UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SISTEMA INSTRUMENTADO DE SEGURIDAD PARA

COMPENSADOR ESTÁTICO DE ENERGÍA REACTIVA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

DANIEL ERNESTO MENDIBURU ZEBALLOS

PROMOCIÓN
1985 - I

LIMA – PERÚ
2005

Dedico este trabajo a:
Mis padres, mis modelos de comportamiento,
Mis tías, por el apoyo que siempre me brindaron,
Mi Esposa y mi Hijo, motores de mi vida.

SISTEMA INSTRUMENTADO DE SEGURIDAD PARA COMPENSADOR ESTÁTICO DE ENERGÍA REACTIVA

SUMARIO

El presente trabajo trata del diseño de un Sistema Instrumentado de Seguridad para un Compensador Estático de Energía Reactiva. Las normas y tecnología para los Sistemas Instrumentados de Seguridad, disponibles en la actualidad, permiten mejorar la seguridad en los sistemas potencialmente peligrosos, como el Compensador Estático de Energía Reactiva.

En el capítulo I se describe los componentes y operación de un Compensador Estático de Energía Reactiva, y se plantea la necesidad de mejorar la seguridad diseñando un Sistema Instrumentado de Seguridad. El capítulo II se refiere a las normas y definiciones utilizadas para Sistemas Instrumentados de Seguridad. En el capítulo III se procede al diseño del Sistema Instrumentado de Seguridad, desde el análisis del riesgo, hasta el cálculo de la probabilidad de falla. En el capítulo IV se hace una evaluación de costo inicial y costo anual del sistema.

ÍNDICE

PRÓLOGO

Los procesos industriales se han vuelto más eficientes y confiables gracias a los sistemas de automatización. Los procesos automatizados van desde los pequeños y simples, como el control de nivel en un tanque, hasta más grandes y complejos, como una refinería de petróleo.

Los procesos no sólo deben ser automatizados sino que también deben mantenerse en condiciones de seguridad, para que no se produzca daño a personas, equipos, instalaciones o medio ambiente. Los sistemas de seguridad se utilizan para disminuir el riesgo de daño. Para procesos pequeños y simples se puede utilizar relés, pero cuando los procesos son más grandes y complejos es más conveniente utilizar sistemas instrumentados de seguridad programables.

Los controladores lógicos programables (PLCs) fueron diseñados para reemplazar a los relés, pero no para trabajar en aplicaciones de seguridad crítica. Ante la necesidad de utilizar sistemas programables, los fabricantes han desarrollado PLCs de seguridad, con características de falla segura. También se han desarrollado

normas para sistemas programables de seguridad a partir de la última década del siglo XX.

En la actualidad se cuenta con varias arquitecturas de sistemas programables de seguridad, y diferentes métodos de diseño para estos sistemas, teniendo como marco de referencia las normas ya existentes.

Los sistemas instrumentados de seguridad, al igual que sus normas, están en constante actualización, para mejorar sus prestaciones. También es necesario modificar los sistemas de seguridad, en función de los cambios que se den en el proceso industrial, en el cual se está disminuyendo el riesgo.

El presente trabajo pretende dar una visión de los sistemas instrumentados de seguridad, y mostrar la aplicación de un método de diseño aplicado a un compensador estático de energía reactiva.

CAPÍTULO I

COMPENSADOR ESTÁTICO DE ENERGÍA REACTIVA

El Compensador Estático de Energía Reactiva, a quién nos referiremos como SVC (Static VAR Compensator), tiene como objetivo el regular el voltaje de línea de la red eléctrica de Lima, a nivel de mediana tensión en las barras de 60 kV.

Para regular la tensión, el SVC se comporta como una carga reactiva variable, capacitiva cuando el voltaje de línea baja, e inductiva cuando el voltaje aumenta.

En este capítulo describiremos los componentes del SVC, su operación y la necesidad de un sistema instrumentado de seguridad.

1.1 Descripción de los componentes.

El compensador tiene una variedad de componentes que trabajan desde 60 kVac hasta 24 Vdc. A continuación pasaremos a describir los componentes.

En la figura 1.1 se muestra un diagrama multifilar del compensador de energía reactiva, donde podremos ubicar los componentes del sistema.

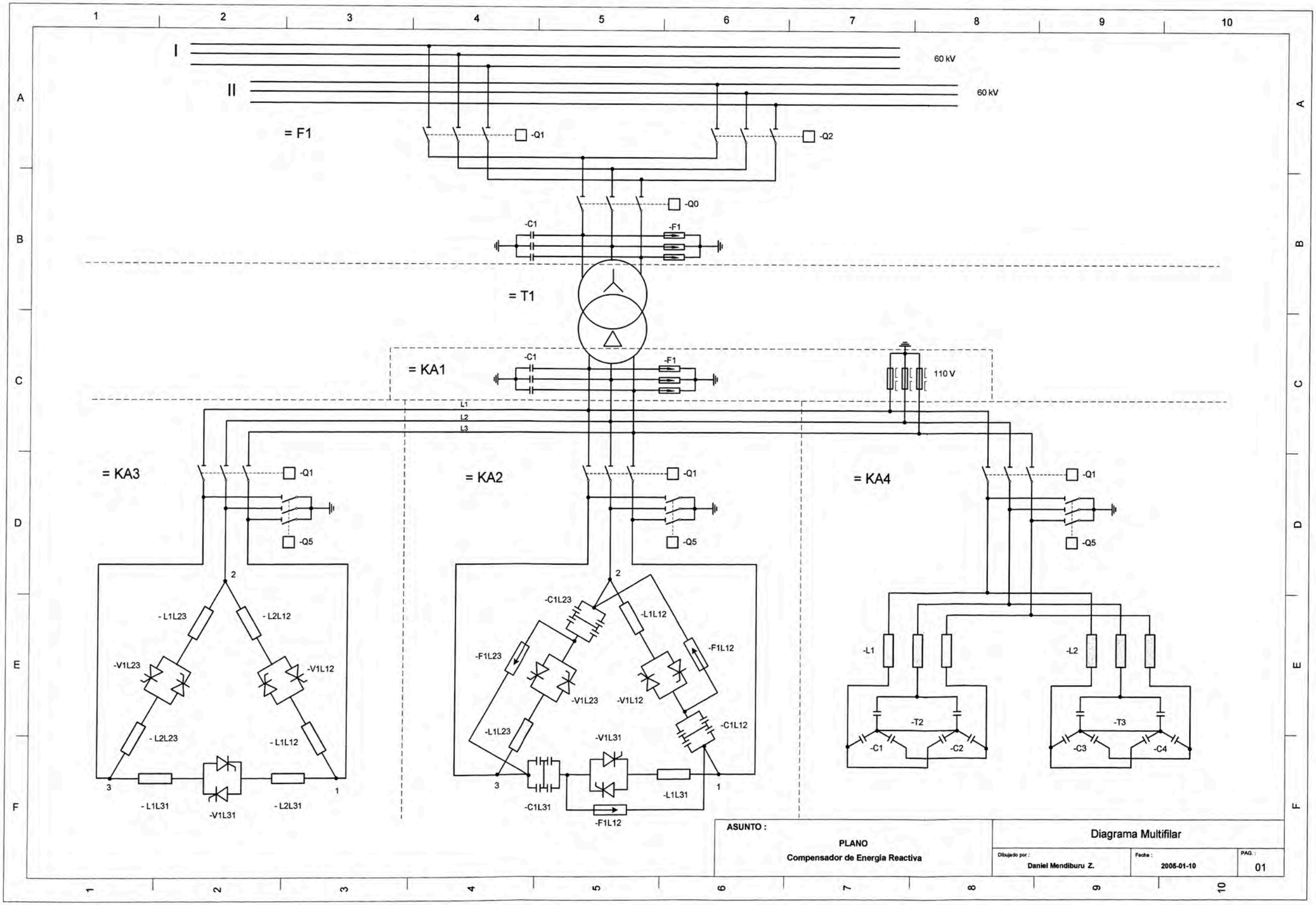


Figura 1.1: Compensador Estático de Energía Reactiva

1.1.1 Interruptor, Seccionadores y Transformadores.

Para seleccionar la conexión a una de las ternas de 60 kV se utilizan el seccionador = F1-Q1 y el seccionador = F1-Q2. Para que el compensador funcione se debe cerrar el interruptor = F1-Q0.

Para reducir el voltaje para las cargas reactivas se utilizan tres transformadores monofásicos conectados en estrella / delta.

1.1.2 Elementos Reactivos.

El compensador tiene tres bancos de cargas reactivas:

- Banco fijo de condensadores (FC: Fixed Capacitor): en la zona = KA4, que siempre están conectados.
- Banco conmutable de condensadores (TSC: Thyristor Switching Capacitor): en la zona = KA2, cuya conexión o desconexión es realizada a través de válvulas de tiristores. Las válvulas de tiristores son arreglos de tiristores para poder trabajar con corriente en ambas direcciones y mayor voltaje.
- Banco controlado de inductancia: (TCR Thyristor Controlled Reactor): en la zona = KA3, se comporta como una carga inductiva variable al variar el ángulo de disparo de las válvulas de tiristores.

Para poder trabajar con corriente bi-direccional las válvulas de tiristores están formadas por pares de tiristores en anti-paralelo, y para trabajar a mayor voltaje se colocan en serie estos pares de tiristores.

En cada uno de estos tres bancos hay seccionadores de tierra (–Q5) y seccionadores de línea (-Q1). Los de tierra sirven para descargar la energía reactiva cuando el compensador no está operando, y los de línea para conectar las cargas reactivas.

1.1.3. Sistemas de control.

Los sistemas de control para el PLC son dos:

- Regulador automático de voltaje (AVR: Automatic Voltage Regulator): encargado de calcular el ángulo de disparo del TCR, y la conexión o desconexión del TSC, en función del voltaje en 60 kV.
- Control On-Off: encargado de verificar las condiciones de arranque del compensador, de la secuencia de arranque y de la secuencia de parada. Este sistema también se encarga de la parada de emergencia.

1.1.4 Servicios Auxiliares.

Hay dos servicios auxiliares.

- Sistema de refrigeración: permite refrigerar a los tiristores, para ello se controla la temperatura, y se monitorea la conductividad del agua que absorbe el calor generado en los tiristores del TSC y TCR. En la figura 1.2 se muestra el sistema de refrigeración donde se identifica el tanque de expansión, las dos bombas, los tres ventiladores, y las válvulas TSC y TCR,
- Cargador de baterías que alimenta a un banco de baterías de 120 Vdc para asegurar que los sistemas de control estén siempre alimentados, a pesar que se pierda la alimentación de corriente alterna.

1.1.5 Protección Eléctrica.

La protección eléctrica ha sido diseñada para que el SVC trabaje dentro de sus límites de corriente, voltaje y frecuencia, si se excede algún límite se produce una parada normal, y de ser necesario una parada de emergencia.

Se usan relés de protección para sub-frecuencia, sobrevoltaje, sobre-corriente, corriente de neutro, diferencial de corriente y falla a tierra.

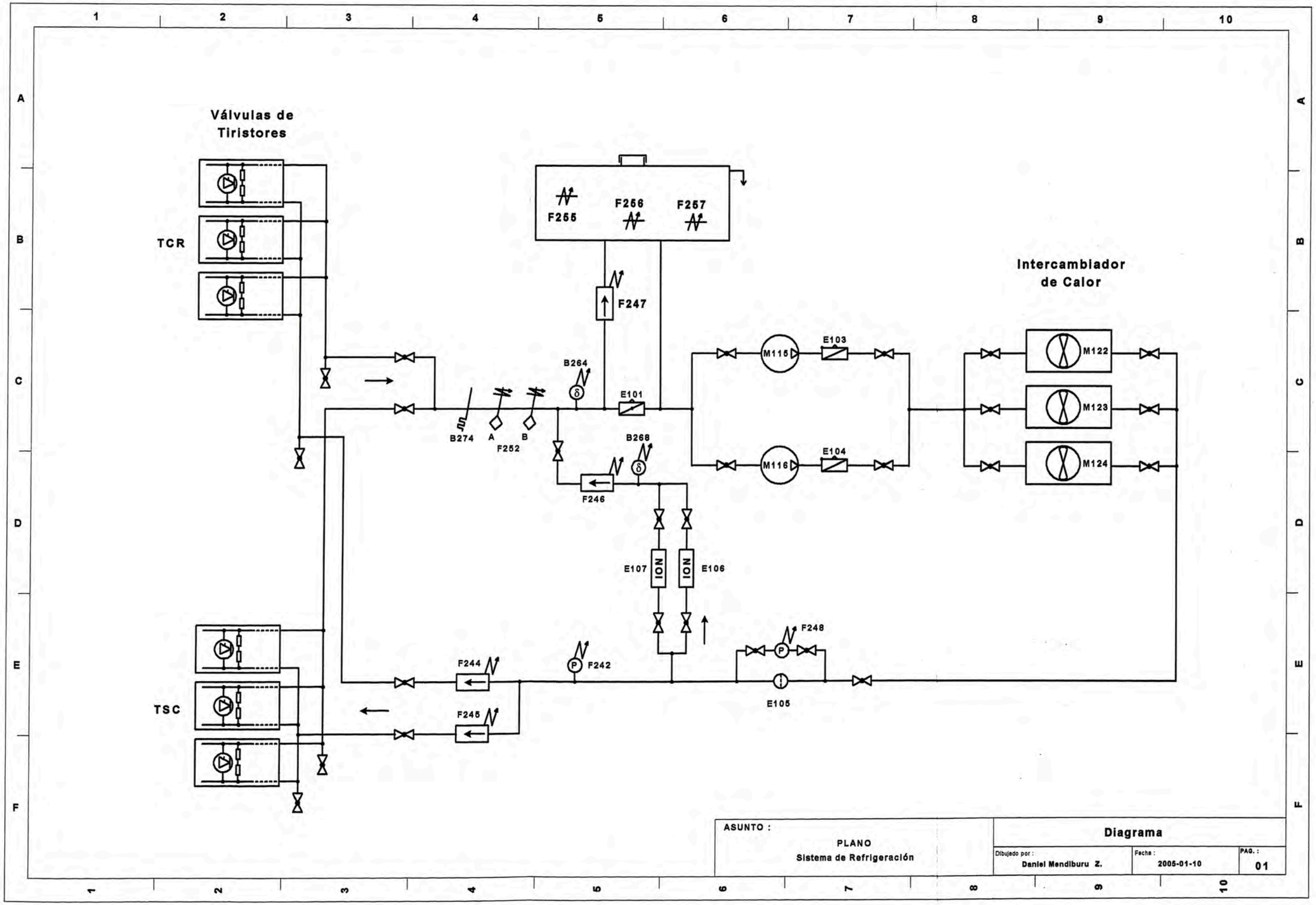


Figura 1.2: Sistema de Refrigeración de Tiristores.

1.2 Operación del Compensador de Energía Reactiva.

El SVC puede trabajar en modo automático y en modo manual, el cambio entre estos dos modos se realiza en el regulador automático de voltaje (AVR).

En modo automático el compensador mantiene constante la tensión, para lo cual su reactancia varía en forma continua controlando el ángulo de disparo del TCR, si es necesario mayor energía capacitiva se conecta el TSC.

En modo manual se puede modificar la reactancia del compensador, cambiando el ángulo de disparo del TCR.

1.2.1 Preparación previa al arranque.

Para que el compensador pueda operar se necesita realizar unos pasos previos al arranque que se describirán a continuación:

Poner el selector de Atendido/ No atendido en Atendido.

Verificar que las lámparas de estado estén indicando una condición normal.

Verificar que las lámparas de estado "Tiristores Bloqueados" del TSC y TCR estén encendidas.

Verificar que las lámparas de alarma estén apagadas.

Abrir uno a uno los seccionadores de tierra, y cerrar uno a uno los seccionadores de línea de media tensión de las cargas reactivas.

Cerrar el seccionador de barras de 60 kV seleccionado.

Después de todos los pasos enumerados debe encenderse la lámpara "Listo para Arranque". El compensador se encuentra listo para arrancar.

1.2.2 Arranque.

Después de seguir la secuencia de preparación para el arranque, y estar encendida la lámpara "Listo para Arranque", cerrar el interruptor de 60 kV.

La válvula TCR es desbloqueada y tomará la potencia de la rama FC, para tener una energía reactiva total igual a 0 MVAR.

Luego se pulsa los botones "Arrancar" y "Ejecutar" y el compensador variará su energía reactiva hasta que su voltaje alcance el valor de referencia al que ha sido ajustado, con lo cual termina el arranque.

1.2.3 Parada.

Para parar al compensador se pulsa los botones "Parar" y "Ejecutar".

El compensador comienza a disminuir su energía reactiva hasta llegar a 0 MVAR.

Cuando está en 0 MVAR se puede abrir el interruptor.

La parada que se ha descrito corresponde a una parada normal NSD (Normally Shut Down).

En caso de un peligro inminente como incendio, inundación o atentado, se puede realizar en forma manual una parada de emergencia ESD (Emergency Shut Down), para lo cual se cuenta con pulsadores rojos tipo hongo en los tableros local, remoto y centro de despacho.

1.3 Necesidad del Sistema de Seguridad.

Para evitar el daño al compensador y al personal que lo opera o mantiene, es necesario implementar un sistema de seguridad.

Los enclavamientos de seguridad que tiene el compensador son controlados en la actualidad por el sistema denominado "Control On-Off". Este sistema es de tecnología de mediados de los 80's del siglo XX. En esa época no se habían desarrollado las normas, ni los equipos para sistemas de seguridad que existen en la actualidad. La seguridad de sistemas complejos como el compensador está encomendada a PLC o controladores con prestaciones similares, como es el caso del "Control On-Off" del compensador.

En la actualidad existen Sistemas Electrónicos Programables PES (Programmable Electronic Systems), como los PLCs de Seguridad, que incorporan funciones de autodiagnóstico, prueba de circuitos de entrada y salida, redundancia de etapas. Las ventajas del PLC de Seguridad permiten aumentar la seguridad y la disponibilidad de los equipos que estamos controlando.

La evolución no sólo se ha dado en PES sino también en la metodología para diseñar un sistema de seguridad. Los nuevos sistemas y las metodologías ya se vienen aplicando en nuestro país en refinerías de petróleo, turbinas de generación y plantas de gases.

El "Control On-Off" del compensador es un sistema cerrado, que no puede ser modificado con facilidad, ni tampoco puede integrarse a un sistema de supervisión. El sistema instrumentado de seguridad que se propone tiene las herramientas para poder configurarlo y supervisarlo con software HMI/ SCADA disponible en el mercado.

Por las ventajas mencionadas, seguridad, disponibilidad, cumplimiento de las normas, mantenimiento de software del sistema, integración con sistemas de supervisión es necesario diseñar un sistema de seguridad instrumentado para el compensador de energía reactiva.

CAPÍTULO II

SISTEMAS INSTRUMENTADOS DE SEGURIDAD

Los sistemas instrumentados de seguridad mejoran la seguridad y disponibilidad del proceso que está siendo controlado. Para diseñar e implementar estos sistemas es necesario conocer las normas y definiciones utilizadas en ellos.

En este capítulo definiremos el peligro y el riesgo, y veremos como las normas existentes dan distintas categorías al riesgo. Identificaremos la relación entre los SIS y los sistemas de control, se identificarán las capas de protección. Se definirán los niveles de integridad de seguridad, y las distintas arquitecturas que puede tener un SIS . Al final del capítulo se identifica las distintas etapas del ciclo de vida del diseño de un Sistema Instrumentado de Seguridad.

2.1 Peligro y Riesgo.

De acuerdo al AIChE (Instituto Americano de Ingenieros Químicos) el peligro es:

Una característica inherente física o química que tiene el potencial de causar daño en las personas, propiedad o ambiente.

Es la combinación de material peligroso, ambiente de operación, y eventos no planeados que pueden resultar en un accidente.

El riesgo es la combinación de severidad y probabilidad de un evento que causa daño, se evalúa cuan frecuente y cuan dañino es cuando sucede. El riesgo puede ser evaluado cuantitativamente y cualitativamente.

Tal como se ve en la figura 2.1 todo proceso tiene un riesgo inherente. La reducción del riesgo se consigue con la mejora en el diseño del proceso y de su sistema de control, el uso de un Sistema Instrumentado de Seguridad, y otros como personal bien entrenado y capas de mitigación, estas últimas se tratan en la sub-sección 2.4.2.

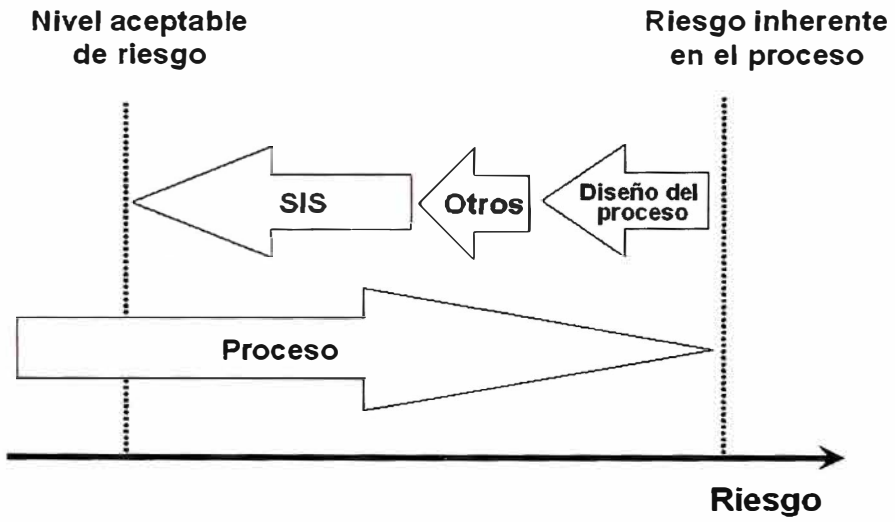


Figura 2.1: Reducción del Riesgo.

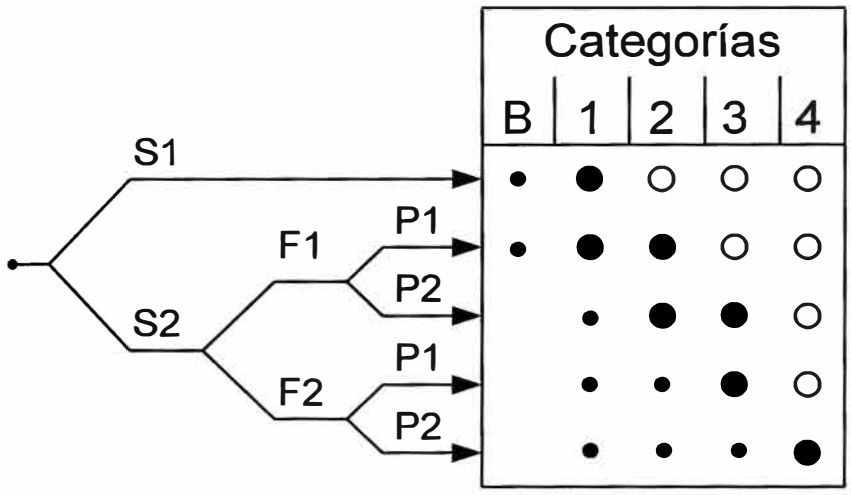
2.2 Normas para Sistemas de Seguridad.

Existen normas norte-americanas y europeas, que utilizan sus propias definiciones y establecen distintas categorías para valorar el riesgo, la normas se exponen a continuación.

2.2.1 EN 954-1. Partes Relacionadas a la Seguridad en los Sistemas de Control. Principios generales para diseño.

Es la norma europea. Cubre las partes relacionadas a la seguridad, estableciendo cinco categorías de valoración del riesgo para el comportamiento de estas partes, las

que reducirán el riesgo total gracias a su tolerancia a fallas. Las categorías las vemos en la figura 2.2.



● Categoría preferida.

• Categoría que necesita medidas adicionales de seguridad.

○ Categoría sobredimensionada para el riesgo.

Figura 2.2: Valoración del riesgo. Norma EN 954.

Donde:

S = Severidad del daño.

S1: Menor, normalmente reversible.

S2: Serio, incluye la muerte.

F = Frecuencia y/o tiempo de exposición al peligro.

F1: Pocas a veces a poco frecuente y/o el tiempo de exposición es corto.

F2: Frecuente a continuo y/o el tiempo de exposición es largo.

P = Posibilidad de evitar el daño.

P1: Posible ante condiciones específicas.

P2: Apenas posible.

De acuerdo a las variables S, F y P los requerimientos para las partes de la categoría B son las menos exigentes, los componentes deben soportar el esfuerzo esperado, pero una sola falla puede hacer que se pierda la función de seguridad. La

categoría 4 es la más exigente, cubre todo los requerimientos de las otras categorías, una sola falla debe ser detectada, y la acumulación de fallas, normalmente 2, no debe hacer que se pierda la función de seguridad.

Esta norma no tiene en cuenta a sistemas donde las funciones de seguridad dependen sólo de PES (Programmable Electronic Systems).

2.2.2 IEC 61508. Seguridad Funcional de Sistemas Eléctricos / Electrónicos / Electrónicos Programables Relacionados con la Seguridad, E/E/PES.

Esta norma tiene siete partes, cubre los aspectos relacionados a la probabilidad de que el sistema tenga una falla peligrosa. El sistema puede tener una combinación de electricidad, electrónica y electrónica programable.

Las siete partes de la norma son:

1. Requerimientos generales.
2. Requerimientos para sistemas Eléctricos / Electrónicos / Electrónicos Programables Relacionados con la seguridad.
3. Requerimientos de Software.
4. Definiciones y Abreviaturas.
5. Ejemplos de métodos para la determinación de los niveles de integridad de seguridad.
6. Pautas para la aplicación de la IEC 61508-2 e IEC 61508-3.
7. Visión general de técnicas y medidas.

Esta norma observa el comportamiento de todo el sistema, y no de las partes individuales.

Se establecen tres áreas de responsabilidad:

- Usuario final.

Contratistas de diseño de ingeniería.

Fabricantes.

Las funciones de seguridad se especifican en términos de:

Funcionalidad, la acción requerida.

Integridad, la probabilidad de que la acción sea ejecutada para lograr la reducción necesaria de riesgo.

Se consideran cuatro niveles de integridad de la seguridad (SIL). Las operaciones del sistema pueden ser clasificadas en modos de operación de baja demanda o de alta demanda a continua. Para baja demanda el objetivo debe ser la probabilidad de falla en demanda (PFD). Para sistema de alta demanda a continua el objetivo debe ser la probabilidad de falla peligrosa (PDF).

Los métodos para determinar el SIL se encuentran en la parte cinco de la norma. Allí se muestran lineamientos para reducción del riesgo, y métodos cuantitativo y cualitativo para la evaluación del riesgo. El método cuantitativo usa los datos del fabricante y tablas. El método cualitativo usa un gráfico similar al de la norma EN 954.

2.2.3 DIN V 19250. Aspectos Básicos de Seguridad para Dispositivos de Protección en Control e Instrumentación.

Es similar al EN 954 al considerar la tolerancia a fallas. En un diagrama de riesgo considera 8 clases de requerimientos (AK: Anforderungsklaseen). Una AK de mayor número es más exigente en los dispositivos para medición y control de la protección. En la figura 2.3 vemos los 8 niveles de AK.

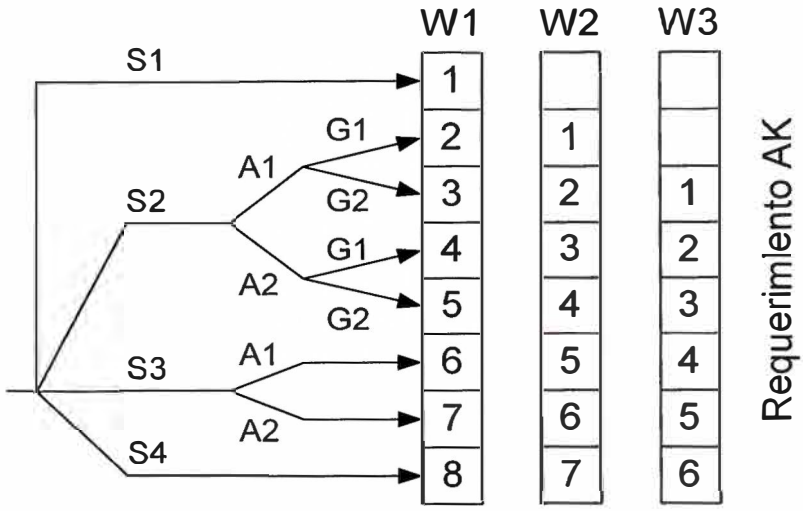


Figura 2.3: Requerimiento AK.

Donde:

S = Severidad del daño.

S1: Menor, normalmente reversible.

S2: Daño serio irreversible o muerte de una persona.

S3: Muerte de varias personas.

S4: Catástrofe, muchas fatalidades.

A = Exposición al peligro.

A1: Pocas veces a poco frecuente.

A2: Frecuente a continuo.

G = Posibilidad de evitar el daño.

G1: Posible.

G2: Apenas posible.

W = Probabilidad de ocurrencia.

W1: Muy baja.

W2: Baja.

W3: Relativamente alta

2.2.4 ANSI/ISA S84.01-1996 Aplicación de Sistemas Instrumentados de Seguridad para Procesos Industriales.

Este estándar ha sido desarrollado con la intención que pueda ser parte de los estándares de la IEC, por lo que su formato y estructura puede diferir de estándares ISA anteriores, tiene como referencia a la norma IEC 61508.

Tiene como objetivo desarrollar las especificaciones de los Sistemas Instrumentados de Seguridad, considera los requerimientos de entradas, funcionalidad de seguridad e integridad de seguridad.

Los requerimientos de entrada se usan para el Análisis de Peligros de Proceso (PHA), requerido para desarrollar las Especificaciones de Requerimientos de Seguridad, se incluye información del proceso, funciones de seguridad y el correspondiente SIL de cada una, consideraciones de falla de causa común, y los requerimientos regulatorios. El SIL debe ser una extensión del análisis de peligros.

Los requerimientos de funcionalidad de seguridad incluyen la definición del estado seguro para cada evento identificado, las entradas del SIS y sus puntos de disparo, las salidas del SIS y sus acciones, la selección del disparo desenergizado o energizado, consideraciones del disparo manual, el tiempo de respuesta del SIS y las interfaces humano máquina.

Los requerimientos de integridad de seguridad incluyen: el SIL de cada función, diagnóstico, mantenimiento y prueba necesarios para el SIL requerido, y los disparos no deseados que pueden ser peligrosos.

La norma ISA no considera dentro del PES a los sensores y actuadores.

En el año 2002 ISA publicó un reporte técnico con fines informativos, ISA-TR84.00.02-2002. Funciones Instrumentadas de Seguridad (SIF) – Nivel de

Integridad de Seguridad (SIL) - Técnicas de Evaluación, no es parte de la norma S84.01.

2.3 Sistema de Control de Procesos y Sistema de Seguridad.

Las funciones de seguridad eran realizadas por sistemas cableados de relés, al aparecer los sistemas de control programables como los PLCs y DCSs algunos pensaban que ellos podían realizar también las funciones de seguridad; sin embargo, las normas siempre han recomendado la separación de los dos sistemas. Se debe entender las diferencias entre los sistemas de control de procesos y el control de seguridad.

Los sistemas de control de procesos son activos, dinámicos, tienen entradas y salidas análogas y lazos de realimentación, si fallan la variable controlada se desvía del valor deseado, no hay falla escondida. Se realizan frecuentes cambios como: rango de variables, setpoint, ajustes de sintonía, se puede poner el control en modo manual.

Los sistemas de seguridad son pasivos, inactivos, no realizan ninguna acción y deseamos que nunca lo hagan. Muchas de las fallas no se auto-revelarán. Una válvula de alivio atorada, una salida con triacs que pueden fallar al energizarlos. Para poder confiar en un sistema que no está actuando se debe hacer pruebas, o el sistema debe ser capaz de auto-probarse. Se necesita un sistema con diagnóstico intensivo, o sistemas con falla segura inherente, las dos posibilidades aumentan el costo, por lo que los sistemas de control no las usan.

Para mejorar la confiabilidad los sistemas de control y los sistemas de seguridad deben ser sistemas separados, tal como se muestra en la figura 2.4.

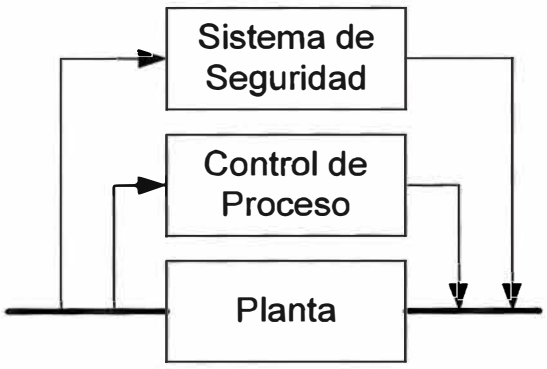


Figura 2.4: Sistemas de Control y de Seguridad.

Distintas instituciones como la AIChE , la IEC, ANSI/ISA, el API, la NFPA , la IEEE recomiendan o exigen la separación de los sistemas de control de proceso de los sistemas de seguridad. La separación disminuye la probabilidad que las funciones de control y de seguridad no estén disponibles al mismo tiempo, o que cambios inadvertidos afecten la funcionalidad del SIS.

También se debe considerar la separación para la comunicación de los dos sistemas u otros equipos. Todos los SIL aceptan que no haya comunicación entre el SIS y el sistema de control u otros equipos, cuando el SIL es más alto se debe asegurar la protección contra escritura de la función de seguridad, el SIL 3 no acepta la no protección o protección limitada de la función de seguridad.

La separación puede ser idéntica o diversa, la separación diversa reduce la probabilidad de fallas sistemáticas y reduce la probabilidad de falla por causa común. Para SIL 1 se puede utilizar el mismo sensor o el mismo actuador para el sistema de control y el SIS, pero el procesador de la lógica debe estar separado.

2.4 Capas de protección.

Los accidentes pueden ocurrir debido a la combinación de eventos que se consideran independientes y que no podrían darse al mismo tiempo, para protegerse contra esa situación se usan múltiples capas de protección. Las capas de protección son de

prevención o de mitigación, las de prevención sirven para evitar que ocurra el daño, mientras que las de mitigación son para contener o disminuir las consecuencias cuando ocurre el daño. En la figura 2.5 se muestran las capas de planta, control de proceso, alarmas y sistema de parada que son de prevención, la capa de fuego y gas es de mitigación.

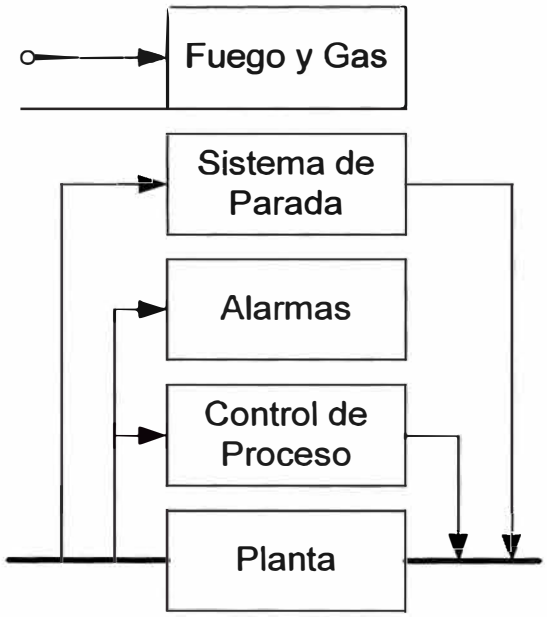


Figura 2.5: Capas de protección.

2.4.1 Capas de Prevención.

La planta es diseñada teniendo en cuenta la seguridad. Por eso se realizan los estudios de HAZOP (estudios de Peligro y operatibilidad), árboles de falla, lista de comprobación, entre otros. Se busca el diseño de plantas inherentemente seguras. Las plantas seguras pueden tener un costo inicial mayor, pero tienen un menor costo de propiedad a lo largo de su vida.

Eliminar o reducir los peligros conlleva generalmente a un diseño más simple, que reduce el riesgo. La alternativa es agregar equipo de protección, que añade complejidad al diseño.

El sistema de control de proceso es la segunda capa de protección, realiza el control para lograr el óptimo uso de la materia prima, consumo de la energía y asegurar la calidad, así como mantener las variables del proceso en un rango seguro. Largos periodos de monitoreo pasivo por parte de los operadores, puede hacer que no estén preparados para actuar ante una emergencia, una solución a este problema es involucrarlos en el análisis de la seguridad y decisiones de diseño.

Los sistemas de alarmas se usan para alertar a los operadores cuando el sistema de control falla. Los sistemas de alarma deben detectar los problemas lo más rápido posible, a un nivel lo suficientemente bajo para que se pueda hacer una acción correctiva antes que se alcancen niveles peligrosos. Deben ser independientes de los sistemas que están monitoreando, si los sistemas monitoreados fallan los sistemas de alarmas no deben fallar. Deben ser lo menos complejos posible, y fáciles de mantener, comprobar y calibrar.

Los sistemas de parada de emergencia actúan cuando falla el sistema de control o los operadores no logran corregir las fallas. Estos sistemas suelen tener completamente separados sus propios sensores y actuadores. Requieren un nivel de seguridad mayor para prevenir cambios inadvertidos y alteraciones, y un nivel mayor de diagnóstico.

2.4.2 Capas de Mitigación.

Cuando el sistema de seguridad falla, los sistemas de fuego y gas son usados para mitigar o disminuir las consecuencias del daño. Estos sistemas pueden ser sólo de alarma, donde se espera que el grupo contra incendios actúe y apague el fuego. Los sistemas pueden tomar acción de control o pueden estar integrados al sistema de parada.

Una diferencia que suele darse entre los sistemas de parada y los de fuego y gas, es que los primeros suelen ser normalmente energizados, des-energizándose cuando se da la parada, los de fuego y gas son normalmente des-energizados, energizándose cuando actúan. Esto se debe a que los sistemas de fuego y gas son diseñados para proteger equipos y personas, la operación no deseada de estos equipos puede destruir piezas del equipo o inclusive muertes, si los sistemas fueran normalmente energizados estas fallas serían muy probables.

Los sistemas de contención evitan que el daño se extienda, como los diques que existen alrededor de los tanques de combustible.

Los procedimientos de evacuación son usados en caso de catástrofes, para evacuar al personal, e inclusive a la comunidad.

En la figura 2.6 se ve en mayor detalle las capas de protección y las capas de mitigación.

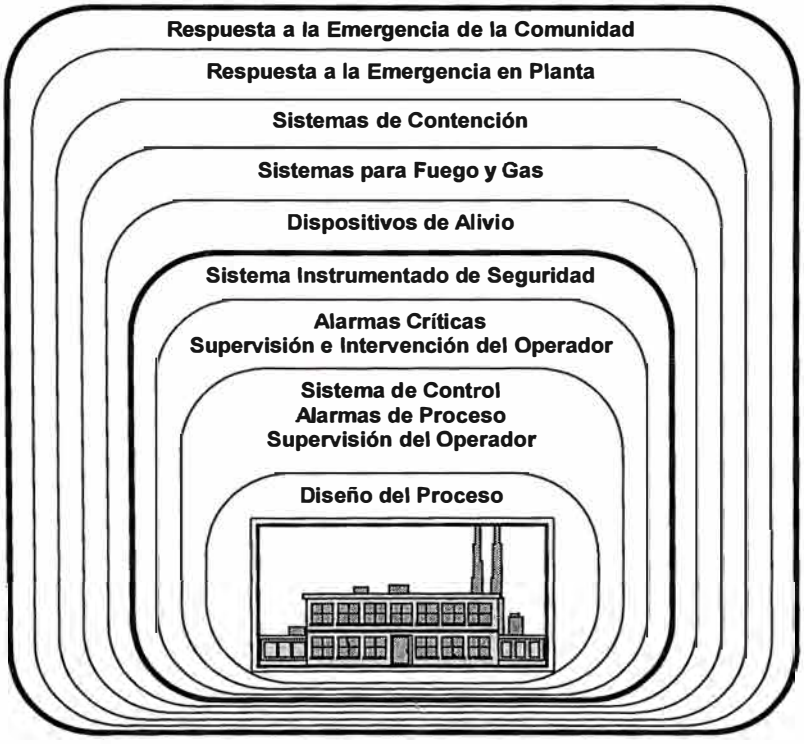


Figura 2.6: Capas de prevención y de mitigación.

2.5 Modos de Falla.

Todo elemento del SIS puede fallar, la probabilidad de que no falle se denomina disponibilidad, la probabilidad de falla es el complemento de la disponibilidad tal como se muestra en la figura 2.7.

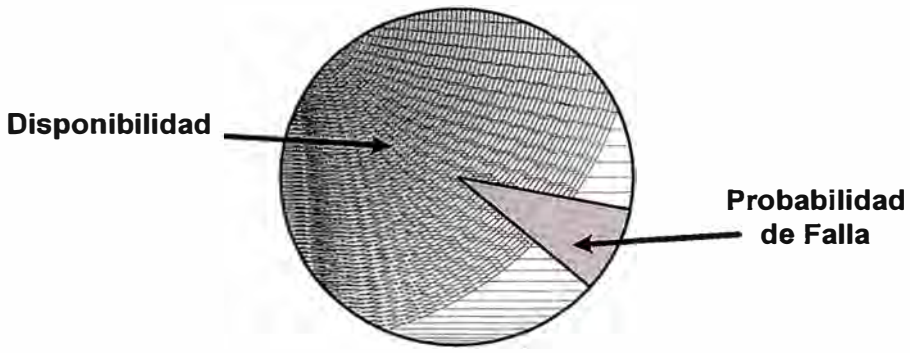


Figura 2.7: Disponibilidad y Probabilidad de Falla.

Las fallas se dividen en fallas seguras y fallas peligrosas. Todas las fallas que pueden hacer que el proceso pare sin una demanda del proceso se denominan fallas seguras, por estas fallas se ejecuta un disparo no deseado o espurio. Todas las fallas que pueden hacer que la función de seguridad falle al responder ante una demanda del proceso se denominan fallas peligrosas.

Las fallas detectadas en línea cuando el SIS está operando se denominan fallas detectadas. Las fallas no detectadas en línea cuando el SIS no está operando se denominan fallas no detectadas. La detección de las fallas depende de las funciones de diagnóstico del elemento del SIS.

Las fallas pueden dividirse en cuatro categorías mutuamente excluyentes como se muestra en la figura 2.8:

- SD: Seguras detectadas.
- SU: Seguras no detectadas.
- DD: Peligrosas detectadas.

- DU: Peligrosas no detectadas.

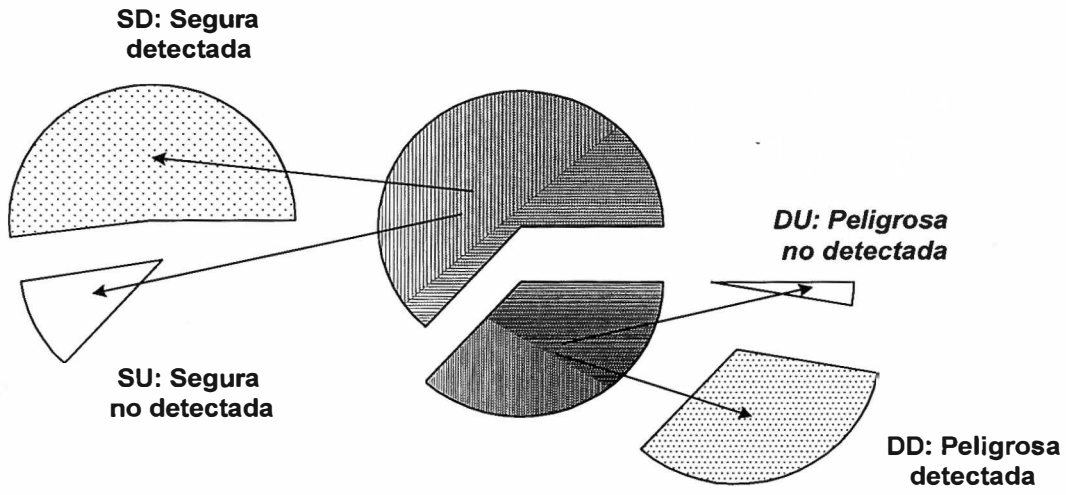


Figura 2.8: Fallas Seguras y Peligrosas.

Las relaciones entre las razones de falla se muestran a continuación:

$$\lambda^{S} = \lambda^{SD} + \lambda^{SU} \tag{2.1}$$

$$\lambda^{D} = \lambda^{DD} + \lambda^{DU} \tag{2.2}$$

Si consideramos un factor de cobertura de diagnóstico C, para fallas seguras y para fallas peligrosas podemos expresar:

$$\lambda^{SD} = \lambda^{S}\, C^{S} \tag{2.3}$$

$$\lambda^{SU} = \lambda^{S}\left(1 - C^{S}\right) \tag{2.4}$$

$$\lambda^{DD} = \lambda^{D}\, C^{D} \tag{2.5}$$

$$\lambda^{DU} = \lambda^{D}\left(1 - C^{D}\right) \tag{2.6}$$

La razón de fallas peligrosas no detectadas (λ^{DU}) disminuye considerablemente de acuerdo al factor de cobertura del diagnóstico (C^{D}).

2.6 Nivel de Integridad de Seguridad.

Es un nivel discreto para especificar los requerimientos de integridad de funciones instrumentadas de seguridad que se utilizan en un SIS. Los niveles considerados por la norma IEC 61508 son cuatro, la norma ANSI/ISA S84.01-1996 considera sólo tres niveles, y la norma DIN V 19250 ocho niveles AK. Un nivel con un número más alto tiene mayor integridad.

En la siguiente tabla se muestra los rangos disponibilidad, PFD promedio y factor de reducción del riesgo de acuerdo al nivel SIL.

Tabla 2.1: SIL

Nivel de Integridad de Seguridad	**1**	**2**	**3**
Requerimientos de Perfomance SIS	Rango de Disponibilidad de Seguridad		
	0,9 a 0,99	0,99 a 0,999	0,999 a 0,999 9
	Rango PFD promedio		
	10^{-1} a 10^{-2}	10^{-2} a 10^{-3}	10^{-3} a 10^{-4}
	Rango Factor de Reducción del Riesgo		
	10 a 100	100 a 1 000	1 000 a 10 000

La probabilidad de falla en demanda (PFD), es la probabilidad de que una función instrumentada de seguridad falle de manera que no pueda realizar la función deseada de seguridad ante una demanda. Generalmente se expresa como PFD_{avg}, que es el valor promedio a lo largo del intervalo de prueba, y es utilizado para definir el SIL. El PFD depende de la arquitectura del SIS, tanto de los elementos de campo

como de los procesadores de lógica, también se debe tener en cuenta la calidad de los elementos. El factor de reducción del riesgo (RRF) es la inversa del PFD_{avg}.

En la figura 2.9 se muestra la equivalencia entre las normas y la reducción del riesgo.

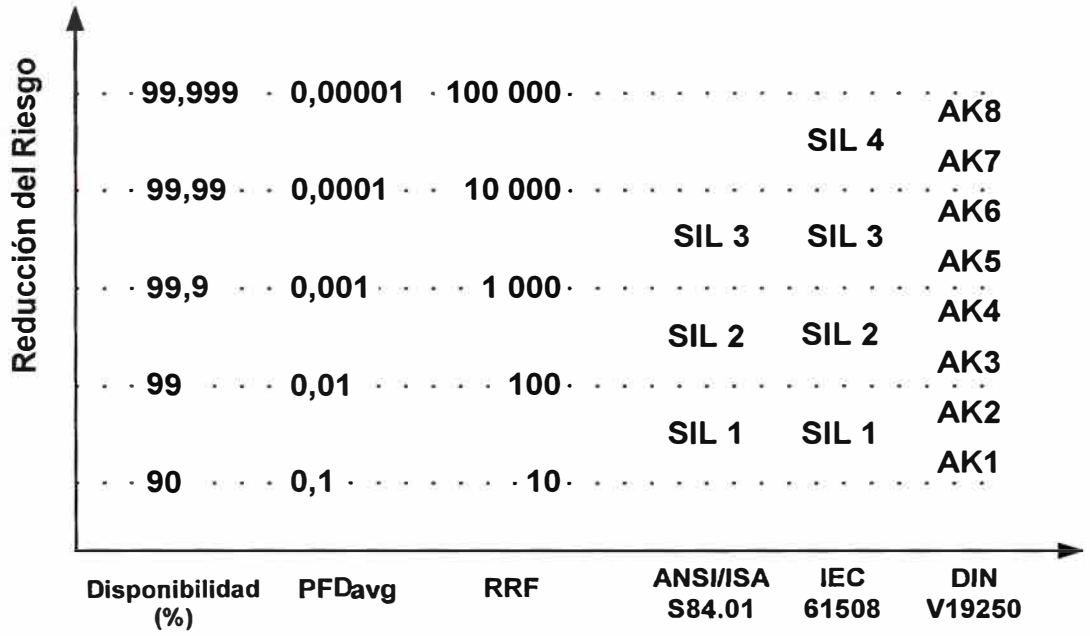


Figura 2.9: Reducción de Riesgo y Normas.

2.7 Arquitecturas.

Un SIS está formado por sensores, procesadores de lógica y elementos finales de control, como se ve en la figura 2.10. Los sensores pueden ser: detectores, sensores o transmisores; los procesadores de lógica pueden ser relés, lógica de estado sólido, o sistemas programables; los elementos finales de control pueden ser: interruptores, o válvulas solenoides.

Figura 2.10: Arquitectura SIS.

Para que el sistema sea tolerante a fallas para una misma función instrumentada de seguridad se utilizan arquitecturas redundantes, resistencia a causas comunes y extenso diagnóstico.

La redundancia mejora la tolerancia a fallas y puede mejorar el SIL, se debe determinar los requerimientos de redundancia para lograr el nivel SIL y disponibilidad requeridos tanto en los sensores, como en los procesadores de lógica y actuadores. La redundancia puede implementarse con uno a tres sensores, de uno a tres procesadores de lógica, y uno o dos elementos finales de control. Estas posibilidades nos lleva a tener sistemas 1oo1 (1 out of 1), 1oo2, 2oo2, 2oo3, 1oo1D (1oo1 con diagnóstico), 1oo2D, las que se muestran en las siguientes páginas.

La redundancia diversa de sensores puede darse con un sensor discreto y un sensor analógico, si se utilizan dos sensores analógicos existe la ventaja de la comparación. La correcta operación del sensor discreto sólo se puede comprobar con una prueba o bajo demanda del proceso.

En las figuras siguientes se muestran distintas arquitecturas en los procesadores de lógica, para ejecutar la parada de emergencia el contacto de salida debe abrirse. La figura 2.11 muestra un sistema 1oo1 como se da en un PLC convencional.

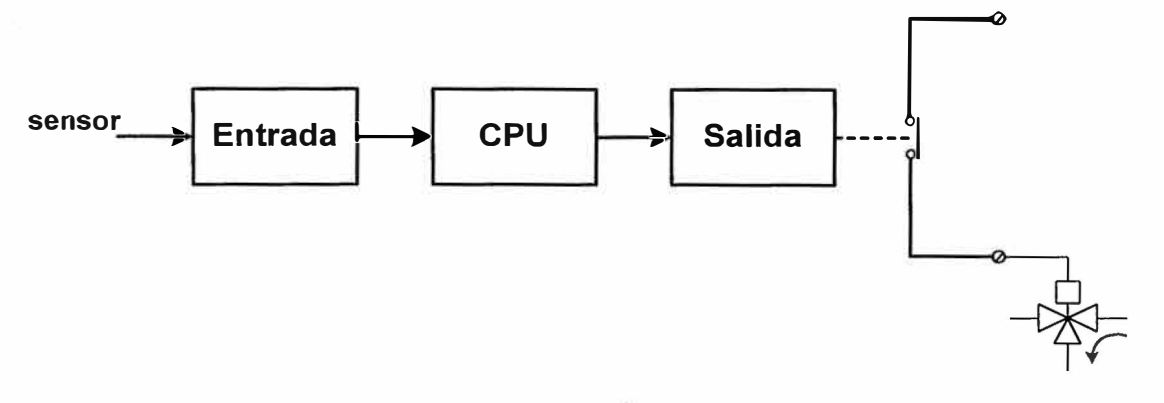


Figura 2.11: Arquitectura 1oo1 en procesador de lógica.

En la figura 2.12 se muestra una arquitectura 1oo2 que nos proporciona alta seguridad pero baja disponibilidad, porque la probabilidad de falla peligrosa es pequeña y la probabilidad de disparo no deseado es grande.

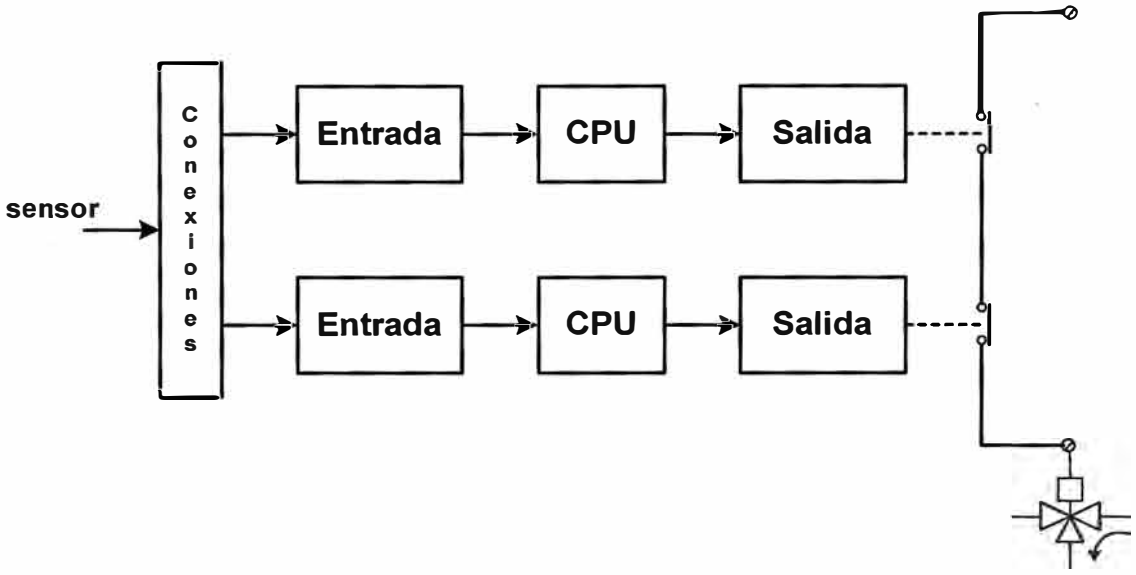


Figura 2.12: Arquitectura 1oo2 en procesador de lógica.

La figura 2.13 se muestra una arquitectura 2oo2 que nos proporciona baja seguridad pero alta disponibilidad.

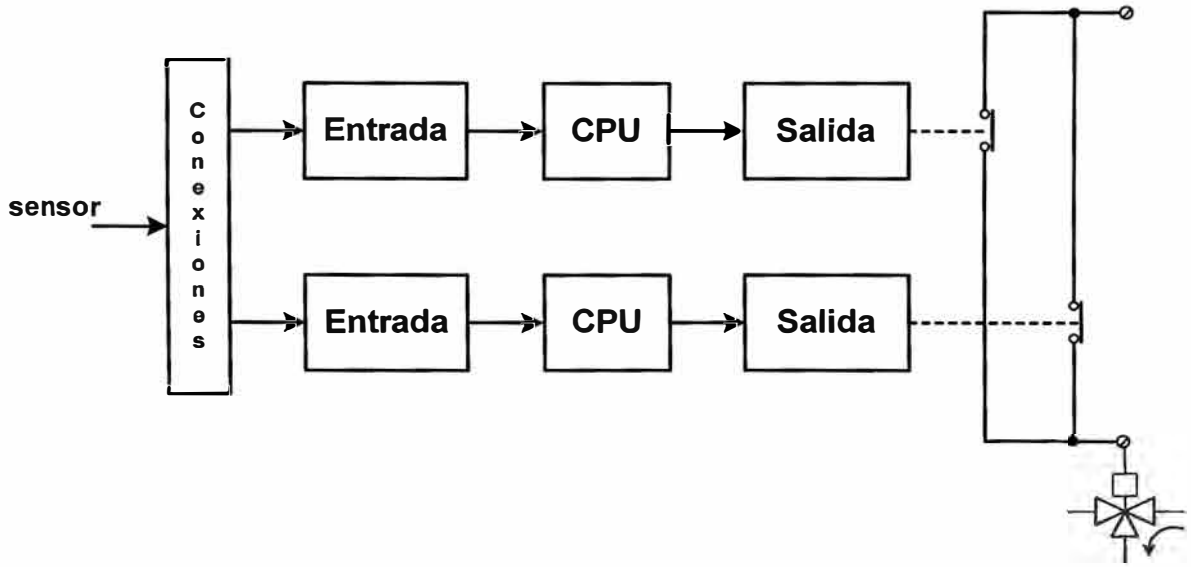


Figura 2.13: Arquitectura 2oo2 en procesador de lógica.

En la figura 2.14 se muestra una arquitectura 2oo3 que nos proporciona alta seguridad y alta disponibilidad, pero con una mayor complejidad. Esta arquitectura también es conocida como Triple Modular Redundant (TMR).

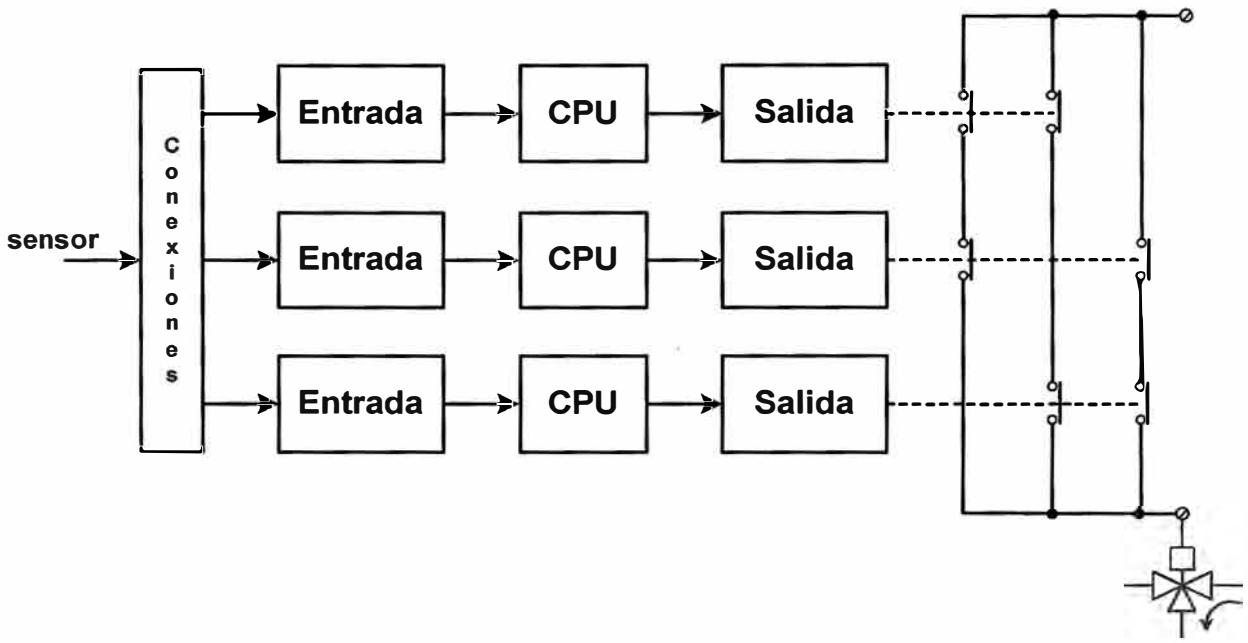


Figura 2.14: Arquitectura 2oo3 en procesador de lógica.

En la figura 2.5 se muestra una arquitectura 1oo1D que nos proporciona mejor seguridad que la arquitectura 1oo1. Esta arquitectura tiene un segundo canal de disparo controlado por el circuito de diagnóstico, de manera que si se detecta una falla peligrosa, el segundo canal es abierto para ejecutar la parada del proceso.

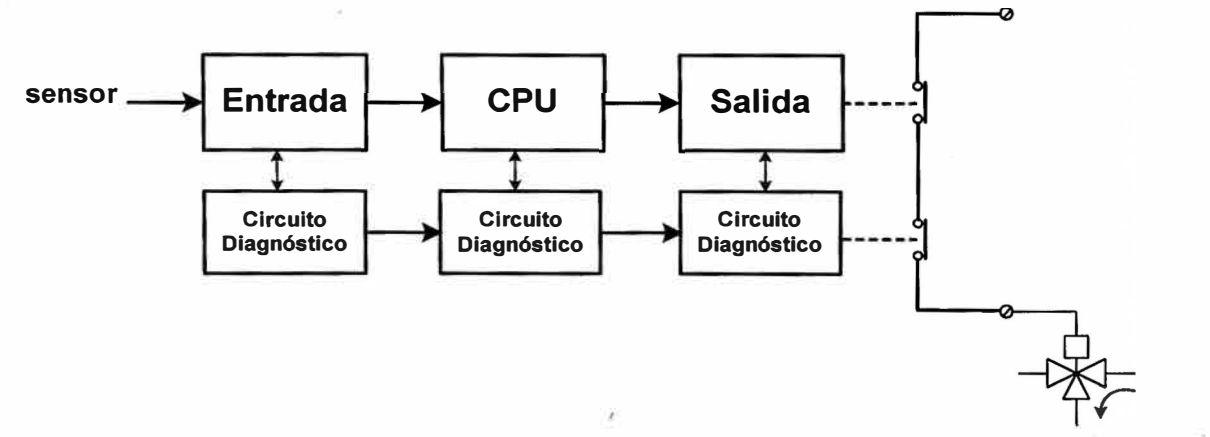


Figura 2.15: Arquitectura 1oo1D en procesador de lógica.

En la figura 2.16 se muestra una variante de la arquitectura 1oo1D, usa dos CPUs para mejorar el PFD total del procesador de lógica.

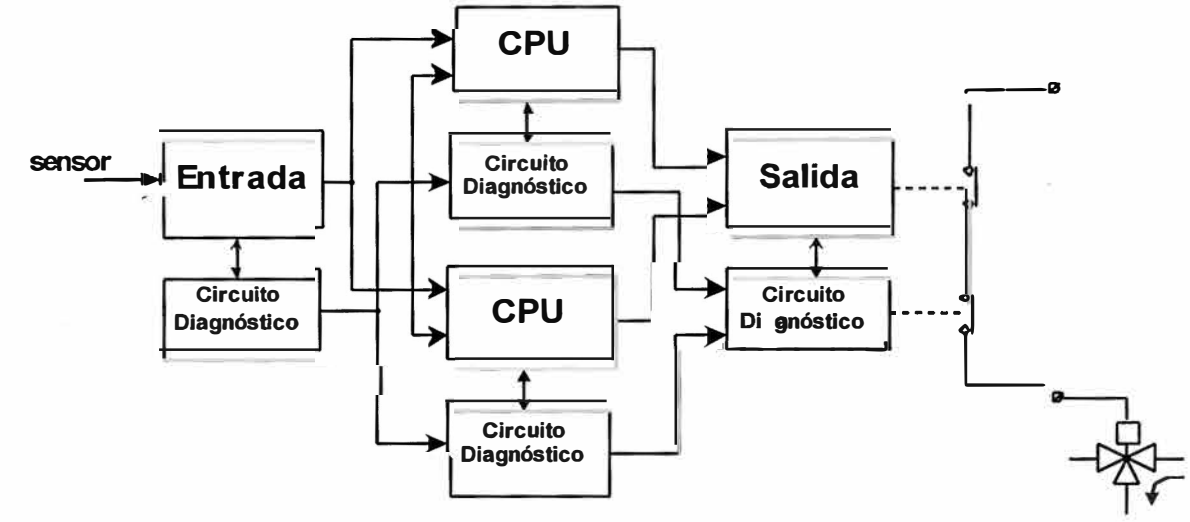


Figura 2.16: Arquitectura 1oo1D en procesador de lógica con redundancia de CPU.

En la figura 2.17 se muestra una arquitectura 1oo2D que nos proporciona alta seguridad y alta disponibilidad, pero con menor complejidad que un TMR. Si se detecta una falla en uno de los dos lados del sistema, el otro lado mantiene el control y por lo tanto la disponibilidad.

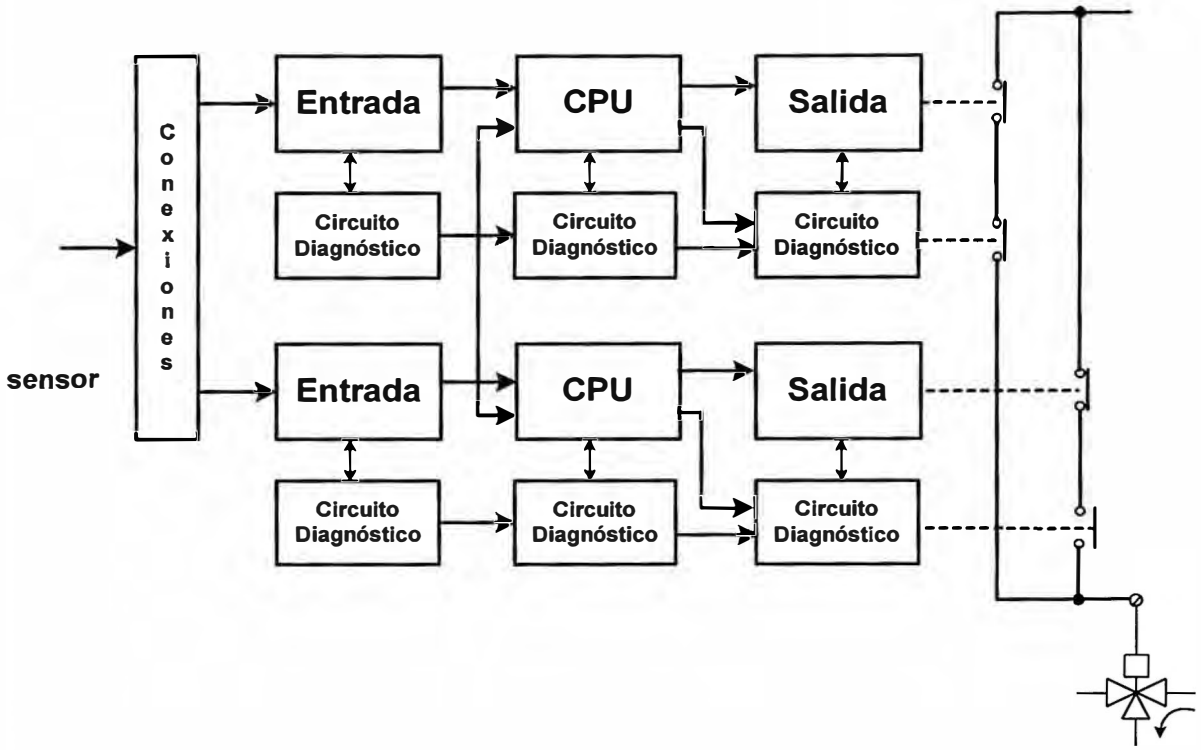


Figura 2.17: Arquitectura 1oo2D en procesador de lógica.

La figura 2.18 muestra un SIS con transmisores de presión 1oo2, procesador de lógica 1oo2 y válvulas solenoides 1oo2.

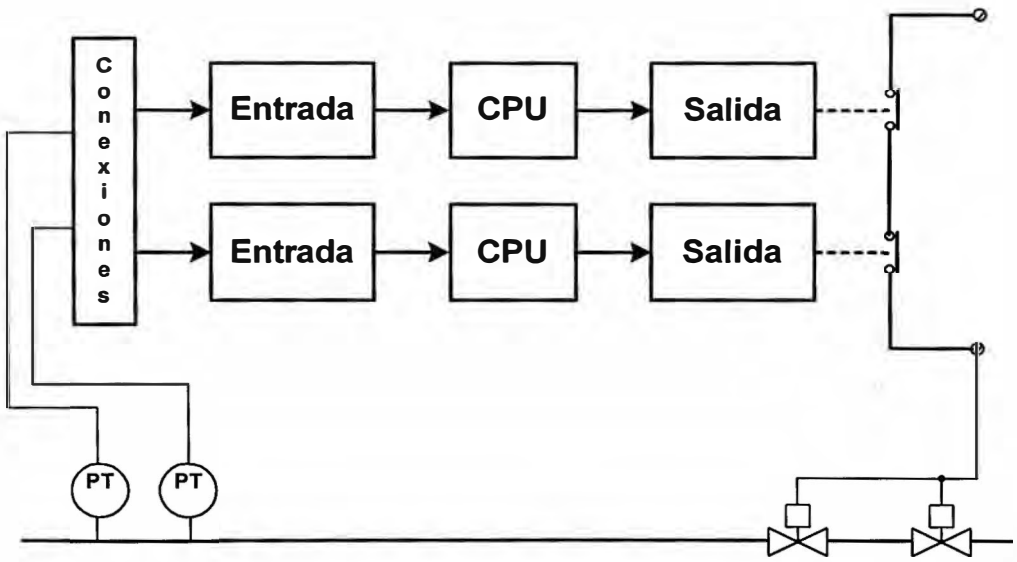


Figura 2.18: Arquitectura 1oo2.

En la tabla 2.2 se muestra el MTTF y el PFD_{avg} para las distintas arquitecturas.

Tabla 2.2: MTTF y PFD_{avg}

Arquitectura	**MTTF** **Fallas seguras**	**PFD_{avg}** **Fallas peligrosas**
1oo1	$\frac{1}{\lambda_S}$	$\lambda_D \frac{TI}{2}$
1oo2	$\frac{1}{2\lambda_S}$	$\lambda_D{}^2 \frac{TI^2}{3}$
2oo2	$\frac{1}{2\lambda_S{}^2 MTTR}$	$\lambda_D TI$
2oo3	$\frac{1}{6\lambda_S{}^2 MTTR}$	$\lambda_D{}^2 TI^2$

Donde:

D : Dangerous failure, falla peligrosa.

MTTF: Mean Time to Failure: tiempo promedio entre fallas.

MTTR: Mean Time To Repair: tiempo promedio para reparar.

PFD: Probability of Failure on Demand.

S: Safe failure, falla segura.

TI : Manual Test Interval, Intervalo Manual de Prueba.

TI_a : Intervalo de diagnóstico automático.

$\lambda = 1 / MTBF$: Failure Rate, razón de falla.

El intervalo de prueba no debe ser pequeño, de esa manera se reduce el posible error humano asociado a pruebas muy frecuentes. El intervalo de prueba no debe ser tampoco muy grande para no aumentar el PFD_{avg}.

En la figura 2.19 se muestra la relación entre las distintas arquitecturas y el SIL para diferentes normas.

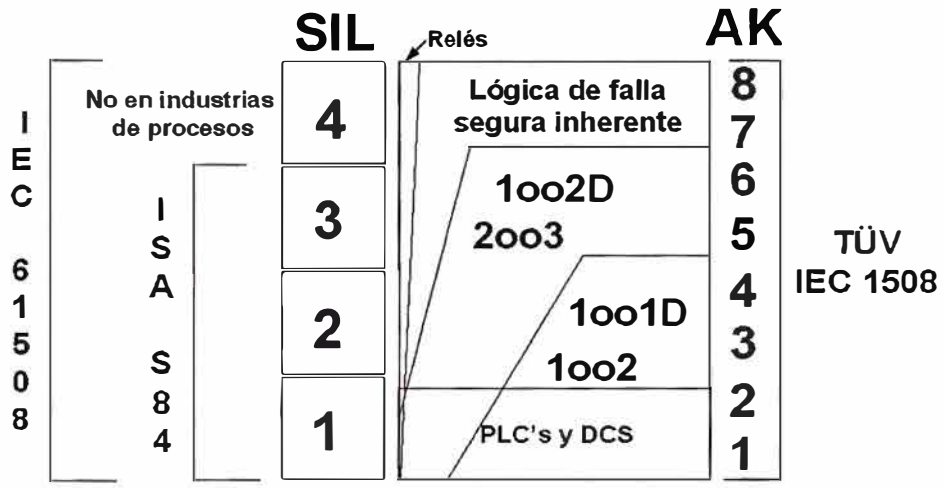


Figura 2.19: Arquitecturas, SIL y normas.

2.8 Ciclo de vida del Diseño.

El modelo del ciclo de vida de diseño del SIS definido por ANSI/ISA-84.01-1996 se muestra en la figura 2.20.

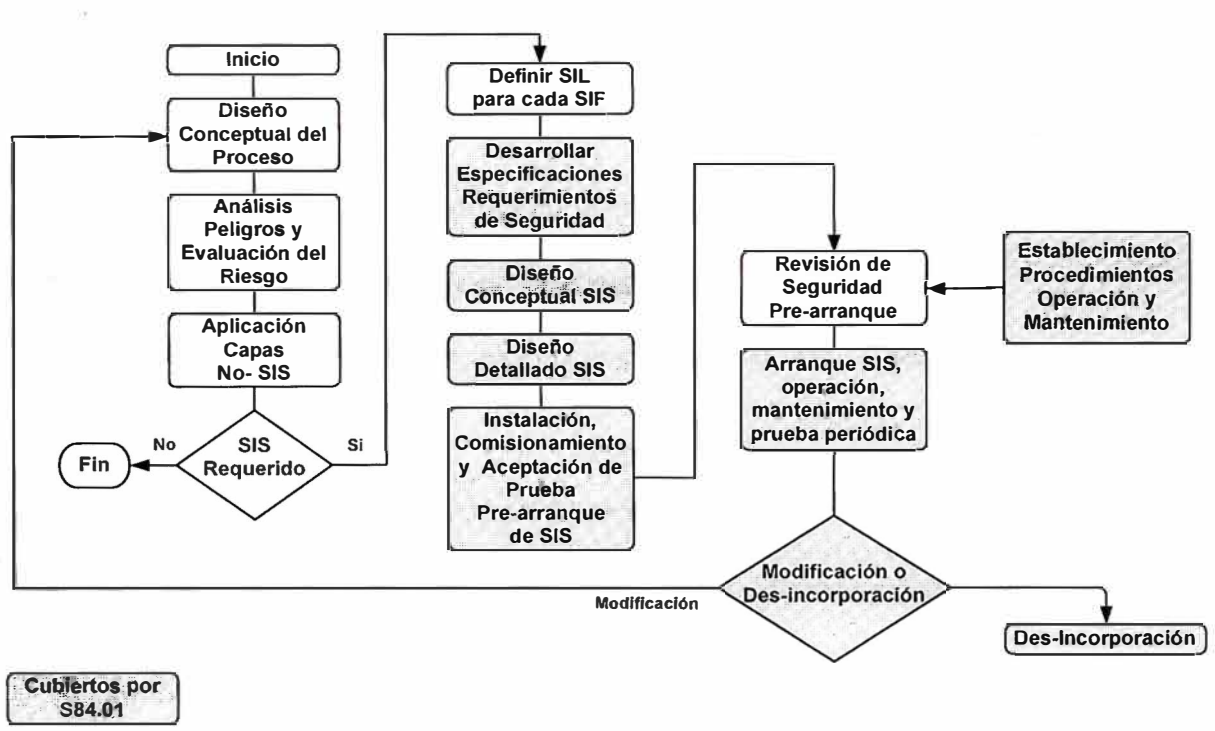


Figura 2.20: Ciclo de vida de diseño de SIS.

2.8.1 Diseño Conceptual del Proceso.

El primer paso es entender el proceso, el equipo, y las condiciones físicas, sociales, políticas y legales para permitir el desarrollo de todo el ciclo de vida. Se debe diseñar una planta segura.

2.8.2 Análisis de los Peligros y Evaluación del Riesgo.

En este paso se debe entender los riesgos que pueden causar daño en el personal, el producto, la maquinaria, el medio ambiente e inclusive la imagen corporativa. El análisis de los Peligros consiste en identificar los peligros utilizando técnicas como: Hazop, árbol de fallas o lista de verificación. La evaluación del riesgo consiste en

darle un rango de riesgo a los peligros identificados, la evaluación se puede hacer con métodos cualitativos o cuantitativos.

2.8.3 Aplicación de Capas no pertenecientes al SIS.

Cuando se han identificado los peligros y evaluado los riesgos, se aplica la tecnología apropiada, y las modificaciones del proceso y equipo para atenuar las consecuencias o disminuir la posibilidad del evento.

2.8.4 Requerimiento de un Sistema Instrumentado de Seguridad.

Se evalúa el efecto de las capas que no pertenecen al SIS, para ver si es necesario utilizar SIS.

2.8.5 Determinación del SIL.

Si el SIS es necesario, se debe determinar el SIL (Nivel de Integridad de Seguridad). Este nivel define la performance necesaria para lograr el objetivo de seguridad. La determinación del SIL se puede hacer con métodos cualitativos o cuantitativos.

En la figura 2.21 se muestra el método cualitativo de Matriz de Riesgo con diferentes Capas de Protección. En los ejes vertical y horizontal se evalúa probabilidad de ocurrencia y la severidad del daño si es que el SIS u otra capa no protegen al sistema.

El tercer eje tiene en cuenta la efectividad de otras capas de protección. Cuando la efectividad aumenta, el SIL del SIS es menor e incluso puede ser que no se requiera. Otra capa de protección puede ser la respuesta del operador.

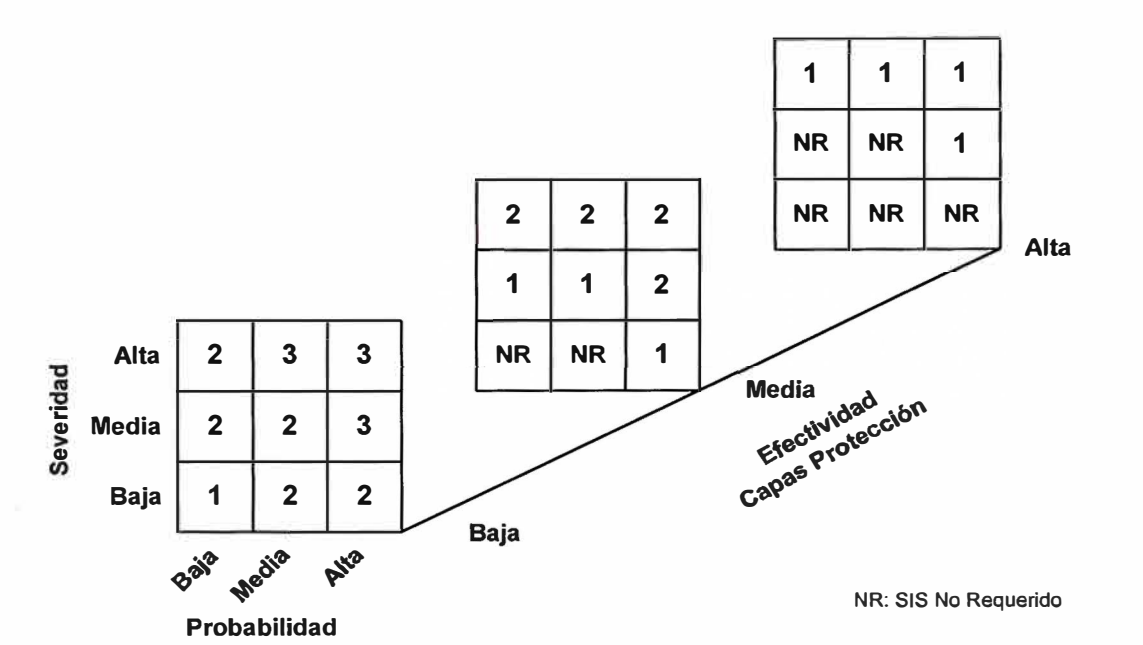


Figura 2.21: Matriz de Riesgo con Capas de Protección.

En el método de Sólo Consecuencias se considera que el evento es probable y sólo se toma en cuenta la severidad del daño.

El método de HAZOP Modificado determina el SIL requerido a partir del HAZOP y teniendo en cuenta la severidad del daño, la probabilidad y otros factores como el costo de mantenimiento.

El método de Árbol de Fallas estima cuantitativamente la frecuencia de ocurrencia. Los árboles de fallas son diagramas lógicos que muestran sistemáticamente secuencias de fallas. Las secuencias comienzan con eventos básicos, como la falla de un sensor o de un actuador, y se muestra el camino a un evento superior que es consecuencia del evento básico, de esta manera se puede estimar la frecuencia del evento superior. Razones de falla y probabilidades condicionales de falla son asignadas a cada evento básico, de manera que a través del árbol de fallas se puede evaluar el impacto en la frecuencia del evento superior de acuerdo al SIL utilizado.

2.8.6 Especificaciones de Requerimientos de Seguridad.

En este paso se definen las funciones lógicas del sistema. Cada función debe tener un SIL asociado, y se debe considerar la confiabilidad con respecto a disparos indeseados. Todas las condiciones deben ser consideradas, desde el arranque hasta la parada, así como el mantenimiento. El sistema será programado y probado de acuerdo a las funciones que se hayan definido.

Se deben considerar las fallas de causa común como corrosión, alimentación, atoramiento.

2.8.7 Diseño Conceptual del SIS.

El diseño debe satisfacer las especificaciones de requerimientos de seguridad. Se debe seleccionar la arquitectura para las funciones de seguridad: 1oo1, 1oo2, 2oo3, etc. Cuando múltiples funciones comparten componentes, los componentes deben satisfacer el SIL más alto. Se debe considerar como causa común a la programación, accesibilidad, mantenimiento, alimentación de energía, prácticas de cableado y seguridad.

2.8.8 Diseño Detallado del SIS.

El objetivo es terminar el diseño y documentarlo. La ingeniería y construcción deben tener procedimientos conservadores para prevenir errores de diseño e implementación. La documentación sirve también para propósitos de revisión. Se debe asegurar la compatibilidad del hardware y software. Se debe considerar un diseño integral del CPU, módulos de entrada y salida, comunicaciones, interfaces de diagnóstico, y software utilitario.

Para los dispositivos de campo se debe monitorear la integridad del circuito, cada dispositivo de campo debe tener su propio cableado a los módulos de entrada y

salida, salvo que múltiples sensores o actuadores monitoreen o sirvan a la misma condición del proceso. Se debe tener protección contra escritura para evitar la modificación no deseada de parámetros.

2.8.9 Instalación, Comisionamiento y Aceptación de Prueba de Pre-arranque de SIS.

El objetivo es asegurar que ha sido instalada de acuerdo al diseño y cumple con las especificaciones de los requerimientos de seguridad. Cualquier modificación en este paso debe llevar a la revisión de los pasos previos afectados.

El comisionamiento asegura que la instalación se ha realizado de acuerdo al diseño detallado, y está listo para la aceptación de la prueba de pre-arranque. Se debe confirmar la instalación de acuerdo a los documentos de detalle de diseño y que se cumple con las especificaciones de requerimientos de seguridad, las tareas a realizar: equipos correctamente cableados e instalados, fuentes de energía operativas, instrumentos calibrados debidamente, dispositivos de campo operativos, procesador y sus entradas y salidas operativos.

2.8.10 PSAT: Prueba de Aceptación de Pre-Arranque.

Es una prueba total de funcionalidad del SIS para demostrar la conformidad con las especificaciones de los requerimientos de seguridad. Se debe confirmar: la comunicación necesaria con el BPCS (sistema básico de control de procesos), funcionamiento de sensores, controladores y elementos finales de control, los dispositivos de seguridad se disparan a los setpoints requeridos, la secuencia adecuada de parada es activada, la parada manual funciona correctamente, el SIS muestra los estados, los bypass funcionan correctamente, el intervalo de prueba está

documentado y los procedimientos de mantenimiento son los requeridos para el SIL, los documentos son consistentes con la instalación actual y los procedimientos.

El documento que confirma la finalización de PSAT debe contener: identificación del SIS que ha sido probado, confirmación que el comisionamiento ha sido completado, fecha en que el PSAT fue realizado, referencia a los procedimientos realizados, y la firma autorizada que indica que el PSAT fue completado satisfactoriamente.

2.8.11 Procedimientos de Operación y Mantenimiento.

El objetivo es asegurar que el SIS cumple las funciones de acuerdo con las especificaciones de los requerimientos de seguridad durante toda su vida operativa.

Los empleados que están involucrados en la operación y mantenimiento deben recibir entrenamiento. El usuario debe tener la documentación adecuada y actualizada.

Los procedimientos de operación deben estar escritos para explicar los métodos correctos y seguros para operar el SIS. Estos procedimientos deben indicar los puntos de disparo de seguridad y las implicancias de sobrepasar estos límites, cómo el SIS lleva a un estado seguro, el uso correcto de los bypasses, reset del sistema, y la respuesta correcta a las alarmas y disparos del SIS.

Se debe establecer un programa de mantenimiento que incluya procedimientos para mantenimiento, prueba y reparación del SIS. Este programa debe incluir el cronograma regular para la prueba funcional del SIS, el cronograma del mantenimiento preventivo, y la reparación de las fallas detectadas, con la correspondiente prueba después de la reparación.

Las pruebas funcionales deben incluir: operación de los dispositivos de entrada considerando los sensores y los módulos de entrada, los setpoints de disparos de las entradas, las funciones de alarma, la operación de la secuencia lógica del programa, funcionamiento de los módulos de salida y de los elementos finales de control, función de la parada manual, función de los diagnósticos, la funcionalidad completa del sistema, y que éste quede operativo después de la prueba.

La descripción de todas las pruebas debe estar documentada, el usuario debe mantener los registros para certificar que las pruebas e inspecciones han sido realizadas. En la documentación se debe incluir: la fecha de la inspección, nombre de la persona que realizó la prueba o la inspección, el número de serie o el identificador único del equipo, resultados de la inspección o prueba "cómo se encontró" y "cómo se dejó".

2.8.12 PSSR: Revisión de Seguridad de Pre-Arranque.

Antes de arrancar el SIS se debe realizar la revisión de seguridad de pre-arranque (PSSR: Pre-Startup Safety Review), debiendo incluir:

Verificación de que el SIS ha sido construido, instalado y probado de acuerdo a las especificaciones de los requerimientos de seguridad.

Los procedimientos de seguridad, operación, mantenimiento, gestión del cambio y emergencia están en su lugar y son los adecuados.

Las recomendaciones de los PHA (análisis de peligros de proceso) han sido resueltas o implementadas.

El entrenamiento del personal en el SIS se ha completado e incluyó la información apropiada.

2.8.13 Arranque del SIS, Operación, Mantenimiento y Prueba Periódica.

Después del PSSR el SIS debe ser puesto en operación, para lo cual se ejecutan los procedimientos de operación y mantenimiento establecidos.

2.8.14 Modificación o Des-incorporación.

Si se proponen modificaciones, la implementación de ellas debe seguir un procedimiento de gestión del cambio (MOC: Management of Change), se deben repetir los pasos del ciclo de vida del SIS para asegurar el manejo del impacto en la seguridad del cambio.

Debe escribirse un procedimiento para iniciar, documentar, revisar el cambio, y aprobar los cambios al SIS. El procedimiento MOC puede necesitarse si se modifica: el procedimiento de operación, el proceso, las especificaciones de los requerimientos de seguridad, legislación nueva o modificada, para arreglar errores del software o del firmware, como resultado de una razón de falla mayor a la esperada.

El procedimiento MOC debe asegurar que las siguientes consideraciones han sido tomadas en cuenta antes de realizar algún cambio: la base técnica del cambio propuesto, el impacto del cambio en la seguridad y la salud, modificaciones en los procedimientos de operación, el tiempo necesario para realizar el cambio, la autorización para el cambio propuesto, la disponibilidad de memoria, el efecto en el tiempo de respuesta, el cambio en línea vs. el cambio fuera de línea y lo riesgos que implica.

La revisión del cambio debe asegurar: que se mantiene la integridad de seguridad requerida, y el personal de las disciplinas apropiadas ha sido incluido.

El personal al cual afectará el cambio debe ser informado y entrenado antes de realizar el cambio.

Todos los cambios en los procedimientos de operación, información de seguridad, y documentación del SIS, incluido el software, deben ser tomados en cuenta y actualizarse. La documentación debe ser protegida de modificaciones no autorizadas, destrucción o pérdida. Todos los documentos del SIS deben ser revisados, corregidos, aprobados y estar bajo el control de un adecuado procedimiento de documentación.

2.8.15 Des-Incorporación.

El objetivo de paso de des-incorporación es asegurar la revisión apropiada antes de retirar permanentemente un SIS. Procedimientos de gestión del cambio deben ser implementados para todas las actividades de des-incorporación. El impacto de la des-incorporación en la operación de unidades relacionadas y servicios debe ser evaluado antes de la des-incorporación.

2.9 Errores en un Sistema de Seguridad.

Un estudio de 34 accidentes, realizado por la British Health and Safety Executive (HSE), identifica los errores cometidos en sistemas de control y seguridad. En la figura 2.22 se ve los resultados del estudio, se aprecia que los errores se dan en distintas etapas del ciclo, no sólo durante la operación y el mantenimiento. En este estudio la mayor parte de los accidentes fueron por causa de especificación incorrecta, y se tiene también un porcentaje significativo en los cambios realizados después del comisionamiento. Los errores cometidos pueden llevar a sobreproteger o sub-proteger el sistema en algunas funciones de seguridad.

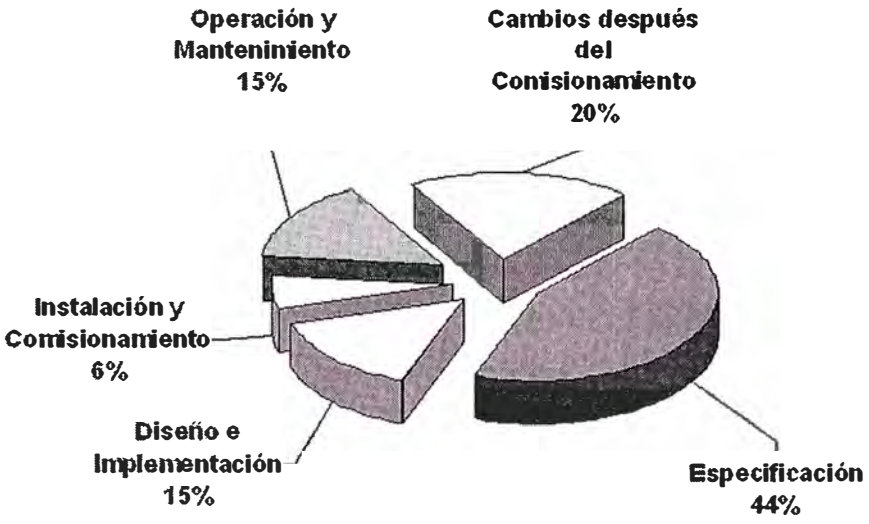


Figura 2.22: Causas de Fallas.

CAPÍTULO III

DISEÑO DEL SISTEMA INSTRUMENTADO DE SEGURIDAD

En este capítulo se diseñará el Sistema Instrumentado de Seguridad. Los pasos a seguir son: análisis HAZOP, definición del SIL para cada función de seguridad, se desarrolla la especificación de los requerimientos de seguridad, se realiza el diseño conceptual y finalmente el diseño detallado.

3.1 Análisis de Riesgo Operacional (HAZOP).

El HAZOP es un análisis sistemático de las desviaciones de los valores de las variables respecto a los valores de diseño, de cuáles son las causas, y como los efectos de estas desviaciones puede resultar en daños

Los objetivos de este análisis son:

- Identificar los riesgos potenciales como son problemas operacionales o fallas de diseño en las instalaciones, para esto se evalúa sistemáticamente los nodos.
- Comprobar rigurosamente la seguridad y operatividad de la instalación.
- Hacer recomendaciones para implementar acciones de previsión o protección ante los riesgos potenciales identificados.

Los alcances que permite el HAZOP son:

- Identificar de las causas de una situación peligrosa o un problema operativo.

- Revisar y actualizar los procedimientos de operación.
- Implementar las recomendaciones, modificaciones y elaborar estudios mas detallados para prevenir, proteger o mitigar ante situaciones peligrosas o problemas de tipo operativo.
- El obtener una operación mas segura, con personal mejor capacitado y conciente de las amenazas potenciales existentes en la operaciones.
- Determinar el SIL necesario para cada riesgo evaluado.

Para realizar el estudio HAZOP se necesita los planos del SVC y del sistema de refrigeración de tiristores.

3. 1.1 Definiciones.

Causas: Son los eventos que originan una desviación, por ejemplo si aumenta la temperatura en la línea de salida de TSC y TCR las causas son:

- Aumento de la temperatura en las válvulas TSC o TCR.
- Disminución del flujo de agua de refrigeración.
- Falla en el intercambiador de calor.

Consecuencias: Son los efectos sobre la operación que pueden determinar la ocurrencia de las causas posibles de desviación. De acuerdo al ejemplo anterior, las posibles consecuencias por el aumento de temperatura en la línea de salida de TSC y TCR las posibles consecuencias son:

- Aumento de la temperatura de TSC o TCR.
- Falla en las válvulas TSC o TCR.

Respuesta del Sistema: Es la respuesta para atender la desviación, tal como alertas o salvaguardas para control, o ante el fallo de algún equipo o error humano. De acuerdo al ejemplo considerado las respuestas pueden ser:

- Alarma por temperatura alta.
- Encendido de ventilador de intercambiador de calor.
- Parada del SVC: ESD o NSD.

Condiciones Peligrosas: Son las que pueden hacer daño al equipo o personal. En nuestro ejemplo pueden ser:

- Sobrecalentamiento de válvula TSC o TCR, que puede originar el quemado de tiristores o un cortocircuito.

3.1.2 Nodos Propuestos

Los nodos propuestos para el análisis HAZOP y las variables a evaluar se muestran en la tabla 3.1.

Tabla 3.1: Nodos propuestos.

		Variables Analizadas										
Nodo	Descripción	V	I	f	P	T	L	F	C	PDT	BOD	NT
1	Interruptor = F1-Q0				X							
2	Transformador = T1. Lado alta.	X	X									
3	Transformador = T1		X		X	X						
4	Transformador = T1. Lado baja.	X	X									
5	Banco FC = KA4-C1 / C2		X	X								
6	Banco FC = KA4-C3 / C4		X	X								
7	Válvula TSC = KA2 - V1L12	X	X							X	X	X
8	Válvula TSC = KA2 - V1L23	X	X							X	X	X
9	Válvula TSC = KA2 - V1L31	X	X							X	X	X
10	Válvula TCR = KA3 - V1L12		X								X	X
11	Válvula TCR = KA3 - V1L23		X								X	X
12	Válvula TCR = KA3 - V1L31		X								X	X
13	Tanque expansión refrigeración						X	X	X			
14	Línea entrada refrigeración TSC y TCR				X							
15	Línea entrada refrigeración TSC							X				
16	Línea entrada refrigeración TCR							X				
17	Línea salida refrigeración TSC y TCR					X		X				
18	Desionizador							X	X			
19	Filtro refrigeración				X							

Donde las variables analizadas son:

C: conductividad.

f: frecuencia.

F: flujo.

I: corriente.

L: nivel.

P: presión.

T: temperatura.

V: voltaje.

PDT: Pérdida de disparo de tiristores.

BOD: disparo del BOD.

N T: Número de tiristores.

3.1.3 Palabras Guía.

Las palabras guía se utilizan para evaluar las desviaciones de la variables de proceso.

En la tabla 3.2 se listan las palabras guías que se utilizarán.

Tabla 3.2: Palabras Guía.

Palabra Guía	Significado	Ejemplo
No	No se obtiene la intención prevista en el diseño.	No Flujo.
Mas	Aumento cuantitativo sobre la intención de diseño.	Más presión.
Menos	Disminución cuantitativa sobre la intención de diseño.	Menos Temperatura.

Las desviaciones se toman en cuenta sólo si afecta la operación del nodo que se esta evaluando, por ejemplo una desviación de menos corriente puede no afectar la operación.

3.1.4 Causas, Consecuencias, Alertas y Salvaguardas.

En la tabla 3.3 se muestra el estudio HAZOP.

Tabla 3.3: (1/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	1			
Linea	Interruptor = F1-Q0			
Variable	Desviacion	Causas	Consecuencias	Alertas-Salvaguardas
Presión	No	Escape del SF6.	No se puede maniobrar el interruptor	Alarma por baja presión. Rellenar SF6.
	Mas	No aplica.	No aplica.	No aplica.
	Menos	Pérdida de SF6.	No se puede maniobrar el interruptor.	Alarma por baja presión y NSD. Rellenar SF6.
Nodo	2			
Linea	Transformador = T1 Lado alta.			
Variable	Desviación	Causas	Consecuencias	Alertas-Salvaguardas
Voltaje	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Sobre tensión en la línea de 60 kV.	Calentamiento del transformador.	Para-rayos =F1-F1. ESD.
	Menos	No aplica.	No aplica.	No aplica.
Corriente	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Sobre-corriente, Corto circuito.	Sobre calentamiento devanados del transformador. Daño en la celda de 60 k V.	Alarma y ESD por sobre-corriente. Alarma y ESD por corriente diferencial.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Desbalance	No	No aplica.	No aplica.	No aplica.
	Mas	Corto circuito. Falla a tierra.	Sobre calentamiento devanados del transformador. Sobre tensiones en fases.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.

Tabla 3.3: (2/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	3			
Linea	Transformador = T1			
Variable	Desviación	Causas	Consecuencias	Alerta-Salvaguarda
Corriente	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Sobre-corriente, Corto circuito.	Sobre calentamiento devanados del transformador.	Relés de sobre-corriente 50 y 51 T y ESD. Relé diferencial 87T y ESD. Relé Buchholz y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Neutro	No	No aplica.	No aplica.	No aplica.
	Mas	Falla a tierra de una o dos fases.	Sobrecorriente en devanado. Desbalance de corriente. Riesgo a personal por potencial en tierra.	Relé de corriente de neutro 51 E y ESD.
	Menos	No aplica..	No aplica.	No aplica..
Temperatura Aceite	No	No aplica.	No aplica.	No aplica..
	Mas	Sobre-corriente. Problemas en el aceite. Falsos contactos.	Deterioro del devanados. Aceite malogrado. Deterioro del contactos.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica..
Presión	No	No aplica.	No aplica.	No aplica..
	Mas	Sobre-corriente. Problemas en el aceite. Falsos contactos.	Deterioro del devanados. Aceite malogrado. Deterioro del contactos.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica..

Tabla 3.3: (3/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	4			
Línea	Transformador = T1. Lado baja			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Voltaje	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Sobre tensión en la línea.	Sobre calentamiento cargas reactivas. Sobre tensión en válvulas de tiristores.	Para-rayos =KA1-F1. Disparo de válvula TCR por BOD y Alarma.
	Menos	No aplica.	No aplica.	No aplica.
Voltaje Diferencial	No	No aplica.	No aplica.	No aplica.
	Mas	Falla a tierra.	Sobre tensión en cargas reactivas. Sobre tensión en válvulas de tiristores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Corriente	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Sobre-carga, Corto circuito.	Calentamiento del transformador.	Alarma y ESD por sobre-corriente. Alarma y ESD por corriente diferencial de barras.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Desbalance	No	No aplica.	No aplica.	No aplica.
	Mas	Corto circuito en cargas reactivas. Falla a tierra en cargas reactivas..	Sobre calentamiento devanados del transformador. Sobre tensiones en fases.	Alarma y ESD por corriente diferencial de barras.
	Menos	No aplica.	No aplica.	No aplica.

Tabla 3.3: (4/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	5			
Línea	Banco FC = KA4-C1 / C2			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Corriente	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Sobre-carga, Corto circuito.	Deterioro de la válvula,. Quemado de las válvula.	Alarma y ESD por sobre-corriente. Alarma y ESD por sobre-voltaje.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Desbalance	No	No aplica.	No aplica.	No aplica.
	Mas	Capacitancia alterada.	Corrientes no uniformes en condensadores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Frecuencia	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Línea de 60 kV con más frecuencia.	Mayor corriente en los condensadores.	No aplica.
	Menos	Línea de 60 kV con menos frecuencia.	Menor potencia reactiva.	AVR. Alarma y ESD.
Nodo	6			
Línea	Banco FC = KA4-C3 / C4			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Corriente	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Sobre-carga, Corto circuito.	Deterioro de la válvula,. Quemado de las válvula.	Alarma y ESD por sobre-corriente. Alarma y ESD por sobre-voltaje.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Desbalance	No	No aplica.	No aplica.	No aplica.
	Mas	Capacitancia alterada.	Corrientes no uniformes en condensadores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Frecuencia	No	Interruptor abierto. Falta de Fluido eléctrico.	El SVC no opera.	No aplica.
	Mas	Línea de 60 kV con más frecuencia.	Mayor corriente en los condensadores.	No aplica.
	Menos	Línea de 60 kV con menos frecuencia.	Menor potencia reactiva.	AVR. Alarma y ESD.

Tabla 3.3: (5/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	7			
Linea	Válvula TSC = KA2 - V1L12			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Voltaje	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre tensión en la línea. Falla disparo de tiristor. Pérdida de tiristor.	Sobre tensión en válvulas de tiristores.	Para-rayos =KA2-F1. AVR. TSC-BOD y Alarma.
	Menos	Baja tensión en la línea.	No aplica.	AVR.
Corriente	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre-carga, Corto circuito.	Deterioro de las válvulas de tiristores. Quemado de las válvulas de tiristores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Desbalance	No	No aplica.	No aplica.	No aplica.
	Mas	Capacitancia alterada.	Corrientes no uniformes en condensadores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Pérdida Disparo Tiristor	No	No aplica.	No aplica.	No aplica.
	Mas	Falla circuito de disparo.	Mala regulación del SVC.	Disparo continuo y ESD.
	Menos	No aplica.	No aplica.	No aplica.
BOD disparo	No	No aplica.	No aplica.	No aplica.
	Mas	Sobretensión en tiristor. Tiristor no dispara.	Deterioro de tiristrores.	Alarma y ESD por sobre-corriente. Supervisión BOD.
	Menos	No aplica..	No aplica..	
Número Tiristores	No	No aplica..	No aplica..	No aplica.
	Mas	No aplica..	No aplica.	No aplica.
	Menos	Tiristor malogrado.	Sobre-tensión en tiristores.	Supervisión de tiristores. Supervisión en el regulador. Alarma y ESD.

Tabla 3.3: (6/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	8			
Línea	Válvula TSC = KA2 - V1L23			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Voltaje	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre tensión en la línea. Falla disparo de tiristor. Pérdida de tiristor.	Sobre tensión en válvulas de tiristores.	Para-rayos =KA2-F1. AVR. TSC-BOD y Alarma.
	Menos	Baja tensión en la línea.	No aplica.	AVR.
Corriente	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre-carga, Corto circuito.	Deterioro de las válvulas de tiristores. Quemado de las válvulas de tiristores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Desbalance	No	No aplica.	No aplica.	No aplica.
	Mas	Capacitancia alterada.	Corrientes no uniformes en condensadores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Pérdida Disparo Tiristor	No	No aplica.	No aplica.	No aplica.
	Mas	Falla circuito de disparo.	Mala regulación del SVC.	Disparo continuo y ESD.
	Menos	No aplica.	No aplica.	No aplica.
BOD disparo	No	No aplica.	No aplica.	No aplica.
	Mas	Sobretensión en tiristor. Tiristor no dispara.	Deterioro de tiristrores.	Alarma y ESD por sobre-corriente. Supervisión BOD.
	Menos	No aplica..	No aplica..	
Número Tiristores	No	No aplica..	No aplica..	No aplica.
	Mas	No aplica..	No aplica.	No aplica.
	Menos	Tiristor malogrado.	Sobre-tensión en tiristores.	Supervisión de tiristores. Supervisión en el regulador. Alarma y ESD.

Tabla 3.3: (7/13) Causas, Consecuencias, Alertas y Salvaguardas

Nodo	9			
Línea	Válvula TSC = KA2 - V1L31			
Variable	Desviación	Causas	Consecuencias	Alerta-Salvaguarda
Voltaje	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre tensión en la línea. Falla disparo de tiristor. Pérdida de tiristor.	Sobre tensión en válvulas de tiristores.	Para-rayos =KA2-F1. AVR. TSC-BOD y Alarma.
	Menos	Baja tensión en la línea.	No aplica.	AVR.
Corriente	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre-carga, Corto circuito.	Deterioro de las válvulas de tiristores. Quemado de las válvulas de tiristores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Corriente Desbalance	No	No aplica.	No aplica.	No aplica.
	Mas	Capacitancia alterada.	Corrientes no uniformes en condensadores.	Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Pérdida Disparo Tiristor	No	No aplica.	No aplica.	No aplica.
	Mas	Falla circuito de disparo.	Mala regulación del SVC.	Disparo continuo y ESD.
	Menos	No aplica.	No aplica.	No aplica.
BOD disparo	No	No aplica.	No aplica.	No aplica.
	Mas	Sobretensión en tiristor. Tiristor no dispara.	Deterioro de tiristrores.	Alarma y ESD por sobre-corriente. Supervisión BOD.
	Menos	No aplica..	No aplica..	
Número Tiristores	No	No aplica..	No aplica..	No aplica.
	Mas	No aplica..	No aplica.	No aplica.
	Menos	Tiristor malogrado.	Sobre-tensión en tiristores.	Supervisión de tiristores. Supervisión en el regulador. Alarma y ESD.

Tabla 3.3: (8/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	10			
Linea	Válvula TCR = KA3 - V1L12			
Variable	**Desviacion**	**Causas**	**Consecuencias**	**Alerta-Salvaguarda**
Voltaje	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre tensión en la línea. Falla disparo de tiristor. Pérdida de tiristor.	Sobre tensión en válvulas de tiristores.	Para-rayos =KA1-F1. TCR-BOD y Alarma.
	Menos	Baja tensión en la línea.	No aplica.	AVR.
Corriente	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre-carga, Corto circuito en bobina.	Deterioro de las válvulas de tiristores. Quemado de las válvulas de tiristores.	Alarma y ESD por sobre-corriente. Alarma y ESD por corriente de neutro.
	Menos	No aplica.	No aplica.	No aplica.
BOD disparo	Mas	Sobretensión en tiristor. Tiristor no dispara.	Deterioro de tiristrores.	Alarma y ESD por corriente de neutro. Supervisión BOD y Alarma.
	Menos	No aplica..	No aplica..	No aplica..
Número Tiristores	No	No aplica..	No aplica..	No aplica.
	Mas	No aplica..	No aplica.	No aplica.
	Menos	Tiristor malogrado.	Sobre-tensión en tiristores.	Supervisión de tiristores. Alarma y ESD por corriente de neutro.

Tabla 3.3: (9/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	11			
Linea	Válvula TCR = KA3 - V1L21			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Voltaje	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre tensión en la línea. Falla disparo de tiristor. Pérdida de tiristor.	Sobre tensión en válvulas de tiristores.	Para-rayos =KA1-F1. TCR-BOD y Alarma.
	Menos	Baja tensión en la línea.	No aplica.	AVR.
Corriente	No	No aplica.	No aplica.	No aplica.
	Mas	Sobre-carga, Corto circuito en bobina.	Deterioro de las válvulas de tiristores. Quemado de las válvulas de tiristores.	Alarma y ESD por sobre-corriente. Alarma y ESD por corriente de neutro.
	Menos	No aplica.	No aplica.	No aplica.
BOD disparo	Mas	Sobretensión en tiristor. Tiristor no dispara.	Deterioro de tiristrores.	Alarma y ESD por corriente de neutro. Supervisión BOD y Alarma.
	Menos	No aplica..	No aplica..	No aplica..
Número Tiristores	No	No aplica..	No aplica..	No aplica.
	Mas	No aplica..	No aplica.	No aplica.
	Menos	Tiristor malogrado.	Sobre-tensión en tiristores.	Supervisión de tiristores. Alarma y ESD por corriente de neutro.

Tabla 3.3: (10/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	12			
Linea	Válvula TCR = KA3 - V1L31			
Variable	**Desviacion**	**Causas**	**Consecuencias**	**Alerta-Salvaguarda**
Voltaje	**No**	No aplica.	No aplica.	No aplica.
	Mas	Sobre tensión en la línea. Falla disparo de tiristor. Pérdida de tiristor.	Sobre tensión en válvulas de tiristores.	Para-rayos =KA1-F1. TCR-BOD y Alarma.
	Menos	Baja tensión en la línea.	No aplica.	AVR.
Corriente	**No**	No aplica.	No aplica.	No aplica.
	Mas	Sobre-carga, Corto circuito en bobina.	Deterioro de las válvulas de tiristores. Quemado de las válvulas de tiristores.	Alarma y ESD por sobre-corriente. Alarma y ESD por corriente de neutro.
	Menos	No aplica.	No aplica.	No aplica.
BOD disparo	**Mas**	Sobretensión en tiristor. Tiristor no dispara.	Deterioro de tiristrores.	Alarma y ESD por corriente de neutro. Supervisión BOD y Alarma.
	Menos	No aplica..	No aplica..	No aplica.
Número Tiristores	**No**	No aplica..	No aplica..	No aplica.
	Mas	No aplica..	No aplica.	No aplica.
	Menos	Tiristor malogrado.	Sobre-tensión en tiristores.	Supervisión de tiristores. Alarma y ESD por corriente de neutro.

Tabla 3.3: (11/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	13			
Linea	Tanque de expansión			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Nivel	No	Se descargó el agua.	Sistema refrigeración sin agua.	Detector por Nivel Muy Bajo redundante F256 y F257 y ESD.
	Mas	No aplica.	No aplica.	No aplica.
	Menos	Evaporación del agua. Fuga de agua.	Mala refrigeración del válvulas de tiristores.	Alarma por Nivel Bajo F255. Detector por Nivel Muy Bajo redundante F256 y F257 y ESD.
Flujo	No	Sistema refrigeración detenido. Bomba detenida. Se descargó el agua.	Quemado de las válvulas de tiristores.	Detector de Flujo F247 y NSD.
	Mas	No aplica.	No aplica.	No aplica.
	Menos	Bomba detenida. Fuga de agua,	Mala refrigeración del válvulas de tiristores.	Detector de Flujo F247 y NSD.
Conductividad	No	No aplica.	No aplica.	No aplica.
	Mas	Desionizador saturado. Agua de relleno conductividad alta.	Corto circuito en válvulas de tiristores.	Detector de Conductividad B264, Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.
Nodo	14			
Linea	Línea entrada refrigeración TSC y TCR			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Presión	No	Bomba detenida. Tubería rota.	Quemado de las válvulas de tiristores.	Presostato F242. Arrancar bomba de reserva. ESD si se mantiene o dos bombas fallan.
	Mas	No aplica.	No aplica.	No aplica.
	Menos	Fuga de agua.	Mala refrigeración del válvulas de tiristores.	Presostato F242. Arrancar bomba de reserva. ESD si se mantiene o dos bombas fallan.

Tabla 3.3: (12/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	15			
Linea	Línea entrada refrigeración TSC			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Flujo	No	Sistema refrigeración detenido. Bomba detenida. Tubería rota.	Quemado de las válvulas de tiristores.	Detector de Flujo F244 y ESD. Presostato.
	Mas	No aplica.	No aplica.	No aplica.
	Menos	Fuga de agua,	Mala refrigeración del válvulas de tiristores.	Detector de Flujo F244 y ESD. Presostato.
Nodo	16			
Linea	Línea entrada refrigeración TCR			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Flujo	No	Sistema refrigeración detenido. Bomba detenida. Tubería rota.	Quemado de las válvulas de tiristores.	Detector de Flujo F245 y ESD . Presostato.
	Mas	No aplica.	No aplica.	No aplica.
	Menos	Fuga de agua,	Mala refrigeración del válvulas de tiristores.	Detector de Flujo F245 y ESD . Presostato.
Nodo	17			
Linea	Línea salida refrigeración TSC y TCR			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Temperatura	No	No aplica.	No aplica.	No aplica.
	Mas	Ventiladores detenidos. Bomba detenida.	Sobrecalentamiento de las válvulas de tiristores.	Detector de temperartura redundante F252 A y B Alarma y ESD.
	Menos	No aplica.	No aplica.	No aplica.

Tabla 3.3: (13/13) Causas, Consecuencias, Alertas y Salvaguardas.

Nodo	18			
Linea	Desionizador			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Flujo	No	Sistema refrigeración detenido. Bomba detenida. Tubería rota.	Quemado de las válvulas de tiristores.	Detector de Flujo F246 y NSD.
	Mas	No aplica.	No aplica.	No aplica.
	Menos	Fuga de agua,	Mala refrigeración del válvulas de tiristores.	Detector de Flujo F246 y NSD.
Conductividad	No	No aplica.	No aplica.	No aplica.
	Mas	Desionizador saturado. Agua con conductividad alta.	Corto circuito en válvulas de tiristores.	Detector de Conductividad B268, Alarma y NSD.
	Menos	No aplica.	No aplica.	No aplica.
Nodo	19			
Linea	Filtro refrigeración			
Variable	Desviacion	Causas	Consecuencias	Alerta-Salvaguarda
Presión Diferencial	No	No aplica.	No aplica.	No aplica.
	Mas	Filtro saturado.	Agua con impurezas.	Presostato Diferencial F248 y Alarma. Cambiar el filtro.
	Menos	No aplica.	No aplica.	No aplica.

3.2 Funciones de Seguridad y SIL

En base al HAZOP se utilizará un método cualitativo para definir el SIL de cada función de seguridad. En la matriz de riesgo de la tabla 3.4 se define el SIL en función de la severidad del daño y la frecuencia de ocurrencia.

Tabla 3.4: Severidad, Probabilidad y SIL.

	Frecuencia		
Severidad	Baja	Media	Alta
Poca	1	2	2
Seria	2	2	3
Grave	2	3	3

La severidad Seria se ha considerado cuando el costo involucrado está entre US$ 10 000 y US$ 100 000, por lo que severidad Poca es cuando el costo es menor de US$ 10 000, y por encima de US$ 100 000 es severidad Grave.

La frecuencia de ocurrencia Media se ha considerado entre 10^{-2}/año y 10^{-1}/año, por lo que frecuencia Baja es menor que 10^{-2}/año, y frecuencia Alta es mayor que 10^{-1}/año.

En la tabla 3.5 se muestra la definición del SIL para cada función de seguridad.

Tabla 3.5: Funciones de Seguridad y SIL.

Función	Descripción	Severidad	Frecuencia	SIL
1	Sobre-voltaje lado alta del transformador.	S	B	2
2	Sub-frecuencia.	P	M	2
3	Sobre-corriente lado de alta del transformador.	G	B	2
4	Diferencia de corriente en transformador.	S	M	2
5	Corriente de neutro primario transformador.	S	M	2
6	Temperatura de aceite en transformadores T1, T2 yT3.	G	B	2
7	Presión en transformador T1, T2 yT3.	G	B	2
8	Falla de tierra en lado baja de transformador.	S	B	2
9	Diferencia corriente barras lado baja.	S	M	2
10	Sobre-corriente temporizado en TSC, grupo A y B.	S	M	2
11	Desbalance de condensadores en TSC.	S	M	2

Tabla 3.5: (continuación) Funciones de Seguridad y SIL.

Función	Descripción	Severidad	Frecuencia	SIL
12	Desbalance de condensadores en FC.	S	M	2
13	Relé de sobre-corriente temporizado en FC.	S	M	2
14	Sobre-corriente temporizado en TCR del grupo A y B.	S	M	2
15	Falla Grupo A de Relés de protección.	G	B	2
16	Falla Grupo B de Relés de protección.	G	B	2
17	Nivel muy bajo en tanque de expansión, redundante.	S	M	2
18	Temperatura muy alta agua salida TSC/TCR A y B.	S	M	2
19	Temperatura muy alta salida TSC/TCR A y B. Ventiladores	S	M	2
20	Conductividad muy alta a la entrada del tanque de expansión.	S	M	2
21	Presión entrada baja TSC y TCR.	S	M	2
22	Presión entrada baja TSC y TCR y Pérdida de 2 bombas.	S	B	2
23	Detector Flujo en entrada TCR.	S	M	2
24	Detector Flujo en entrada TSC.	S	M	2
25	Pulsador Parada de Emergencia Centro de Despacho.	G	B	2
26	Pulsador Parada de Emergencia Panel Remoto.	G	B	2
27	Pulsador Parada de Emergencia Centro Panel Local.	G	B	2
28	No Disponibilidad del AVR.	S	B	2
29	Disparo Continuo de TSC.	S	M	2
30	Falla en válvula TSC.	S	M	2
31	Falla en electrónica de disparo de TSC.	S	M	2
32	Falla en válvula TCR.	S	M	2
33	Falla en electrónica de disparo de TCR.	S	M	2

3.3 Especificación de los Requerimientos de Seguridad.

La especificación de los requerimientos de seguridad nos permite llegar al Diseño Conceptual del SIS y desarrollar el Diseño Detallado. A continuación se definen los distintos requerimientos.

3.3.1 Requerimientos de Documentación y Entrada.

Se requiere los siguientes documentos:

a) Descripción del funcionamiento del SVC.

La descripción del funcionamiento se realizó en el capítulo 1.

En la parte de potencia se debe considerar que sobre-corrientes, sobre-voltajes o fallas a tierra pueden dañar la celda de 60 kV, el interruptor, los seccionadores, los transformadores de potencia, las válvulas de tiristores y los bancos de condensadores y las bobinas. El desbalance de condensadores puede originar una falla en el TSC o en el FC. La sub-frecuencia no permite el correcto control de disparo de los tiristores. Se debe utilizar relés de protección en las distintas zonas de protección, así como detectores de temperatura y presión en el transformador.

Una falla en el sistema de refrigeración de tiristores puede traer como consecuencia la falla o daño de las válvulas de tiristores. Por esto debe monitorearse temperatura, flujo, presión y conductividad en este sistema.

b) Diagramas del SVC y del Sistema de Refrigeración.

Estos diagramas han sido presentados en el capítulo 1: Figura 1.1 (Compensador de Energía Reactiva), y Figura 1.2 (Sistema de Refrigeración de Tiristores).

c) Análisis HAZOP.

El resultado de este análisis ha sido presentado en la sub-sección 3.1.4 (Causas, Consecuencias, Alertas y Salvaguardas).

d) SIL para cada función.

La definición del SIL fué mostrada en la sub-sección 3.2 (Funciones de Seguridad y SIL), habiéndose considerado el SIL 2 para todas las funciones de seguridad.

e) Hoja de datos de los instrumentos.

La compañía propietaria del SVC dispone de las hojas de especificaciones técnicas de todos los sensores, relés de protección e interruptor.

f) Consideraciones por fallas por causa común.

Para que el sistema no quede sin control cuando se pierde la alimentación AC se cuenta con un banco de baterías que alimenta al sistema de control y que alimenta también al SIS.

g) Requerimientos Regulatorios.

Se debe cumplir con las normas internas de la compañía dueña del SVC y las normas nacionales como la referida a la de calidad de la energía eléctrica.

3.3.2 Requerimientos Funcionales de Seguridad.

El SVC está en estado seguro cuando se abre el interruptor =F1-Q0.

a) Entradas al SIS y sus puntos de disparo.

Los relés de protección y sensores tienen definidos sus puntos de disparo desde que el SVC entró en funcionamiento, se han realizado reajustes a los puntos de disparo que han sido documentados.

b) Rango normal de operación.

Los rangos normales de tensión, corriente, energía reactiva, frecuencia, temperatura, conductividad, flujo y presión se encuentran definidos y documentados desde que el SVC entró en funcionamiento. Los cambios que se han dado también han sido documentados.

c) Salidas del SIS y su acción.

El SIS tiene dos salidas para la apertura del interruptor =F1-Q0, dos salidas para el arranque de las bombas del sistema de refrigeración, y tres salidas para el arranque de los ventiladores del intercambiador de calor.

d) Relaciones funcionales entre las entradas y salidas del SIS de proceso.

Si alguno de los relés de protección, los medidores de temperatura o presión en el transformador, o alguno de los detectores considerados en el sistema de refrigeración llegan a su punto de disparo, se da la orden al interruptor para abrir. Si hay pérdida de presión en el sistema de refrigeración, se arrancan las dos bombas. Si la temperatura del sistema de refrigeración es muy alta, se encienden los tres ventiladores del intercambiador de calor.

e) Selección de disparo des-energizado o energizado.

Se usará el disparo energizado.

f) Consideraciones para parada manual.

En caso de un daño inminente para el SVC como de incendio, inundación o atentado u otra situación, se dispone de pulsadores de emergencia ubicados en: panel de control del SVC, en el panel remoto de la sub-estación, y en el centro de despacho.

g) Acción a ser tomada en caso de pérdida de energía.

El banco de baterías permite abrir el interruptor en caso de pérdida de energía. El operador tiene la posibilidad de abrir sub-localmente el interruptor.

h) Tiempo de respuesta para llevar el proceso a estado seguro.

El tiempo de respuesta es adecuado gracias a la velocidad del procesador

i) Acción de respuesta a cualquier falla detectada.

Si el operador advierte una falla puede dar una parada normal o una parada de emergencia desde el centro de despacho, el panel remoto o el panel local de control.

j) Interfaz Humano Máquina.

Alarmas de valores altos en el sistema de Control On-Off.

Capacidad de parada manual.

Alarma de disparo del SIS.

Alarmas de diagnóstico del SIS.

k) Función de Reset.

Si el SIS es disparado, el operador debe pulsar el botón de reconocimiento de alarma y tener las condiciones iniciales de arranque antes de poner en operación el SVC.

3.3.3 Requerimientos de Integridad de Seguridad.

Estos requerimientos incluyen lo siguiente:

a) SIL Requerido.

El requerido es SIL 2 para todas las funciones de seguridad.

b) Mantenimiento y Prueba.

El SIS será inspeccionado una vez por mes y se probará cada 3 meses. Además, si se detecta cualquier problema se procederá a la corrección hasta que la reparación sea completada.

c) Disparos no deseados.

Los disparos no deseados no causan ningún problema relacionado con la seguridad.

3.4 Diseño Conceptual.

Las siguientes consideraciones definen los requerimientos del diseño conceptual para el SIS.

3.4.1 Consideraciones.

En base a la Especificación de los Requerimientos del Seguridad Se tiene en cuenta las siguientes consideraciones:

a) Separación.

El SIS debe estar separado del Control On-Off a excepción del interruptor =F1-Q0.

b) Redundancia.

Se utilizan dos bobinas para abrir el interruptor.

c) Consideraciones de diseño de software.

El PES se configurará utilizando bloques de función, y las funciones de seguridad con la matriz causa – efecto.

d) Selección de Tecnología.

Se utilizará un PES con certificación TÜV.

e) Arquitectura.

De acuerdo al diseño original del SVC y al análisis HAZOP los requerimientos son los siguientes:

Para los sensores se utiliza la arquitectura 1oo1. Para los relés de sobre-corriente de TSC, TCR, y los sensores de temperatura y nivel del tanque de expansión del sistema de refrigeración se utiliza la arquitectura 1oo2. Para el PES se usa la arquitectura 1oo1D.

Para la apertura del interruptor arquitectura 1oo2, y el arranque de las bombas y ventiladores arquitectura 1oo1.

f) Fuentes de alimentación

El PES utiliza una fuente de alimentación de 24 Vdc independiente.

g) Causa común.

Para que el sistema no quede sin control cuando se pierde la alimentación AC se cuenta con un banco de baterías que alimenta al sistema de control y alimentará también al SIS.

h) Dispositivos de campo.

Los dispositivos de campo tienen salida discreta.

i) Interfaz del usuario.

Cuenta con un panel con alarmas, pulsador de parada y pulsador de reconocimiento de alarmas. Hay tres ubicaciones: local, en el panel de control del SVC, remoto, en panel de la sub-estación, y en el centro de despacho. Las alarmas son proporcionadas por el sistema de Control On-Off. El mayor detalle de identificación de alarmas se encuentra en el panel de control del SVC, y el menor detalle en el centro de despacho.

j) Seguridad en el acceso.

El PES debe ser ubicado en la sala de control del SVC.

Los sensores y actuadores de seguridad del SIS deben ser identificados con etiquetas rojas, adicionalmente a la identificación estándar, para que el personal de planta identifique su estado de función de seguridad.

El PES debe tener protección de escritura para evitar cambios inadvertidos.

h) Prácticas de cableado.

El cableado debe hacerse de acuerdo al Código Nacional de Electricidad. Se debe separar la ruta del cableado de alimentación del de señal. Los terminales del SIS deben estar identificados y separados de los terminales del sistema de control, pueden compartir cajas de conexión.

i) Documentación.

La documentación es obligatoria.

g) Intervalo de prueba.

El SIS debe ser probado cada 3 meses.

3.5 Diseño Detallado.

El diseño detallado se hace en función de la Especificación de los Requerimientos de Seguridad y del Diseño Conceptual.

3.5.1 Diagramas de enclavamientos.

De acuerdo a la Especificación de los Requerimientos de Seguridad y del Diseño Conceptual se muestra los diagramas de enclavamientos del SVC y del sistema de refrigeración en las figuras 3.1 y 3.2 respectivamente.

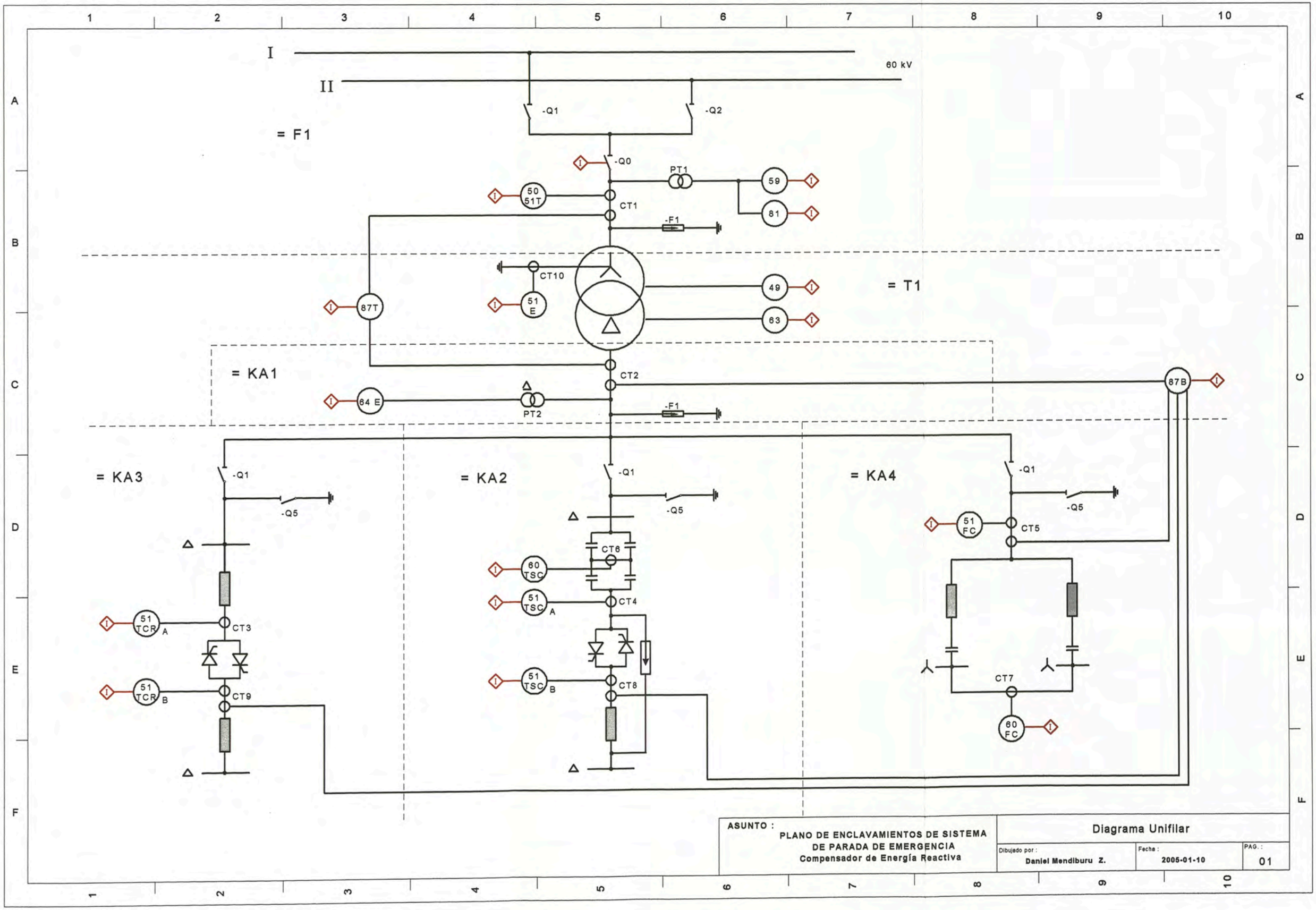


Figura 3.1: Enclavamientos para SVC.

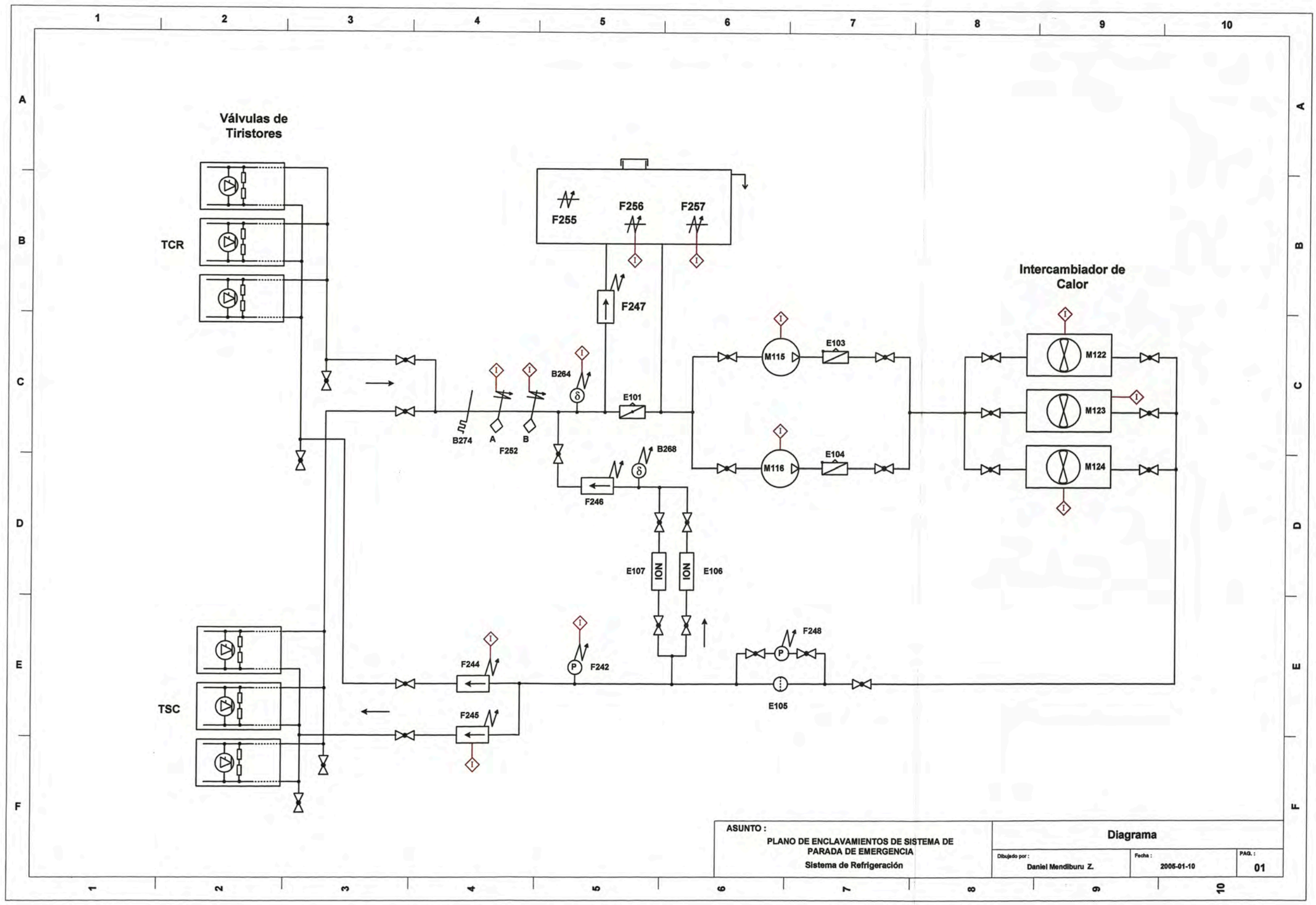


Figura 3.2: Enclavamientos para Sistema de Refrigeración.

3.5.2 Definición de componentes del Sistema Instrumentado de Seguridad.

De acuerdo a las figuras 3.1 y 3.2 se procede a definir los elementos del Sistema Instrumentado de Seguridad.

a) Sensores.

Los sensores a utilizar se muestran en la tabla 3.6.

Tabla 3.6: Sensores.

Ítem	Identificación	Descripción
1	59	Relé de sobre-voltaje en lado de alta del transformador.
2	81	Relé de sub-frecuencia.
3	50/51T	Relé de Sobre-corriente Instantáneo/ Sobrecorriente Temporizado en lado de alta del transformador.
4	87 T	Relé diferencial del transformador.
5	51 E	Relé de corriente de neutro en primario estrella de transformador.
6	49	Detectores de temperatura de aceite en transformadores T1, T2 y T3.
7	63	Relés Buchholz, presión en transformador T1, T2 y T3.
8	64 E	Relé de protección de tierra en lado baja de transformador.
9	87 B	Relé diferencial de barras de lado de baja.
10	51 TSC A	Relé de sobre-corriente temporizado en TSC, grupo A.
11	51 TSC B	Relé de sobre-corriente temporizado en TSC, grupo B.
12	60 TSC F1	Relé de desbalance de condensadores en TSC en L12.
13	60 TSC F2	Relé de desbalance de condensadores en TSC en L23.
14	60 TSC F3	Relé de desbalance de condensadores en TSC en L31.
15	60 FC F4	Relé de desbalance de condensadores en FC de 5to armónico.
16	60 FC F5	Relé de desbalance de condensadores en FC de 7mo armónico.
17	51 FC	Relé de sobre-corriente temporizado en FC.
18	51 TCR A	Relé de sobre-corriente temporizado en TCR del grupo A.
19	51 TCR B	Relé de sobre-corriente temporizado en TCR del grupo B.
20	RGA F	Falla Grupo A de Relés de protección.

Tabla 3.6: (continuación) Sensores.

Ítem	Identificación	Descripción
21	RGB F	Falla Grupo B de Relés de protección.
22	F256	Detector de nivel muy bajo en tanque de expansión.
23	F257	Detector de nivel muy bajo en tanque de expansión.
24	F252 A	Medidor de temperatura del agua en salida TSC y TCR.
25	F252 B	Medidor de temperatura del agua en salida TSC y TCR.
26	B264	Medidor de conductividad a la entrada del tanque de expansión.
27	F242	Detector de presión entrada TSC y TCR.
28	F244	Detector Flujo en entrada TCR.
29	F245	Detector Flujo en entrada TSC.
30	F115-116	Perdida de 2 bombas
31	=KA+-UVA-S208	Pulsador Parada de Emergencia Centro de Despacho.
32	=KA+-U4-S208	Pulsador Parada de Emergencia Panel Remoto.
33	=KA+-U2-S208	Pulsador Parada de Emergencia Centro Panel Local.
34	AVR ND	No Disponibilidad del AVR.
35	TSC CF	Disparo Continuo de TSC.
36	TSC VF	Falla en válvula TSC.
37	TSC-FPE F	Falla en electrónica de disparo de TSC.
38	TCR VF	Falla en válvula TCR.
39	TCR-FPE F	Falla en electrónica de disparo de TCR.

b) Actuadores.

Los actuadores a utilizar se muestran en la tabla 3.7.

Tabla 3.7: Actuadores.

1	=F1-Q0	Interruptor principal 60 kV. 2 Bobinas de apertura.
2	M115	Contactor Bomba de agua 1.
3	M116	Contactor Bomba de agua 2.
4	M122	Contactor Ventilador 1 del intercambiador de calor.
5	M123	Contactor Ventilador 1 del intercambiador de calor.
6	M124	Contactor Ventilador 1 del intercambiador de calor.

c) Sistema Electrónico Programable.

Las partes del PES a utilizar se muestran en la tabla 3.8.

Tabla 3.8: Sistema Electrónico Programable.

Cantidad	Equipo	Modelo
1	QUADLOG Critical Control Module Plus+ - 4MB RAM, 1 MB ROM	QLCCM24AAN
2	Critical Discrete I/O Module 32 canales	QLCDM024DCBAN
1	SIXRAC 6 slots	16289-200
1	POWERAC 200 W 115/230 Vac	39PSR2ANCN
2	SDM/CDM Fused Marshalled Termination Panel	16436-1
2	Marshalled Interconnect I/O Cable - 8 Meter	16137-115

El PES a utilizar es un PLC de Seguridad Quadlog de Siemens Moore con arquitectura 1oo1D que está certificado con SIL 2. Tiene un puerto serie RS-232 que le permite comunicarse utilizando el protocolo Modbus.

3.5.3 Configuración del Sistema Electrónico Programable.

Para la configuración del PES se utiliza el software Process Suite, y para la configuración de la matriz el software Safety Matrix.

En el anexo se muestra la lista de entradas y salidas del PES.

a) Matriz Causa-Efecto.

En la figura 3.3 se muestra la matriz causa efecto.

QUADLOG
The Safety PLC
Safety Matrix

Controller Name: SVC
Matrix Name: SVC_ESD

									Effects	SIL	2	2	2	2	2	2	2									
										Type																
									Description		Disparo 1 Interruptor =F1-QD	Disparo 2 Interr uptor =F1-QD	Bomba 1 Sistema de Refrigeracion	Bomba 2 Sistema de Refrigeracion	Ventilador 1 Intercamb. Calor	Ventilador 2 Intercamb. Calor	Ventilador 3 Intercamb. Calor									
									Output Tag		%F1_QD_trip_1*	%F1_QD_trip_2*	%Bomba_M115*	%Bomba_M116*	%Ventilador_M122*	%Ventilador_M123*	%Ventilador_M124*									
									Action		Abrir	Abrir	Arrancar	Arrancar	Arrancar	Arrancar	Arrancar									
		Causes																								
Input Tag	Func	Limit/Trip	EngUnit	Description	SIL	Num	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
%R59		TRUE		Rele SobreVoltaje Alta Transfor.	2	1	N	N													
%R81		TRUE		Rele Sub-frecuencia	2	2	N	N													
%R50_51_T		TRUE		Rele Sobre-corriente Trafo Alta	2	3	N	N													
%R87_T		TRUE		Rele Diferencial Transformador	2	4	N	N													
%R51_E		TRUE		Rele I neutro Primario Trafo	2	5	N	N													
%R49		TRUE		Detectores Temperatura Transfos.	2	6	N	N													
%R63		TRUE		Reles Buchholz	2	7	N	N													
%R64_E		TRUE		Rele Tierra Primario Transfor.	2	8	N	N													
%R87_B		TRUE		Rele Diferencial Barras	2	9	N	N													
%R51_TSC_A %R51_TSC_B	OR	TRUE		Rele Sobreccoriente TSC Grp A B	2	10	N	N													
%R60_TSC_F1_3		TRUE		Reles Desbalance Condensador TSC	2	11	N	N													
%R60_FC_F4_5		TRUE		Reles Desbalance Condensador FC	2	12	N	N													
%R51_FC_		TRUE		Reles Sobrecorriente FC		13	N	N													
%R51_TCR_A %R51_TCR_B	OR	TRUE		Rele Sobrecorriente TCR Grp A B	2	14	N	N													
%RGA_F		TRUE		Grupo A Reles Proteccion Falla	2	15	N	N													
%RGB_F		TRUE		Grupo B Reles Proteccion Falla	2	16	N	N													
%F256 %F257	OR	TRUE		Detectores Nivel Muy Bajo Tanque	2	17	N	N													
%F252_A %F252_B	OR	TRUE		Medidor T muy alta TSC/TCR	2	18	N	N			N	N	N								
%B265		TRUE		Medidor Conductividad Tanque in	2	19	N	N													
%F242		TRUE		Detector Presion Entrada TSC/TCR	2	20			N	N											
%F242 %F115_116	AND	TRUE		Presion y perdida 2 bombas	2	21	N	N													
%F244		TRUE		Detector Flu g Entrada TCR	2	22	N	N													
%F245		TRUE		Detector Flujo Entrada TSC	2	23	N	N													
%UVA_S208		TRUE		Pulsador ESOFF Centro Despacho	2	24	N	N													
%U4_S208		FALSE		Pulsador ESOFF Panel Remoto	2	25	N	N													
%U2_S208		TRUE		Pulsador ESOFF Panel Control	2	26	N	N													
%AVR_ND		TRUE		AVR No Disponible	2	27	N	N													
%TSC_CF		TRUE		Disparo Continuo TSC	2	28	N	N													
%TSC_VF		TRUE		Falla Valvula TSC	2	29	N	N													
%TSC_FPE_F		TRUE		Falla Electronica Disparo TSC	2	30	N	N													
%TCR_VF		TRUE		Falla Valvula TCR	2	31	N	N													
%TCR_FPE_F		TRUE		Falla Electronica Disparo TCR	2	32	N	N													

Figura 3.3: Matriz Causa-Efecto.

3.6 Cálculos PFD_{avg} y $MTBF_{sp}$.

De acuerdo a las funciones de seguridad definidas, la arquitectura de los sensores, PES, actuadores, y las razones de falla se calculará el PFD_{avg} y $MTBF_{sp}$.

3.6.1 Probabilidad promedio de falla en demanda.

En la tabla 3.9 se muestra los cálculos del PFD_{avg}.

Se verifica que el PFD_{avg} cumple con el SIL 2.

Tabla 3.9: PFD_{avg}.

Función	Descripción	Sensor			PES	Actuador			Total
		Arq.	AD (1/año)	PFDavg	PFDavg	Arq.	AD (1/año)	PFDavg	PFDavg
1	Sobre-voltaje lado alta del transformador.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
2	Sub-frecuencia.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
3	Sobre-corriente lado de alta del transformador.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
4	Diferencia de corriente en transformador.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
5	Corriente de neutro primario transformador.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
6	Temperatura de aceite en transformadores T1, T2 yT3.	1oo1	0,050	6,3E-03	2,1E-06	1oo2	0,014	4,3E-06	6,26E-03
7	Presión en transformador T1, T2 yT3.	1oo1	0,029	3,6E-03	2,1E-06	1oo2	0,014	4,3E-06	3,58E-03
8	Falla de tierra en lado baja de transformador.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
9	Diferencia corriente barras lado baja.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
10	Sobre-corriente temporizado en TSC, grupo A y B.	**1oo2**	0,010	2,1E-06	2,1E-06	1oo2	0,014	4,3E-06	8,42E-06
11	Desbalance de condensadores en TSC.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
12	Desbalance de condensadores en FC.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
13	Relé de sobre-corriente temporizado en FC.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
14	Sobre-corriente temporizado en TCR del grupo A y B.	**1oo2**	0,010	2,1E-06	2,1E-06	1oo2	0,014	4,3E-06	8,42E-06
15	Falla Grupo A de Relés de protección.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
16	Falla Grupo B de Relés de protección.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
17	Nivel muy bajo en tanque de expansión, redundante.	**1oo2**	0,010	2,1E-06	2,1E-06	1oo2	0,014	4,3E-06	8,42E-06
18	Temperatura muy alta agua salida TSC/TCR A y B .	**1oo2**	0,050	5,2E-05	2,1E-06	1oo2	0,014	4,3E-06	5,84E-05
19	Temperatura muy alta salida TSC/TCR A y B. Ventiladores	**1oo2**	0,050	5,2E-05	2,1E-06	**1oo1**	0,013	1,6E-03	1,62E-03
20	Conductividad muy alta a la entrada del tanque de expansión.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
21	Presión entrada baja TSC y TCR.	1oo1	0,010	1,3E-03	2,1E-06	**1oo1**	0,013	1,6E-03	2,81E-03
22	Presión entrada baja TSC y TCR y Pérdida de 2 bombas.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
23	Detector Flujo en entrada TCR.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
24	Detector Flujo en entrada TSC.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
25	Pulsador Parada de Emergencia Centro de Despacho.	1oo1	0,025	3,1E-03	2,1E-06	1oo2	0,014	4,3E-06	3,13E-03
26	Pulsador Parada de Emergencia Panel Remoto.	1oo1	0,002	2,5E-04	2,1E-06	1oo2	0,014	4,3E-06	2,56E-04
27	Pulsador Parada de Emergencia Centro Panel Local.	1oo1	0,002	2,5E-04	2,1E-06	1oo2	0,014	4,3E-06	2,56E-04
28	No Disponibilidad del AVR.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
29	Disparo Continuo de TSC.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
30	Falla en válvula TSC.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
31	Falla en electrónica de disparo de TSC.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
32	Falla en válvula TCR.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03
33	Falla en electrónica de disparo de TCR.	1oo1	0,010	1,3E-03	2,1E-06	1oo2	0,014	4,3E-06	1,26E-03

3.6.2. Tiempo medio entre disparos no deseados.

En la tabla 3.10 se muestra los cálculos del $MTTF_{sp}$. El $MTTF_{sp}$ calculado está entre 3,7 y a 15,4 años.

Tabla 3.10: $MTBF_{sp}$.

Función	Descripción	Sensor			PES	Actuador			Total
		Arq.	AS (1/año)	MTTFsp (año)	MTTFsp (año)	Arq.	AS (1/año)	MTTFsp (año)	MTTFsp (año)
1	Sobre-voltaje lado alta del transformador.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
2	Sub-frecuencia.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
3	Sobre-corriente lado de alta del transformador.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
4	Diferencia de corriente en transformador.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
5	Corriente de neutro primario transformador.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
6	Temperatura de aceite en transformadores T1, T2 yT3.	1oo1	0,100	10	50	1oo2	0,025	20	5,9
7	Presión en transformador T1, T2 yT3.	1oo1	0,050	20	50	1oo2	0,025	20	8,3
8	Falla de tierra en lado baja de transformador.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
9	Diferencia corriente barras lado baja.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
10	Sobre-corriente temporizado en TSC, grupo A y B.	1oo2	0,020	25	50	1oo2	0,025	20	9,1
11	Desbalance de condensadores en TSC.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
12	Desbalance de condensadores en FC.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
13	Relé de sobre-corriente temporizado en FC.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
14	Sobre-corriente temporizado en TCR del grupo A y B.	1oo2	0,020	25	50	1oo2	0,025	20	9,1
15	Falla Grupo A de Relés de protección.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
16	Falla Grupo B de Relés de protección.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
17	Nivel muy bajo en tanque de expansión, redundante.	1oo2	0,020	50	50	1oo2	0,025	20	11,1
18	Temperatura muy alta agua salida TSC/TCR A y B.	1oo2	0,100	5	50	1oo2	0,025	20	3,7
19	Temperatura muy alta salida TSC/TCR A y B. Ventiladores	1oo2	0,100	5	50	1oo1	0,025	40	4,1
20	Conductividad muy alta a la entrada del tanque de expansión.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
21	Presión entrada baja TSC y TCR.	1oo1	0,020	50	50	1oo1	0,025	40	15,4
22	Presión entrada baja TSC y TCR y Pérdida de 2 bombas.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
23	Detector Flujo en entrada TCR.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
24	Detector Flujo en entrada TSC.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
25	Pulsador Parada de Emergencia Centro de Despacho.	1oo1	0,033	30	50	1oo2	0,025	20	9,7
26	Pulsador Parada de Emergencia Panel Remoto.	1oo1	0,004	250	50	1oo2	0,025	20	13,5
27	Pulsador Parada de Emergencia Centro Panel Local.	1oo1	0,004	250	50	1oo2	0,025	20	13,5
28	No Disponibilidad del AVR.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
29	Disparo Continuo de TSC.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
30	Falla en válvula TSC.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
31	Falla en electrónica de disparo de TSC.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
32	Falla en válvula TCR.	1oo1	0,020	50	50	1oo2	0,025	20	11,1
33	Falla en electrónica de disparo de TCR.	1oo1	0,020	50	50	1oo2	0,025	20	11,1

CAPÍTULO IV

EVALUACIÓN DE COSTOS

En este capítulo se evalúan los costos de implementar el SIS con el PES elegido. Se realizará la evaluación del costo inicial y también del anual.

Para justificar un SIS no basta tener en cuenta la seguridad y confiabilidad, sino también el costo del ciclo de vida del sistema de seguridad. El costo del ciclo de vida nos permite evaluar el costo total de propiedad del sistema de seguridad. El costo del ciclo de vida está dividido en costo inicial y costo anual.

4.1 Costo Inicial.

El costo fijo inicial incluye a los costos de diseño, compra, instalación, comisionamiento y arranque del sistema.

En los costos iniciales se considera:

a) Clasificación de SIL: completado el HAZOP y luego de definirse la necesidad del sistema de seguridad, se requiere completar la clasificación del SIL.

b) Requerimientos de Seguridad y Especificaciones de Diseño: tiene en cuenta los costos del desarrollo de los Requerimientos de Seguridad y Diseño Conceptual.

c) Diseño detallado: es el costo del diseño de ingeniería detallado completo, la instalación, prueba y arranque.

d) Sensores: la compra de los sensores.

e) Actuadores: la compra de los actuadores.

f) Sistema lógico: la compra del procesador de lógica.

g) Misceláneos: se considera los distintos equipos necesarios como alimentación, cableado, cajas de unión, interfaz de operador.

h) Entrenamiento inicial: el costo del entrenamiento para diseño, operación y personal de soporte para diseño, instalación y prueba del sistema.

i) Instalación y prueba aceptación de pre-arranque: se consideran los costos de instalación de los equipos y de las pruebas antes del arranque inicial el sistema.

j) Arranque: el costo de arranque inicial del sistema.

En la tabla 4.1 se muestra el costo inicial del sistema.

Tabla 4.1: Costo Inicial.

Costos	Material (US$)	Labores (US$)	Costo Total (US$)
Clasificación SIL			
Especificaciones Requerimientos Seguridad y Diseño Conceptual			
Diseño Conceptual			
Diseño Detallado		2 500	2 500
PES	21 920		21 920
Misceláneos: alimentación, cableado.	1200		1 200
Entrenamiento Inicial.		1 200	1 200
Instalación y prueba de pre-arranque.	1500	3 000	4 500
Arranque inicial.		1 800	1 800
Costo Inicial Total			**33 120**

4.2 Costo Anual.

El costo anual incluye a los costos de operación y mantenimiento.

En los costos anuales se considera:

a) Entrenamiento continuo: se necesita entrenamiento continuo para refrescar al personal de operación y mantenimiento.

b) Cambios de ingeniería: debido a la revisión de requerimientos y actualización de documentos.

c) Costos fijos de operación y mantenimiento: para la operación y programas de mantenimiento.

d) Repuestos: repuestos críticos recomendados.

e) Pruebas en línea: que deben hacerse periódicamente por personal de operación y mantenimiento.

f) Costos de reparación: de módulos defectuosos basados en razones de falla predictivas.

g) Valor presente para el costo anual.

En la tabla 4.2 se muestra el costo anual del sistema.

Para calcular el valor presente de los costos anuales se ha utilizado las siguientes relaciones.

$$VP_N = \frac{CA}{(1+D)^N} \qquad (4.1)$$

$$VP = \sum_{1}^{N} VP_N = \frac{CA}{D}(1-(1+D)^{-N}) \qquad (4.2)$$

Donde:

CA: Costo Anual calculado.

D: Descuento por año.

VP: Valor presente total.

VPN: Valor Presente del año N.

Tabla 4.2: Costo Anual.

Costos	Material (US$)	Labores (US$)	Costo Total (US$)
Entrenamiento continuo.		600	600
Cambios de ingeniería.	200	400	600
Costos de operación y mantenimiento.		1 000	1 000
Repuestos.	500		500
Pruebas en línea.		1 200	1 200
Costo Anual			**3 900**
Valor Presente de costos anuales			**48 603**

Al sumar el costo inicial y el valor presente de los costos anuales se obtiene un costo total de propiedad de US$ 81 723.

GLOSARIO Y SÍMBOLOS

En esta sección se listan a continuación en forma alfabética los términos y símbolos utilizados.

GLOSARIO

AIChE	American Institute of Chemical Engineers, Instituto Americano de Ingenieros Químicos.
ANSI	American National Standards Institute.
API	American Petroleum Institute. Instituto Americano de Petróleo.
AVR	Automatic Voltage Regulator. Regulador Automático de Voltaje, encargado de calcular ángulo de disparo en el TCR y conectar el TSC.
BOD	Break Over Diode. Diodo para disparo de SCR cuando hay sobre-voltaje.
BPCS	Basic Process Control System. Sistema básico de control de proceso.
Confiabilidad	Probabilidad de un sistema de realizar una función determinada ante condiciones indicadas por un periodo de tiempo.
DCS	Distributed Control System. Sistema de Control Distribuido, es utilizado para controlar procesos complicados y con muchas variables como una refinería o una petroquímica, suele ser un sistema con redundancia y comunicaciones integradas.
DIN	Deutsches Institut fur Normung. Instituto Alemán de Normas.
Disponibilidad de Seguridad	Probabilidad, fracción del tiempo que el SIS es capaz de realizar su servicio de seguridad cuando el proceso está operando. Disponibilidad de Seguridad = 1 – PFDavg.

ESD System	Emergency ShutDown System: detiene la planta a un estado seguro en el evento de cualquier proceso fuera de control.
Falla por Causa Común	Una sola fuente puede causar fallas en múltiples elementos del sistema, la fuente puede ser interna o externa al sistema.
Falla Sistemática	Falla debido a errores, incluyendo equivocaciones u omisiones, en las actividades el ciclo de vida de seguridad que causa que el SIS falle bajo determinadas condiciones de entrada o de medio ambiente.
FC	Fixed Capacitor. Banco fijo de condensadores.
FMEA	Failure Mode and Effect Analysis. Estudio de las fallas potenciales y como pueden afectar el proceso.
FMECA	Failure Mode Effect and Criticality Analysis. Estudio de fallas potenciales que pueden afectar la seguridad del proceso.
FMEDA	Failure Modes, Effects and Diagnostic Analysis. Estudio realizado durante el diseño, que indica como falla cada componente en el sistema y como el sistema detecta la falla.
HAZOP	Hazard and Operability Study: técnica cualitativa sistemática para identificar los peligros del proceso y problemas potenciales de operación usando una serie de palabras guía para estudiar las desviaciones del proceso.
IEC	International Electrotechnical Commission. Comisión Electrotécnica Internacional, organización que publica estándares internacionales para electricidad, electrónica y tecnologías relacionadas.
IEEE	Institute of Electric and Electronics Engineers. Instituto de Ingenieros Eléctricos y Electrónicos, asociación profesional con alrededor de 900 estándares activos.
Integridad de Seguridad	Probabilidad de una SIF de ejecutar satisfactoriamente la función de seguridad bajo condiciones indicadas dentro de un periodo de tiempo indicado.
ISA	Instrumentation, Systems, and Automation Society. Sociedad de Instrumentación, Sistemas y Automatización, organización que publica estándares para control de procesos industriales.
MOC	Management of Change. Gestión del Cambio.
MTBF	Mean Time Between Failures. Tiempo promedio entre fallas.
MTTF	Mean Time To Failure. Tiempo promedio para fallar.
MTTF ^{spurious}	Mean Time To Failure to spurious trip: tiempo medio para la falla del SIS que resulta en un falso disparo o disparo no deseado del proceso bajo control.

MTTR	Mean Time To Repair: tiempo promedio para reparar un modulo o elemento del SIS. Es medido desde que la falla ocurre hasta que se termina la reparación y el elemento vuelve a servicio.
NFPA	National Fire Protection Association. Asociación Nacional de Protección contra Fuegos con sede en Estados Unidos de América, ha publicado más de 300 estándares y códigos.
NSD	Emergency Shut Down. Parada Normal.
Peligro	Fuente potencial de daño.
PES	Programmable Electronic System. Sistema Electrónico Programable.
PFD	Probability of Failure on Demand: valor que indica la probabilidad del sistema de fallar al responder una demanda, es la medición de la integridad de la seguridad para una SIF. PFD = 1 – Disponibilidad de Seguridad.
PFDavg	PFD promedio. PFD en un intervalo de tiempo especificado TI.
PFS	Probability to Fail Safe: valor que indica la probabilidad que las fallas sean en un modo seguro.
PHA	Process Hazards Analysis, requerido para desarrollar las Especificaciones de Requerimientos de Seguridad.
PLC	Programmable Logic Controller. Controlador Lógico Programable, controlador especializado en variables discretas, que también tiene capacidad de manejar variables analógicas.
PSAT	Pre-Startup Acceptance Test: paso de aceptación antes de arrancar el sistema y se sometido. a los peligros para los cuales ha sido diseñado.
PSSR	Pre-Startup Safety Review. Revisión de Seguridad antes del arranque inicial.
Redundancia	Uso de elementos o sistemas múltiples para realizar al misma función. Se implementa con elementos idénticos o diferentes. Se usa para mejorar la confiabilidad o la disponibilidad.
Riesgo	Combinación de la probabilidad de la ocurrencia de daño y la severidad del mismo.
RRF	Reduction Risk Factor. Factor de Reducción del Riesgo. $RRF = 1/ PFD_{avg}$.
Seguridad	Libertad de riesgo no aceptable.
SIF	Safety Instrumented Function. Función instrumentada de seguridad necesaria para alcanzar la seguridad.
SIL	Safety Integrity Level.

SIS	Safety Instrumented System: compuesto de sensores, solucionadores de lógica, y elementos finales de control para llevar al proceso a una condición segura cuando no se cumplen determinadas condiciones.
SOP	Standard Operating Procedures. Procedimientos de operación estándar.
SOV	Solenoid Valve. Válvula solenoide.
TCR	Thyristor Controlled Reactor. Banco controlado de inductancia.
TI	Test Interval: intervalo de prueba, tiempo entre dos pruebas funcionales en un SIS o un componente del SIS, para validar su operación.
TMR	Triple Modular Redundant. Sistemas con arquitectura 2oo3.
TSC	Thyristor Switching Capacitor. Banco conmutable de condensadores.
TÜV	Instituto que da servicio de certificación para PES estableciendo el nivel AK. Da servicio técnico para asegurar la confiabilidad, seguridad, calidad y costo efectivo de l interfaz humano-maquina.
Válvulas de Tiristores	Arreglo de tiristores en pares anti-paralelo, pares que se encuentran en serie, para poder controlar la conducción en ambos sentidos soportando una mayor tensión que la que corresponde a un tiristor.
Validación	Confirmación por examen, y provisión de evidencia objetiva, que requerimientos particulares para un uso específico deseado han sido satisfechos.
Verificación	Confirmación por examen, y provisión de evidencia objetiva, que los requerimientos han sido satisfechos.
WDT	Watchdog Timer. Temporizador que supervisa que el sistema no se detenga.

SÍMBOLOS

β	Fracción de falla de un modulo o circuito que resulta en una falla de un modulo o circuito adicional. Es utilizado para modelar fallas de causa común relacionadas con fallas de hardware.
λ	Failure Rate: Razón de falla de un modulo o parte de él, expresada en fallas por millón de horas. $\lambda = 1 / MTBF$.
C	Factor de cobertura del diagnóstico. Fracción de las fallas que son detectadas por un diagnóstico en línea.
S	Valor de β para fallas no detectadas.

CONCLUSIONES

1. Si la evaluación del riesgo lo justifica se debe utilizar un Sistema Instrumentado de Seguridad. Para obtener un nivel de riesgo aceptable se debe definir un nivel de integridad de seguridad (SIL) para cada función de seguridad. El SIS desde el SIL 1 debe tener un procesador de lógica independiente del sistema de control del proceso.

2. En un SIS se pueden elegir distintas arquitecturas para los sensores, los procesadores de lógica y los elementos finales de control. Las arquitecturas pueden ser tan sencillas como 1oo1 o tan complicadas como 2oo3, cuanto mayor es la redundancia se obtiene una mayor tolerancia a fallas y se puede obtener un SIL mayor. La arquitectura elegida depende del SIL necesitado y de los lineamientos de la empresa propietaria del proceso.

3. Se realizó el diseño de un Sistema Instrumentado de Seguridad para un Compensador Estático de Energía Reactiva de acuerdo a los pasos establecidos por el modelo de ciclo de vida del SIS: evaluación del riesgo, definición del SIL para cada SIF, desarrollo de los requerimientos de seguridad, diseño conceptual, y diseño detallado. También se verificó que los valores de PFD_{avg} con los instrumentos definidos en el diseño, y se realizó la evaluación de costo inicial y costo anual, para

poder evaluar el costo total del ciclo de vida. De acuerdo a la operación, mantenimiento y pruebas periódicas del SIS se decide si es necesario hacer modificaciones o inclusive des-incorporar parte del SIS.

4. El PES elegido cuenta con certificación TÜV para AK4, que es equivalente a SIL 2. Este PES usa estándares de comunicación, tanto de interfaz como de protocolo que le permiten integrarse fácilmente a un sistema de supervisión. El software de configuración y programación del PES permite hacer cambios en línea utilizando una computadora personal.

5. El PFD_{avg} total depende de la razón de falla de los sensores, PES y actuadores, así como de la arquitectura utilizada para cada uno de ellos. Al disminuir el intervalo de prueba TI menor se logra disminuir el PFD_{avg}, lo que permite mejora el SIL.

ANEXOS

A. Lista de Entradas Salidas en PES.

B. Costos Detallados del PES.

C. Información Técnica del PES.

C1. CCM: Critical Control Module.

C2. CDM: Critical Discrete Module.

A. Lista de Entradas Salidas en PES.

Se muestra la tabla A.1 con los parámetros de configurados en los canales en el PES.

Tabla A.1 Listado de Entradas/Salidas.

IOModule Address	Channel Number	Channel Tag	Channel Type	Channel Descriptor
R01S02	1	%RGA_F	ADIC	Grupo A|Reles Proteccion|Falla
R01S02	2	%R81	ADIC	Rele|Sub-frecuencia
R01S02	3	%R50_51_T	ADIC	Rele Ins./Temp.|Sobre-corriente|Trafo Alta
R01S02	4	%R49	ADIC	Detectores|Temperatura|Transformadores
R01S02	5	%R64_E	ADIC	Rele|Tierra Primario|Transformador
R01S02	6	%R51_TSC_A	ADIC	Rele|Sobreccoriente|TSC Grupo A
R01S02	7	%R60_TSC_F1_3	ADIC	Reles Desbalance|Condensadores|TSC
R01S02	8	%R51_FC_	ADIC	Reles|Sobrecorriente|FC
R01S02	9	%R5l_TCR_A	ADIC	Rele|Sobrecorriente|TCR Grupo A
R01S02	10	%F256	ADIC	Detector 1 Nivel|Muy Bajo|Tanque expansion
R01S02	11	%F252_A	ADIC	Medidor A |Temperatura|M. Alta TSC/TCR
R01S02	12	%B265	ADIC	Medidor|Conductividad|Entrada Tanque
R01S02	13	%F244	ADIC	Detector|Flujo Entrada|TCR
R01S02	14	%AVR_ND	ADIC	AVR|No Disponible
R01S02	15	%TSC_CF	ADIC	Disparo|Continuo|TSC
R01S02	16	%TSC_VF	ADIC	Falla|Valvula|TSC
R01S02	17	%TSC_FPE_F	ADIC	Falla|Electronica|Disparo TSC
R01S02	18	%UVA_S208	ADIC	Pulsador|ESOFF|Centro Despacho
R01S02	19	%U4_S208	ADIC	Pulsador|ESOFF|Panel Remoto
R01S02	25	%Bomba_M115	CDOC	Bomba 1 Sistema|de Refrigeracion
R01S02	26	%Ventilador_M122	CDOC	Ventilador 1|Intercambiador|de Calor
R01S02	32	%F1_Q0_trip_1	CDOC	Disparo 1 Interr|uptor =F1-Q0
R01S03	1	%RGB_F	ADIC	Grupo B|Reles Proteccion|Falla
R01S03	2	%R59	CDOC	Rele Sobre-|Voltaje Alta|Trasnsformador
R01S03	3	%R87_T	ADIC	Rele|Diferencial|Transformador
R01S03	4	%R51_E	ADIC	Rele Corriente|Neutro Primario|Transformador

Tabla A.1 (continuación) Listado de Entradas/Salidas.

R01S03	5	%R63	ADIC	Reles|Buchholz
R01S03	6	%R87_B	ADIC	Rele|Diferencial|Barras
R01S03	7	%R51_TSC_B	ADIC	Rele|Sobreccoriente|TSC Grupo B
R01S03	8	%R60_FC_F4_5	ADIC	Reles Desbalance|Condensadores|FC
R01S03	9	%R51_TCR_B	ADIC	Rele|Sobrecorriente|TCR Grupo B
R01S03	10	%F257	ADIC	Detector 2 Nivel|Muy Bajo|Tanque expansion
R01S03	11	%F252_B	ADIC	Medidor B |Temperatura|M. Alta TSC/TCR
R01S03	12	%F242	ADIC	Detector|Presion|Entrada TSC/TCR
R01S03	13	%F245	ADIC	Detector|Flujo Entrada|TSC
R01S03	14	%F115_116	ADIC	Perdida|2 Bombas
R01S03	15	%TCR_VF	ADIC	Falla|Valvula|TCR
R01S03	16	%TCR_FPE_F	ADIC	Falla|Electronica|Disparo TCR
R01S03	17	%U2_S208	ADIC	Pulsador|ESOFF|Panel Control
R01S03	25	%Bomba_M116	CDOC	Bomba 2 Sistema |de Refrigeracion
R01S03	26	%Ventilador_M123	CDOC	Ventilador 2|Intercambiador|de Calor
R01S03	28	%Ventilador_M124	CDOC	Ventilador 3|Intercambiador|de Calor
R01S03	32	%F1_Q0_trip_2	CDOC	Disparo 2 Interr|uptor =F1-Q0

B. Costos Detallados del PES.

Tabla B.1 Costos de PES.

Cantidad	Equipo	P/N	Unitario (US$)	Sub-total (US$)
1	QUADLOG Critical Control Module Plus+ - 4MB RAM, 1 MB ROM	16418-41		9 800
1	ACM Transisition Board	16147-51		250
2	Critical Discrete I/O Module 32 canales	16809-41	2 400	4 800
1	SIXRAC 6 slots	16289-200		1 800
1	POWERAC 200 W 115/230 Vac	16114-182		1 400
1	SixRAC Fan Assembly	16289-132	300	1 400
2	SDM/CDM Fused Marshalled Termination Panel	16436-1	990	1980
2	Marshalled Interconnect I/O Cable - 8 Meter	16137-115	245	490
			Total	**21 920**

C. Información Técnica del PES.

C1. CCM: Critical Control Module.

SIEMENS

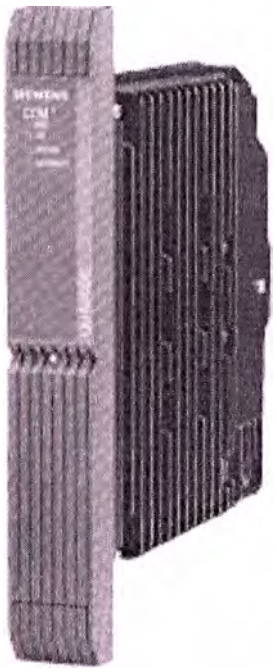
QUADLOG® The Safety PLC™

Critical Control Module (CCM^X)

The eXcelerated Critical Control Module (CCM^X) is a member of the QUADLOG critical control system's family of control modules. The CCM^X performs logic solving and advanced control functions, while interfacing with other QUADLOG modules as well as modules, from the APACS+™ process control system. Each CCM^X has a dedicated IOBUS on which QUADLOG I/O modules reside. The CCM^X also exchanges data with other control and communication modules via the MODULBUS. A block diagram of major circuit functions is shown in Figure 1.

The CCM^X:

- Has improved the scan rates by 100 to 200% over the CCM+, and the program scan time is typically 2 to 4 times faster
- Has a "safety critical rating" for TÜV rated AK 1-6 applications
- Is available in 2MB and 6MB models
- Continuously runs extensive diagnostics to quickly detect potentially dangerous failures
- Provides diagnostics analyzed by failure modes and effects analysis (FMEA) and verified by full fault injection testing for easy problem resolution
- Utilizes the high strength QUADLOG module packaging for uninterrupted service



The QUADLOG Critical Control Module eXcelerated (CCM^X)

- Eases process safety management documentation control by maintaining a master graphical configuration within the control module
- Facilitates efficient and intuitive protection strategy design by allowing four standard configuration languages to be mixed within a single module
- Supports redundant (1oo2D) architecture for SIL3 safety and highest availability
- Provides easy migration from existing QUADLOG controllers
- Reduces servicing time by allowing the module to be inserted or removed while powered without disturbing system wiring
- Reduces servicing time by supporting on-line replacement of the redundant module with automatic reconfiguration
- Complies with the European Union's Electromagnetic Compatibility (EMC) Directive, which requires process control equipment to be immune to electromagnetic interference (EMI) and limit the amount of electromagnetic emissions (See module specifications in Table 1 for more detailed information.)

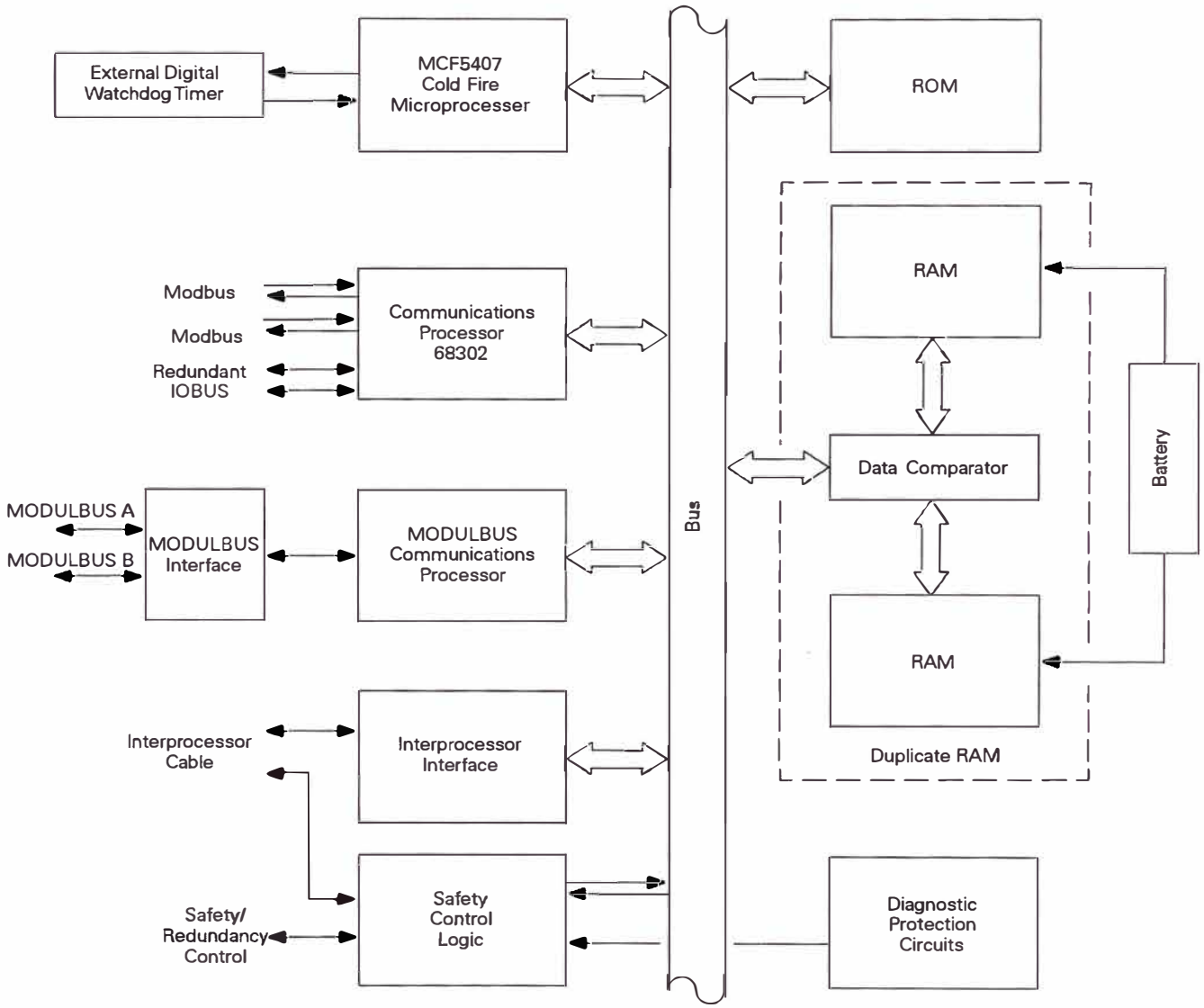


Figure 1 CCM^X Major Functions

Redundancy

The QUADLOG system's architecture incorporates flexible redundancy options to maximize safety and availability while minimizing cost. The CCM^X facilitates this with two types of system redundancy: module-to-module and rack-to-rack.

In module-to-module redundancy, a CCM^X has a redundant twin located in the adjacent module rack slot, and the two CCM^{X}s share a common set of I/O modules. This arrangement provides higher availability of the control function in an economical configuration and allows interprocessor comparison of critical data and calculation results for increased safety.

Rack-to-rack redundancy (1oo2D architecture) completely duplicates a CCM^X and its I/O subsystem, providing high availability of both the control module and I/O. The redundant CCM^{X}s execute the protection

logic and compare results and I/O scan data. The comparison is accomplished through a dedicated interprocessor communication cable that connects the two CCM^{x}s. The two independent racks can be located in different cabinets to maximize common cause strength, further increasing system safety and availability.

Diagnostics

The CCM^x is safety critical rated. As such, no known dangerous undetected failures are permitted. This requires extremely effective self-diagnostics verified by full Failure Modes and Effects Analysis (FMEA) and fault injection testing. The goals of the diagnostics are to:

- Notify the appropriate personnel of a module malfunction
- Perform automatic switchover between calculate/verify units in a fully redundant (1oo2D) QUADLOG system
- Perform automatic shutdown of a channel, module, or system if a dangerous fault is detected (for fail-safe operation)

Microprocessor diagnostics

The main microprocessor in the CCM^x is online tested to assure that potentially dangerous failures are detected. The microprocessor registers, instruction decoder, data bus interface, and address bus interface are self-tested using special routines supplied by the manufacturer.
The watchdog timer is external to the microprocessor to monitor execution timing. A series of calculations performed by the diverse microprocessors in I/O modules are compared with identical calculations made in the main processor. Program execution in the microprocessor is self-checked using task sequence and execution time monitoring. These extra reference diagnostic techniques detect transient and permanent failures in the microprocessing circuitry.

Memory diagnostics

ROM

The ROM memory in the CCM^x is online tested by calculating CRC32 test patterns on critical data and program areas and comparing to stored values. This will detect single and multiple bit failures, as well as selection logic failures. The CRC32 calculation and compare testing will also detect data, address, and control bus failures.

RAM

The RAM memory within the CCM^x is internally duplicated, redundant with hardware comparison done on each read cycle. This secure memory detects transient and permanent failures. The comparison circuits are tested online to verify that they are properly operating. Additional RAM testing is done by checking the integrity of data tables using CRC32 comparisons and online pattern checking.

Communication diagnostics

MODULBUS and IOBUS communication failures are detected by a number of diagnostic techniques, including:

- CRC32 message integrity checking
- Message type checking
- Message format verification
- Message address verification
- Message timeout checking
- Message sequence verification

In redundant CCM^x architectures, message parameters are compared to assure that all communications are accurately received. IOBUS is a safety-critical communication bus. It is:

- Isolated
- Single-fault tolerant
- Constantly switched between A and B
- Able to tolerate the failure of an I/O module

Common circuit diagnostics

The CCM^x receives power from the power buses in a module rack. Voltage levels on each power bus are monitored. Outputs from the on-board power system are monitored for over-voltage and under-voltage failures. Battery voltage is periodically sampled under load to verify battery status.

Redundancy and safety control signals are online checked for invalid bit patterns. These signals are also compared against the same information diversely sent through communication buses.

Software diagnostics

Failure in software systems are known as "systematic" failures. Special diagnostic techniques can

be used to detect systematic failures. The CCM^{x} online software employs program flow control, a technique where the execution of each piece of critical software is measured. The execution time and execution sequence must agree with predefined patterns.

CCM^{x} software also uses data integrity verification at key points in the execution. This technique requires that critical variables be checked to verify they are within permitted ranges. Variables within the CCM^{x} are data-typed. Data type consistency checking is done for calculations.

The CCM^{x} maintains a log of current and historical errors that can be reviewed using the Diagnostic Logger Utility or the *4-mation*™ configuration software. In addition, errors are indicated by the module's LED indicators.

LED indicators

The CCM^{x}'s LEDs support local troubleshooting without an operator interface. The module includes three LEDs which indicate the following module statuses:

- Module OK
- Module faulted
- Module unconfigured
- Module failed
- Module active (calculate mode)
- Module inactive (verify mode)
- Security enabled
- Security disabled

Configuration

The CCM^{x} is configured using the *4-mation* software.

4-mation allows a control strategy to be defined using any mix of four languages, which are based on the IEC specification for programmable controllers (IEC 1131-3). These languages are function blocks, ladder logic, sequential function charts, and structured text. They allow a configuration to be created using the tool(s) most effective for each application.

4-mation is also used to configure a CCM^{x}'s I/O, as well as modules within an APACS+ system. A backup copy of the I/O module's configuration is maintained by the CCM^{x} to allow automatic configuration of an I/O module when it is inserted into a QUADLOG rack.

A CCM^{x}'s configuration can be created off-line and transferred to the module, or a configuration can be created within an on-line CCM^{x} during the initial design phase. On-line configuration is possible because all of the information needed to configure a CCM^{x} is stored in its database, thus eliminating the need to have a disk-based master database for viewing or editing a configuration. Several different restriction levels are available.
The CCM^{x}'s security can be programmed so no unauthorized or inadvertent changes are made to a configuration. When this security feature is activated, a configuration can be opened in "read/write" mode only, ensuring that no further changes are made to the control strategy.

The CCM^{x} also includes features to simplify start-up should operation be disrupted. A CCM^{x}'s configuration is battery-backed so that the configuration for a CCM^{x} and its I/O is maintained when power is lost. Also, variables within a CCM^{x} can be assigned warm start and cold start values. When power is lost, the CCM^{x}'s real-time clock continues to run so that warm start and cold start states can be determined and acted upon once power is restored.

Terminations

The CCM^{x}'s termination strip facilitates the connection to a redundant CCM^{x}. The CCM^{x} termination strip can be short or long, depending on the choice made for termination of the CCM^{x}'s I/O.

Specifications

Refer to Table 1 for a list of CCM^{x} specifications.

TABLE 1 CCM^X Specifications

Catagory	Specification	Data
Module	Supply Voltage Range	24 Vdc, ±10%
	Supply Input Current	0.27 Ampere typical 0.32 Ampere maximum
	Heat Dissipation (typical)	53 BTU/hr.
	Agency Approvals	CSA and FM certified for Class I, Division 2, Groups A, B, C, & D ABS Type Approved TÜV Certified UL Listed
	Module Weight	4.5 lbs. (2.04 kg)
	Power Dissipation	7 Watts (24 Btu/hr.) ±10%
	CPU	Motorola MCF5407 Cold Fire Microprocessor
	Clock Speed	50 MHz (bus operations)
	Internal Caches	16 KB instruction, 8KB data
	I/O Coprocessor	68302 CPU
	Real-Time Clock	Battery-backed
	Memory	Redundant 2Mb or 6 Mb RAM, battery-backed
	Battery Life Expectancy: CCM+ in powered rack Storage w/battery disconnected Storage w/battery connected	 10 Years 10 Years @ 73°F (23°C) 9.5 Years @ 160°F (71°C) 8.5 Years @ 185°F (85°C) 1 Month
	Communication Buses: Backplane I/O Serial Ports 1 and 2	 Redundant MODULBUS interface Redundant IOBUS interface RS-232, 300 to 38,000 baud (software selected)
Environmental	Ambient Temperature Range Operating: -13° to 158°F (-25 to 70°C), 0.5°C/min. Storage: -40 to 185°F (-40 to 85°C), 10°/min.	IEC 60068-2-2 IEC 60068-2-1
	Relative Humidity Operating: 5 to 95%, non-condensing Storage: 0 to 100%, condensing	IEC 60068-2-30

(continued)

TABLE 1 CCM^X Specifications (continued)

Catagory	Specification	Data
Environmental	Vibration 2-150 Hz 2g max.	IEC 60068-2-6Test F_C
	Mechanical Shock Acceleration: .033 lbs. (15g) Duration: 11 ms	IEC 60068-2-27Test E_A
	Corrosives Class G3, 10+ years	ANSI/ISA S71.04
	Radiated Emission, E-Field 0.15-30 MHz 80-50 dB µV/m @ 3m 30-100 MHz 60-54 dB µV/m @ 3m 100-2000 MHz 54 dB µV/m @ 3m Except for 156-165 MKz 24 dB µV/m @ 3m	EN 55011 EN 50081-2
	Conducted Emission Power Lines 10 KHz-150 KHz 120 dB µV - 69 dB µV 0.15 MHz-0.5 MHz 79 dB µV QP, 66 dB µV Avg. 0.5 MHz-30 MHz 73 dB µV QP, 60 dB µV Avg.	EN 55011 EN 50081-2
	Immunity, Conducted Electromagnetic Field 150 KHz-80 MHz, 10V	EN 61000-4-6
	Immunity, Power and Signal Lines Surge 0.5 kV, 2 kV, 1 kV	EN 61000-4-5

(continued)

TABLE 1 CCM^{X} Specifications (continued)

Catagory	Specification	Data
Environmental (continuted)	Immunity, Electrical Fast Transients to Power and Signal Lines 2 kV	EN 61000-4-4
	Immunity, Radiated E-Field 10 V/m, 80 MHz-2000 MHz	EN 61000-4-3
	Immunity, Electrostatic Discharge 6 kV contact, 8 kV air	EN 61000-4-2
	Altitude: Up to 2000 meters	EN 61131-2

SIEMENS

For prompt, personal attention to your instrumentation and control needs, contact the Siemens location nearest you.

Siemens Energy & Automation, Inc.
1201 Sumneytown Pike
P. O. Box 900
Spring House, PA 19477-0900

PIQLCCM-3, Rev.1, 2/04

C2. CDM: Critical Discrete Module.

SIEMENS

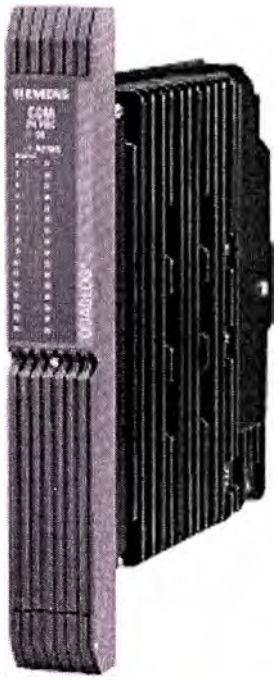
QUADLOG® The Safety PLC™

Critical Discrete Module (CDM)

The Critical Discrete Module (CDM) is a member of the QUADLOG critical control system family of I/O modules. It is an intelligent, configurable module that interfaces discrete DC sensors and actuators with a QUADLOG control module's IOBUS.

The CDM:

- Provides fail safe control of outputs with unique protected outputs
- Has a "safety critical rating" for TÜV rated AK 1-6 applications
- Detects shorts and opens in field wiring with optional Safety Rated Switch Adapter (SRSA)
- Includes a soft-fuse feature to protect individual output channels against short circuit and overload conditions caused by field wiring problems
- Allows the soft-fuse trip to be restored to service remotely or locally without removing the module from the rack
- Supports Sequence of Events Recording (SOER) by sensing and recording events at 1 ms resolution
- Improves error-checking with a per channel built-in output monitor that eliminates the need to wire and program additional input channels for error detection



The QUADLOG Critical Discrete Module (CDM)

- Includes dynamic threshold detection circuits to diagnose failed input channels
- Supports redundant architecture for highest level of availability
- Supports low and high temperature operation (-25 to 60°C) with internal temperature diagnostics that detect if the module is operating outside of these limits
- Simplifies maintenance with onscreen configurable channels that eliminate the need for DIP switches and jumpers
- Reduces servicing time by allowing the module to be inserted or removed while powered without disturbing system wiring
- Isolates field faults by electrically isolating all I/O channels from the backplane and ground

- Complies with the European Union's Electromagnetic Compatibility (EMC) Directive, which requires process control equipment to be immune to electromagnetic interference (EMI) and limits the amount of electromagnetic emissions (See module specifications in Table 1 for more detailed information.)

NOTE: *See Sequence of Events Recording in the APACS+™ Controller (AD39SOE-1) for more information on the CDM's event recording capabilities.*

Channel types

The CDM provides 32 channels, each of which can be configured to be a discrete input (sinking), a discrete output (sourcing), or a discrete pulse output (sourcing). The CDM's configurable channels reduce hardware costs and spare parts requirements by allowing one module to accommodate several I/O requirements. The variety of I/O types supported also allows related signals, such as the I/O for a particular motor or shut-off valve, to be grouped together, decreasing the time needed to find and respond to faults.

Soft-fuse features

QUADLOG's soft-fuse feature protects the CDM output channels against over-current conditions caused by field wiring and field device problems. Each channel contains an over-current detection circuit that switches the output off before damage can occur. Diagnostics report the "blown" fuse channel and permit clearing the blown fuse from an operator interface. In addition, a pushbutton located on the module allows local resetting of blown fuses.

The soft-fuse feature provides equivalent protection of individual hard fuses, permits remote on-line "repair," and eliminates the need for stocking spare fuses.

Protected outputs

The CDM uses a combination of extensive on-line diagnostics and an internal "diagnostic cut-off relay" to automatically protect against energized output failures. Figure 1 contains a block diagram of the CDM module. Output energy flows through "dual-switches" to the load. A solid-state switch provides the normal output. A relay, controlled by the built-in diagnostics, supplies the second switch through a set of normally open contacts. If any dangerous failure is detected, the relay contacts are opened. This action de-energizes the output, ensuring the output fails in a safe manner. Using this technique, CDM protected outputs ensure outputs fail safe, even in the presence of faults.

Diagnostics

The CDM is safety-critical rated. As such, no known dangerous undetected failures are permitted. This requires extremely effective self-diagnostics verified by full Failure Modes and Effects Analysis (FMEA) and fault injection testing. The goals of the CDM's diagnostics are to:

- Notify the appropriate personnel of a module malfunction or wiring error
- Perform automatic switchover in a fully redundant (1oo2D) QUADLOG system
- Perform automatic shutdown of a channel or module if a dangerous fault is detected (for fail-safe operation)

There are two types of circuit diagnostics: those diagnostics that monitor overall module performance, which are common to all I/O modules, and those that cover individual channels.

Overall module performance diagnostics

Diagnostics for overall module performance include failure detection in the communications, processor, and common circuits. These diagnostics include:

- Power supply diagnostics (monitor the three 24 Vdc power input busses for under voltage and the onboard isolated power supply for voltages within tolerance)
- Over temperature diagnostics (check the module for over temperature conditions via an online monitor)
- Memory diagnostics (run a complete IEEE published test on RAM memory at module startup, detect RAM failure modes in the optimal amount of time, and verify critical RAM data and ROM memory online with cyclical redundancy checking [CRC])
- Field power diagnostics (ensure voltage is present and within tolerance for compliance with field load requirements)
- Communication diagnostics (verify IOBUS communications for each message via CRC)
- Redundancy diagnostics (monitor logic signals for valid combinations, compare redundancy status information from the IOBUS with logical signals on the module, reporting any discrepancies as errors)

- Watchdog timer diagnostics (detect processor operation failures via external and CPU hardware timers and monitor IOBUS and scanning operation via additional timers)
- CPU diagnostics (run manufacturer-supplied tests on CPU components, where results from the instruction sequences must match predetermined values)
- Software diagnostics (verify program flow control to ensure that software functions execute in proper sequence and time, perform data integrity checks, and compare data to predetermined ranges)
- Addressing diagnostics (compare module slot/rack addresses against their addresses at startup)

Any errors detected by these diagnostics are reported to the control module. The control module and the CDM maintain a log of current and historical errors that can be reviewed using the Diagnostic Logger Utility or the *4-mation*™ configuration software.

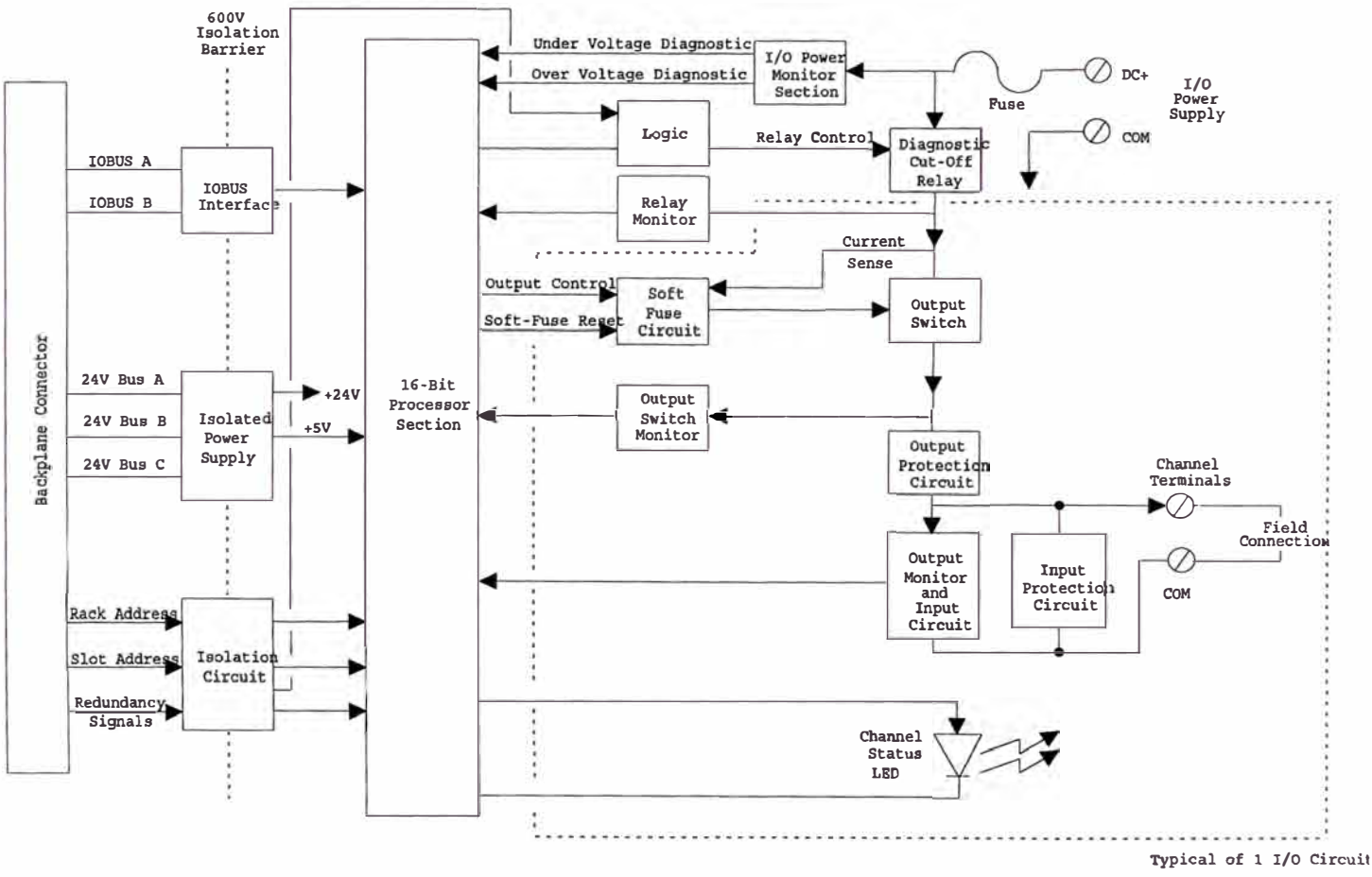


Figure 1 CDM block diagram

Input circuit diagnostics

A simplified diagram of the CDM input circuit is shown in Figure 2. The circuit is optimized for normally energized sensor inputs (input switch closed under normal operation) and offers full self-diagnostic capability including field wiring faults when used with the SRSA.

Full diagnostic coverage is obtained by a combination of test pulses that superimpose bipolar dynamic signals onto the input. A comparator circuit has a variable analog threshold that allows the CDM processor to test the voltage at the input terminal. This combination of dynamic test pulses and analog monitoring allows detection of electronic component failures and field wiring faults such as, open circuits, short circuits, and even short circuit failures between channels.

Output circuit diagnostics

A simplified drawing of the output circuit is shown in Figure 3. The circuit is optimized for normally energized usage and provides full self-diagnostic capability.

Diagnostics use a combination of pulse-testing, voltage/current measurement, and constant switching in the 1oo2D architecture. Circuitry measures several voltage and current levels at the indicated points in the drawing. Momentary pulse off testing provides a dynamic signal that allows detection of open circuit, short circuit, and diagnostic circuit failures.

LED indicators

The CDM's LEDs support local troubleshooting without an operator interface. The module includes one LED per channel to indicate its status and two LEDs that indicate a combination of two of the following module statuses:

- Module OK
- Channel(s) faulted
- Module faulted
- Module unconfigured

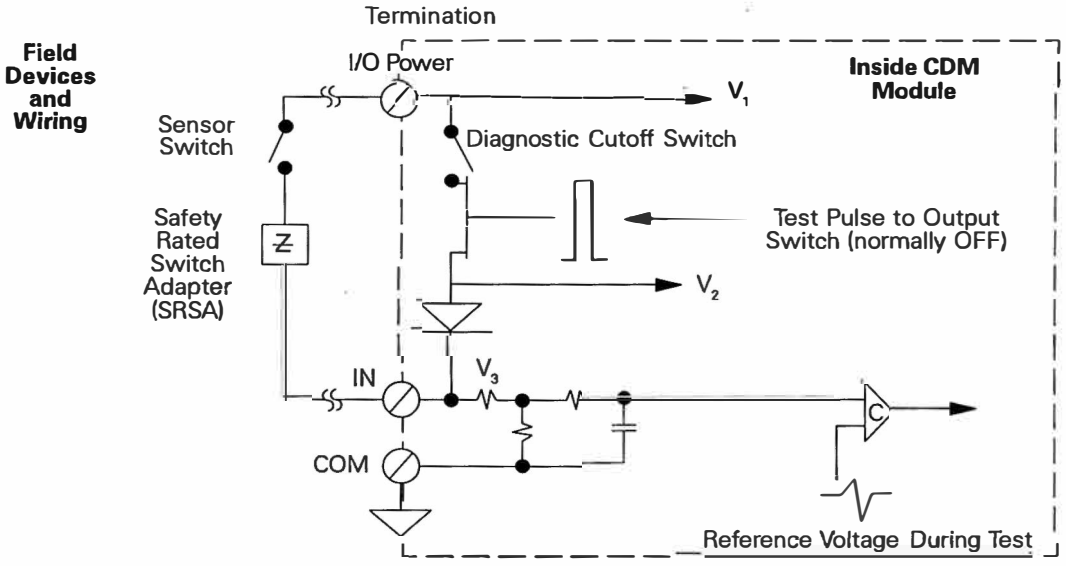


Figure 2 Input circuit logic

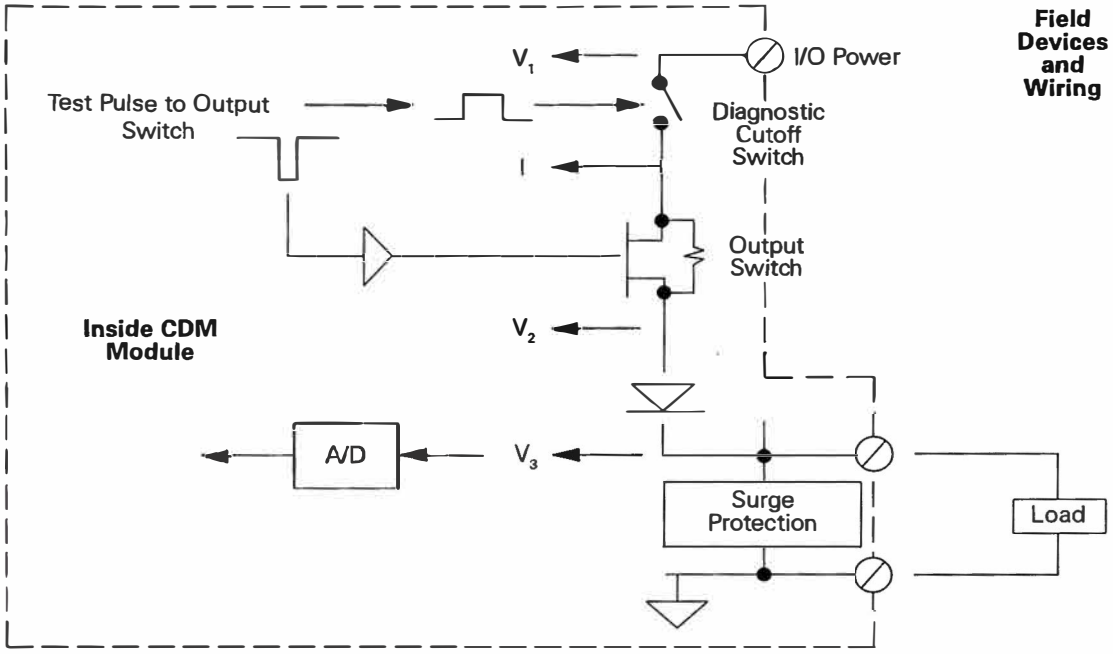


Figure 3 Simplified output circuit logic

- IOBUS communication failed
- Module failed
- Module active (calculate mode)
- Module inactive (verify mode)

Configuration

Like all QUADLOG I/O modules, the CDM is configured using the *4-mation* software. The configuration is loaded into the I/O module's memory, and a copy of the configuration is stored in the associated control module's non-volatile memory. This approach to configuration allows the module to be removed and replaced on-line without the need for reconfiguration. During configuration, *4-mation* is used to assign a type to each channel (input, output, or pulse). In addition, for some channels, additional parameters can be defined. These parameters include:

Discrete input channel parameters

- Input Fault State — if an input channel fails to change state when tested, the input will report the state defined by this parameter
- Shutdown Channel
- Pulse Diagnostic Test — enables pulse testing

Pulse output channel parameters

- Read Back — the state of an output is automatically "read back" by input circuitry on the same channel as a way to diagnose and report faults
- Duration — the duration of a pulse output channel can be specified to be between 10 discrete and 2000 milliseconds in 10 millisecond increments
- Protected Output — if a protected output channel fails when instructed to de-energize, the CDM will disable all of its output circuits
- Shutdown Channel

Discrete output channel parameters

- Read Back
- Protected Output
- Shutdown Channel
- Pulse Diagnostic Test

Terminations

The CDM's field I/O can be terminated locally or remotely according to user needs and preferences. Local terminations reside directly below the CDM. Marshalled Termination Assemblies or Rail Termination Assemblies provide for terminations up to 100 feet (30.5 m) away from the CDM. Figure 4 is an example of the wiring used for any of these options.

The CDM also supports direct, plug-in connection to 32 SPDT relays. This application uses a Relay Marshalled Termination Assembly.

Specifications

Refer to Table 1 for a list of CDM specifications.

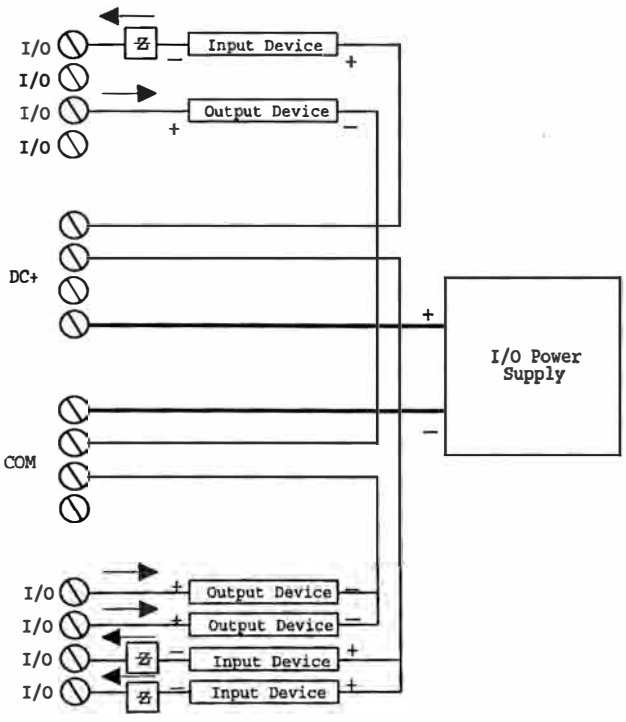


Figure 4 Typical field wiring diagram

TABLE 1 CDM specifications

Component	Specification	Data
Module	Backplane Operating Voltage	24 Vdc, -10%, + 20%
	Backplane Current	0.233 A maximum
	Electrical Isolation	Dielectric strength tested with 2640 Vac between I/O channels and ground for 2 seconds
	Operating (I/O) Voltage	24 Vdc, ±5%
	I/O Channel Loop Resistance	<25Ω
	Heat Dissipation (typical)	27 Watts maximum
	Operating Temperature	-25 to 60°C (-13 to 140°F)
	Operating Humidity	5 to 95%, non-condensing
	Storage Temperature	-25 to 85°C (-13 to 185°F)
	Storage Humidity	0 to 100%, condensing
	Agency Approvals	CSA and FM approval pending for Class I, Div. 2, Groups A, B, C, & D ABS approved TÜV approved
Inputs	Input Delay Filter Time	OFF-ON: 41 ms ON-OFF: 25 ms
	Input Wetting Current	9.96 mA @ 24 Vdc typ.
	"ON" State Voltage Range	15.51 V to 30.0 Vdc
	"OFF" State Voltage Range	-0.5 to 14.02 Vdc
	Maximum "OFF" State Current	5.76 mA
Outputs	Output Current per Channel	0.6 amps maximum
	Total Output Current per Module	12.8 amps maximum at 30°C (86°F) or 4.0 amps maximum at 60°C (140°F)
	Soft-fuse Trip*	1.53 A typical
	Surge Current	2.0 amps maximum for 10 msec
	"OFF" State Leakage Current	1.6 mA maximum

NOTE:

* *See explanation of Soft-fuse feature on page 2.*

SIEMENS

For prompt, personal attention to your process automation needs, contact the Siemens location nearest you.

Siemens Energy & Automation, Inc.
Strategic Machinery Division
1201 Sumneytown Pike
P. O. Box 900
Spring House, PA 19477-0900 USA

Tel: 215-646-7400
www.sea.siemens.com

Order No. PIQLCDM-1-1101
Rev. 3
Printed in USA

BIBLIOGRAFÍA

1. Gruhn, Paul - Cheddie, Harry "Safety Shutdown Systems: Design, Analysis and Justification" Ed. ISA – The Instrumentation, Systems, and Automation Society, 1998.
2. Buschart, Richard "Electrical and Instrumentation Safety for Chemical Processes" Ed. Chapman & Hall, 1991.
3. ISA – The Instrumentation, Systems, and Automation Society "ANSI/ISA–84.01–1996 Application of Safety Instrumented Systems for the Process Industries - American National Standard", 1996.
4. ISA – The Instrumentation, Systems, and Automation Society "ISA-TR84.00.02-2002 - Part 1 - Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL)Evaluation Techniques Part 1: Introduction - Technical Report ", 2002.
5. ISA – The Instrumentation, Systems, and Automation Society "ISA-TR84.00.02-2002 - Part 2 - Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 2: Determining the SIL of a SIF via Simplified Equations - Technical Report", 2002.

6. Pilz Automation Technology "Guide to Programmable Safety Systems", 2002.
7. IEC - International Electrotechnical Commission "Functional safety and IEC 61508 - A basic guide", 2004.
8. Faller, Rainer "The Evolution of European Safety Standards", Ed. Exida 2002.
9. Siemens Energy & Automation, Inc. "Safety Manual for Quadlog® Version 3.32 or Higher", 2003.