENTACIÓN DE ESTABILIZADORA/FONDOS DE ESTABILIZADORA

DC-104
REACTOR GUARDA DE AZUFRE



GA-107 A/B
BOMBA DE CARGA A TORRE ESTABILIZADORA

GA-104 A/B
BOMBA DE REFLUJO A TORRE ESTABILI ADORA

GA-110 A/B
BOMBA DE LPG PRODUCTO

GA-108 A/B
BOMBA DE REBOILER A TORRE ESTABILIZADORA

NUMERO DE CORRIENTE
TEMPERATURA °C
PRESION kg/cm 2
CARGA TERMICA Mkcal/h

INICIO DE CORRIDA EOR (END OF RUN)
FIN DE CORRIDA SOR (START OF RUN)
TEMPERATURA
PRESION
CARGA TERMICA

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-10

EC-103
AEREOENFRIADOR DE NAFTA PESADA

BA-103
REHERVIDOR DE TORRE FRACCIONADORA

DS-102
TORRE FRACCIONADORA

EA-107 A/B
TANQUE DE REFLU O DE TORRE FRACCIONADORA

EC-102
CONDENSADOR DE TORRE FRACCIONADORA

EA-113
ENFRIADOR DE NAFTA PESADA

EA-111
ENFRIADOR DE NAFTA LIGERA

FA-106
TANQUE DE REFLU O DE TORRE FRACCIONADORA

DESFOGUE DE BAJA PRESION

LC
DFP-105

DC-104
DFP-105
NAFTA ESTABILIZADA

Nodo 19

Nodo 20

Nodo 20

Nodo 20

Nodo 20

Nodo 30

Nodo 31

GAS COMBUSTIBLE

Nodo 16

Nodo 29

Nodo 29

Nodo 29

Nodo 21

Nodo 21

EA-110 A/B
DFP-105

GA-107 A/B
DFP-105

FG-101
DFP-101
NAPHTHA RECYCLE

EC-102
12.57
12.54

DS-102

BA-103
12.31
12.31

CONTROL

GA-106 A/B

EA-107 A/B
6.27
6.27

EC-103
3.08
3.08

EA-113
1.43
1.43

EA-111
0.46

FA-106

GA-10 A/B

GA-10 A/B

NNF

DRENAJE

NAFTA PESADA
A REFORMADORA

NAFTA ESADA
A ALMACENAMIENTO

NAFTA LIGERA
A PNX

NAFTA LIGERA
A ALMACENAMIENTO

GA-106 A/B
BOMBA DE FONDOS DE TORRE FRACCIONADORA

GA-105 A/B
BOMBA DE REFLUJO DE TORRE FRACCIONADORA

GA-109 A/B
BOMBA DE NAFTA LIGERA PRODUCTO

NUMERO DE CORRIENTE
TEMPERATURA °C
PRESION kg/cm 2
CARGA TERMICA Mkcal/h

INICIO DE CORRIDA EOR (END OF RUN)
FIN DE CORRIDA SOR (START OF RUN)
TEMPERATURA
PRESION
CARGA TERMICA
SOR
EOR

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-106

EA-114 A/B

ENFRIADOR INTERETAPA DEL COMPRESOR DE HIDROGENO DE REPOSICION

EA-115

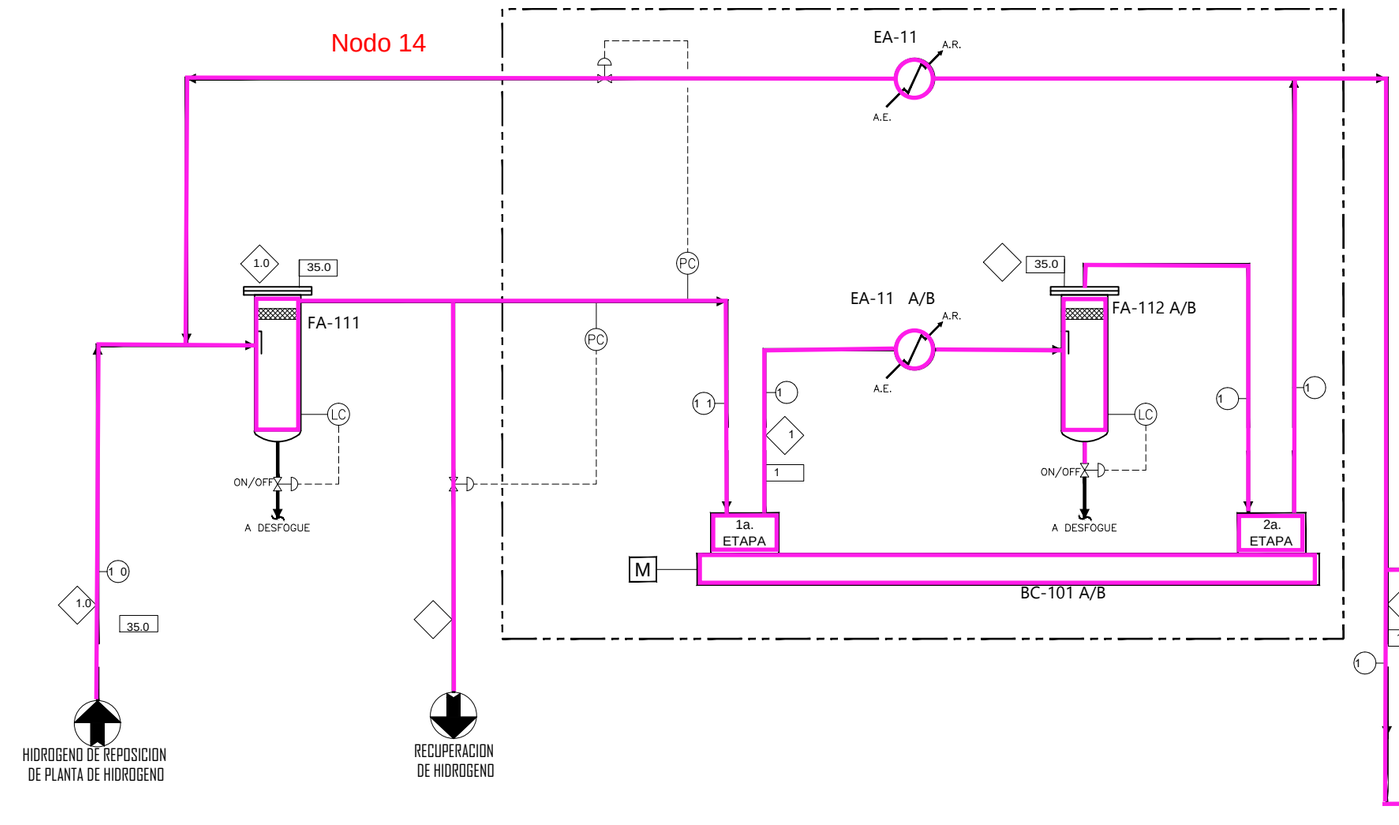
ENFRIADOR DE RECIRCULACION DE HIDROGENO DE RE OSICION

FA-111

TANQUE DE SUCCION DEL COMPRESOR DE HIDROGENO DE REPOSICION

FA-112 A/B

TANQUE SEPARADOR INTERETAPA DEL COMPRESOR DE HIDROGENO DE REPOSICION



Nodo 14

BC-101 A/B

ENFRIADOR DE RECIRCULACION DE HIDROGENO DE RE OSICION

DE PP DFP-101

HZ DE STRIPPING LINEA DE REPOSICION HZ DFP-102

NUMERO DE CORRIENTE

TEMPERATURA °C

PRESION kg/cm 2

CARGA TERMICA Mkcal/h

INICIO DE CORRIDA EOR (END OF RUN)

FIN DE CORRIDA SOR (START OF RUN)

TEMPERATURA SOR EOR

PRESION SOR EOR

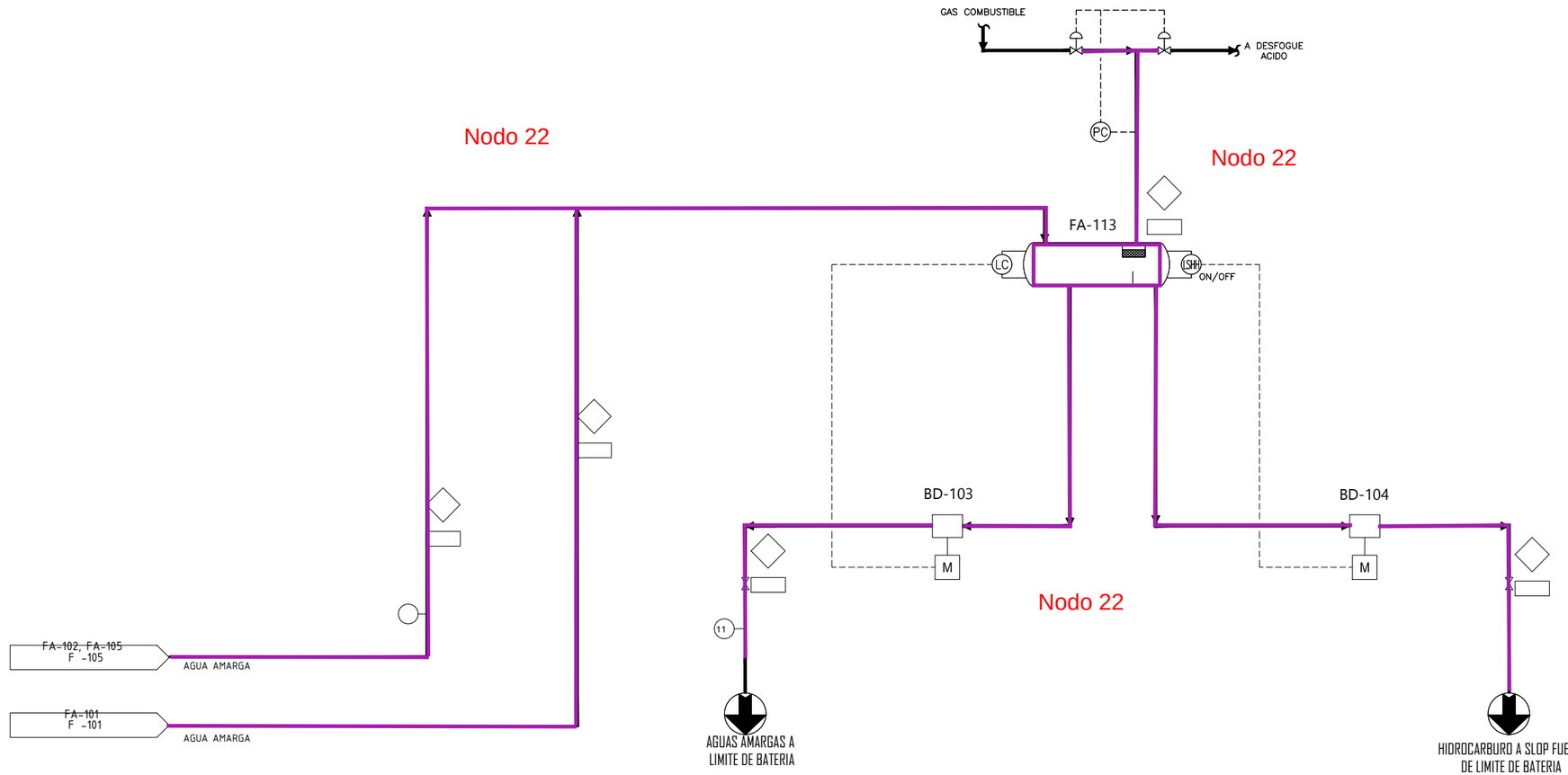
CARGA TERMICA SOR EOR

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-107

FA-113

TANQUE DE AGUAS AMARGAS



BD-103

BOMBA DE AGUAS AMARGAS

BD-104

BOMBA DE HIDROCARBURO A SLOP

NUMERO DE CORRIENTE

TEMPERATURA °C

PRESION kg/cm 2

CARGA TERMICA Mkcal/h

~~INICIO DE CORRIDA EOR (END OF RUN)~~
~~FIN DE CORRIDA SOR (START OF RUN)~~

TEMPERATURA

PRESION

SOR
EOR

CARGA TERMICA

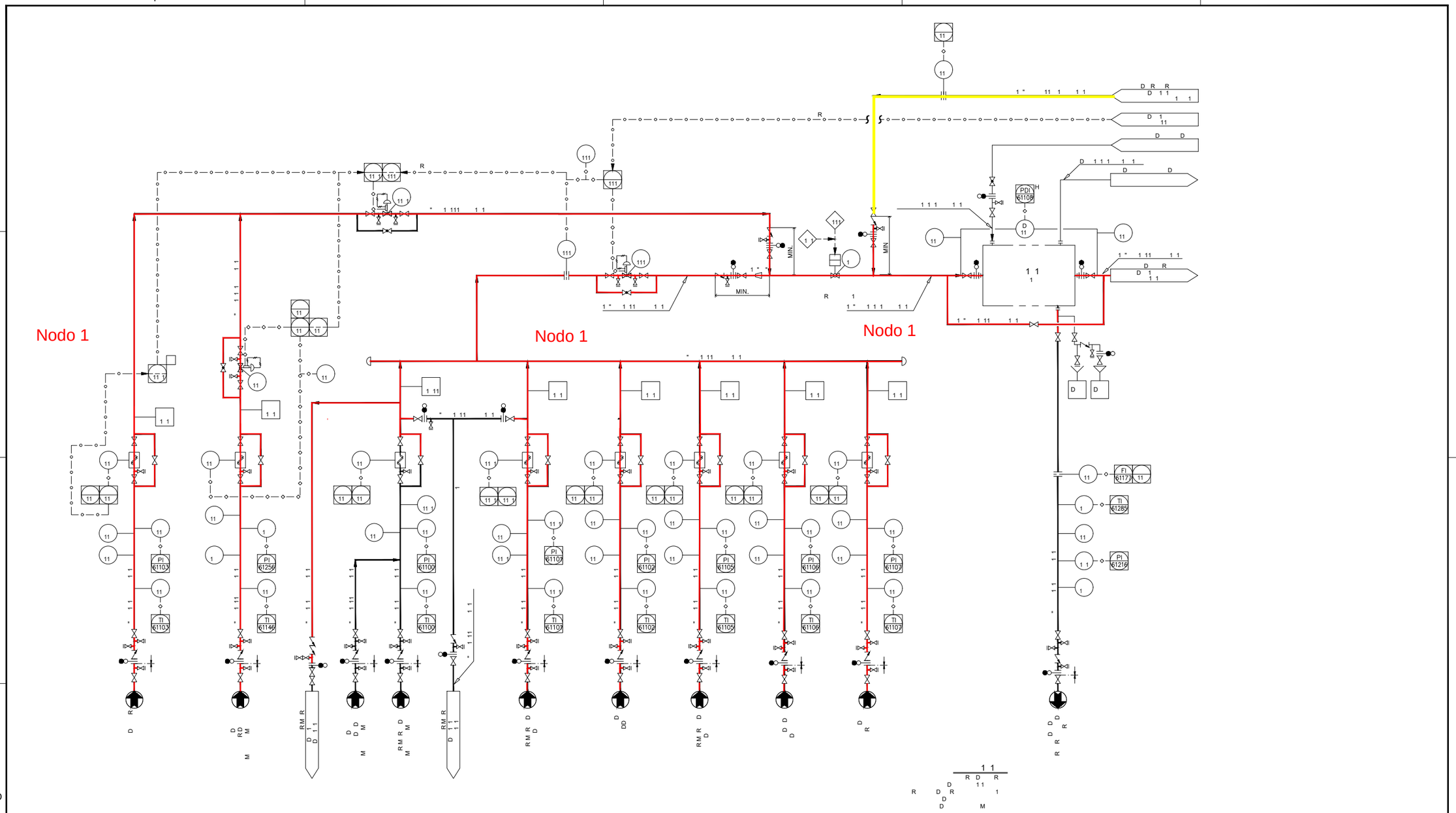
SOR
EOR

SOR
EOR

PLANTA HIDROTRATADORA DE NAFTAS TÍPICA (HDN)

DFP-108

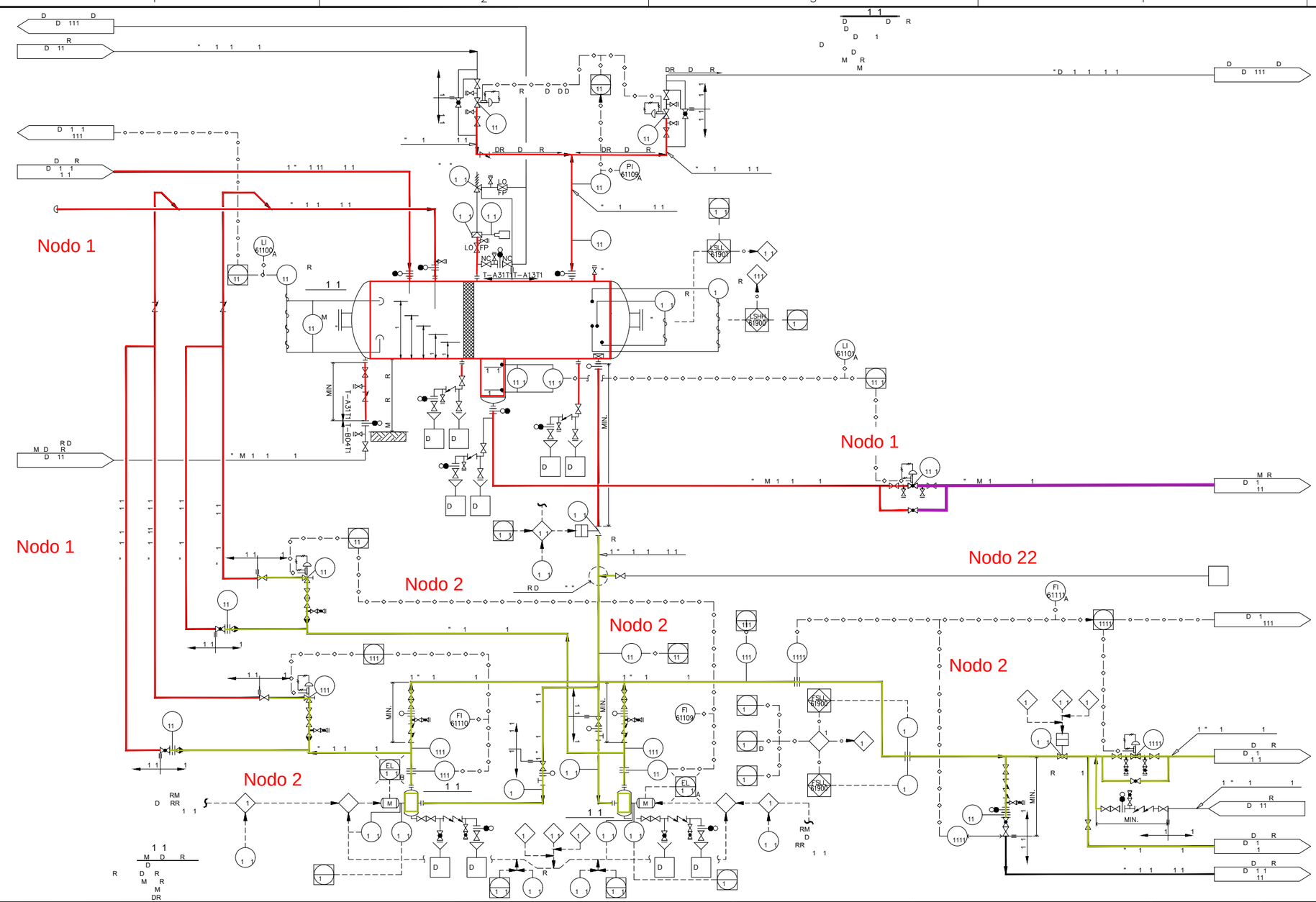
Anexo B
Diagramas de Tubería e Instrumentación Nodeados



Versión para HazOp-SPR

dr r d r d
D

D 1 1



Versión para HazOp-SPR

dr r d r d
D

D 1

B

Anexo C
Hojas de trabajo HazOp.

Nodo1. Sección de Alimentación de Carga			El circuito de carga que comprende desde los limietes de bateria de nafta olefinica y parafinica a (6 kg/cm2 y 38°C ambos) hasta el recipiente de separador trifásico FA-101 (2.5kg/cm2 y 38°C) así como sus lineas asociadas.				
Desviación	Causas						
	Causa	Causa Hackeable	Consecuencias				
			Consecuencia	Salvaguardas			PHA Recommendation
				Salvaguarda	Tipo salvaguarda	Salvaguarda Hackeable	
	1.1.1 Falla del lazo de control de presión PIC-61109 (abriendo PV-61109A y cerrando PV-61109B)	Yes	1.1.1.1 Sobrepresionamiento del tanque de carga FA-101	1 Válvula de seguridad PSV-61021 en el tanque de carga FA-101.	Mecánica	No	2 Verificar que el diseño de las PSV sea acorde a la falla mas crítica.
	1.1.2 Ver "Bajo nivel de este nodo"		1.1.2.1 Pérdida de nivel en el tanque de carga FA-101 con posible dalo mecánico a la bomba de carga GA-101 A/B	2 Válvula de segurdidad PSV- en el paquete de filtrado FG-101	Mecánica	No	
	1.1.3 Falla de la bomba de carga GA-101 A/B	Yes	1.1.3.1 Posible fuga de nafta e uniones bridadas	3 Indicador local de presión local PG-61109	Análoga Local	No	
				4 Presión de diseño de tuberias desde LB hasta sistema de filtrado.	Mecánica	No	11 Configurar una alarma independiente en el SCD FIC-61115 del cabezal de carga de nafta
				23 Medidor de presión diferencial PDI-61108	SCD	Yes	
			1.1.4.1 Posible incendio /explosión.	6 Alarma por alta presión diferencial en PDI-61124 y PDI-61231	SCD	Yes	
			1.1.4.2 Producción diferida.	5 Medidor de presión diferencial PDI-61108	SDC	Yes	
				7 Indicador de nivel LIC-61100 en SCD de la planta con alarma de bajo nivel.	SCD	Yes	
				8 Cristal de nivel LG-61100 en el tanque de carga FA-101.	Análoga Local	No	
				24 Válvula de bloqueo de emergencia XV-61900	SIS	Yes	
				25 Switch de muy bajo nivel LSLL-61901.	SIS	Yes	
				11 Sistema de deteccion de gas y fuego.	SFG	No	
	1.1.4 Taponamiento del paquete de filtrado			12 Sistema de contraincendio.	SFG	No	
1.1 Mayor Presión	de carga FG-101	No	1.1.4.3 Posible paro de planta	26 Plan de respuesta a emergencias.	Procedimiento	No	
			1.2.1.1 Cavitación de la bomba GA-101 A/B	10 Switch de muy bajo nivel LSLL-61901.	SIS	Yes	
				14 Lazo de control de nivel LIC-61100	SCD	Yes	
			1.2.1.2 Alto nivel en el tanque de carga FA-101	14 Lazo de control de nivel LIC-61100	SCD	Yes	
			1.2.1.3 Posible paro de planta	15 Cristal de nivel LG-61100	Análoga Local	No	
			1.2.1.4 Posible figa de nafta en sellos	9 Válvula de bloqueo de emergencia XV-61900	SIS	Yes	
				16 Indicadores locales de presión PI-61110 con alarma po baja presión. a la salida de la bomba GA-101	Análoga Local	No	
				18 Indicador de presión PIC-61109.	SCD	Yes	
				17 lazo de control de nivel FIC-61131 en LB.	SCD	Yes	
				19 Switch por alta alta vibración VSHH-61001 de la bomba GA-101 A/B	SIS	Yes	
	1.2.1 Falla del lazo de control de presión PIC-61109 (abriendo PV-61109B y cerrando PV-61109A)			20 Sistemas de detección de gas y fuego.	SFG	No	
1.2 Menor Presión.		Yes	1.2.1.5 Posible incendio/explosión.	13 Plan de respuesta a emergencias.	Procedimiento	No	
1.3 Mayor Flujo	1.3.1 Ver causas de mayor nivel de este nodo (Nafta)						
1.4 Menor Flujo	1.4.1 Ver causas de menor nivel de este nodo (Nafta)						10 Adicionar alarmas por bajo flujo en el SCD FIC-61115 del cabezad de carga de la nafta.
	1.5.1 Falla del lazo de control de nivel LIC-61100	Yes	1.5.1.1 Presionamiento del tanque de carga FA-101	21 Indicador controlador de presión PIC-61109 con alarma de alta presión, en el tanque FA-101	SCD	Yes	1 Verificar que los sistemas de control distribuido, sistema instrumentado de seguridad y sistema de gas y fuego sean seleccionados con las medidas adecuadas de ciberseguridad, con la finalidad de proteger la integridad cibernetica de estos sistemas contra posibles ciberataques. La selección debe basarse en un estudio de selección de "Security Level" (SL) de acuerdo al IEC-62443.
				209. K.O. Drum del sistema de desfogue.	Mecánica	No	
	1.5.2 Paro de la bomba de carga GA-101 A/B	Yes	1.5.2.1 Potencial arrastre de hidrocarburo líquido a sistema de desfogue.	22 Switch de muy alto nivel LSHH-61900.	SIS	Yes	1 Verificar que los sistemas de control distribuido, sistema instrumentado de seguridad y sistema de gas y fuego sean seleccionados con las medidas adecuadas de ciberseguridad, con la finalidad de proteger la integridad cibernetica de estos sistemas contra posibles ciberataques. La selección debe basarse en un estudio de selección de "Security Level" (SL) de acuerdo al IEC-62443.
				7 Indicador de nivel LIC-61100 en SCD de la planta con alarma de bajo nivel.	SCD	Yes	
				8 Cristal de nivel LG-61100 en el tanque de carga FA-101.	Análoga Local	No	
				27 Bomba de carga de relevo GA-101 B	Mecánica	No	
				17 lazo de control de nivel FIC-61131 en LB.	SCD	Yes	
				18 Indicador de presión PIC-61109.	SCD	Yes	
	1.5.3 Falla de lazo de control de flujo FIC-61131			1 Válvula de seguridad PSV-61021 en el tanque de carga FA-101.	Mecánica	No	
1.5 Mayor Nivel (Nafta)		Yes	1.5.3.1 Producción diferida				
	1.6.1 Falla de lazo de control de nivel-flujo LIC-61100 cerrando FV-61115	Yes	1.6.1.1 Arrastre de agua a sección de reacción con daño a catalizador	28 indicador de nivel de interfase LIC-61101 con alarma por alto nivel.	SCD	Yes	1 Verificar que los sistemas de control distribuido, sistema instrumentado de seguridad y sistema de gas y fuego sean seleccionados con las medidas adecuadas de ciberseguridad, con la finalidad de proteger la integridad cibernetica de estos sistemas contra posibles ciberataques. La selección debe basarse en un estudio de selección de "Security Level" (SL) de acuerdo al IEC-62443.
				31 Cristal de nivel LG-61101 de la pierna del tanque de carga.	Análoga Local	No	
				29 Programa de muestreo (causa 1.6.2)	Protocolo	No	
1.6 Mayor Nivel (agua amarga)	1.6.2 Mayor cantidad de agua en la alimentación.	No	1.6.2.1 Menor tiempo de corrida de la planta por daño al catalizador	28 indicador de nivel de interfase LIC-61101 con alarma por alto nivel.	SCD	Yes	

	1.7.1 Falla de lazo de control de nivel-flujo LIC-61100.	Yes	1.7.1.1 Cavitación de bomba de carga GA-101 A/B con probable daño mecánico a los internos de la misma.	SIN SALVAGUARDAS			15 Se recomienda verificar si las SIS por bajo flujo a la salida de la bomba de carga FSLL-61900, que indica paro, es suficiente para evitar la cavitación del equipo.
1.7 Menor/No nivel (Nafta)	1.7.2 Falla en el suministro de Nafta en LB	No	1.7.2.1 Envio de nafta al tanque de agua amarga FA-113	SIN SALVAGUARDAS			
1.8 Menor /No nivel (agua amarga)							
	1.9.1 Alimentación de nafta de coquer con mayor temperatura	No	1.9.1.1 Presionamiento del tanque de carga FA-101 (ver consecuencias de mayor presión de este nodo)	32 Ver salvaguardas de mayor presión de este nodo			
				33 Indicador local TG-61071 al 78 en LB	Análogo y local	Yes	
1.9 Mayor temperatura	1.9.2 Fuego externo	No	1.9.2.1 Variación de las condiciones de operación de la bomba de carga.	19 Switch por alta alta vibración VSHH-61001 de la bomba GA-101 A/B	SIS	Yes	
1.10 Menor temperatura							

Nodo 2. Sección de bombeo del tanque de carga.			**La bomba del tanque de carga GA-101 (que aumenta la presión hasta 81.6 kg/cm2) y lineas asociadas hasta las entradas al tren de calentamiento previo a la reacción.**				
Desviación	**Causas**						
	Causa	**Causa Hackeable**	**Consecuencias**				
			Consecuencia	**Salvaguardas**			**PHA Recommendation**
				Salvaguarda	**Tipo salvaguarda**	**Salvaguarda Hackeable**	
				36 Presión de diseño de tubería superior a la la presión de cierre estimada de la bomba GA-101 AB	Mecánica	No	5 Configurar una alarma independiente por alta presión en el PI-61110 en el cabezal de la bomba de carga GA-101 AB
				34 Recirculación de la bomba controlada con el lazo FIC-61109	SCD	Yes	
	2.1.1 Falla del lazo de control de flujo FIC-61111	Yes	2.1.1.1 Se alcanza la presión de cierre de la bomba GA-101 A/B	35 FIS por bajo flujo FSLL-61900 que manda a paro de bomba.	SIS	Yes	
				37 indicador local TG-61110	Análoga local	No	
	2.1.2 Falla del lazo de control de flujo FIC-61113	Yes	2.1.2.1 Mayor temperatura a la entrada del cambiador EA-102.	38 Lazo de control de temperatura TIT-61111.	SCD	Yes	
2.1 Mayor Presión				39 Bomba de relevo GA-101 B	Mecánica	No	
2.2 Menor presión	2.2.1 Falla o paro de la bomba de carga	Yes	2.2.1.1 Producción diferida o paro de planta.	34 Recirculación de la bomba controlada con el lazo FIC-61109	SCD	Yes	
2.3 Mayor Flujo	2.3.1 Operación simultanea de las bombas de carga GA-101 A/B	Yes	2.3.1.1 Pérdida de nivel en el tanque de carga FA-101	40 Luces de estado EL-61001 AB de bombas GA-101 A/B	SCD	Yes	1 Verificar que los sistemas de control distribuido, sistema instrumentado de seguridad y sistema de gas y fuego sean seleccionados con las medidas adecuadas de ciberseguridad, con la finalidad de proteger la integridad cibernetica de estos sistemas contra posibles ciberataques. La selección debe basarse en un estudio de selección de "Security Level" (SL) de acuerdo al IEC-62443.
2.4 Menor Flujo / No flujo	2.4.1 (Ver Menor presión de este nodo)						
2.5 Flujo inverso	2.5.1 Falla o paro de bomba de carga	Yes	2.5.1.1 Sobrepresiónamiento del tanque de carga FA-101	41 Válvulas check en la linea de descarga de la bomba de carga GA-101	Mecánica	No	
2.6 Mayor temperatura	2.6.1 Sin causas apartentes en el Nodo						
2.7 Menor temperatura	2.7.1 Sin causas apartentes en el Nodo						

Nodo 3. Tren de calentamiento previo a la reacción de saturación de diolefinas.			**El tren de calentamiento previo a la reacción que consta de los Cambiadores EA-101 (81.6 kg/cm2 y 193°C) y EA-102 (81 kg/cm2 216°C) ambos equipos procesan el fluido del lado tubos. Desde la entrada de EA-101 hasta la entrada del reactor DC-101**				
Desviación	**Causas**						
	Causa	**Causa Hackeable**	**Consecuencias**				
			Consecuencia	**Salvaguardas**			**PHA Recommendation**
				Salvaguarda	**Tipo salvaguarda**	**Salvaguarda Hackeable**	
3.1 Mayor Presión	3.1.1 SIn causas aparentes dentro del nodo						
			3.2.1.1 Descontrol del proceso	42 Diseño de los cambiadores, siguiendo la regla de los 10/13	Mecánica	No	
				43 Medidores de presión locales PG-61117 y PG-61116	Análoga local	No	12 Añadir alarma por baja presión en el SCD PI-61161 a la salida del lado tuos del EA-101AB y definir un procedimiento operativo en caso de una baja en la presión.
3.2 Menor Presión	3.2.1 Ruptura de tubos en los cambiadores EA-101 AB o EA-102	No	3.2.1.2 Producción diferida	44 Medidores de temperatura locales TG-61105 y TG-61110	Análoga local	No	
3.3 Mayor Flujo	3.3.1 SIn causas aparentes dentro del nodo						
3.4 Menor Flujo	3.4.1 Ver menor presión de este nodo.						
				45 Indicador local de temperatura flujo TG-61110	Análoga local	No	13 Añadir alarma por alta temperatura en el SCD TI-61109 a la salida del lado tuos del EA-101AB
				46 Indicador local de presión flujo PG-61269	Análoga local	No	
3.5 Mayor temperatura	3.5.1 Falla del lazo de control FIC-61114	Yes	3.5.1.1 Mayor temperatura de la carga al reactor.	47 FIS por alta temperatura en el reactor DC-101 IS-6102	SIS	Yes	
3.6 Menor temperatura	3.6.1 Sin causas aparentes dentro del nodo						

Anexo D
Requerimientos de SL

Número	*Descripción*	*Niveles de seguridad definidos del 1 al 4*			
FR 1	***Autentificación e identificación de control.***	***SL 1***	***SL 2***	***SL 3***	***SL 4***
SR 1.1	Identificar y autenticar a todos los usuarios humanos.	X	X	X	X
RE (1)	identificar de forma unica y autenticar a todos los usuarios humanos.		X	X	X
RE (2)	Emplear la autenticación multifactor para el acceso de usuarios humanos al sistema de control a través de na red no confiable.			X	X
RE (3)	Emplear la autenticación multifactor para todos los accesos de usuarios humanos al sistema de control.				X
SR 1.2	Identificación y autentificación de dispositivos y procesos de software.		X	X	X
RE (1)	Identificar de forma única y autenticara todos los dispositivos y procesos de software.			X	X
SR 1.3	Administrar todas las cuentas de acuerdo con los usuarios autorizados, lo que incluye añadir, activar, modificar, deshabilitar y eliminar cuentas.	X	X	X	X
RE (1)	Apoyar la gestión de cuentas unificadas.			X	X
SR 1.4	Administrar identificadores por ususario, grupo, rol o interfaz del sistema de control.	X	X	X	X
SR 1.5	Inicializar el contenido autenticador, cambiar todos los autenticadores predeterminados en la instalación del sistema de control, cambiar/actualizar todos los autenticadores, y proteger los autenticadores de la divulgación o modificación no autorizada.	X	X	X	X
RE (1)	Hardware de seguridad para los procesos de software de identifiación de credenciales.			X	X
SR 1.6	Administrar el acceso inalámbrico.			X	X
RE (1)	Identificar y autenticar de forma única a todos los usuarios involucrados en la comunicación inalámbrica.	X	X	X	X
SR 1.7	Hacer cumplir la seguridad de la contraseña configurable, según la longitud mínima y la variedad de tipo de caracteres.	X	X	X	X
RE (1)	Evitar que cualquier cuenta de usuario humano reutilice una contraseña durante un número configurable de accesos.			X	X
RE (2)	Hacer cumplir las restricciones de vida mínima y máxima de la contraseña para todos los usuarios humanos.				X
SR 1.8	Utilizar certificados de clave pública.		X	X	X
SR 1.9	Garantizar la solidez del certificado de clave pública.		X	X	X
RE (1)	Hardware de seguridad para autenticación de clave pública.			X	X
SR 1.10	Retroalimentación oculta de la información de autenticación durante el proceso de autenticación.	X	X	X	X
SR 1.11	Aplicar un límite configurable de número de intentos de acceso no validos consecutivos por parte de cualquier usuario (humano, proceso de software o dispositivo).	X	X	X	X
SR 1.12	Mostrar un mensaje de notificación de uso del sistemaantes del proceso de autentificación.	X	X	X	X
SR 1.13	Supervisar y controlar todos los métodos de acceso al sistema de control a través de redes no confiables.	X	X	X	X
RE (1)	Denegar solicitudes de acceso a través de tres redes a menos que se apruebe el rol asignado.		X	X	X
FR 2	***Control de uso (UC)***	***SL 1***	***SL 2***	***SL 3***	***SL 4***
SR 2.1	Hacer cumplir las autorizaciones asignadas a todos los usuarios humanos para controlar el uso del sistema de control para respaldar la segregación de funcionees y el privilegio mínimo.	X	X	X	X
RE (1)	Hacer cumplir las autorizaciones asignadas a todos los usuarios (humanos, procesos de software y dispositivos) para controlar el uso del sistema de control para respaldar la segregación de funciones y el privilegio mínimo.		X	X	X
RE (2)	Usuarios o roles autorizados para definir y modificar la asignacion de permisos a roles para todos los usuarios humanos.		X	X	X
RE (3)	Permitir que el supervisor anule manualmente las autorizaciones de usuarios humanos actuales durante un tiempo configurable o una secuencia de eventos.			X	X
RE (4)	Requerir una doble aprovación cuando una acción pueda tener un impacto grave en el proceso industrial.				X
SR 2.2	Autorizar, monitorear y hacer cumplir las restricciones de uso para la conectividad inalámbrica al sistema de control.	X	X	X	X
RE (1)	Identifiacr y reportar dispositivos inalámbricos no autorizados que transmiten dentro del entorno físisco del sistema de control.			X	X
SR 2.3	Aplicar automáticamente restricciones de uso configurables.	X	X	X	X

RE (1)	Verificar que los dispositivos portátiles o moviles que intenten conectarse a una zona cumplan con los requisitos de seguridad de esa zona.			X	X
SR 2.4	Hacer cumplir las restricciones de uso para las técnologías de códigos móviles segúnl a posibilidad de causar daños al sistema de control.	X	X	X	X
RE (1)	Verificar la integridad del código móvil antes de permitir la ejecución del código.			X	X
SR 2.5	Evitar mas accesos iniciando un bloqueo de sesión despues de un tiempo configurable de inactividad o por inicio manual.	X	X	X	X
SR 2.6	Terminar una sesión remota ya sea automáticamentedespues de un tiempo de inactividad configurable o manualmente por el usuario que inició la sesión.		X	X	X
SR 2.7	Limitar el número de sesiones simultáneas por interfaz para un usuario determinado (humano, proceso de software o dispositivo) a un número configurable de sesiones.			X	X
SR 2.8	Generar requisitos de auditoría relevantes para la seguridad para las siguientes categorías: control de acceso, errores de solicitud, eventos del sistema operativo, eventos del sistema de control, eventos de respaldo y restauración, cambios de configuración, actividad de reconocimiento potencial y eventos de registro de auditoría. Los registros individuales de la auditoría deben incluir el sello de tiempo, la fuente (dispositivo de origen, proceso de software o cuenta de usuario humano), categoría, tipo, ID de evento y resultado del evento.	X	X	X	X
RE (1)	Administrar de manera centralizada los eventos de auditoría y compilar registros de auditoría de multiples componentes en todo el sistema de control en una pista de auditoría correlacionada en el tiempo de todo el sistema (lógica o física) Que el sistema de control proporcione la capacidad de exportar estos registros de auditoría en formatos estandar de la industria para sus análisis mediante herramientas de análisis de registros comerciales estandar, por ejemplo, información de seguridad y gestión de eventos (SIEM).			X	X
SR 2.9	Asignar suficiente capacidad de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la administración de registros y la configuración de registros y la configuración del sistema	X	X	X	X
RE (1)	Emitir una advertencia cuando el volumen de almacenamiento de registros de auditoría asignado alcance un porcentaje configurable de la capacidad máxima de almacenamiento de registros de auditoría.			X	X
SR 2.10	Alertar al personal y prevenir la pérdida de servicios y funciones escenciales en caso de una falla en el procesamiento de auditoría	X	X	X	X
SR 2.11	Marcas de tiempo para su uso en la generación de registros para auditoría.		X	X	X
RE (1)	Sincronizar los relojes internos del sistema a una frecuencia configurable.			X	X
RE (2)	Proteger la fuente de tiempo de alteraciones no autorizadas y provocar un evento de auditoría sobre la alteración.				X
SR 2.12	Determinar si un usuario humano específico realizó una acción en particular			X	X
RE (1)	Determinar si un usuario especifico (humano, proceso de software o dispositivo) realizó una acción en particular.				X
FR 3	***Control de uso (UC)***	***SL 1***	***SL 2***	***SL 3***	***SL 4***
SR 3.1	Proteger la integriad de la información transmitida.	X	X	X	X
RE (1)	Emplear mecanismos criptográficos para reconocer cambios en la información durante la comunicación.			X	X
SR 3.2	Emplear mecanismos de protección para prevenir, detectar, informar y mitigar los efectos de códigos maliciosos o software no autorizado.	X	X	X	X
RE (1)	Emplear mecanismos de protección de códigos maliciosos en todos los puntos de entrada y saida.		X	X	X
RE (2)	Gestion centralizada de los mecanismos de protección contra codigo malicioso.			X	X
SR 3.3	Verificar el funcionamiento previsto de las funciones de seguridad e informar cuando se descubran anomalías durante, las pruebas de aceptación de fábrica (FAT), las pruebas de aceptación del sitio (SAT) y el mantenimiento programado.	X	X	X	X
RE (1)	Emplear mecanismos automatizados para respaldar la gestión de la verificación de seguridad durante FAT y SAT y el mantenimiento programado.			X	X
RE (2)	Apoyar la verificación del funcionamiento previsto de las funciones de seguridad durante las operaciones normales.				X
SR 3.4	Detectar, registrar, informar y proteger contra cambios no autorizados del software y la información en reposo.		X	X	X

RE (1)	Utilizar herramientas automatizadas que notifiquen a un conjunto configurable de destinatarios sobre el descubrimiento de discrepancias durante la verificación de integridad.			X	X
SR 3.5	Validar la sintaxis y el contenido de cualquier entrada que se utilice como entrada de control de procesos industriales o entrada que impacte directamente la acción del sistema de control.	X	X	X	X
SR 3.6	Establecer las salidas en un estado predeterminado si el funcionamiento normal no se puede mantener debido a un ataque	X	X	X	X
SR 3.7	Identificar y manejar las condiciones de error de manera que pueda ocurrir una reparación efectiva.		X	X	X
SR 3.8	Proteger la integridad de las sesiones, el sistema de control debe reachazar cualquier uso de ID no valido en sesión.		X	X	X
RE (1)	Invalidar los ID de sesión al cerrar la sesión del usuario al finalizar otra sesión (incluidas las sesiones del navegador).			X	X
RE (2)	Generar un ID de sesión único para cada sesión y tratar todos los ID de sesión inesperados como inválidos.			X	X
RE (3)	Generar ID de sesión únicos con fuentes de aleatoriedad comunmente aceptadas.				X
SR 3.9	Proteger la información de auditoría y las herramientas de auditoría (si están presentes) del acceso, modificación y eliminación no autorizada		X	X	X
RE (1)	Producir registros de auritoría en medios de escritura única reforzados por hardware.				X
FR 4	***Confidencialidad de datos (DC)***	***SL 1***	***SL 2***	***SL 3***	***SL 4***
SR 4.1	Proteger la confidencialidad de la información para la que se admite una autorización de lectura explícita, ya sea en reposo o en tránsito	X	X	X	X
RE (1)	Proteger la confidencialidad de la información en reposo y las sesiones de acceso remoto que atraviezan una red que no es de confianza.		X	X	X
RE (2)	Proteger la confidencialidad de la información que atraviesa cualquier límite de zona.				X
SR 4.2	Purgar toda la información para la que se admite autorización de lectura explicita de los componentes que se liberarán en servicio activo y/o se darán de baja.		X	X	X
RE (1)	Evitar la transferencia no autorizada o involuntaria de información a través de recursos de memoria compartida volatil.			X	X
SR 4.2	Utilizar algoritmos criptográficos, tamaños adecuados de clave y mecanismos para el establecimiento y la administración de claves.	X	X	X	X
FR 5	***Flujo de datos restringido (RDF)***	***SL 1***	***SL 2***	***SL 3***	***SL 4***
SR 5.1	Segmentar logicamente las redes de sistemas de control de redes de sistemas sin control y segmentar lógicamente las redes de sistemas de control críticos de otras redes de sistemas de control.	X	X	X	X
RE (1)	Segmentar físicamente las redes del sistema de control de las que no lo son, y segmentar físicamente segmentar las redes de control critico de las redes de sistemas de control no críticos.		X	X	X
RE (2)	Proporcionar servicios de red para controlar las redes del sistema, críticas o no, sin una conexión a las redes del sistema sin control.			X	X
RE (3)	Aislar lógica y físicamente las redes de sistemas de control críticas de las redes de sistemas de control no cíticas.				X
SR 5.2	Monitorear y controlar las cominicaciones en los límites de las zonas para hacer cumplir la compartimentación definida en el modelo de conduits y zonas basado en riesgos.	X	X	X	X
RE (1)	Denegar el tráfico de red de forma predetermiada y permitir el tráfico de red por excepción (tambien denominado denegar todo, permitir por excepción).		X	X	X
RE (2)	Evitar cualquier comunicación a través del límite del sistema de control cuando haya una falla operativa de los mecanismos de protección del límite (tambien denominado cierre por falla)			X	X
RE (3)	Diseñar una funcionalidad de cieere de falla de manera que no interniera con el funcionamiento de un SIS u otras funciones relacionadas con la seguridad.			X	X
SR 5.3	Evitar que se reciban mensajes de persona a persona de propósito general de usuarios o sistemas externos al sistema de control.	X	X	X	X
RE (1)	Impedir tanto la transmisión como la recepción de mensajes de uso general de persona a persona.			X	X
SR 5.4	Admitir la partición de datos, aplicaciones y servicios según la criticidad para facilitar la implementación de un modelo de zonificación.	X	X	X	X
FR 6	***Respuesta oportuna a eventos (TRE)***	***SL 1***	***SL 2***	***SL 3***	***SL 4***

SR 6.1	Permitir que los humanos autorizados y/o las herramientas accedan a los registros de auditoría en una base de solo lectura.	X	X	X	X
RE (1)	Acceso pragmático a los registros de auditorpia mediante una interfaz de programacion de aplicaciones (API).			X	X
SR 6.2	Supervisar continuamente el rendimiento de todos los mecanismos de seguridad utilizando las prácticas y recomendaciones de la industria de la seguridad comunmente aceptadas para detectar, caracterizar e informar las brechas de seguridad de manera oportuna.		X	X	X
FR 7	***Dispinibilidad de recursos (RA)***	***SL 1***	***SL 2***	***SL 3***	***SL 4***
SR 7.1	Operar en un modo graduado durante un evento de denegación de servicio (DoS)	X	X	X	X
RE (1)	Administrar las cargas de comunicación (como el uso de la limitación de velocidad) para mitigar los efectos de los tipos de eventos DoS que inundan la información.		X	X	X
RE (2)	Restringir la capacidad de todos los usuarios (humanos, procesos de software y dispositivos) para causar eventos DoS que afecten a otros sistemas de control o redes.			X	X
SR 7.2	Limitar el uso de recursos por las funciones de seguridad para evitar el agotamiento de los recursos.	X	X	X	X
SR 7.3	Admitir la identificación y localización de archivos críticos y tener la capacidad de realizar copias de seguridad de la información a nivel de usuario y de sistema (incluida la información de estado del sistema) sin afectar las operaciones normales de la planta	X	X	X	X
RE (1)	Verificar la confiabilidad de los mecanismos de respaldo.		X	X	X
RE (2)	Automatizar la función de respaldo en función de respaldo en función de una frecuencia configurable.			X	X
SR 7.4	Recuperar y reconstruir a un estado seguro conocido despues de una interrupción o falla.	X	X	X	X
SR 7.5	Cambiar hacia y desde una fuente de alimentación de emergencia sin afectar el estado de seguridad existente.	X	X	X	X
SR 7.6	Configurar de acuerdo con las configuraciones de red y seguridad recomendadas como se describe en las pautas proporcionadas por el provedor.El sistema de control debe proporcionar una interfaz para la red actualmente implementada y los ajustes de configuración de seguridad.	X	X	X	X
RE (1)	Generar un informe que enumere la configuración de seguridad implementada actualmente en un formato legible por una maquina.			X	X
SR 7.7	Prohibir escpecificamente y/o restringir el uso de funciones, puertos, protocolos y/o servicios innecesarios.	X	X	X	X
SR 7.8	Informar la lista actual de componentes instalados y sus propiedades asociadas.		X	X	X