Universidad del País Vasco Euskal Herriko Unibertsitatea

BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

GRADO EN INGENIERÍA EN TECNOLOGÍA INDUSTRIAL

TRABAJO FIN DE GRADO

SISTEMAS DE SEGURIDAD PARA MAQUINARIA (SAFETY): ESTUDIO TEÓRICO Y APLICACIÓN PRÁCTICA

Alumno: Barbolla Zautua, Unai

Director: Orive Revillas, Darío

Curso: 2018 - 2019

Fecha: 17 / 07 / 2019

- **Título del Trabajo:** Sistemas de seguridad para maquinaria (safety): estudio teórico y aplicación práctica.

Resumen: Mediante este trabajo se pretende hacer un estudio de como abordar la seguridad de máquinas en el ámbito industrial. Para ello se estudiará la legislación vigente y la estrategia de seguridad que se ha de seguir. Se analizarán las medidas de protección existentes en el mercado, y, además, se profundizará en dos normas que calculan el nivel de protección del sistema. Tras este estudio teórico de la seguridad, se realizará una aplicación práctica del dispositivo que más presencia tiene en máquinas: el pulsador de parada de emergencia. Para ello se hará un montaje, con el hardware y software (TIA Portal) necesarios, en el laboratorio del Departamento de Ingeniería de Sistemas y Automática de la Escuela de Ingeniería de Bilbao.

Palabras clave: Seguridad. Legislación. Dispositivos. Parada de emergencia. TIA Portal.

- **Izenburua:** Segurtasun sistemak makinetan (safety): azterlan teorikoa eta aplikazio praktikoa.

Laburpena: Lan honen bidez, industriaren alorrean makinen segurtasunari nola aurre egin behar den aztertu nahi da. Horretarako, egungo legeria eta jarraitu beharreko segurtasun estrategia aztertuko dira. Merkatuan dauden babes neurriak aztertuko dira eta, gainera, sistemaren babes maila kalkulatzeko bi arau sakonduko dira. Segurtasunaren azterlan teoriko honen ondoren, makinerian presentzia handiena duen gailuaren aplikazio praktikoa egingo da: larrialdiko gelditze botoia. Horretarako, muntai bat egingo da, beharrezko hardware eta softwarearekin (TIA Portal), Bilboko Ingeniaritza Eskolako Sistemen Ingenieritza eta Automatizazio Saileko laborategian.

Hitzgakoak: Segurtasuna. Legeria. Gailuak. Larrialdiko geldialdia. TIA Portal.

- **Title:** Safety systems in machines: theoretical study and practical application.

Abstract: The intention of this work is to make a study of how to address the safety of machines in the industrial field. For this purpose, the current legislation and the security strategy to be followed will be studied. The protection measures existing in the market will be analysed and in addition, two rules that calculate the level of protection of the system will be deepened. After this theoretical study of safety, a practical application of the device that has the most presence in machinery will be made: the emergency stop button. To do this, an assembly will be made, with the necessary hardware and software (TIA Portal), in the laboratory of Systems Engineering and Automation Department of the School of Engineering of Bilbao.

Keywords: Safety. Legislation. Devices. Emergency stop. TIA Portal.

Índice

Índice de ilustraciones

Índice de tablas

1. Introducción

En la actualidad la seguridad se ha convertido en un pilar importante a la hora de realizar cualquier tipo de interacción con maquinaria industrial. Pero conseguir un sistema de protección completo y funcional que cumpla un alto grado de seguridad es una tarea compleja, ya que esto incluye desde problemáticas puramente técnicas hasta cuestiones legales.

Por lo tanto, se convierte en una disciplina en la que es necesario formar especialistas. Además, esta formación se hace más necesaria ya que, al ser un tema que no se trata en los centros de docencia clásicos, hay pocas personas que tienen conocimientos avanzados sobre él.

Este trabajo pretende ser una primera introducción al concepto de la seguridad en máquinas. Para ello se comenzará con una contextualización histórica de la seguridad industrial y con el alcance y objetivos de este documento.

Después se realizará un estudio teórico de la seguridad para maquinaria; abordando la legislación vigente, la estrategia de seguridad, las medidas de protección disponibles y, terminando con, la profundización de las dos normas que se usan para calcular el nivel de protección de los sistemas de seguridad.

Una vez finalizado este estudio, se presentará una aplicación práctica de una función de seguridad, en concreto, la que más habitualmente se usa en cualquier maquina industrial, la del pulsador de parada de emergencia. Para esto, se realizará una descripción detallada de cómo funcionan tanto el hardware como el software de esta aplicación.

Posteriormente se incluirá una descripción de tareas que se definirán con un diagrama Gantt y un desglose de gastos donde se precisará la inversión necesaria para la realización de este proyecto.

Se finalizará el trabajo con un apartado de conclusiones a modo de resumen.

2. Contexto

Como ya se ha mencionado, a día de hoy, en las sociedades de las regiones desarrolladas, nadie se cuestiona la seguridad personal en ningún ámbito, y la industria no se queda al margen. Por eso, esta ha tenido que ir introduciendo sistemas de seguridad cada vez más avanzados y complejos para asegurar el máximo nivel de protección a los trabajadores. Pero, si se viaja atrás en el tiempo, se puede comprobar que la salud y la seguridad no han sido siempre una prioridad para las empresas.

Remontando hasta el comienzo de la revolución industrial (1760), donde se comenzó a usar maquinaria y procesos de fabricación, la nula falta de seguridad y salud hacía que las muertes, ya fueran por aplastamientos, decapitaciones, etc., las pérdidas de miembros, las quemaduras y demás accidentes fueran habituales. Además, esto era aún más grave en los niños, ya que, al estar expuestos a gases y líquidos tóxicos, ocasionaba el desarrollo enfermedades como el cáncer de pulmón.

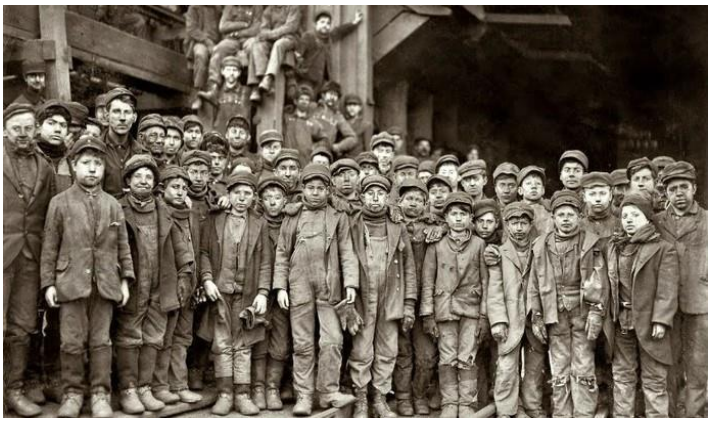


ILUSTRACIÓN 1. NIÑOS TRABAJADORES DE UNA FÁBRICA EN LA INGLATERRA VICTORIANA

Fue a principios del siglo XIX, en 1802, en el Reino Unido, donde debido a unas fuertes protestas por la lamentable situación del trabajo infantil, se redactó la considerada como primera ley que regulaba la salud y seguridad; la Ley de Fabrica de 1802. Aunque esta ley solo afectaba a los niños, fue un importante paso para el futuro desarrollo de la legislación.

Tres décadas más tarde, y tras nuevas protestas, se escribió la Ley de Fabrica de 1833. Esta ley estableció el máximo de horas de trabajo en 12, pero lo más importante fue que introdujo la figura del inspector de fábrica. A pesar de ser únicamente cuatro inspectores para todas las fábricas del país, gracias a su trabajo se comenzó a legislar sobre la protección de maquinaria.

El primer paso para esto fue la Ley de Fabrica de 1844. Esta obligó a que el engranaje de los molinos estuviera protegido y a que no se pudiesen realizar labores de limpieza de la maquinaria en caso de que esta estuviera en movimiento.

Con estos primeros pasos ya dados, la legislación comenzó a ser más rigurosa. La Ley de Fábricas y Talleres de 1878 aumentó la edad mínima para trabajar a los 10 años y esto se aplicaba para todos los oficios, ya que hasta ese momento solo se aplicaba en la minería. En 1887, con la Ley de Compensación de los Trabajadores, los trabajadores pudieron empezar a buscar compensaciones por lesiones ocurridas durante el trabajo. Pocos años más tarde, en 1891, se hicieron reglas más estrictas sobre el cercado de las máquinas.

Pero fue en el siglo XX, cuando las cosas comenzaron a ser similares a los estándares actuales, con las Leyes de Fábricas de 1937 y 1961. Y con la Ley de Seguridad y Salud en el Trabajo de 1974 se formaron las bases de la legislación de salud y seguridad en todo el mundo. Esta ley atribuye la responsabilidad tanto al empleador, como al empleado, para que esté garantizada la salud, la seguridad y el bienestar de las personas en todos los lugares de trabajo.

Dieciocho años más tarde, con el Reglamento de Provisión y Uso de Equipos de Trabajo de 1992 y la Directiva de Maquinas de 1995, se consiguió el actual marco para la seguridad de la maquinaria.

3. Objetivos y alcance

El principal objetivo de este trabajo es realizar una introducción a la seguridad de maquinaria, intentando resumir, en la medida de lo posible, las ideas principales que abordan este tema.

Para ello será necesario un estudio de la legislación vigente, ya que el tema de la seguridad está estrechamente unido a las directivas y normas que las diferentes organizaciones y naciones legislan. Tras esto, se desarrollará la estrategia de seguridad que se ha de seguir para conseguir una protección lo más eficaz posible para evitar los riesgos. Esto se acompañará con una explicación de los diferentes dispositivos de protección que se usan para conseguir esta protección. Y se finalizara con la introducción de dos normas que se utilizan a la hora de calcular el nivel de protección que tiene un sistema de seguridad.

El segundo objetivo por el que se desarrolla este trabajo, es realizar una aplicación práctica relativa a la seguridad de máquinas. En este caso, se desarrollará la función de parada de emergencia accionada mediante un pulsador de parada de emergencia. Esto se hará gracias al hardware y el software con el que cuenta el laboratorio del Departamento de Ingeniería de Sistemas y Automática de la Escuela de Ingeniería de Bilbao. En lo relativo al hardware, se emplearán componentes de Siemens, exceptuando el pulsador de parada de emergencia de la empresa Schneider Electric, y para el software, se utilizará la herramienta TIA Portal de Siemens.

Con todo esto se espera que este trabajo despierte el interés respecto al tema de la seguridad de máquinas, ya que con los avances que está trayendo consigo la Industria 4.0 se plantearan nuevos retos a la hora de implementar seguridad. Y que, asimismo, sirva de base para futuros desarrollos más detallados.

4. Estudio teórico

4.1. *Safety and Security*

Antes de comenzar con el desarrollo del trabajo, es indispensable aclarar que, en castellano y en otros idiomas, la palabra seguridad se usa para describir tanto *safety* como *security*. Por lo que frecuentemente se pierde el matiz de ambas definiciones.

Safety: "La condición de estar a salvo de sufrir o causar daño, lesión o pérdida." [1]
Se usa para referirse al estado en el que se tiene el control de los aspectos que causan el riesgo, por lo tanto, se protege contra el riesgo totalmente involuntario.

Security: "Protección de individuos, edificios, organizaciones, países o activos contra amenazas externas como delitos o ataques externos." [2]
Por lo que, el termino *security* está enfocado a las acciones deliberadas.

En este trabajo el uso de la palabra seguridad hará referencia exclusivamente al significado de *safety*.

4.2. Legislación relativa a la seguridad de maquinas

4.2.1. Directivas de la Unión Europea

Teniendo en mente el objetivo de impulsar un mercado abierto en el Espacio Económico Europeo (EEE), el cual está compuesto por todos los estados miembros de la Unión Europea e Islandia, Liechtenstein y Noruega, todos los miembros están tratando de legislar con leyes comunes. Esta comunión de leyes también se aplica en aquellas que definen los requisitos de seguridad para la maquinaria y su uso, estableciendo así, que maquinas pueden suministrarse a o dentro del EEE.

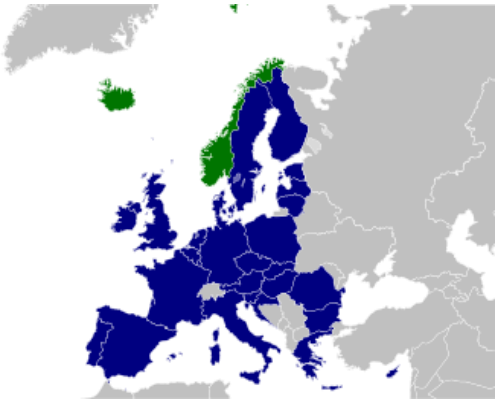


ILUSTRACIÓN 2. PAÍSES PERTENECIENTES AL EEE

De este modo surgen varias directivas europeas (legislación de obligado cumplimiento) para seguridad de máquinas y equipos industriales. Este trabajo se sustentará en la que más relevancia tiene: **La Directiva de maquinaria (2006/42/EC)**. La Directiva de maquinaria cubre el suministro de nueva maquinaria, modificaciones en maquinaria y hasta componentes de seguridad.

En la Directiva, además, se da una definición para maquinaria, la cual se aplica en la industria: "Conjunto de partes o componentes vinculados entre sí, de los cuales al menos uno es móvil, asociados para una aplicación determinada, provisto o destinado a estar provisto de un sistema de accionamiento distinto de la fuerza humana o animal." [3]

La versión que está actualmente en vigor de la Directiva de maquinaria, la (2006/42/CE), entró en vigencia el 29 de diciembre de 2009, y reemplazó a la anterior (98/37/EC). Esta nueva versión fue hecha ya que necesitaba ser actualizada para introducir legislación en los cambios tecnológicos y los métodos que se habían dado en esos años.

4.2.2. Términos relativos a la legislación

- Los **requisitos esenciales de seguridad y salud**, también denominados RESS, tienen como objetivo garantizar que la maquinaria sea segura y que este diseñada y construida de forma que sea posible su uso, regulación y mantenimiento, en todas las fases de su ciclo de vida útil, sin poner en peligro a ninguna persona que opere con ella.

- La **evaluación de conformidad** es el procedimiento con el cual se determina el grado de cumplimiento de un proceso, producto o servicio con los requisitos establecidos.

  Para la evaluación de conformidad se deberá presentar un archivo por parte del diseñador o empresa que diseñe la maquina, en el que se demuestre la conformidad con los RESS. Este

documento deberá incluir toda la información pertinente, como resultados de pruebas, esquemas, especificaciones, etc.

- Las **normas armonizadas EN** son "un tipo concreto de normas europeas elaboradas por un organismo europeo de normalización a raíz de una solicitud, llamada "mandato", de la Comisión Europea. Las empresas pueden aplicar normas armonizadas para probar que sus productos o servicios cumplen los requisitos técnicos de la legislación europea." [4]

  Por lo tanto, estas normas armonizadas son voluntarias. Sin embargo, por lo anteriormente mencionado, es aconsejable cumplir con estas normas, ya que así se cumple con la Directiva, y por lo tanto la labor de demostrar conformidad con los RESS queda simplificada y el fabricante se asegura de cumplir indudablemente con la legislación. Además, conseguir la conformidad por otros métodos alternativos resulta demasiado compleja.

- El **expediente técnico** es el que proporciona prueba de conformidad con los RESS. Este documento tiene que incluir toda la información relativa, como resultados de pruebas, esquemas, especificaciones, etc. Debe estar disponible para entregarlo a la autoridad competente a la hora de que esta realice una inspección.

- La **Declaración CE de conformidad** se otorga a una maquina cuando esta cumple con todas las Directivas Europeas que le afectan y ha completado con éxito la evaluación de conformidad. Además posibilita la colocación de una etiqueta CE (Conformidad Europea).

4.2.3. Normas

Como ya se ha comentado, actualmente muchos países de todo el mundo están legislando con la intención de conseguir una armonización global de las normas, y el área de la seguridad en maquinaria no se queda fuera de esta idea, es más, es uno de las áreas en los que más se observa la armonización.

Así, existen dos organizaciones que legislan globalmente las normas de seguridad en maquinaria: **IEC (International Electrotechnical Commission)** la cual prepara y publica normas internacionales para tecnologías eléctricas, electrónicas y otras afines e **ISO (International Organization for Standardization)** que genera normas para diseñar, fabricar y usar maquinaria de manera más eficiente, segura y limpia. Estas organizaciones están compuestas por un centenar de países, y las normas que redactan son creadas por expertos internacionales en sus respectivos campos.

ILUSTRACIÓN 3. LOGOS DE IEC E ISO

Aunque existan estas dos grandes organizaciones, cada región y país aún mantiene sus organizaciones para legislar. En el caso de la EEE son **CENELEC (Comité Europeo de Normalización Electrotécnica)** y **CEN (Comité Europeo de Normalización)**. Las normas comunes que derivan de estas son Normas Europeas Armonizadas, reconocibles por el acrónimo EN.

ILUSTRACIÓN 4. LOGOS DE CENELEC Y CEN

Están normas están divididas en tres categorías jerarquizadas (ver ilustración 5):

- **Normas A.** Abarcan aspectos aplicables a todo tipo de máquinas.
- **Normas B:**
  - **Normas B1**. Abarcan aspectos específicos de seguridad.
  - **Normas B2**. Abarcan componentes y dispositivos de protección.
- **Normas C.** Abarcan tipos o grupos específicos de máquinas.

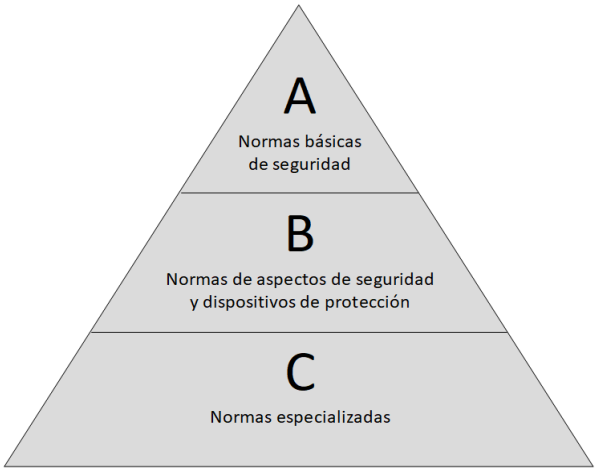


ILUSTRACIÓN 5. JERARQUÍA DE LAS NORMAS ARMONIZADAS EUROPEAS

Teniendo en cuenta lo que abarca cada tipo de norma, con el cumplimiento de una norma C, los RESS de dicha norma quedan automáticamente conformes. En caso de no contar con una norma C, es posible usar una A o B, teniendo así una conformidad total o parcial de los RESS.

Puntualizar que, aunque existan todas estas organizaciones, estas colaboran estrecha y constantemente, por lo que muchas de las normas EN van totalmente en línea con las ISO o IEC, llegando incluso a tener idénticos textos.

4.3. Estrategia de seguridad

Como se viene comentando en este trabajo, hace no muchos años, en la industria, se le daba importancia a lo puramente funcional. Es decir, lo mejor era una máquina que realizara su tarea de la manera más rápida posible.

Pero desde hace unos años a aquí, se ha ido observando que, para que una máquina sea viable, también tiene que ser segura. Y actualmente la seguridad ha pasado a ser una consideración principal.

Por eso, al ser un pilar importante a la hora de diseñar maquinaria, se ha de desarrollar una **estrategia de seguridad** apropiada. Para esto existen dos pasos que funcionan coordinadamente: la evaluación de riesgos y la reducción de riesgos (ver ilustración 6).

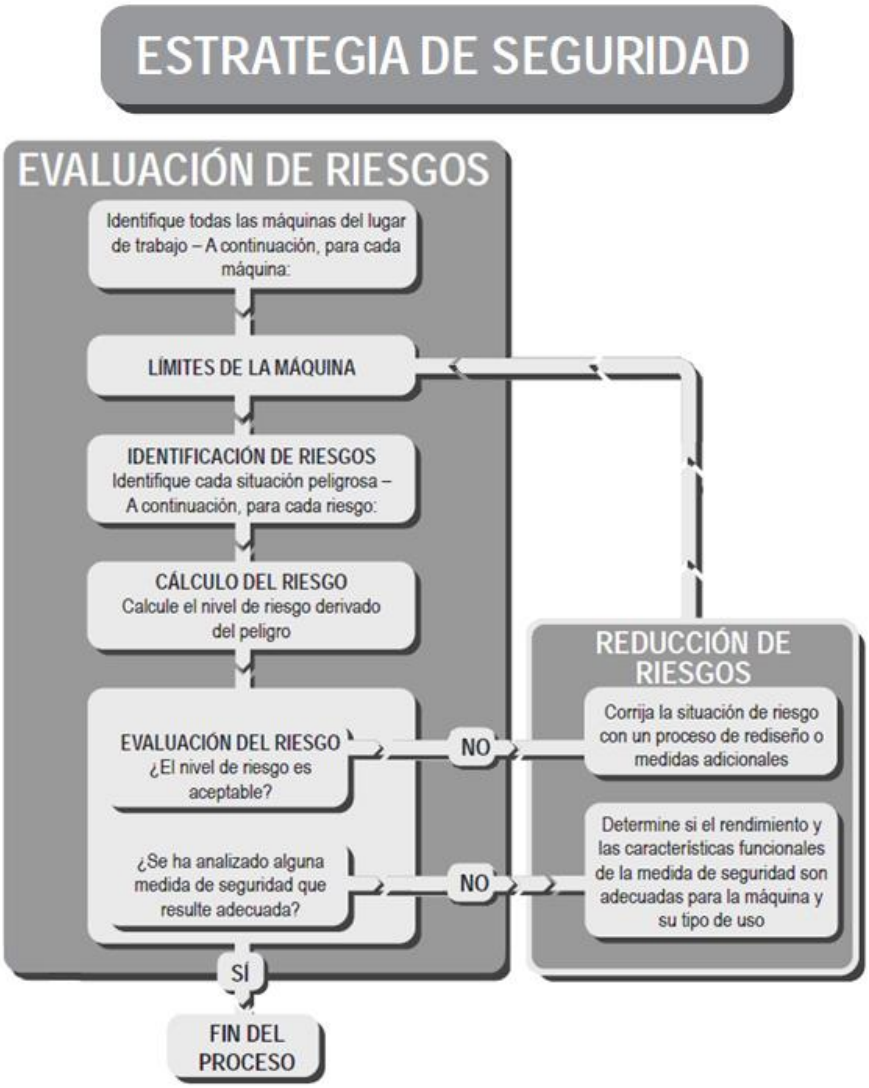


ILUSTRACIÓN 6. DIAGRAMA DE LA ESTRATEGIA DE SEGURIDAD

La **evaluación de riesgos** ha de estar fundamentada en la clara comprensión tanto de los límites de la maquina, como de sus funciones. Además de en todas las tareas que puedan requerírsele durante su vida útil.

Por su parte, en la **reducción de riesgos**, de ser necesaria, se escogen medidas de seguridad en función de la información adquirida en la fase de evaluación de riesgos.

Esta estrategia ha de ser muy minuciosa, documentando todo lo que se realice en el proceso. De esta forma podrá ser revisado fácilmente por terceras personas. Además, remarcar que esta estrategia no es únicamente para los fabricantes, también es válida para los usuarios de la máquina.

La posibilidad de que tanto el fabricante como el usuario puedan realizar la estrategia de seguridad es de gran importancia, ya que cabe la posibilidad de que una máquina haya sido

declarada segura por el fabricante, pero se utilice en situaciones no previstas por este. Un ejemplo puede ser una máquina fresadora que en vez de ser usada en un taller industrial es empleada en el taller de un colegio. Esta máquina escolar necesitara consideraciones adicionales con respecto a la otra, y estas serán aplicadas por el usuario. También está la posibilidad de que máquinas que individualmente sean seguras, al juntarlas se acoplen de un modo eventualmente inseguro.

Explicado esto, se entrará en detalle en los pasos esenciales a seguir para la obtención de una estrategia de seguridad adecuada.

4.3.1. Evaluación de riesgos

La evaluación de riesgos es un proceso útil con el que se obtiene información esencial que permite al fabricante o al usuario tomar decisiones razonables sobre cómo lograr la seguridad. También es un proceso repetitivo, ya que se realiza en distintas etapas del ciclo de vida de la máquina. Esto se debe a que la información obtenible varía dependiendo en la etapa del ciclo en la que se encuentre esta. No es lo mismo tomar la información en la etapa de diseño, que en la de construcción, instalación, puesta en servicio, mantenimiento o desmantelamiento.

Existen diversas normas que abarcan este tema, pero este trabajo se va a centrar en la más utilizada y la que mejor explica y abarca el tema a escala global: **EN ISO 12100**: "Seguridad de las máquinas. Principios generales para el diseño. Evaluación del riesgo y reducción del riesgo". Además, se usará de apoyo el informe técnico ISO: **ISO/TR 14121**: "Seguridad de maquinaria. Evaluación de riesgos". Más en concreto, la segunda parte de esta norma: ISO/TR 14121-2, la cual ofrece orientación práctica y ejemplos de métodos para realizar la evaluación de riesgos.

Determinación de los límites de la máquina

El objetivo de esta fase es el de obtener una clara comprensión de la máquina y sus usos. Para ello se realiza una recopilación y análisis de información correspondiente a los componentes, mecanismos y funciones de una máquina, teniendo en consideración todos los tipos de interacción humana con la misma (ya sean de correcto uso y operación, o de mal uso previsible).

Identificación de peligros y tareas

Como su nombre indica, se trata de identificar y también, listar todos los peligros de la máquina, así como su naturaleza y ubicación. Hay una amplia variedad de peligros a tener en cuenta, como pueden ser: trituración, corte, enredo, expulsión de piezas, substancias tóxicas, vapores, radiación, calor, ruido, etc.

También se ha de realizar una identificación de tareas que se realizan en esa máquina. Con estos datos y los datos de peligros se hace una comparación. Así, se comprueba si existe una posibilidad de que se dé una situación peligrosa. Es decir, de que exista la posibilidad de convergencia de un riesgo y una persona.

Estimación de riesgos

Esta es una de las fases más esenciales de la evaluación de riesgos. Donde lo más importante es el uso del sentido común. Hay que tener en cuenta lo que es factible y realista. Usar todos los datos y experiencias de los que se cuenta, e intentar trabajar con un equipo multidisciplinar.

Existen diversas formas de abordarla, pero como ya se ha mencionado, se seguirá el método y los principios establecidos en la norma EN ISO 12100, además de los parámetros indicados en la ISO/TR 14121-2. Estas dos normas servirán para cuantificar los riesgos. Esto es de vital importancia para saber qué medidas se han de tomar, ya que una máquina que tenga cualquier probable situación de peligro presenta un riesgo de daño personal. Cuanto mayor sea el riesgo de que este daño suceda, más importante es tomar medidas al respecto.

La norma EN ISO 12100 se apoya en dos normas a la hora de realizar la estimación del riesgo en maquinaria: **IEC/EN 62061**: "Seguridad de la maquinaria. Seguridad funcional de sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad", y **EN ISO 13849-1**: "Seguridad de la maquinaria. Partes de los sistemas de mando relativas a la seguridad. Parte 1: Principios generales para el diseño". (ver apartado 4.6.1. IEC/EN 62061 y EN ISO 13849-1)

4.3.2. Reducción de riesgos

Después de haber evaluado los riesgos, es el momento de tomar medidas para solucionar todos los peligros.

Las medidas de reducción de riesgo están jerarquizadas. Esta jerarquía está compuesta por tres puntos, que deben aplicarse en orden:

1- **Diseño inherentemente seguro**. Eliminación o reducción de todo tipo de peligros en la mayor medida posible. Es el único modo de reducir un riesgo a cero.

2- **Utilización de medidas de protección adicionales**. En casos en que el punto 1 no sea posible, se usan estas medidas para proteger a los operarios de las maquinas. Por ejemplo: resguardos fijos y móviles, barreras fotoeléctricas, tapetes de seguridad, dispositivos de enclavamiento, etc.

3- **Equipo de protección personal y/o formación técnica**. Cuando un riesgo no se puede eliminar con ninguna de los procedimientos anteriores, se debe formar a los operarios sobre cómo realizar un uso seguro de la máquina, y suministrarles equipo de protección específico. Además, la propia máquina debe llevar indicaciones, señales y dispositivos de advertencia. Todo esto indicado y suministrado por el proveedor de la máquina.

La reducción de riesgos frecuentemente resulta en el uso de una combinación de estas medidas.

Diseño inherentemente seguro (supresión del riesgo)

Como su nombre indica, este primer punto se realiza en la fase de diseño. Haciendo una buena evaluación y teniendo en consideración factores como materiales, requisitos de acceso, superficies calientes, métodos de transmisión, puntos de atrapamiento, niveles de voltaje, etc, es posible que el diseñador pueda evitar muchos de los posibles peligros que podrían darse en un futuro, pudiendo, en algunos casos, llegar a reducir los riesgos a cero.

El caso más simple es el de un área peligrosa que no requiera acceso. Con un buen diseño se puede meter dentro del cuerpo de la maquina o protegerla con un resguardo fijo, para que no pueda haber ningún tipo de contacto con el riesgo.

Sistemas y medidas de protección

Tras haber realizado el diseño inherentemente seguro, en la maquina solo deberían existir peligros en áreas que requieran acceso.

Se utiliza una amplia variedad de medidas de protección, dependiendo de las características de la máquina y las prestaciones que se deseen, para garantizar que únicamente se pueda acceder a la maquina mientras esta está en condición de seguridad. Asimismo, siempre se ha de tener presente que estas medidas no deben afectar a la eficiencia de la máquina.

Otro aspecto a tener presente es que estas medidas han de eliminar el riesgo de una puesta en marcha intempestiva. Esto es especialmente importante en las labores que requieran un largo periodo de intervención con la maquina; como las operaciones de mantenimiento, reparación o desmontaje. Para estas operaciones también se deberán utilizar equipos que aseguren el aislamiento y disipación de la energía en la máquina. Estos equipos deberán ser posteriormente bloqueados mediante elementos de bloqueo-etiquetado. El objetivo es posibilitar un acceso seguro de las personas a las áreas peligrosas de una máquina.

Prevención de puesta en marcha intempestiva

Una puesta en marcha intempestiva es cualquier puesta en marcha (arranque) inesperada. Puede ser causada debido a diversos motivos: por un fallo interno del sistema de control, por una acción humana inoportuna sobre un control de arranque, sensor, contactor o válvula, debido al restablecimiento de la alimentación de energía después de una interrupción o por alguna influencia externa (gravedad, viento, etc.) o interna sobre elementos de la máquina.

Según la norma **EN ISO 14118**: **"**Seguridad de las máquinas. Prevención de una puesta en marcha intempestiva", lo principal para evitar la activación inesperada es desconectar la energía del sistema y bloquear el sistema en estado desactivado.

Dispositivo aislador de energía

Un dispositivo aislador de energía es un dispositivo mecánico que evita físicamente la transmisión o la liberación de energía. Esta energía puede tener diferentes orígenes; eléctrico, neumático, hidráulico, de gas, de vapor, de líquidos, de láser o de gravedad.

Existe una amplia variedad de dispositivos para los diferentes tipos de energía. Algunos ejemplos son: el interruptor automático, el desconectador, el interruptor operado manualmente, una combinación de conector/socket o la válvula de operación manual.

Bloqueo y etiquetado

El bloqueo y etiquetado en la EEE lo regula la Directiva 89/655/CEE. Donde se determina que "todas las partes de un equipamiento deben fijarse con dispositivos claramente visibles con los cuales puedan ser separados de todas las fuentes de energía".

Como se ha mencionado, el bloqueo y etiquetado de seguridad tiene como objetivo evitar el arranque intempestivo de la máquina y la disipación de energía. Se emplea mientras se realizan tareas de servicio o mantenimiento, ya que las intervenciones durante las operaciones de fabricación normales deben estar cubiertas por las medidas de protección.

Se realiza con dispositivos de bloqueo LOTO (lockout-tagout) específicos para aislar las diferentes fuentes, que se fijan directamente a la máquina. Estos dispositivos se inmovilizan mediante candados y se marcan con etiquetas, las cuales indican, las personas con autorización para manejar los dispositivos y, la duración de los trabajos. Tras esto, se comprueba que los equipos están correctamente bloqueados y se señalizar la zona de trabajo con cintas, conos, etc. Al finalizar el trabajo el bloqueo sólo puede ser retirado por quien lo haya puesto.

ILUSTRACIÓN 7. DISPOSITIVO DE BLOQUEO, CANDADOS Y ETIQUETAS LOTO

Evaluación

Tras seleccionar la medida de protección, es importante repetir la estimación de riesgos antes de realizar su implementación. Éste paso a menudo se pasa por alto y esto resulta peligroso. Ya que, es posible, que al instalar una medida de protección, el operador de la máquina se sienta protegido contra el riesgo y comience a estar expuesto o acceda con mas frecuencia al peligro. Existiendo así un riesgo mayor que el previsto anteriormente en caso de que la medida de protección fallara.

Asimismo, mediante esta repetición de la estimación de riesgos, se comprueba si las medidas de protección planteadas son las adecuadas.

Formación técnica, equipo protector personal, etc.

Es fundamental que los operadores de cualquier maquina tengan la formación técnica necesaria en los procedimientos de trabajo seguros de dicha máquina, además de equipos de protección personal como guantes especiales, gafas de protección, máscaras, etc. Por su parte, la máquina debe llevar señales y marcas que aclaren donde se ubican los posibles riesgos residuales. Es responsabilidad del diseñador de la maquinaria especificar el tipo de formación, equipo y señales que son necesarias.

Remarcar que esto no constituye un método de protección principal, por lo que no se deben omitir las medidas de protección principales anteriormente mencionadas.

4.4. Sistemas de control de seguridad

La parte del sistema de control relativa a la seguridad que evita que se llegue a dar una condición peligrosa en cualquier máquina se conoce como sistema de control de seguridad. Cualquier sistema de seguridad debe continuar funcionando correctamente en todas las condiciones previsibles.

Como se irá desarrollando en los siguientes apartados, el sistema de seguridad puede ser un sistema independiente o puede estar integrado al sistema de control estándar. Además, su complejidad puede ir desde un sistema simple (una barrera fotoeléctrica y un pulsador de parada de emergencia conectados en serie), hasta un sistema con múltiples componentes que se comunican mediante software y hardware.

Los componentes del sistema de control de seguridad ejecutan una **función de seguridad.** Esta función de seguridad mantiene el equipo en un estado de seguridad con respecto a uno o varios peligros específicos.

Cualquier fallo de la función de seguridad puede derivar en una situación peligrosa. Una situación peligrosa no es aquella en la que una persona sufre daño, ya que esta puede identificar el peligro y evitar la lesión, si no que se da simplemente cuando una persona puede verse expuesta a un riesgo.

El sistema de seguridad tiene que diseñarse con un nivel de integridad de seguridad funcional o un nivel de rendimiento, según su capacidad para garantizar la actuación de su función de seguridad.

4.5. Componentes del sistema de control de seguridad

En este apartado se realizará una descripción de las medidas de protección de las que disponen los fabricantes y usuarios de maquinaria para eliminar o minimizar las fuentes de peligro (detectadas mediante la evaluación de riesgos) que una maquina o proceso tiene, y que tienen el riesgo de causar lesiones personales.

Las formas de hacer frente a esto se pueden englobar en dos grupos, y lo que los diferencia es, únicamente, la necesidad de acceso o no a la zona o área donde se encuentra la fuente del peligro.

- En caso de que la fuente de peligro este localizada en una zona de la máquina que no requiere acceso, se debe contar con un **resguardo fijo** en la maquinaria.

  Estos resguardos están regulados por la norma **ISO 14120**: "Seguridad de las máquinas. Resguardos. Requisitos generales para el diseño y construcción de resguardos fijos y móviles".

  Este tipo de resguardos, como su nombre indica, son fijos y permanentes (ver ilustración 8). Solo pueden ser desinstalados mediante el uso de herramientas. Pueden disponer de ventanillas para supervisar, de manera cómoda y sencilla, lo que está ocurriendo dentro del recinto que encierran.

  Tanto para el resguardo como para la ventanilla hay que tener muy en consideración una característica, el material con el que se fabrica. Este material ha de resistir durante un largo tiempo el entorno de operación; debe detener posibles proyectiles móviles que salgan de la máquina, resistir posibles fluidos de corte, rayos ultravioleta y demás interacciones con productos químicos. Por otro lado, ellos mismos no deben crear nuevos peligros, por lo que no deben tener bordes afilados ni puntiagudos, y deben estar situados a una distancia apropiada de la zona de riesgo.

ILUSTRACIÓN 8. RESGUARDO FIJO

- Si la fuente de peligro se localiza en una zona de la máquina que requiere acceso, se debe contar con **medidas de protección para detectar el acceso** a ese área peligrosa.

  Algunas bibliografías, reducen estas medidas únicamente al dispositivo de protección: resguardos móviles con interruptores de enclavamiento, barreras fotoeléctricas, tapetes de seguridad, controles bimanuales, mandos de validación, etc. Y esto es un error, ya que cuando se elige la detección como método de reducción de riesgos hay que tener claro que estos dispositivos no proporcionan la reducción de riesgo necesaria. Lo que conseguirá la función de seguridad deseada es un sistema de seguridad completo que inicie con el comando y termine con la implementación.

  Este sistema de seguridad usualmente consta de tres bloques:

  1- Uno o varios dispositivos de entrada que detecten el acceso al peligro: **dispositivos de protección.**

  2- Uno o varios **dispositivos lógicos** que procesen las señales de los dispositivos de protección, comprueben el estado del sistema de seguridad y activen o desactiven los dispositivos de salida.

  3- Uno o varios **dispositivos de salida** que son controlados por los accionadores.

4.5.1. Dispositivos de protección

Actualmente existe una amplia variedad de dispositivos para detectar la presencia de una persona que entra o que está dentro de una zona peligrosa. La selección de la mejor opción para una maquina en particular depende de varios factores, los más sencillos de tener en cuenta son: el lugar de colocación del dispositivo, la frecuencia de acceso, el tiempo de parada del peligro y la capacidad de contención de proyectiles, fluidos, etc. Es decir, la mejor medida de protección es aquella que proporcione la máxima protección con la mínima obstrucción a la operación normal de la máquina.

A la hora de conectar cualquier dispositivo de protección a un dispositivo lógico es necesario que este sea de seguridad. Además es habitual utilizar dos canales para conectar un sensor (1oo2) (ver apartado 4.5.3. Dispositivos lógicos). De esta manera se detectan posibles discrepancias que se puedan dar entre los canales, y así se consiguen niveles de seguridad más altos.

Para realizar la configuración hardware de cualquier dispositivo de protección, es necesario disponer de, por lo menos, una CPU que soporte seguridad (ver apartado 4.5.3. Dispositivos lógicos), módulos de entradas digitales estándar, módulos de potencia, módulos de entrada de seguridad y módulos de salida de seguridad (ver apartado 5.1.1. Montaje del hardware).

Resguardos móviles e interruptores de seguridad

Es frecuente optar por elegir protección mediante resguardos móviles (o accionables) cuando el acceso a la máquina es poco frecuente o existe la posibilidad de proyección de algún elemento. Al igual que para los resguardos fijos, la norma que regula los resguardos móviles es la ISO 14120.

Estos resguardos requieren de un interruptor de enclavamiento. Este interruptor se une a la puerta del resguardo y asegura que siempre que la puerta del resguardo no esté cerrada, se inicie una instrucción que desconecte la alimentación de la fuente de energía (eléctrica, neumática, hidráulica, etc) de la zona de peligro, ya sea directamente o mediante un contactor.

Otra función que poseen algunos interruptores es la de enclavar la puerta en posición cerrada y no permitir que se abra mientras la máquina no esté en condición segura.

Existen diferentes tipos de interruptores de enclavamiento dependiendo de la necesidad del usuario (ver ilustración 9). Todos ellos se rigen por la norma **EN ISO 14119**: "Seguridad de las máquinas. Dispositivos de enclavamiento asociados a resguardos. Principios para el diseño y la selección".

ILUSTRACIÓN 9. RESGUARDOS MÓVILES CON VARIOS TIPOS DE INTERRUPTORES DE ENCLAVAMIENTO (PILZ)

Dispositivos de detección de presencia

Cuando es necesario un acceso frecuente y la posibilidad de proyección de objetos es baja, se opta por los dispositivos de detección de presencia. Son apropiados, sobretodo, para maquinas que se detienen con rapidez después de que se desconecte el suministro de la fuente de energía. Estos dispositivos incluyen barreras fotoeléctricas de seguridad, escáneres láser de seguridad, tapetes de seguridad y bordes sensibles a la presión. Se catalogan como

dispositivos de activación ya que no restringen el acceso, sino que lo detectan. A la hora de seleccionar el dispositivo adecuado se recomienda el uso de la norma **EN IEC 62046**: **"**Seguridad de las máquinas. Aplicación del equipo de protección para detectar la presencia de personas".

Debido a que un operador puede entrar directamente al área peligrosa, es imprescindible que los dispositivos de detección se coloquen a una distancia de seguridad mínima que garantice que la maquina se ha detenido antes de que el operador llegue a la zona de peligro.

El cálculo de la distancia de seguridad se realiza, en el EEE, aplicando la norma **EN ISO 13855**: "Seguridad de las máquinas. Posicionamiento de los protectores con respecto a la velocidad de aproximación de partes del cuerpo humano".

La distancia de seguridad mínima de la zona de peligro hasta el punto de detección más cercano es:

$$S = K \times T + C$$

Donde:

K es la velocidad de aproximación previsible del cuerpo humano o de partes del cuerpo. Este parámetro, basado en datos de investigación, se define en la norma con 1600 mm/s para velocidad de paso y 2000 mm/s para la velocidad de extensión de un miembro superior.

T es el tiempo de parada general del sistema (en segundos). Este tiempo puede representarse como la suma de tres tiempos: $T = Ts + Tc + Tr$.

- Ts es el tiempo de parada de la máquina o equipo en el peor de los casos.
- Tc es el tiempo de parada del sistema de control en el peor de los casos.
- Tr es el tiempo de respuesta del dispositivo de protección.

C es el factor de penetración de profundidad. Es la posible aproximación a una zona peligrosa sin detección por parte del dispositivo de protección. Los factores de penetración de profundidad varían según el tipo de dispositivo y de aplicación. En el caso de las barreras fotoeléctricas, por ejemplo, varia dependiendo de la dirección de aproximación, el numero de haces, etc. Es necesario revisar la norma correspondiente a cada dispositivo para determinar el mejor factor de penetración de profundidad posible.

Barreras fotoeléctricas de seguridad

Las barreras fotoeléctricas están formadas por un transmisor (o emisor) y un receptor. El transmisor emite pulsos rápidos de un haz tras otro dentro de una secuencia. El receptor detecta los pulsos de los haces enviados, y abre sucesivamente los elementos de recepción con la misma secuencia. Así se crea un campo de protección entre el transmisor y el receptor (ver ilustración 10).

Están particularmente diseñadas para proteger a los operarios contra lesiones relacionadas al movimiento peligroso de la máquina. Debido a que permiten el acceso frecuente, rápido y seguro al área peligrosa, proporcionan un grado de seguridad óptimo permitiendo un incremento de la productividad.

La norma que las regula es la **EN 61496-1 y -2**: "Seguridad de las máquinas. Equipos de protección electrosensibles. Parte 1: Requisitos generales y ensayos. Parte 2: Requisitos particulares para equipos que utilizan dispositivos de protección optoelectrónicos activos".

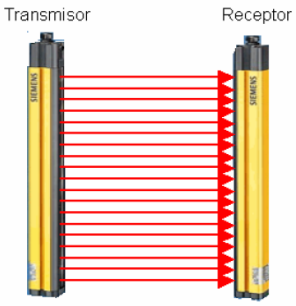


ILUSTRACIÓN 10. CAMPO DE PROTECCÓN DE UNA BARRERA FOTOÉLECTRICA

Además de estos dos elementos, las barreras fotoeléctricas pueden disponer de cuatro o dos sensores muting. El muting es una anulación prescrita de la función de protección. Es habitual que se emplee en el transporte de material a una zona peligrosa. Existen dos tipos de muting: el paralelo y el diagonal.

- Muting paralelo:

Cuando el producto entrante activa los sensores de muting MS11 y MS12 con un tiempo menor a un tiempo parametrizable, se activa el modo muting. El modo se mantiene activo siempre que MS11 y MS12 estén activados por el producto. De esta forma el producto puede pasar la barrera fotoeléctrica sin provocar el paro de la máquina. Antes de que los sensores MS11 y MS12 se desactiven, los sensores muting MS21 y MS22 deberán activarse dentro de otro tiempo parametrizable. De esta manera el muting continúa activo. El muting se termina cuando

uno de los sensores MS21 o MS22 se desactiva. El modo muting puede estar activo como máximo durante un tercer tiempo parametrizable.

El modo muting activo se indica por luces blancas de señalización.

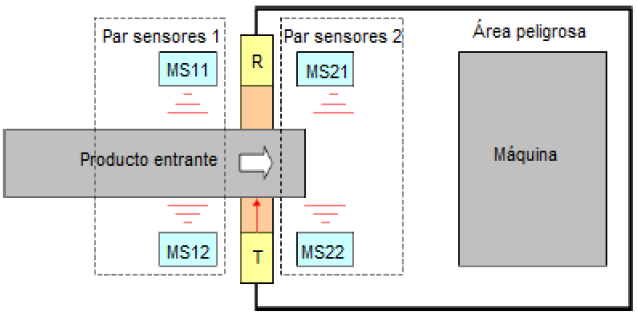


ILUSTRACIÓN 11. MUTING PARALELO DE BARRERA FOTOÉLECTRICA

- Muting diagonal:

El muting diagonal sigue el mismo principio que el paralelo, pero en vez de utilizar cuatro sensores de muting, utiliza dos sensores cruzados. Por lo que resulta más barato que realizar un muting paralelo, pero está limitado por el tamaño del producto entrante.

Si el producto entrante activa los sensores de muting MS11 y MS12 con un tiempo menor a un tiempo parametrizable, se activa el modo muting. El muting se mantiene activo siempre que MS11 y MS12 estén activados por el producto. El muting se termina si uno de los sensores MS11 o MS12 se desactiva. El modo muting puede estar activo como máximo durante un tiempo parametrizable.

Al igual que en el muting paralelo, este modo muting activo se indica por luces blancas de señalización.

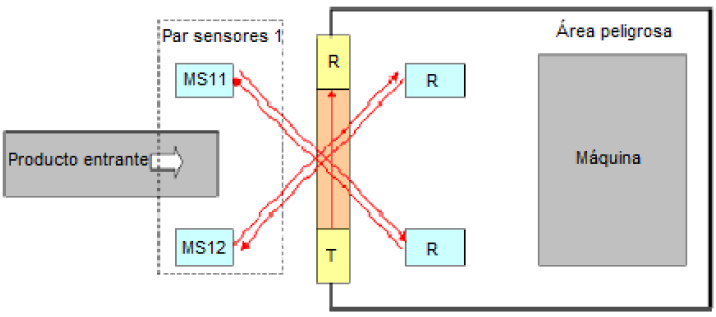


ILUSTRACIÓN 12. MUTING DIAGONAL DE BARRERA FOTOÉLECTRICA

La configuración hardware de una barrera fotoeléctrica con muting, tras realizar la correspondiente conexión de todos los módulos necesarios (ej. ver apartado 5.3. Cableado final), sigue los siguientes pasos:

1- Se conecta el receptor al módulo de potencia, y al módulo de entradas de seguridad con la configuración 1oo2.
2- Se conecta el transmisor a los pines del receptor que estén conectados al módulo de potencia.
3- Los sensores de muting al módulo de entradas digitales estándar. Son necesarias cuatro entradas.
4- La luz de señalización del muting se conecta al módulo de salidas de seguridad.

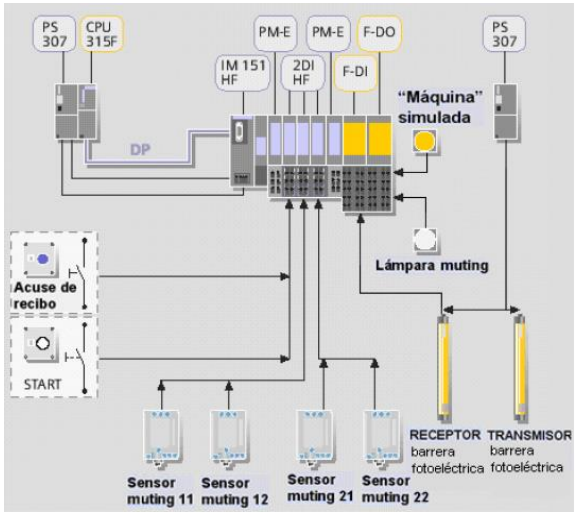


ILUSTRACIÓN 13. CONEXIÓN DE UNA BARRERA FOTOÉLECTRICA CON MUTING PARALELO (SIEMENS)

Escáneres láser de seguridad

Los escáneres láser crean un plano de detección (ver ilustración 14) mediante un espejo giratorio que desvía los pulsos de luz sobre un arco. El ángulo de rotación del espejo determina la ubicación del objeto. Por medio de una técnica conocida como “tiempo de vuelo”, el escáner es capaz de detectar la distancia a la que se encuentra del objeto. Sabiendo la ubicación y la distancia, el escáner es capaz de determinar la posición exacta del objeto.

Al igual que las barreras fotoeléctricas los escáneres láser están regulados por la norma **EN 61496-1.**

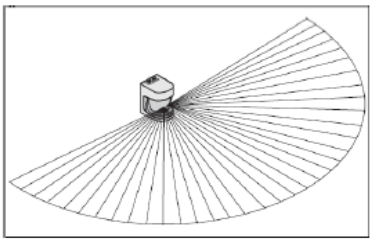


ILUSTRACIÓN 14. PLANO DE DETECCIÓN CREADO POR UN ESCANER LÁSER

Para el correcto funcionamiento de un escáner láser, únicamente es necesario realizar conexión a un módulo de entradas seguras. En caso de necesitar una luz indicadora de activación del escáner, esta tendría que ir conectada al módulo de salidas seguras.

Tapetes o alfombras de seguridad sensibles a la presión

Los tapetes de seguridad se utilizan para proporcionar resguardo a una zona concreta del suelo alrededor de una máquina. Se usan frecuentemente en zonas cerradas que encierran varios equipos, sistemas de fabricación flexibles o celdas robóticas. Generalmente se colocan varios tapetes interconectados alrededor del área de peligro formando una matriz (ver ilustración 15). La presión aplicada al tapete origina que se inicie una instrucción que desactive la alimentación de la fuente de energía al punto de peligro.

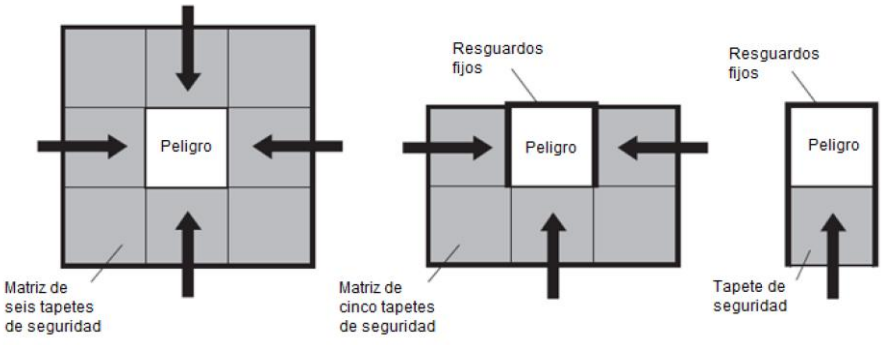


ILUSTRACIÓN 15. FORMAS DE COLOCACIÓN DE TAPETES DE SEGURIDAD

Es fundamental utilizar un sistema de fijación adecuado y seguro para evitar cualquier movimiento de los dispositivos.

Los tapetes de seguridad se conectan directamente a módulos de entradas de seguridad con configuración 1oo2. En caso de que se utilice una matriz de tapetes, estos deberán ir interconectados.

La norma que regula los tapetes de seguridad es la **EN ISO 13856-1**: "Seguridad de las máquinas. Dispositivos de protección sensibles a la presión. Parte 1: Principios generales para el diseño y ensayo de alfombras y suelos sensibles a la presión".

Bordes sensibles a la presión

Los bordes sensibles a la presión son tiras que se instalan al borde de piezas móviles que presenten algún riesgo de atrapamiento, trituración o corte. En caso de que la pieza móvil golpea al operador, o viceversa, el borde sensible se comprime e inicia una instrucción que desactiva el suministro de la fuente de energía del peligro.

Los bordes se rigen por la norma **EN ISO 13856-2**: "Seguridad de las máquinas. Dispositivos de protección sensibles a la presión. Parte 2: Principios generales para el diseño y el ensayo de los bordes y las barreras sensibles a la presión".

ILUSTRACIÓN 16. BORDE SENSIBLE A LA PRESIÓN

Para conseguir un borde sensible a la presión funcional, solamente es necesario conectarlo a un módulo de entradas de seguridad con la configuración 1oo2. Los bordes posibilitan tanto conexión en serie como en paralelo (ver ilustración 17).

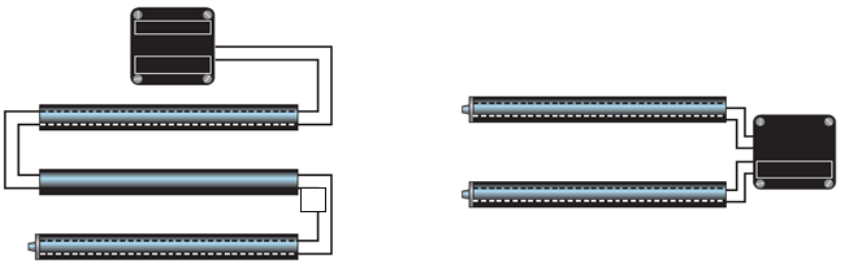


ILUSTRACIÓN 17. CONEXIONES EN SERIE Y PARALELO DE BORDES SENSIBLES A LA PRESIÓN

Mandos bimanuales o a dos manos

Los mandos bimanuales se utilizan para evitar el acceso mientras la máquina está en condición de peligro. Están regulados por la norma **ISO 13851**: "Seguridad de las máquinas. Dispositivos de mando a dos manos. Aspectos funcionales y principios para el diseño".

Están formados por dos controles que deben operarse simultáneamente (a 0,5 segundos uno de otro) para iniciar la máquina. Esto garantiza que ambas manos del operador estén ocupadas

en una posición segura, de tal manera que no puedan estar en el área peligrosa. La operación de los controles ha de ser continua durante condiciones peligrosas. En el instante en el que el operador suelte cualquiera de los controles la operación de la máquina debe detenerse. En caso de que esto ocurra, es necesario soltar el otro control para que la maquina pueda volver a arrancar. Esto imposibilita la manipulación de uno de los controles y accionar el mando con una sola mano. Además, la máquina no puede ir de un ciclo a otro sin soltar y pulsar ambos botones. Esto evita la posibilidad de que se bloqueen los controles y la máquina funcione de manera continua. Asimismo, es habitual que los mandos bimanuales incluyan un pulsador de parada de emergencia. Por último, el diseño físico del mando debe garantizar una correcta operación a dos manos, e imposibilitar cualquier otro tipo de operación, con una mano y el codo, por ejemplo.

ILUSTRACIÓN 18. MANDO BIMANUAL O A DOS MANOS

El control a dos manos únicamente protege a la persona que los utiliza. Por lo que el operador debe ser capaz de ver los accesos a la zona peligrosa, ya que otro trabajador podría no estar protegido.

Las conexiones hardware del mando bimanual tienen una complejidad mayor que las conexiones vistas hasta ahora. La ilustración 19 muestra los contactos de un mando bimanual, y la tabla 1 detalla las conexiones de los terminales de un mando bimanual y un módulo de terminales de un módulo de entradas de seguridad

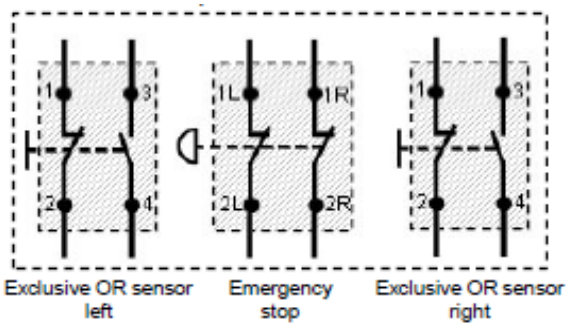


ILUSTRACIÓN 19. CONTACTOS DE UN MANDO BIMANUAL O A DOS MANOS

TABLA 1. CONEXIONES ENTRE UN MANDO BIMANUAL Y UN MODULO DE TERMINALES PARA F-DI

Mando bimanual		Módulo de terminales de F-DI
Exclusive OR sensor left	1	5
	3	1
	2	9
	4	
Emergency stop	1L	3
	2	7
	1R	11
	4	15
Exclusive OR sensor right	1	6
	3	2
	2	10
	4	

Nota: Para la numeración de los terminales del módulo de entrada de seguridad ver apartado 5.3. Cableado final

Dispositivos o mandos de validación

Los dispositivos de validación son controles que usualmente se utilizan para que los operadores accedan a una zona peligrosa en condiciones de riesgo reducido.

Hay interruptores de dos o tres posiciones:

- Cualquier interruptor de dos posiciones se encuentra:
  - Activado cuando se opera el accionador.
  - Desactivado cuando no se opera.

- Un interruptor de tres posiciones está:
  - Posición 1: Inactivo mientras no se acciona.
  - Posición 2: Activo cuando se mantiene en la posición intermedia.
  - Posición 3: Inactivo cuando el accionador se desplaza más allá de la posición intermedia.

  Además, al retornar de la posición 3 a la 1, el circuito de salida no debe cerrarse al pasar por la posición 2.

La norma **IEC/EN 60947-5-8**: "Aparamenta de baja tensión. Parte 5-8: Aparatos y elementos de conmutación para circuitos de mando. Interruptores de mando de validación de tres posiciones" regula los interruptores de tres posiciones.

Los dispositivos de validación deben disponer de una señal que indique si están activos, y deben emplearse junto con otras funciones de seguridad.

ILUSTRACIÓN 20. DISPOSITIVOS O MANDOS DE VALIDACIÓN

4.5.2. Parada de emergencia

La parada de emergencia no se encuentra dentro de la protección ya que no se considera como tal, sino que se considera un sistema de control relacionado con la seguridad. Esto es debido a que los dispositivos de parada de emergencia no evitan ni detectan el acceso a piezas peligrosas. Además, dependen de la interacción humana.

La función de parada de emergencia debe ser iniciada por una única acción humana. Al accionarla desconecta el suministro de las fuentes de alimentación de energía (corriente eléctrica, aire a presión, etc.) y detiene la máquina lo más rápidamente posible, sin crear peligros adicionales.

En algunos casos puede no interrumpir ciertos circuitos de la máquina que, al ser interrumpidos, podrían generar un nuevo peligro para el operario o la máquina, por ejemplo, los circuitos auxiliares (alumbrado, refrigeración, etc.). En otros casos pone en marcha ciertos movimientos, sin que estos representen un nuevo peligro, por ejemplo, los órganos de frenada de emergencia para obtener una parada más rápida.

Adicionalmente, según lo establezca la evaluación de riesgos, la parada de emergencia debe funcionar como parada de categoría 0 o de categoría 1. Las categorías de función de parada de emergencia se clasifican según la norma **IEC/EN 60204-1**, apartado 9.2.2. Existen tres categorías de función de parada:

- Categoría 0: Parada por supresión inmediata de la energía en los accionadores. En ocasiones se considera como una parada no controlada porque, por ejemplo, un motor seguiría girando libremente hasta que parase por inercia o una máquina que retiene accesorios podría dejar caer material.

- Categoría 1: Parada controlada. Mantiene disponible la energía en los accionadores para obtener la parada de la máquina y luego, cuando se obtiene la parada, desconecta la alimentación eléctrica.

- Categoría 2: Parada controlada. Mantiene disponible la energía en los accionadores. Una parada de producción normal se considera parada categoría 2.

El dispositivo de paro de emergencia debe estar siempre operativo y disponible, y con facilidades para el acceso rápido. En la Directiva de máquinas se especifica que los paneles del operador deben tener como mínimo un dispositivo de paro de emergencia. Queda en manos del usuario de la máquina, y así se recomienda, utilizar dispositivos adicionales en otras ubicaciones.

Todo lo relativo a las paradas de emergencia esta detallado en la norma **EN ISO 13850**: "Seguridad de las máquinas. Función de parada de emergencia. Principios para el diseño".

Pulsadores de paro de emergencia

Son los dispositivos más usados en maquinaria.

El pulsador tiene que ser un botón de tipo hongo o seta, de color rojo y con fondo amarillo (ver ilustración 21). Cuando se accione, este deberá bloquearse, y el comando de parada no podrá generarse si esto no ocurre. El reinicio del dispositivo de paro de emergencia debe ser manual y no debe crear una nueva situación de peligro.

ILUSTRACIÓN 21. PULSADOR DE PARADA DE EMERGENCIA

Interruptores accionados por cable

Para máquinas de gran longitud, como los transportadores, habitualmente es más eficaz emplear como dispositivo de parada de emergencia algún dispositivo accionado por cable a lo largo de la zona peligrosa.

Estos dispositivos utilizan un cable de acero conectado a interruptores de accionamiento de seguridad. Al tirar del cable se activa el interruptor y se corta la alimentación de la fuente de energía de la máquina (ver ilustración 22). Para distancias cortas, se coloca un interruptor en un extremo del cable y un resorte de tensión en el otro. Para distancias mayores, en cambio, se debe montar un interruptor en cada extremo, y el cable ha de ir apoyado y guiado con hembrillas, para asegurar que una sola acción inicie un comando de parada.

Es importante que los interruptores accionados por cable, además de detectar el tiro, detecten la holgura excesiva en el cable. Ya que esto permite controlar que el cable no se haya cortado.

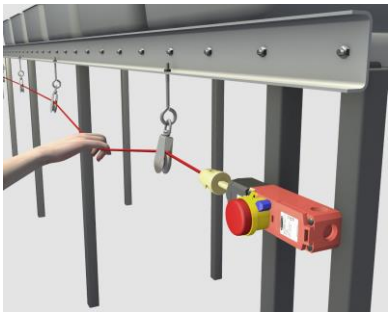


ILUSTRACIÓN 22. INTERRUPTOR ACCIONADO POR CABLE GUIADO CON HEMBRILLAS

4.5.3. Dispositivos lógicos

Los dispositivos lógicos desempeñan una función imprescindible en el sistema de control de seguridad. Estos dispositivos realizan la evaluación y la monitorización del sistema de seguridad, y permiten que la máquina se inicie o ejecutan instrucciones para detenerla.

Relés de seguridad

Los relés de seguridad (ver ilustración 23) generalmente se agrupan y forman lo que se conoce como módulos de relé de control de seguridad. Estos módulos desempeñan un papel clave en muchos sistemas de seguridad.

Los relés de seguridad realizan numerosas verificaciones en el sistema de seguridad, así como autoverificaciones de sus componentes internos. En consecuencia, un relé de seguridad correctamente escogido y configurado es capaz de proporcionar detección de fallos del sistema por medio de la comprobación de su entrada conectada y los dispositivos de salida.

ILUSTRACIÓN 23. RELÉ DE SEGURIDAD (PILZ)

Como los dispositivos de protección cuentan con diferentes clases de entradas, debido a que cuentan con características eléctricas distintas, es importante comprobar que dispositivo y relé sean compatibles. Existen dos tipos de relés: aquellos que están específicamente diseñados para un dispositivo en concreto u otros que pueden configurarse para interactuar con cada uno de los tipos de dispositivos.

Controladores programables de seguridad

Los controladores programables de seguridad fueron diseñados para proporcionar a los usuarios la misma facilidad para realizar una aplicación de control de seguridad a la que estaban acostumbrados con los PLC estándar. No obstante existen grandes diferencias entre ambos tipos de PLC.

Los PLC de seguridad utilizan numerosos microprocesadores para procesar las entradas y salidas (E/S), la memoria y las comunicaciones de seguridad.

Emplean un tipo de arquitectura que se conoce como 1oo2. Ya que cualquiera de los dos microprocesadores puede realizar la función de seguridad. Se efectúan análisis de diagnósticos para garantizar que ambos microprocesadores estén operando de manera sincronizada.

Cada circuito de entrada se prueba internamente múltiples veces por segundo para asegurar que siempre funcione correctamente. Lo mismo ocurre con las salidas, para garantizar que el PLC es capaz de desactivar la salida. En caso de que una de las salidas falle, esta es desactivada por las demás, y el fallo es reportado por el circuito de monitorización interno.

ILUSTRACIÓN 24. PLC DE SEGURIDAD (SIEMENS)

Software

Los PLC de seguridad se programan de manera similar a los PLC estándar. Todos los diagnósticos adicionales y la verificación de errores se realizan automáticamente por el sistema operativo.

La mayoría de softwares de los PLC de seguridad cuentan, además de con instrucciones lógicas, matemáticas, etc., con instrucciones especiales para escribir el programa para el sistema de seguridad. Estas instrucciones de seguridad están certificadas por terceros que garantizan que su operación este ajustada a la legislación vigente. Dentro de estas hay bloques de funciones disponibles para hacer interfaz con todos los dispositivos de seguridad, a excepción del borde de seguridad (debido a que utiliza tecnología resistiva).

Por último, gracias a la posibilidad de poder asignar los terminales haciendo uso del software, los dispositivos de entrada y salida se pueden conectar a cualquier terminal de entrada de seguridad y de salida de seguridad, respectivamente.

Controladores de seguridad integrada

Más adelante se desarrollaron controladores que integraban en una sola arquitectura de control las funciones de seguridad y las funciones de control estándar.

ILUSTRACIÓN 25. PLC DE SEGURIDAD INTEGRADA (SIEMENS)

Esta integración de ambos controles ofrece ventajas considerables. Como la posibilidad de ejecutar funciones secuenciales de alta velocidad, de movimiento, de accionamiento, etc., y de seguridad en un único hardware de control común. Esto reduce los costes de diseño, adquisición, instalación, puesta en servicio y mantenimiento. Aumentando así, la productividad y la velocidad de resolución de problemas.

Redes de seguridad

Las redes de seguridad actuales posibilitan a los fabricantes y usuarios utilizar múltiples entradas y salidas (E/S) de seguridad, dispositivos de seguridad, PLCs de seguridad, etc. con un único cable de red para comunicaciones de control estándar y de seguridad. Obteniendo así, con menores costes de instalación, sistemas de seguridad más complejos.

Adicionalmente, las redes de seguridad están diseñadas para detectar errores de transmisión e iniciar una función de reacción ante fallos adecuada. En la mayoría de los casos esto conduce a la desactivación de los dispositivos (estado de seguridad).

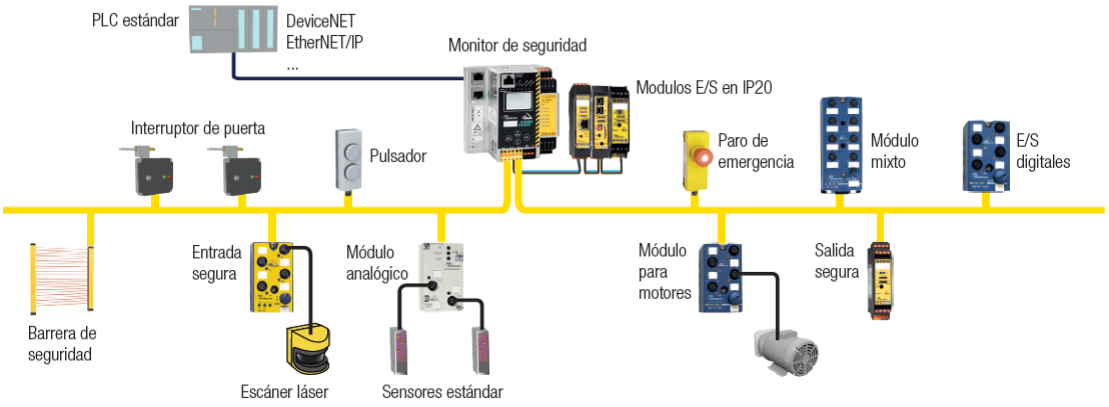


ILUSTRACIÓN 26. CONEXIÓN DE MULTIPLES DISPOSITIVOS MEDIANTE REDES DE SEGURIDAD

4.5.4. Dispositivos de salida

Relés de seguridad y contactores de seguridad

Al igual que los contactores y los relés estándar, los de seguridad se usan para desconectar la alimentación del accionador. Sin embargo tienen características especiales para poder usarlos con fines de seguridad.

A diferencia de los relés y los contactores estándar que permiten que se actúe manualmente sobre el contactor, los de seguridad están protegidos y no se puede actuar en ellos manualmente ya que los sistemas de seguridad sólo deben activarse o desactivarse en lugares y momentos específicos.

Además, los estándar están diseñados para conmutar cargas de entre 0,5 A y más de 100 A. Pero los dispositivos lógicos del sistema de seguridad generan una señal de respuesta que oscila entre unos miliamperios y decenas de miliamperios (normalmente a 24V CC). Por ello, para conmutar de manera fiable esta baja corriente, los relés y los contactores de seguridad utilizan contactos bifurcados con recubrimiento de oro.

ILUSTRACIÓN 27. CONTACTOR DE SEGURIDAD

Variadores y servos de seguridad

Los variadores y servos de seguridad pueden utilizarse para evitar el riesgo de movimiento mecánico al ejecutar tanto paradas de seguridad de producción normal como paradas de emergencia.

Para que un variador o un servo sea considerado de seguridad, tienen que tener canales redundantes para desconectar la alimentación del circuito de control. Es decir, deben tener múltiples canales para que en caso de que alguno falle otro ocupe su lugar.

Este enfoque redundante permite que el variador o servo de seguridad se emplee en circuitos de parada de emergencia sin necesidad de un contactor.

4.6. Seguridad funcional de sistemas de control

La seguridad funcional de sistemas de control se fundamenta en la norma **IEC 61508**: "Seguridad funcional de sistemas eléctricos, electrónicos y electrónicos programables relacionados con la seguridad".

Esta norma contiene los requisitos y las disposiciones aplicables al diseño de complejos sistemas y subsistemas electrónicos y programables. Además, ofrece dos definiciones que dejan claro a que hace referencia el término seguridad funcional:

- "La seguridad funcional es la parte de la seguridad general que depende de un sistema o equipo que funcione correctamente en respuesta a sus entradas". [5]

- "La seguridad funcional es la detección de una condición potencialmente peligrosa que resulta en la activación de un dispositivo o mecanismo de protección o corrección para evitar que ocurran eventos peligrosos o proporcionar mitigación para reducir las consecuencias del evento peligroso". [5]

Por lo tanto, la seguridad funcional es la interconexión de una amplia gama de dispositivos para formar un sistema de seguridad, el cual realiza una función específica relacionada con la seguridad.

Para lograr seguridad funcional se necesita, por un lado, el análisis de peligros y tareas (realizado en la evaluación de riesgos) que lleva a los requisitos funcionales de seguridad, esto es, a la función de seguridad. Y, por otro lado, la cuantificación de riesgos, la cual proporciona los requisitos de integridad de seguridad o el nivel de rendimiento.

Hay varias normas importantes de seguridad funcional pero en este trabajo se desarrollaran las dos que más relevancia tienen, las ya mencionadas anteriormente:

- **IEC/EN 62061**: Seguridad de la maquinaria. Seguridad funcional de sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad.

- **EN ISO 13849-1**: Seguridad de la maquinaria. Partes de los sistemas de mando relativas a la seguridad. Parte 1: Principios generales para el diseño.

4.6.1. IEC/EN 62061 y EN ISO 13849-1

Las normas IEC/EN 62061 y EN ISO 13849-1 proporcionan a los usuarios dos métodos para calcular la magnitud de riesgo que debe reducirse y la capacidad del sistema de control de reducir dicho riesgo. Ambas son normas armonizadas bajo la Directiva Europea de Maquinarias.

La norma IEC/EN 62061 describe dicha reducción en términos de SIL (*Safety Integrity Level*). Existen tres niveles de integridad de seguridad que se emplean en las maquinas, siendo el SIL

1 el más bajo y el SIL 3 el más alto. Excepcionalmente, en algunos sectores, en los que pueden producirse riesgos de mayor magnitud, se emplean normas específicas que incluyen el SIL 4.

EN ISO 13849-1 no utiliza el SIL, en su lugar, introduce el término PL (*Performance Level*). Existen cinco niveles de prestaciones, siendo PLa el más bajo y PLe el más alto. El término PL también puede traducirse como nivel de desempeño o nivel de rendimiento.

TABLA 2. RELACIÓN ENTRE PL Y SIL

PL	SIL
a	Ninguno
b	1
c	1
d	2
e	3

Nota: La tabla 2 únicamente sirve como orientación general. Nunca debe usarse para realizar conversiones.

Como los resultados que arrojan ambas normas son comparables, es habitual que los usuarios tengan problemas a la hora de decantarse por que norma aplicar. Estas son algunas consideraciones básicas para seleccionar la norma:

- La complejidad del sistema de seguridad:
  - Baja complejidad: EN ISO 13849-1
  - Alta complejidad: IEC/EN 62061

- Tipo de tecnología:
  - Sistemas eléctricos y electrónicos: IEC/EN 62061 o EN ISO 13849-1 (menos recomendable).
  - Sistemas neumáticos, hidráulicos y mecánicos: EN ISO 13849-1.

Pero además de estas consideraciones se dan situaciones en los que se debe elegir una de las normas por obligación.

- En caso de que el cliente exija específicamente demostrar la integridad de seguridad en términos de SIL.

- Cuando previamente se ha realizado una reducción de riesgos a la maquinaria con alguna de las normas con sus versiones menos recientes o antecesoras. (más habitual para EN ISO 13849-1).

Una vez seleccionada la norma, a la hora de aplicarla, ambas siguen esencialmente los mismos pasos:

1- Evaluar los riesgos.
2- Seleccionar las medidas de seguridad.
3- Arquitectura de diseño.
4- Validar.

Para finalizar, destacar la existencia de diversas herramientas software para el cálculo del SIL y PL. A pesar de que las normas cuentan con explicaciones detalladas, tablas de valores y otros medios que facilitan el cálculo de estos niveles, sigue siendo una labor complicada. Estas herramientas simplifican en gran medida estos aspectos de cuantificación y cálculo de la implementación de la norma.

Una de las herramientas más utilizada es SISTEMA (Safety Integrity Software Tool for the Evaluation of Machine Applications). Es la herramienta de software de integridad de seguridad para la evaluación de aplicaciones de máquinas de IFA (Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung), esto es, el instituto de investigación y pruebas del seguro legal de accidentes en Alemania. SISTEMA, además de ser de acceso abierto, emplea una amplia variedad de bibliotecas de diversos fabricantes, ofreciendo así a los usuarios una gran flexibilidad a la hora de introducir los componentes que forman su sistema de control.

ILUSTRACIÓN 28. LOGOS DE IFA Y SISTEMA

Además de esta herramienta, la mayoría de los fabricantes cuentas con herramienta propia. Por ejemplo, Pilz tiene Safety Calculator PAScal o Siemens dispone de SET (Safety Evaluation Tool).

4.6.2. Diseño del sistema según IEC/EN 62061

La norma IEC 62061: "Seguridad de la maquinaria. Seguridad funcional de sistemas de mando eléctricos, electrónicos y electrónicos programables relativos a la seguridad.", esta basada en los requisitos de la IEC 61508, pero centrada en el sector de la maquinaria.

1- Evaluación de riesgos

Para la asignación SIL, se debe evaluar, para cada riesgo identificado, la gravedad de la lesión, la frecuencia y/o tiempo de exposición al peligro, la probabilidad de que se produzca un suceso peligroso y la posibilidad de evitar o de limitar el daño. Estos tres últimos se agrupan en un factor conocido como clase CI. Más tarde esta clase se mapea contra la gravedad de la lesión en una matriz simple y así se establece el SIL necesario para el riesgo (ver tabla 3).

Gravedad de la lesión (Se)

Irreversible: muerte, pérdida de un ojo o brazo	4 puntos
Irreversible: extremidades fracturadas, pérdida de uno o más dedos	3 puntos
Reversible: se precisan tratamiento médico	2 puntos
Reversible: se precisan primeros auxilios	1 punto

Frecuencia y/o tiempo de exposición al peligro (Fr)

Duración de la exposición	> 10 min	≤10 min
≤1h	5 puntos	5 puntos
> 1h a ≤ 1 dia	5 puntos	4 puntos
> 1dia a ≤ 2 semanas	4 puntos	3 puntos
> 2 semanas a ≤ 1 año	3 puntos	2 puntos
> 1 año	2 puntos	1 punto

Los siguientes dos parámetros son de una gran importancia. Por ello, para realizar una correcta elección la norma ofrece explicaciones detalladas.

Probabilidad de que se produzca un suceso peligroso (Pr)

Muy alta	5 puntos
Probable	4 puntos
Posible	3 puntos
Raro	2 puntos
Insignificante	1 punto

Posibilidad de evitar o de limitar el daño (Av)

Imposible	5 puntos
Raro	3 puntos
Probable	1 punto

Clase CI = Fr + Pr + Av

TABLA 3. ASIGNACIÓN DEL SIL

Consecuencias	Gravedad	Clase CI				
		4	5 - 7	9 - 10	11 - 13	14 - 15
Muerte, pérdida de un ojo o brazo	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Irreversible, pérdida de dedos	3		(OM)	SIL 1	SIL 2	SIL 3
Reversible: tratamiento médico	2			(OM)	SIL 1	SIL 2
Reversible: primeros auxilios	1				(OM)	SIL 1

OM (Otras Medidas): Se recomienda el uso de otros parámetros

2- Selección de las medidas de seguridad

Se seleccionan todos los componentes del sistema de control de seguridad que serán necesarios para reducir el riesgo en cuestión y realizar la función de seguridad. Es decir, los dispositivos de protección, dispositivos lógicos y dispositivos de salida adecuados. Como ya se ha comentado, no es necesario seleccionar los tres tipos. En caso de que la reducción de riesgo se pueda realizar, por ejemplo, con un dispositivo de protección y uno lógico, no es necesario escoger uno de salida.

3- Arquitecturas hardware

En cuanto a las arquitecturas hardware EN 62061 define cuatro arquitecturas de subsistemas: A, B, C y D. Un subsistema es la subdivisión de primer nivel de un sistema que, en caso de fallar, provocaría un fallo de la función de seguridad.

En caso de que el fabricante no la proporcione, con estas arquitecturas se realiza el calculo de la probabilidad de fallo peligroso por hora (PFHd). Este termino se puede considerar otra forma de definir el SIL. Por lo que comparándolos se podrá validar si los componentes seleccionados cumplen el nivel de integridad necesario para la función de seguridad.

Antes de entrar en detalle con los tipos de subsistemas se definen los términos que se usaran en las formulas:

- Tolerancia a fallos de hardware: capacidad del sistema de realizar su función en presencia de fallos.
  - Tolerancia a fallos cero: la función no se realiza cuando se produce un fallo.
  - Tolerancia a fallos uno: la función se realiza cuando se produce un solo fallo.

- λ = tasa de fallos. Las unidades son fallos por hora.
- λ_D = tasa de fallos peligrosos.
- λ_{DssA} = tasa de fallos peligrosos del subsistema.
- β = probabilidad de fallos por causa común.
- T_1 = intervalo de prueba de calidad o vida útil.
- T_2 = intervalo de prueba de diagnóstico.
- DC = cobertura de diagnósticos. La relación de la frecuencia de fallos peligrosos detectados comparado con la frecuencia de todos los fallos peligrosos.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

Donde:

- λ_{DD} = tasa de fallos peligrosos detectados
- $\lambda\lambda_{Dtotal}$ = tasa de fallos peligrosos totales

Subsistema A

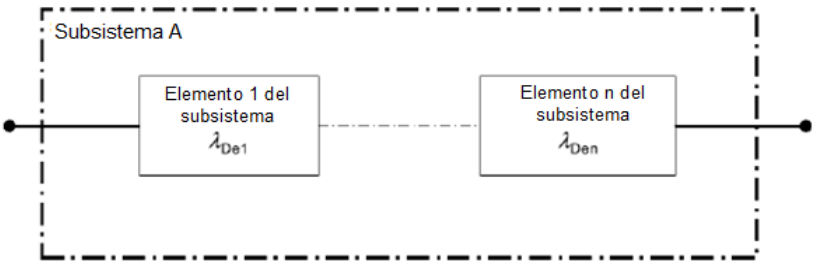


ILUSTRACIÓN 29. ARQUITECTURA LÓGICA DE SUBSISTEMA A

Esta es una arquitectura de canal único sin función de diagnósticos.

La probabilidad de fallo del subsistema es la suma de las tasas de fallos de los elementos individuales (e1, e2, ..., en). La probabilidad de fallos peligrosos se multiplica por 1 hora para calcular la probabilidad de fallo peligroso por hora.

$$\lambda_{DssA} = \lambda_{De1} + ... + \lambda_{Den}$$

$$PFH_{DssA} = \lambda_{DssA} \times 1h$$

Subsistema B

ILUSTRACIÓN 30. ARQUITECTURA LÓGICA DE SUBSISTEMA B

Esta arquitectura es tolerante a un solo fallo sin función de diagnósticos.

La PFHd del subsistema se calcula con las fórmulas:

$$\lambda_{DssB} = (1-\beta)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DssB} = \lambda_{DssB} \times 1h$$

Subsistema C

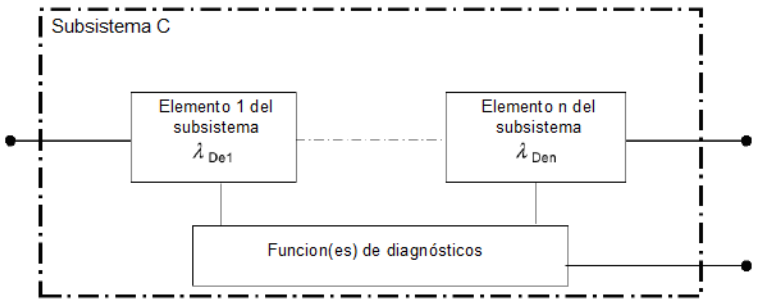


ILUSTRACIÓN 31. ARQUITECTURA LÓGICA DE SUBSISTEMA C

El subsistema C es tolerante a cero fallos con una función de diagnósticos.

La PFHd del subsistema se calcula mediante las fórmulas:

$$\lambda_{DssC} = \lambda_{De1}(1-DC_1) + ... + \lambda_{Den}(1-DC_n)$$

$$PFH_{DssC} = \lambda_{DssC} \times 1h$$

Se puede ver como las tasas de fallos de cada uno de los subsistemas se reducen gracias a la cobertura de diagnóstico de cada subsistema.

Subsistema D

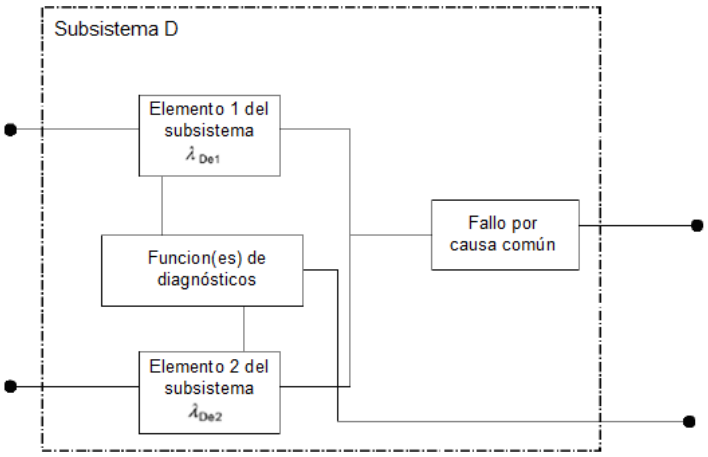


ILUSTRACIÓN 32. ARQUITECTURA LÓGICA DE SUBSISTEMA D

Este subsistema es tolerante a un solo fallo e incluye una función de diagnóstico.

La PFHd del subsistema depende del diseño de los elementos del subsistema.

- Si los elementos del subsistema son los mismos las formulas son:

$$\lambda_{DssD} = (1-\beta)^2\{[\lambda_{De}{}^2 \times 2 \times DC] \times T_2/2 + [\lambda_{De}{}^2 \times (1-DC)] \times T_1\} + \beta \times \lambda_{De}$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

- Si los elementos del subsistema son diferentes las fórmulas son:

$$\lambda_{DssD} = (1-\beta)^2\{[\lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2)] \times T_2/2 + [\lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2)] \times T_1/2\} + \beta \times (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

Subsistemas alineados en serie

Es habitual que una función de seguridad este formada por varios subsistemas alineados en serie, y que estos tengan diferentes arquitecturas.

Por ejemplo, es posible que se tenga un dispositivo de detección de subsistema B conectado a un dispositivo lógico de tipo D con un dispositivo de salida de subsistema C. En este caso, cada subsistema individual tendrá su PFHd calculado mediante las formulas anteriormente descritas. Estos valores se suman para obtener la PFHd global, y esta PFHd definirá el SIL logrado por esa función de seguridad.

Fracción de fallos seguros (no peligrosos) (SFF)

El SIL que se puede declarar para una función de control relativa a la seguridad está limitado, además de por la PFHd y la tolerancia a fallos de hardware, por la fracción de fallos seguros de los subsistemas (ver tabla 4).

La parte más crítica desde el punto de vista de la integridad de seguridad reside en cuantos fallos peligrosos no detectados hay en comparación con los otros tipos de fallos. Esto se expresa con la siguiente formula:

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{total}}$$

Donde:

- λ_{SD} = tasa de fallos seguros detectados
- λ_{SU} = tasa de fallos seguros no detectados
- λ_{DD} = tasa de fallos peligrosos detectados
- λ_{total} = tasa de fallos totales

La SSF y la tolerancia a fallos del hardware, imponen un SIL máximo para la arquitectura de un subsistema (ver tabla 4).

TABLA 4. RESTRICCIONES DE SIL CON RESPECTO A LA SSF Y LA TOLERANCIA A FALLOS DEL HARDWARE

Fracción de fallos seguros (SFF)	Tolerancia a fallos de hardware		
	0	1	2
< 60%	No permitido	SIL 1	SIL 2
60% - <90%	SIL 1	SIL 2	SIL 3
90% - <99%	SIL 2	SIL 3	SIL 3
≥ 99%	SIL 3	SIL 3	SIL 3

En caso de tener subsistemas alineados en serie, el nivel de integridad está limitado a ser menor o igual al SIL más bajo de cualquiera de los subsistemas.

4 - Validación

El SIL y la PFHd obtenidos en los anteriores pasos se comparan mediante el siguiente gráfico.

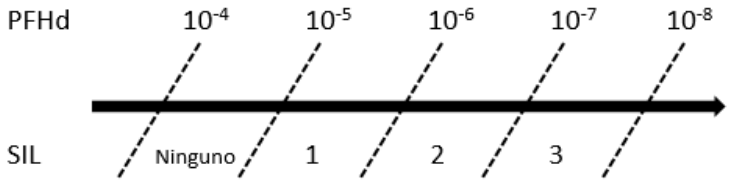


ILUSTRACIÓN 33. COMPARACIÓN DE SIL Y PFHD

Si la PFHd alcanzado es menor o igual que el requerido por el rango SIL asignado, los componentes escogidos cumplirán correctamente con la función de seguridad.

En caso de que la PFHd sea mayor que el rango SIL, no cumplirán la función de seguridad. El usuario tendría que escoger otros componentes u otro tipo de subsistema y volver a realizar el cálculo de la PFHd hasta alcanzar uno adecuado.

4.6.3. Diseño del sistema según EN ISO 13849-1

La norma ISO 13849-1: "Seguridad de la maquinaria. Partes de los sistemas de mando relativas a la seguridad. Parte 1: Principios generales para el diseño" entró en vigor por primera vez en 2007, y desde entonces anulo la anterior norma EN 954-1 (del mismo nombre), la cual se retiró completamente a finales de 2011. Esta nueva norma facilitó en gran medida

diversos cálculos, ya que se reemplazaron fórmulas matemáticas complejas por tablas precalculadas.

1- Evaluación de riesgos

El primer paso es calcular, para cada peligro, el nivel de prestaciones requerido (PLr). Este se determina durante la evaluación de riesgos. Para definir el PLr, la norma proporciona un gráfico de riesgos de tipo árbol de decisiones (ver ilustración 34), dentro del cual se introduce la gravedad de lesión, la frecuencia de exposición al peligro y la posibilidad de evitar el peligro.

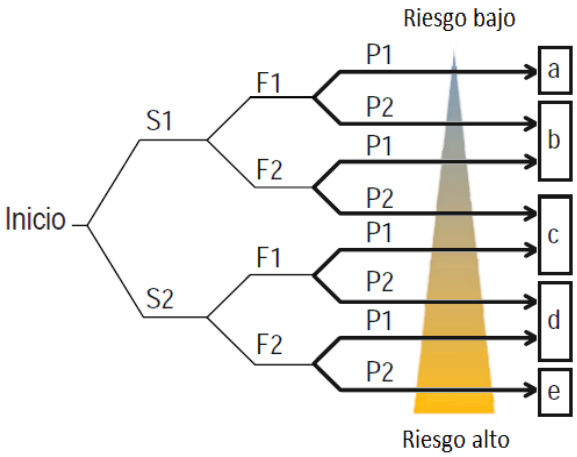


ILUSTRACIÓN 34. GRÁFICO DE RIESGOS PARA DEFINIR EL PLR

Gravedad de la lesión (S)

S1 = Lesión leve (normalmente reversible)
S2 = Lesión grave (normalmente irreversible o muerte)

Frecuencia o tiempo de exposición al peligro (F)

F1 = Raro a bastante frecuente o tiempo de exposición corto
F2 = Frecuente a continuo o tiempo de exposición largo

Posibilidades de evitar el peligro (P)

P1 = Posible bajo determinadas circunstancias
P2 = Apenas posible

El hecho de seleccionar el nivel de prestaciones mediante el uso de este tipo de grafico puede parecer algo subjetivo, pero la norma ofrece una guía estandarizada detallada que ayuda al usuario a seleccionar los pasos adecuados.

2- Asignación de medidas de seguridad

Se seleccionan todos los componentes del sistema de control de seguridad que serán necesarios para reducir el riesgo en cuestión y realizar la función de seguridad. Es decir, los dispositivos de protección, dispositivos lógicos y dispositivos de salida adecuados. Como ya se ha comentado no es necesario seleccionar los tres tipos. En caso de que la reducción de riesgo se pueda realizar, por ejemplo, con un dispositivo de protección y uno lógico, no es necesario escoger uno de salida.

3- Arquitecturas hardware

En cuanto a las arquitecturas hardware ISO 13849-1 continúa utilizando el termino categoría que se empleaba en EN 954-1. Existen cinco categorías diferentes: B, 1, 2, 3 y 4.

Categoría B

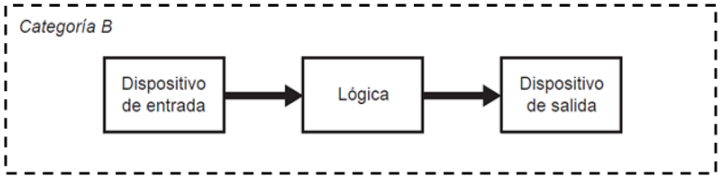


ILUSTRACIÓN 35. CATEGORÍA B DE ARQUITECTURA DESIGNADA

La categoría de arquitectura designada B es de canal simple sin diagnóstico. En el caso de un fallo único se puede perder la función de seguridad.

Las partes relacionadas con la seguridad de los sistemas de control y/o sus equipos de protección, así como sus componentes, deben diseñarse, construirse, seleccionarse, ensamblarse y combinarse de acuerdo con las normas pertinentes para que puedan resistir la influencia esperada. Se deben usar los principios de seguridad básicos.

Categoría 1

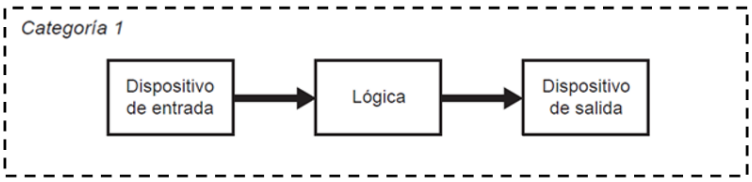


ILUSTRACIÓN 36. CATEGORÍA 1 DE ARQUITECTURA DESIGNADA

Al igual que la categoría B, esta arquitectura es de canal simple sin diagnóstico y puede fallar en caso de un fallo único, pero la probabilidad de ocurrencia es menor.

Además de los requerimientos de B, debe emplear principios y componentes de seguridad de eficacia probada.

Categoría 2

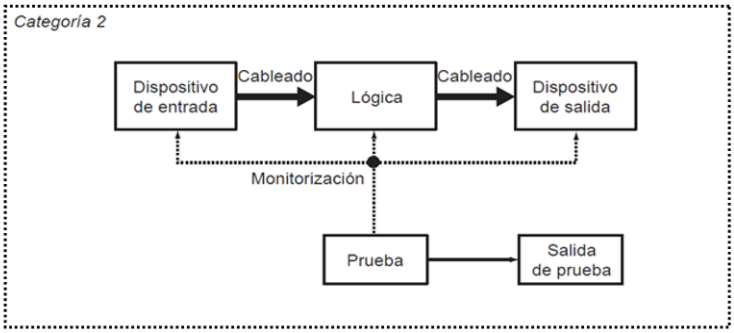


ILUSTRACIÓN 37. CATEGORÍA 2 DE ARQUITECTURA DESIGNADA

La categoría 2, además de los requerimientos de B y emplear principios y componentes de seguridad de eficacia probada, debe tener monitorización de diagnóstico a través de una prueba funcional del sistema o del subsistema. Ésta debe darse durante la puesta en marcha, y luego, periódicamente con una frecuencia de por lo menos cien pruebas por cada demanda sobre la función de seguridad.

Categoría 3

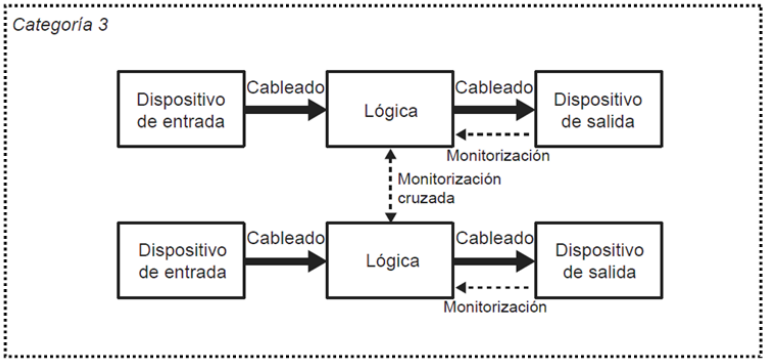


ILUSTRACIÓN 38. CATEGORÍA 3 DE ARQUITECTURA DESIGNADA

La categoría de arquitectura designada 3 tiene tolerancia a fallo único con diagnóstico.

Además de los requerimientos de B y emplear principios y componentes de seguridad de eficacia probada, en el caso de un fallo único no puede perderse la función de seguridad. La

forma más habitual de cumplir este requisito consiste en emplear una arquitectura de doble canal. Asimismo, también se demanda que, siempre que sea posible, se detecte el fallo único. La cobertura de diagnóstico (DC) debe ser mayor que el 60%.

Categoría 4

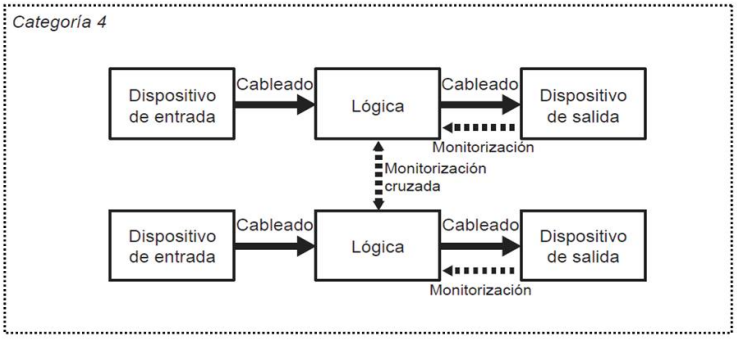


ILUSTRACIÓN 39. CATEGORÍA 4 DE ARQUITECTURA DESIGNADA

La categoría 4 tiene, al igual que la 3, tolerancia a fallo único con diagnóstico.

Tiene requisitos similares que la categoría 3, pero exige mayor monitorización, es decir, mayor cobertura de diagnóstico. En la categoría 4 tienen que detectarse todos los fallos individuales peligrosos y las combinaciones de fallos peligrosos. La DC tiene que ser mayor o igual al 99%.

Subsistemas alineados en serie

Es habitual que una función de seguridad este formada por varios subsistemas alineados en serie con diferentes arquitecturas.

Por ejemplo, es posible que se tenga un dispositivo de detección de categoría 1 conectado a un dispositivo lógico de categoría 4 con un dispositivo de salida de categoría 2. En este caso, cada subsistema individual tendrá su PFHd calculado mediante los métodos apropiados. Estos valores se suman para obtener la PFHd global, y esta PFHd definirá el PL logrado por esa función de seguridad.

4- Verificación del PL

Es habitual que el fabricante suministre la probabilidad de fallo peligroso por hora (PFHd).

En este caso únicamente es necesario comprobar que la PFHd sea menor o esté dentro del rango PLr definido. De no estarlo es preciso seleccionar otros componentes con menor PFHd que los anteriormente elegidos.

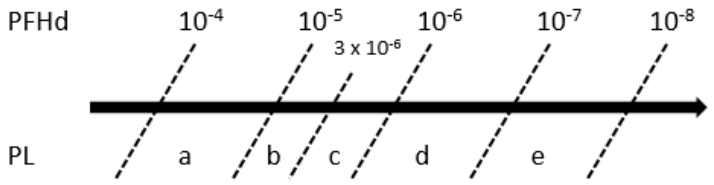


ILUSTRACIÓN 40. COMPARACIÓN DE PL Y PFHD

En caso de que el fabricante no proporcione la PFHd la norma EN ISO 13849-1 utiliza una combinación de diferentes factores para realizar la verificación del PL logrado:

- La arquitectura (categoría)

- El tiempo medio hasta el fallo peligros (MTTFd)

Representa el tiempo medio antes de la ocurrencia de un fallo que podría ocasionar el fallo de la función de seguridad. Se expresa en años y se calcula mediante las siguientes formulas.

- Canal individual o doble canal ambos idénticos

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$

- Doble canal ambos diferentes

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

TABLA 5. NIVELES DEL MTTFD

Rango del $MTTF_D$ de cada canal	Denotación del $MTTF_D$ de cada canal
3 años ≤ $MTTF_D$ < 10 años	Bajo
10 años ≤ $MTTF_D$ < 30 años	Mediano
30 años ≤ $MTTF_D$ < 100 años	Alto

Hay que tener en cuenta que la norma limita el MTTFd de un canal individual a 100 años, pero es habitual que los valores reales sean mucho más altos.

- La cobertura de diagnóstico (DC)

La cobertura de diagnósticos, como ya se ha explicado, es la relación de la frecuencia de fallos peligrosos detectados comparado con la frecuencia de todos los fallos peligrosos.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

TABLA 6. NIVELES DE LA DC

Rango de la DC	Denotación de la DC_{avg}
DC < 60%	Ninguno
60% ≤ DC < 90%	Bajo
90% ≤ DC < 99%	Medio
DC ≥ 99%	Alto

Por tanto para verificar que se ha conseguido el PLr se compara la arquitectura y la cobertura de diagnóstico con el MTTFd de cada canal haciendo uso de la siguiente figura.

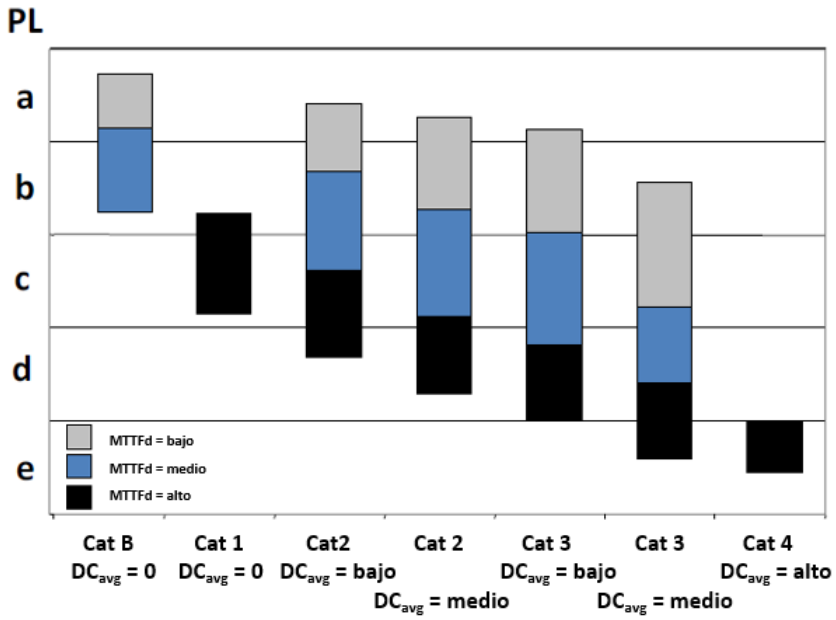


ILUSTRACIÓN 41. DETERMINACIÓN GRAFICA DEL PL

5. Aplicación práctica: función de parada de emergencia

En esta parte del trabajo se van a poner en práctica los conceptos abordados anteriormente. Para ello se va a desarrollar en detalle una función de parada de emergencia, tanto la parte de hardware necesaria, como el software programado en TIA Portal.

Se hará uso del equipo disponible en el laboratorio del Departamento de Ingeniería de Sistemas y Automatización de la Escuela de Ingeniería de Bilbao.

TABLA 7. COMPONENTES DE HARDWARE Y SOFTWARE

Componente	Nº	Tipo	Referencia hardware
Entrenador SIMATIC S7 [*]	1	1516F-3PN/DP Safety	ES2:C018OFOCT1717
Periferia descentralizada ET 200S	1	IM 151-3 PN HF	6ES7 151-3BA22-0AB0
Módulo de potencia	1	PM-E DC24..48V / AC24..230V	6ES7 138-4CB11-0AB0
Módulo de entradas digitales seguras	1	4 / 8 F-DI DC24V	6ES7 138-4FA03-0AB0
Módulo de salidas digitales seguras	1	4 F-DO DC24V / 2A	6ES7 138-4FB02-0AB0
Módulo de terminales	1	TM-P15S23-A0	
Módulo de terminales	2	TM-E30S46-A1	
Pulsador de parada de emergencia [**]	1	E-Stop Unit 2NC	
Contactor	1	Siemens SIRIUS	3RT1015-1BB42
Cable Ethernet	1		
Cable	1	Tipo y longitud a necesidad	
Conectores banana	4		
STEP 7 Professional	1	Versión V14	
STEP 7 Safety	1	Versión V14	

[*] No es necesarios el conjunto completo para la realización de la función de parada de emergencia. Únicamente son necesarios una fuente de alimentación, una CPU tipo F y un módulo de entradas digitales.

[**] En caso de no disponer de un pulsador de parada de emergencia, este se simula mediante el uso de dos cables. Son necesarios dos cables ya que estos pulsadores cuentan con dos canales normales cerrados para conseguir el nivel de seguridad requerido.

Antes de comenzar se debe comprobar el software que se tiene instalado. En la pantalla de inicio del TIA Portal, en el apartado de Software instalado, ha de aparecer instalado el paquete de seguridad STEP 7 Safety (ver ilustración 42). En caso contrario no se podrán realizar funciones de seguridad.

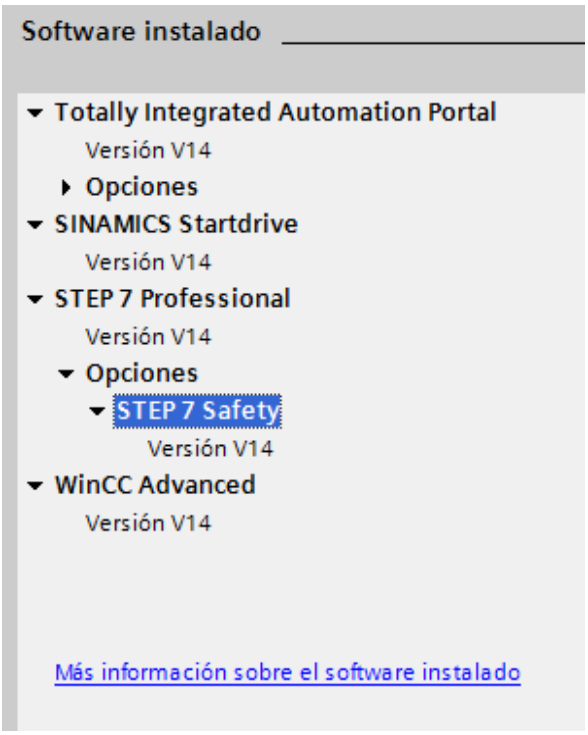


ILUSTRACIÓN 42. SOFTWARE INSALADO EN TIA PORTAL

5.1. Hardware

A continuación se ilustra una vista general de la configuración del hardware:

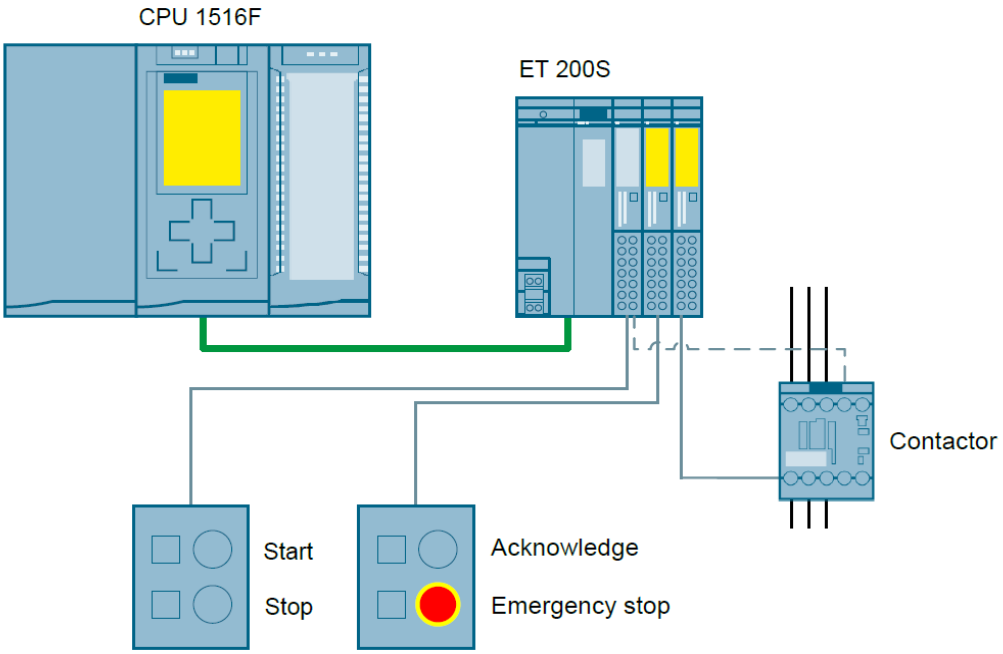


ILUSTRACIÓN 43. VISTA GENERAL DE LA CONFIGURACIÓN HARDWARE

5.1.1. Montaje del hardware

La **parte estándar** está montada y cableada sobre un bastidor en el que se especifican todas las entradas y salidas disponibles. Por lo que no es necesario entrar en detalles sobre esta.

ILUSTRACIÓN 44. PARTE ESTANDAR DEL HARDWARE

La **parte de seguridad** cuenta con un esclavo Profinet IO de seguridad.

Generalmente los esclavos Profinet IO de seguridad están compuestos de tres partes conectadas mediante módulos de terminales: una cabecera, un módulo de potencia y los módulos de la seguridad.

- Cabecera: Se ha de colocar una cabecera que soporte funciones seguridad. Para ello se emplean las cabeceras tipo HF (High Feature) y no las tipo ST (estándar). Estas últimas no son válidas para aplicaciones de seguridad debido a que poseen menos prestaciones.

- Módulo de potencia: Es imprescindible a la hora de iniciar una línea de seguridad. Es el módulo que suministra la alimentación a los módulos de seguridad.

- Módulos de seguridad: Son módulos de color amarillo. Como con los módulos estándar, existen módulos de entradas de seguridad, de salidas de seguridad y de ambas combinadas.

Se realiza el montaje del esclavo: una cabecera, un módulo de potencia, un módulo de entradas seguras y un módulo de salidas seguras.

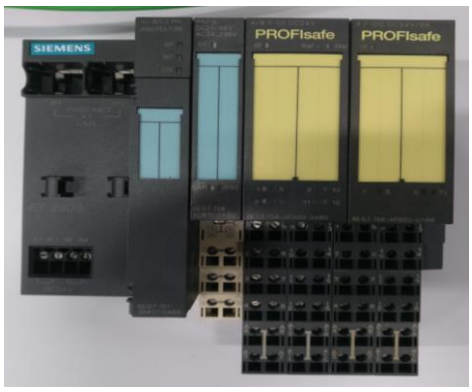


ILUSTRACIÓN 45. PARTE DE SEGURIDAD DEL HARDWARE

Una vez se tienen la parte estándar y el esclavo de seguridad montados, se realiza su conexión vía Profinet IO mediante un cable Ethernet. Se conecta un extremo del cable al PLC y el otro a la entrada X1 del esclavo.

5.1.2. Introducción del hardware en TIA Portal

Para comenzar la configuración, se busca en el Catálogo la CPU de la que se dispone. En este caso la CPU tiene número de hardware (o de referencia) 6ES7 516-3FN01-0AB0. Se realiza lo mismo para todos los módulos del PLC estándar. Se buscan los módulos PM, DI, DQ, AI y AQ,

haciendo uso de la referencia hardware que aparece en los mismos módulos. Obteniendo así la configuración del PLC.

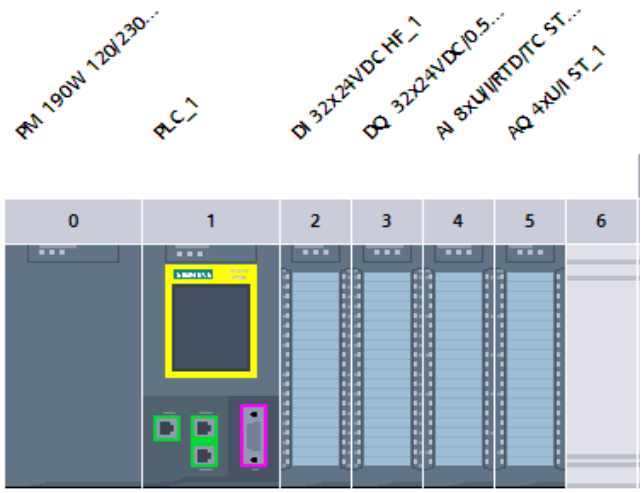


ILUSTRACIÓN 46. PARTE ESTANDAR DEL HARDWARE EN TIA PORTAL

El siguiente paso es introducir el esclavo Profinet IO a modo de periferia descentralizada. La cabecera en este caso es la IM 151-3 PN (Profinet) con número de referencia 6ES7 151-3BA22-0AB0. Tras esto se introducen los demás módulos de seguridad; módulo de potencia (o de alimentación), módulo de entradas seguras y módulo de salidas seguras. Obteniendo de esta forma la configuración que se observa en la imagen inferior.

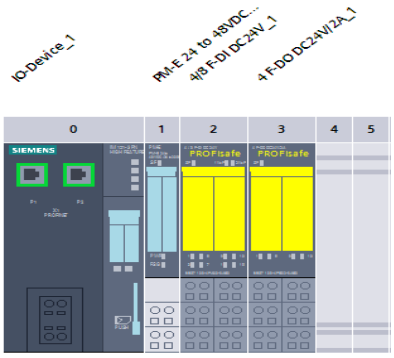


ILUSTRACIÓN 47. PARTE DE SEGURIDAD DEL HARDWARE EN TIA PORTAL

A continuación se realiza la conexión Profinet IO entre el PLC y la periferia descentralizada que se acaba de introducir. En este caso la periferia queda nombrada como IO-Device_1 (ver ilustracion 48).

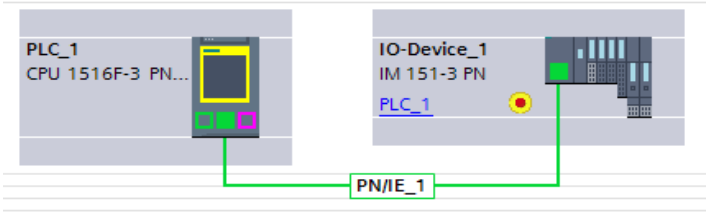


ILUSTRACIÓN 48. CONEXIÓN PROFINET IO

Por último hay que asignar una dirección IP al PLC y otra a la periferia. Mediante la pestaña "Online" → "Dispositivos accesibles", se verifica que la designación de IPs se ha realizado de manera correcta, y que se muestran ambos dispositivos.

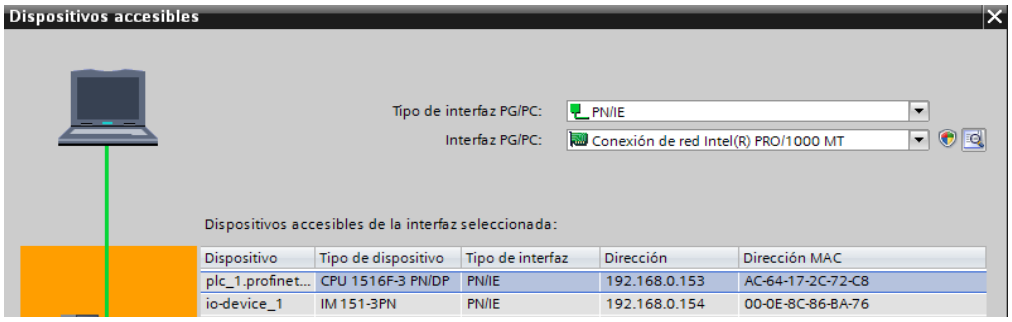


ILUSTRACIÓN 49. VERIFICACIÓN DE LA DESIGNACION DE IPS

Nota: La forma de direccionar una periferia descentralizada es mediante su nombre, y no su IP. La periferia posee un nombre, y mediante el TIA Portal se le configura una IP. Más tarde, cuando el PLC trate de realizar una conexión con dicha periferia, la buscara por su nombre. Una vez que la haya encontrado, le asignara la IP que previamente se la había configurado.

El siguiente paso es realizar la configuración de todos los módulos de los que se dispone, tanto de los estándar como de los de seguridad.

Módulos estándar

Al módulo de entradas digitales se le asigna como primera dirección la 0.0, y, como dispone de 32 entradas, abarcará hasta la dirección 3.7.

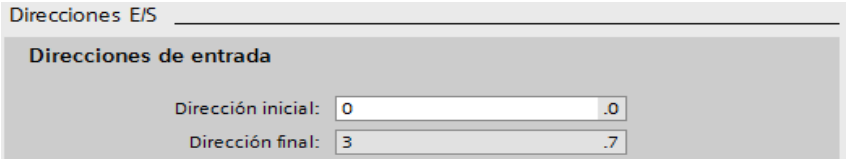


ILUSTRACIÓN 50. DIRECCIONES E/S DEL MÓDULO DE ENTRADAS DIGITALES

A los siguientes módulos estándar se les asignaran direcciones consecutivas. Estas direcciones no aparecerán en el programa, pero han de ser asignadas para que, al realizar la compilación del programa, este no de error.

- Salidas digitales: 0.0 - 3.7
- Entradas analógicas: 4 - 19
- Salidas analógicas: 4 - 19

Módulo de entradas de seguridad

Se comienza con la configuración de "F-parameters" (ver ilustración 51).

En la tecnología disponible en el laboratorio (una tecnología con varios años de antigüedad), el método para definir la dirección del módulo correspondiente es utilizando los switches de los que este dispone en uno de los laterales. Ha de coincidir la posición de estos switches con la entrada "F-destination adress" que se está configurando en el TIA Portal. En este caso se opta por la dirección 200, y, por lo tanto, se colocan los switches en 0011001000 (200 en número binario). Este número binario lo proporciona TIA Portal mediante "DIP-switch setting".

En caso de que un canal falle o se detecte divergencia de canales, el programa se comporta de dos maneras: pasiviza solo el canal o pasiviza el modulo al completo. Se decide pasivizar el canal ya que es lo habitual a la hora de programar seguridad en máquinas.

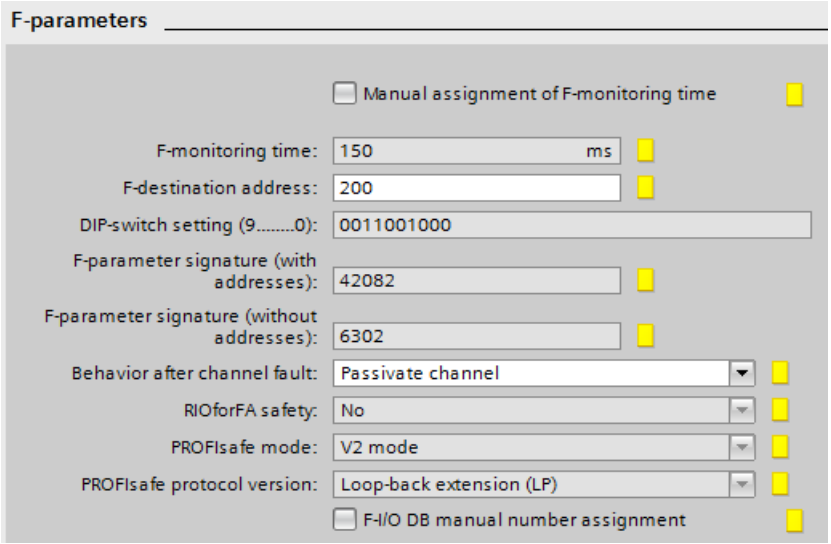


ILUSTRACIÓN 51. F-PARAMETERS DEL MÓDULO DE ENTRADAS DE SEGURIDAD

Nota: En todo el programa no pueden existir dos módulos iguales. No se pueden repetir dos direcciones. Además, dependiendo del tipo de CPU que se utilice, es posible que esta no abarque direcciones tan altas. Se recomienda usar direcciones más bajas, o en

caso de que esto no sea posible, modificar el "F- destination adress max" en los ajustes del PLC.

La configuración de "DI parameters" (ver ilustración 52) implica una configuración individual de canales.

Primer canal (Channel 0,4): Activado.

1- Se exige una evaluación 1oo2, ya que se va a cablear un pulsador de parada de emergencia. Con este tipo de evaluación se utilizan dos canales para un solo sensor.
2- Se selecciona que los dos canales sean equivalentes. Es decir, cuando uno de los canales tenga valor 0, el otro también lo ha de tener, e idem para el caso de valor 1.
3- Si existe discrepancia entre los canales estos se han de poner a 0.
4- La discrepancia dura 10 milisegundos como máximo. Esto es, La diferencia de tiempo aceptable entre que cae un canal y cae el otro no puede ser superior a 10 ms.
5- Se opta por no usar la señal "Test0-Signal" para reintegrar un canal después de que este se haya pasivizado por un error de discrepancia. Es lo habitual en programación de seguridad.

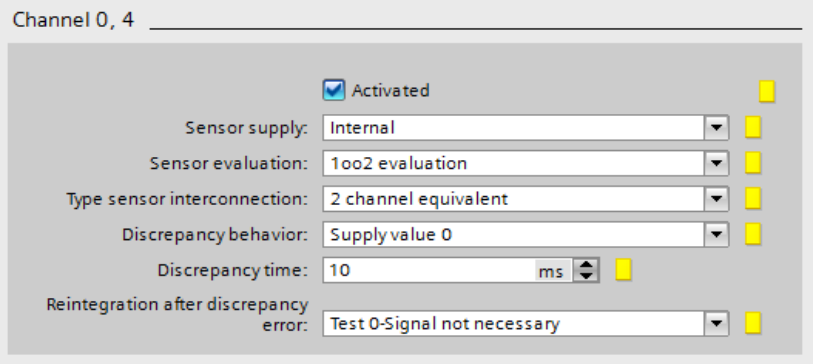


ILUSTRACIÓN 52. DI PARAMETERS DEL PRIMER CANAL DEL MÓDULO DE ENTRADAS DE SEGURIDAD

Los restantes canales del módulo de entradas seguras se desactivan ya que no van a ser usados (ver ilustración 53). En seguridad es imperativo desactivar todas las entradas o salidas que no vayan a ser utilizadas.

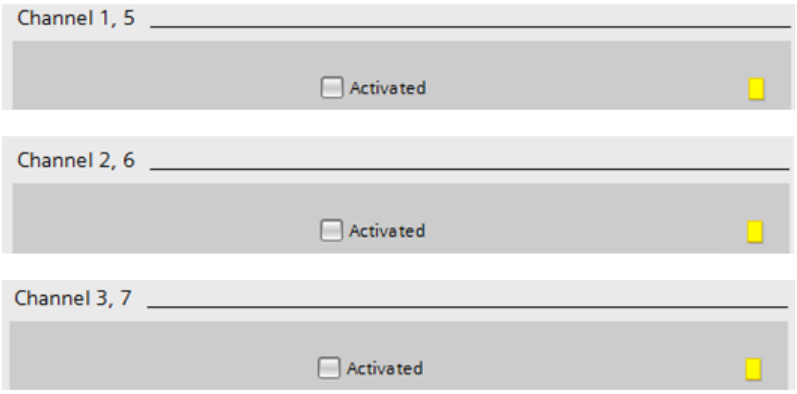


ILUSTRACIÓN 53. DI PARAMETERS DE LOS RESTANTES CANALES DEL MÓDULO DE ENTRADAS DE SEGURIDAD

Para finalizar la configuración del módulo, se seleccionan las direcciones de entrada. Estas serán las direcciones en la que irán las entradas del pulsador de parada de emergencia. En este caso se elige la 100. Por lo tanto el módulo de entradas seguras va a abarcar desde la dirección 100.0 hasta la 105.7.

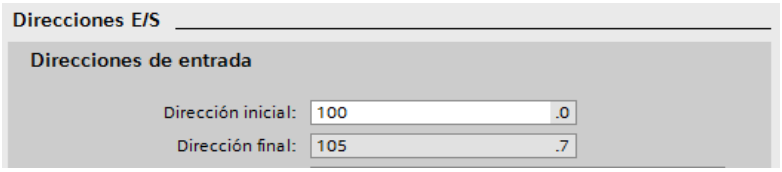


ILUSTRACIÓN 54. DIRECCIONES E/S DEL MÓDULO DE ENTRADAS DE SEGURIDAD

Módulo de salidas de seguridad

Configuración de "F-parameters" (ver ilustración 55). Se opta por elegir la dirección 201 (0011001001 en binario) y de pasivizar solamente el canal después del fallo de canal.

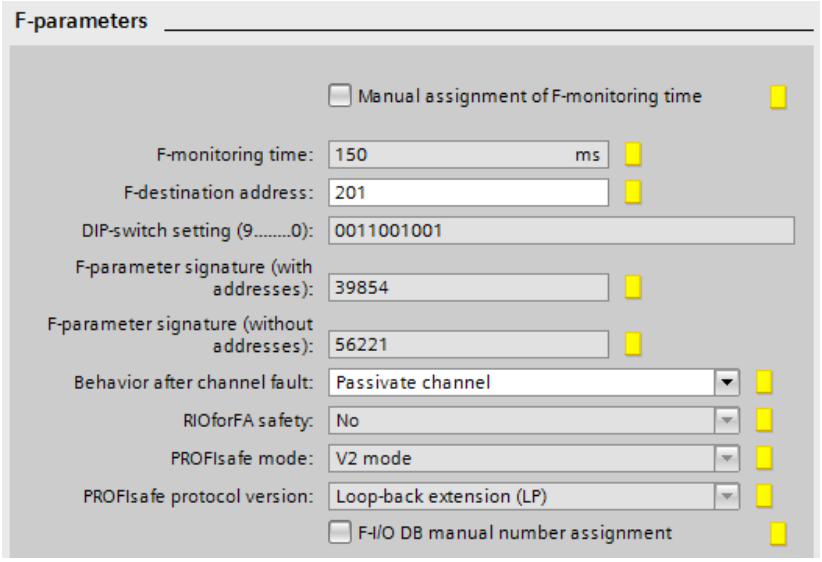


ILUSTRACIÓN 55. F-PARAMETERS DEL MÓDULO DE SALIDAS DE SEGURIDAD

En el caso de "DI parameters" (ver ilustración 56), el programa ofrece al usuario la posibilidad de activar o desactivar cada canal y de si se desea diagnosticar la rotura de hilo o no. En este caso solamente se activa el primer canal (Channel 0), puesto que en las salidas seguras únicamente se tendrá conectado un contactor. Para este canal se activa la rotura de hilo.

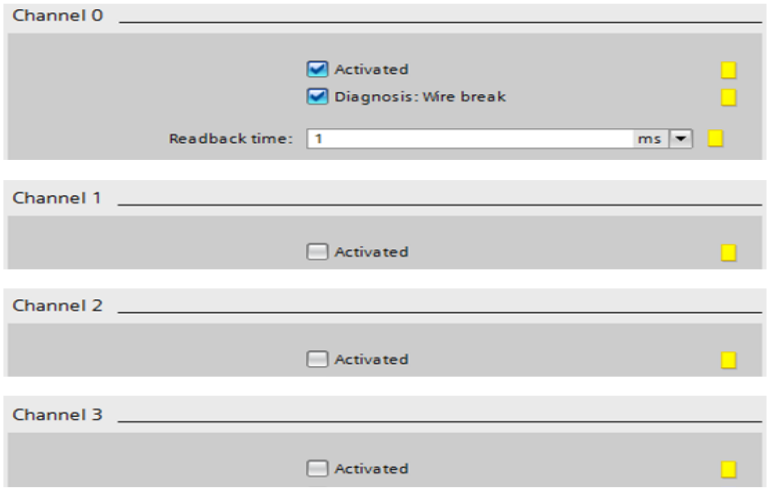


ILUSTRACIÓN 56. DI PARAMETERS DEL MÓDULO DE SALIDAS DE SEGURIDAD

Nota: En caso de no disponer de un contactor, y que únicamente se desee la visualización del LED en el módulo de salidas seguras, se ha de desactivar la rotura de hilo. Ya que, en caso contrario, el programa al no detectar paso de corriente se irá a error.

Se configuran las direcciones de salida al igual que con el módulo de entrada. En este caso se escoge la 110 (desde 110.0 hasta 114.7).

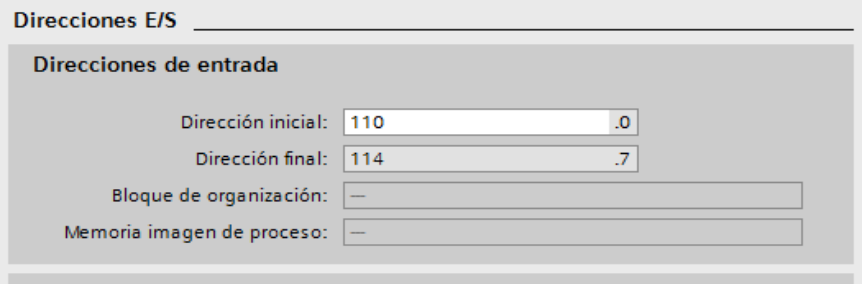


ILUSTRACIÓN 57. DIRECCIONES E/S DEL MÓDULO DE SALIDAS DE SEGURIDAD

Tras esto se realiza una compilación para comprobar que no existe error alguno y se da por finalizada la parte del hardware.

5.2. Software

Es un programa que tiene tanto parte estándar como de seguridad. Ambas partes se ejecutan en paralelo.

5.2.1. Parte estándar

La parte estándar de esta función de parada de emergencia procesa la señal para arrancar la máquina.

Consta de un OB1 que llama a un FB. Mediante estos se evalúan las siguientes señales:

- El botón de arranque.
- El botón de parada.
- La señal de error “fault” que se obtiene mediante el intercambio de datos entre estándar y seguridad (ver apartado 5.2.3. Intercambio de información).

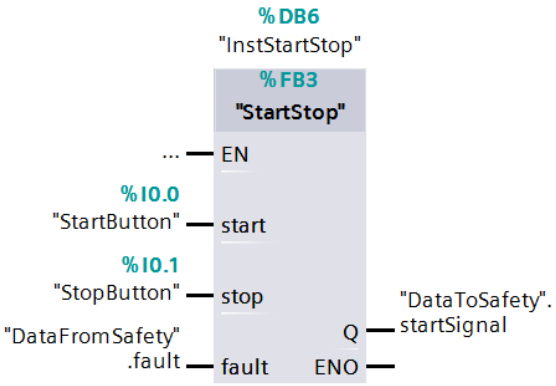


ILUSTRACIÓN 58. OB1: LLAMADA AL FB "STARTSTOP"

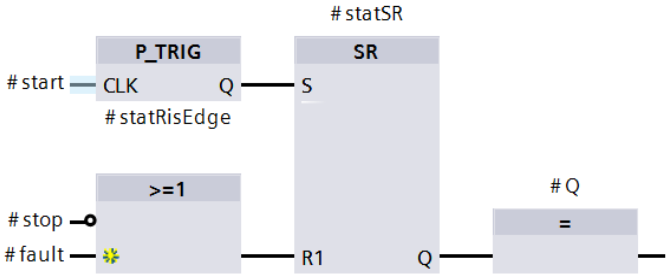


ILUSTRACIÓN 59. FB "STARTSTOP"

Como se puede extraer de los bloques, para obtener una señal “startSignal” de valor 1 se ha de cumplir que:

- La entrada estándar “StopButton” (%I1.0) tenga valor 1 (es normal cerrada).
- Por la entrada estándar “StartButon” (%I0.0) entre un valor 1.

Si el botón de parada es pulsado o se detecta un error mediante la señal “fault”, la señal "startSignal" se resetea (se pone a 0).

Nota: Es habitual que el pulsador de parada sea normal cerrado (NC). Ya que en caso de que fuera normal abierto (NA), y el cable sufriera una rotura o corte, no sería posible detener la máquina. Siendo NC la maquina se detendría, y el problema residiría en que no se podría volver a iniciar. Para la seguridad es mejor no poder activar una máquina que no poder detenerla. Por esto mismo, los botones de parada de emergencia son siempre NC.

5.2.2. Parte de seguridad

OB ("FOB_1")

Toda la seguridad se encuentra en "F-runtime group" (ver ilustración 60). Este se va a estar ejecutando con un OB cíclico ("FOB_1") que tiene como características propias: un número, un tiempo de ciclo y una prioridad. Este "FOB_1" tiene la tarea de llamar a un FB ("FB2"). Este "FB2" es el programa principal de seguridad (MainSafety). Es decir, todo lo que se haga de seguridad en este proyecto va a estar dentro de este FB o llamado desde el.

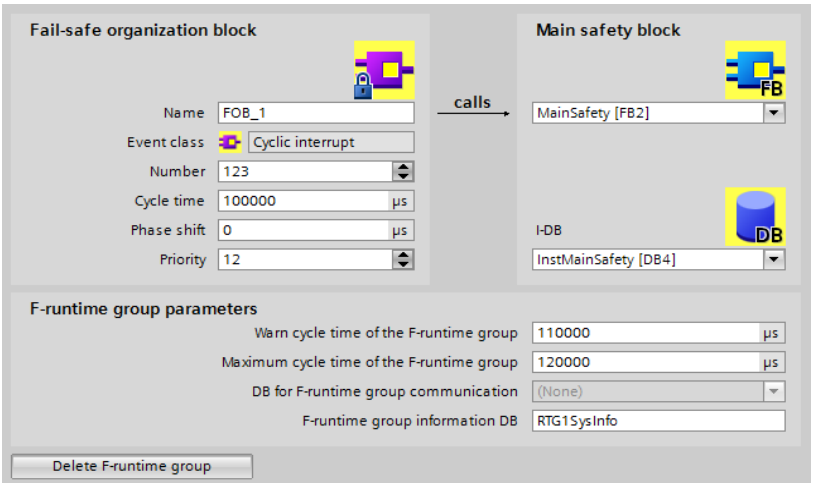


ILUSTRACIÓN 60. F-RUNTIME GROUP DEL PROGRAMA DE SEGURIDAD

Nota: Los tres bloques de seguridad que se utilizan para el programa de seguridad se encuentran en la librería del TIA Portal: "Instrucciones básicas" → "Safety functions".

FB ("MainSafety[FB2]")

- El primer segmento contiene un bloque ESTOP1.

Este bloque monitoriza el pulsador de parada de emergencia. Si el pulsador de parada de emergencia no ha actuado, la instrucción establece que la salida Q tiene un valor true.

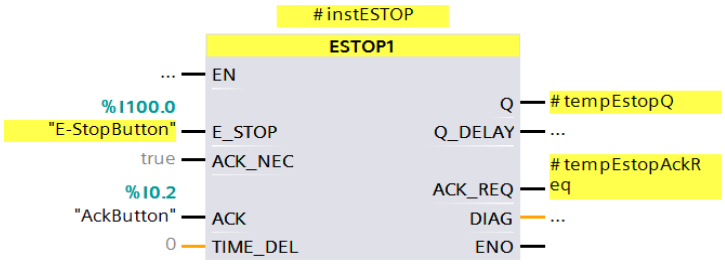


ILUSTRACIÓN 61. SEGMENTO 1: BLOQUE ESTOP1

En caso de presionar la parada de emergencia, además de tener que desbloquear "E-StopButton" (%100.0), se requiere de un reconocimiento (ack). A través de ACK_REQ se envía la instrucción de que se requiere un reconocimiento, y mediante ACK_NEC (con valor true) que este ack es necesario. Esto se consigue por medio de "AckButton" (%I0.2).

Nota: Esta necesidad de ack es imprescindible a lo hora de reactivar una máquina después de una parada de emergencia. No sirve únicamente con que alguien desbloquee el botón de parada, si no que se tiene que reconocer que todo se encuentra como antes de la parada.

TIME_DEL tiene valor 0 ya que se ha programado una parada de categoría 0. En caso de requerir una parada de categoría 1, habría que asignar un valor numérico a TIME_DEL.

Nota: En algunas aplicaciones es conveniente determinar un TIME_DEL. Un ejemplo de esto es un elevador con parada tipo rampa. Debido a que, en caso de realizar una parada brusca, por inercia, los objetos del elevador pueden elevarse del suelo y romperse al caer.

- El segundo segmento se compone de un bloque FDBACK y un bloque AND a su entrada.

Este bloque FDBACK cambia los valores de salida del contactor y monitoriza su correcto funcionamiento gracias al circuito de feedback.

Nota: Este feedback del funcionamiento del contactor es obligatorio si se desean obtener niveles altos de PL o SIL. Ya que el contactor no es un elemento de seguridad, y, por lo tanto, necesita ser monitorizado.

El contactor se encenderá cuando:

- La etiqueta temporal "#tempEstopQ" (señal de salida del bloque ESTOP1) tenga valor 1.
- La señal "startSignal" (señal de salida del programa estándar) tenga valor 1.

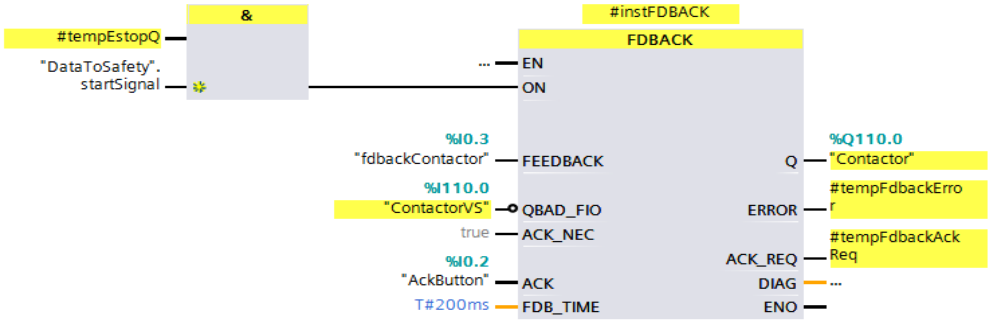


ILUSTRACIÓN 62. SEGMENTO 2: BLOQUE FDBACK CON BLOQUE AND

La señal FEEDBACK ("fdbackContactors" (%I0.3)) tiene que cambiar de forma inversa a la señal de salida Q dentro del tiempo FDB_TIME. En caso de que esto no suceda, el programa lo considerara un error y el contactor se apagara de nuevo.

Si el contactor cae se necesita un ack mediante "AckButton". Esto lo exigen, como en el caso anterior, ACK_REQ y ACK_NEC.

Nota: Al disponer de un contactor se selecciona un FDB_TIME de valor bajo para que la función de parada de emergencia cumpla con niveles de seguridad elevados. Pero, en caso de no disponer de un contactor, y que solamente se deseen visualizar los LEDs de las salidas de los módulos, se recomienda subir este tiempo a 2 o 3 segundos para tener margen para activar el feedback manualmente.

- El tercer segmento está compuesto por un bloque OR.

Mediante este bloque se recoge la información de posibles errores y se escriben en el valor "fault" para reportarlos al programa estándar.

ILUSTRACIÓN 63. SEGMENTO 3: BLOQUE OR

El valor de "fault" es false si se cumple alguna de las siguientes afirmaciones:

- La etiqueta temporal "#tempFdbackError" tiene valor true.
- La etiqueta temporal "#tempEstopQ" tiene valor false.

Esto es, cuando se pulse el botón de parada de emergencia o cuando no se reciba feedback de los contactores.

- El cuarto segmento es un bloque ACK_GL.

Con este bloque se consigue que en caso de que algún canal de seguridad se haya pasivizado se pueda reintegrar pulsando "AckButton" (%I0.2).

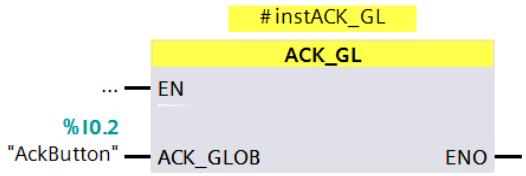


ILUSTRACIÓN 64. SEGMENTO 4: BLOQUE ACK_GL

Nota: Ejemplos de causas que pueden llevar a la pasivización son una rotura de hilo en el módulo de salidas seguras o falta de alimentación en el módulo de entradas seguras.

5.2.3. Intercambio de datos

Para intercambiar datos entre el programa estándar y el programa de seguridad, se han creado dos bloques de datos globales: "DataToSafety" y "DataFromSafety".

El primero lo escribe el programa estándar y es leído por el de seguridad. Se transfieren la información de si "startSignal" está en true o false. Es decir, si la maquina se puede poner en marcha o no.

El segundo lo escribe el programa de seguridad y es leído por el estándar. Se transfiere el dato de si "fault" está en true o false. Esto es, si existe algún error o no en el programa de seguridad y hay que detener la maquina o no.

Con esto se realiza una compilación para comprobar que no existe error alguno y se da por finalizada la parte del hardware.

5.3. Cableado final

Una vez se tienen montados los componentes del hardware y programado el software, teniendo de esta forma asignadas las direcciones de entradas y salidas, se comienza con el cableado final del hardware.

Para realizar la función de parada de emergencia es necesario cablear los componentes del hardware como se plasma en el siguiente dibujo:

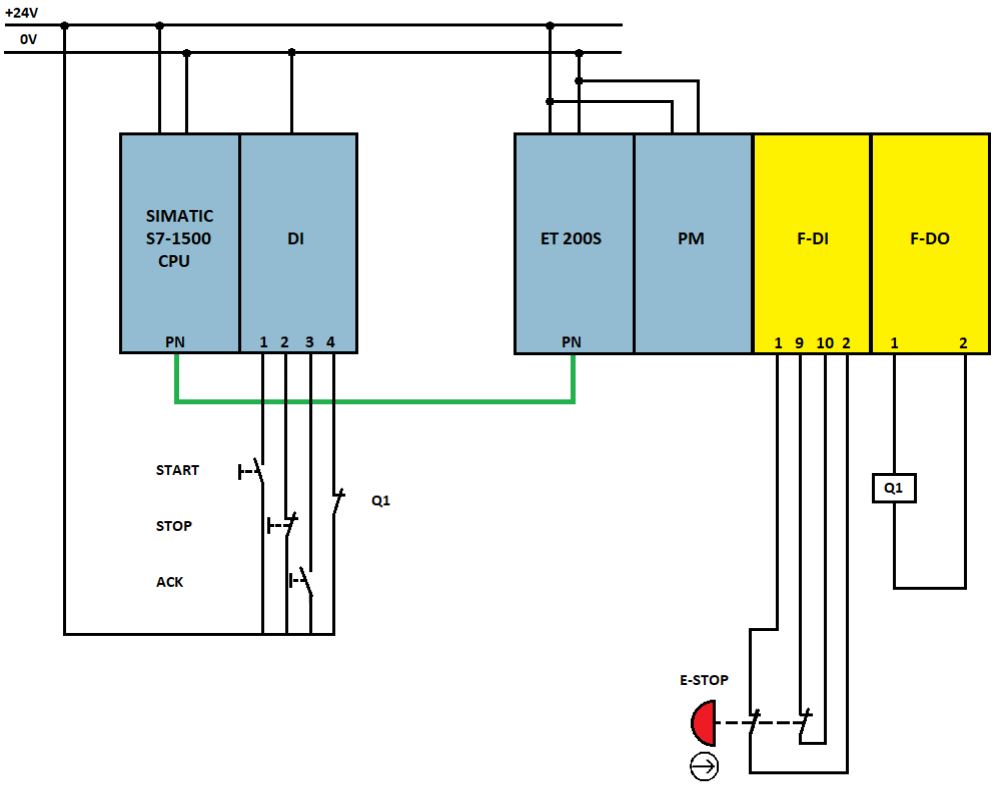
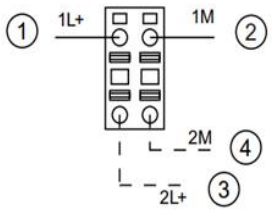


ILUSTRACIÓN 65. CABLEADO DE LOS COMPONENTES DEL HARDWARE

Es necesario comprender la función de cada uno de los pines de la cabecera de la periferia descentralizada y de los módulos de terminales. Estos pines de los módulos de terminales corresponden a los canales del módulo de potencia, del módulo de entradas seguras y del módulo de salidas seguras. Es decir, corresponden a las entradas y salidas antes programada.

Esta información se encuentra disponible en los manuales de Siemens para la periferia descentralizada que se esté utilizando, ET 200S en este caso. En concreto, en el manual de "Instrucciones de servicio" [6] y el "Manual de montaje y manejo" [7].

La cabecera cuenta en la parte delantera con cuatro entradas cableables con el siguiente esquema:



① + 24V DC de la fuente de alimentación
② Masa de la fuente de alimentación
③ + 24V DC de la fuente de alimentación para conectar en cadena
④ Masa de la fuente de alimentación para conectar en cadena

ILUSTRACIÓN 66. CONEXIÓN DE LA FUENTE DE ALIMENTACIÓN DE LA PERIFERIA DESCENTRALIZADA ET 200S

Por lo que, para alimentar la cabecera, se conecta la parte positiva de la alimentación de corriente directa (+24V) al pin 1L+, y la parte negativa (0V) al pin 1M.

Después, para alimentar el módulo de potencia, se conecta la cabecera con el PM. El módulo de terminales al que esta acoplado el PM sigue el siguiente esquema:

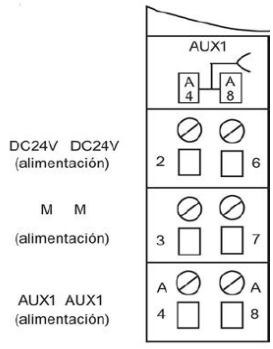
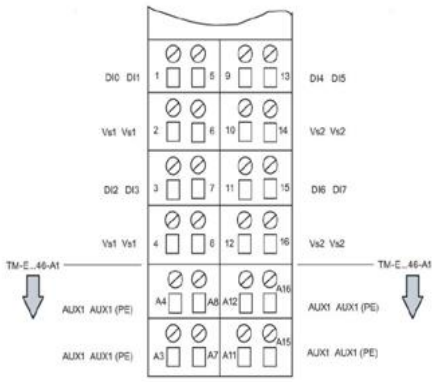


ILUSTRACIÓN 67. ASIGNACIÓN DE TERMINALES TM-P PARA PM-E

Por lo tanto, se une el pin 2L+ de la cabecera con el pin 2 del módulo de terminales del PM, y el pin 2M con pin 3 (la masa).

El módulo de terminales del módulo de entradas seguras, que es donde va cableado el pulsador de parada de emergencia, tiene este esquema:



DI	Entrada digital de seguridad
Vs1	Alimentación interna de sensor 1 para DI 0 hasta DI 3
Vs2	Alimentación interna de sensor 2 para DI 4 hasta DI 7

ILUSTRACIÓN 68. ASIGNACIÓN DE TERMINALES TM-E PARA F-DI

El esquema del pulsador de parada de emergencia se reduce a dos contactos normales cerrados.

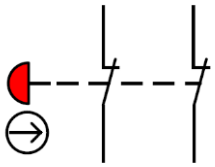
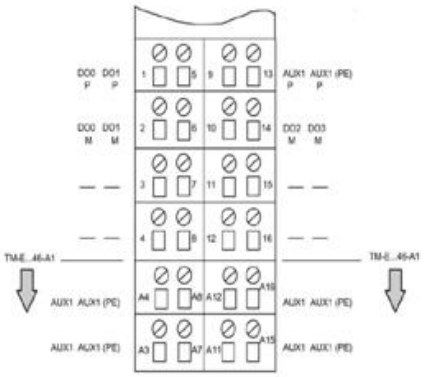


ILUSTRACIÓN 69. ESQUEMA DE UN PULSADOR DE PARADA DE EMERGENCIA

En el software se tiene programado que las entradas sean evaluadas a pares ya que el pulsador tiene canal doble NC. En concreto esto se ha hecho para el canal (0,4). Por lo tanto, el pulsador se cablea entre

- Canal 0: Pin 1 y su masa pin2
- Canal 4: Pin 9 y su masa pin10

El módulo de terminales del módulo de salidas seguras, que es donde va cableado el contactor, tiene el siguiente esquema:



Dox P: Conexión para salida digital de seguridad (conmutación P/M)
Dox M: Conexión para salida digital de seguridad (conmutación P/M)

ILUSTRACIÓN 70. ASIGNACIÓN DE TERMINALES TM-E PARA F-DO

Por otro lado, el esquema de funcionamiento de los pines del contactor se encuentra en su data sheet [8].

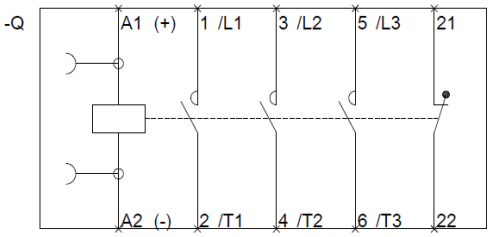


ILUSTRACIÓN 71. ESQUEMA DEL CONTACTOR SIEMENS SIRIUS

En el software únicamente se tiene activada la salida de canal 0. Por lo que, se conecta:

- Entrada de la bobina: El pin1 del módulo de salidas seguras al pin A1+.
- Salida de la bobina: El pin2 del módulo al pin A2-.

Por otro lado, para que se realice el feedback del contactor que exige la programación de seguridad, es necesario conectar el NC del contactor.

- El pin22 se une a la entrada I0.3 ("fdbackContactor") del programa estándar.
- El pin21 se conecta con +24V de corriente continua.

Se realiza una compilación para comprobar que no existe error alguno y se carga en el dispositivo.

5.4. Funcionamiento final

En este apartado se van a utilizar diagramas de tiempos para especificar qué pasos se han de realizar para obtener un correcto funcionamiento de la parada de emergencia. Los diagramas también se usarán para observar en que variables significativas repercute cada acción realizada.

Carga del programa o reintegración tras pasivización de canales

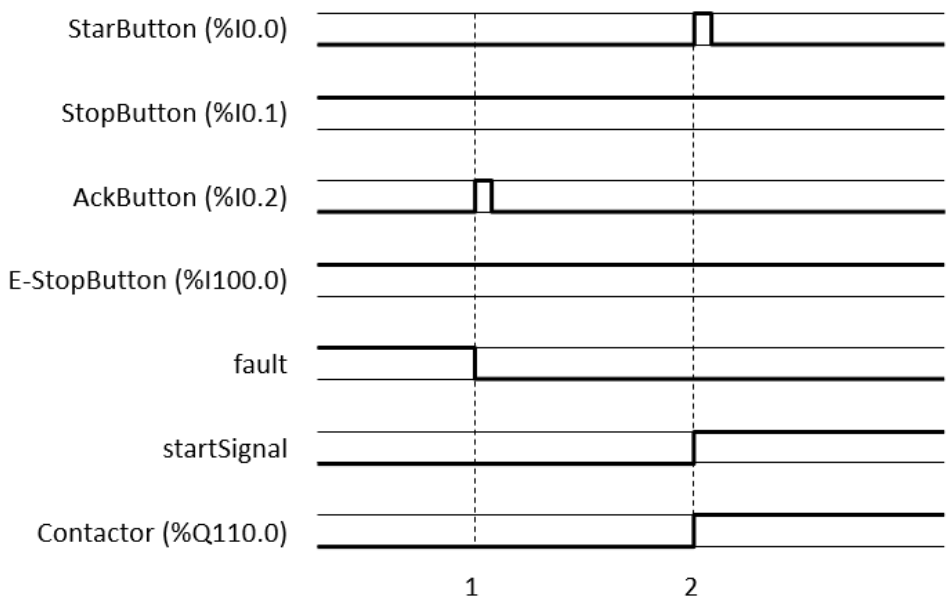


ILUSTRACIÓN 72. DIAGRAMA DE TIEMPOS: CARGA DEL PROGRAMA O REINTEGRACIÓN TRAS PASIVACIÓN

En este caso el programa se inicia con un "fault" en true. Esto se debe a que la señal de ack que exige el programa para reconocer que el pulsador está operativo no ha sido introducida.

1- Se introduce el ack accionando "AckButton". La señal "fault" se va a false. Se tiene el pulsador reconocido.
2- Se pulsa "StartButton" para arrancar el contactor. La señal "startSignal" se pone en true y también lo hace el contactor. En caso de tener algún tipo de maquina conectada al contactor, esta se pondría en marcha.

Maniobra de parada y arranque normal

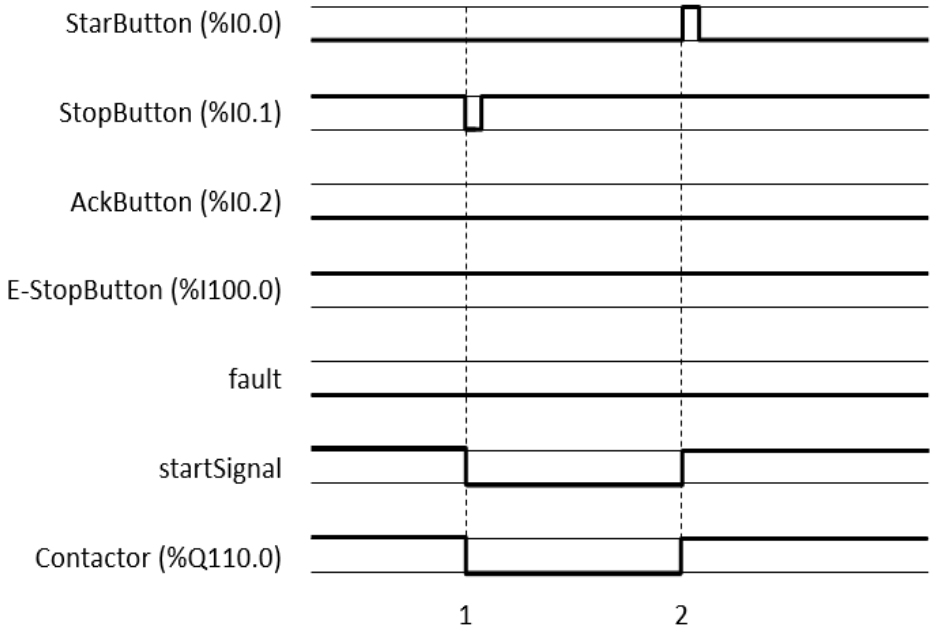


ILUSTRACIÓN 73. DIAGRAMA DE TIEMPOS: MANIOBRA DE PARADA Y ARRANQUE NORMAL

En este caso se parte de una situación de funcionamiento normal; por ejemplo, la situación en la que se encontraba el sistema tras el diagrama anterior.

1- Se pulsa "StopButton" para realizar una parada normal. "startSignal" se va a 0 y cae el contactor.
2- Se pulsa "StartButton" para volver a activar el contactor. "startSignal" se pone a 1 y el contactor se activa.

En este caso no es necesario el ack ya que no se ha producido ningún "fault" en el sistema.

Parada de emergencia

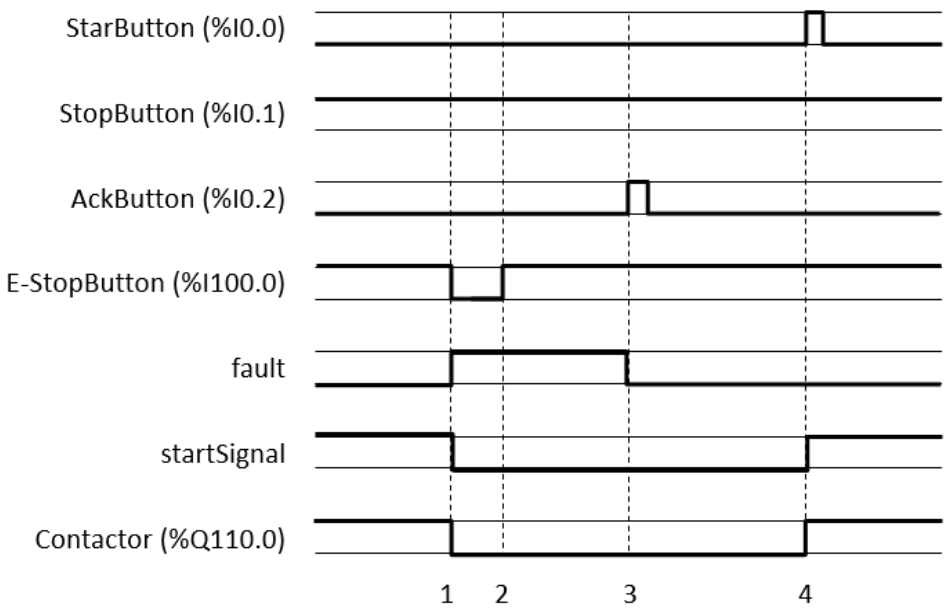


ILUSTRACIÓN 74. DIAGRAMA DE TIEMPOS: PARADA DE EMERGENCIA

Este caso también comienza desde una situación normal de funcionamiento.

1- Se acciona "E-StopButton". Caen "startSignal" y el contactor. La señal "fault" se pone a true. El programa detecta que ha ocurrido un error de algún tipo y detiene todo.
2- Se rearma el pulsador de parada de seguridad cuando se haya solucionado el problema. Esto no tiene repercusión en el sistema, ya que para que el programa reconozca que ya no hay error es necesario el ack.
3- Se pulsa "AckButton". La señal "fault" se va a false. El error ha pasado y el sistema está en condiciones de encender de nuevo la máquina.
4- Se pulsa "StartButton". "startSignal" se pone en true y el contactor se activa.

5.5. Evaluación de la función de seguridad

Como ya se ha comentado, existen diversas herramientas para evaluar la función de seguridad. En este trabajo se hace uso de SISTEMA, ya que esta herramienta realiza la evaluación de acuerdo con la norma ISO 13849-1, y al ser la complejidad del sistema de seguridad baja, es la norma que se ha de aplicar.

Nota: El software SISTEMA se descarga gratuitamente mediante la web de IFA. [9]

Una vez se tiene la herramienta instalada hay que crear un nuevo proyecto (1) (ver lustración 75), y darle un nombre al proyecto.

Tras esto se crea una nueva función de seguridad (2) (ver lustración 75). Se nombra dicha función y, en caso de desearlo, se le da una descripción (ver ilustración 76).

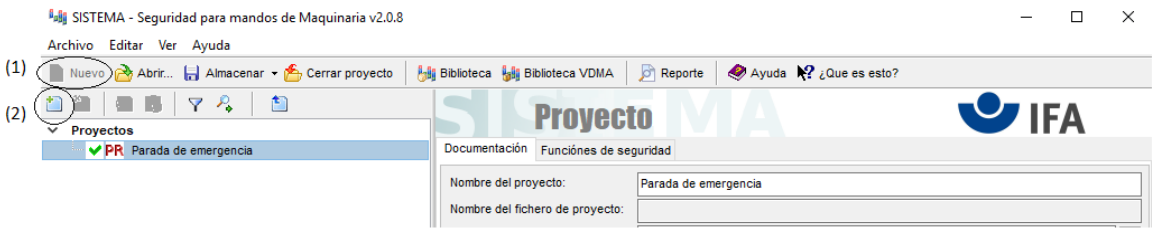


ILUSTRACIÓN 75. CREAR NUEVO PROYECTO Y NUEVA FUNCIÓN DE SEGURIDAD

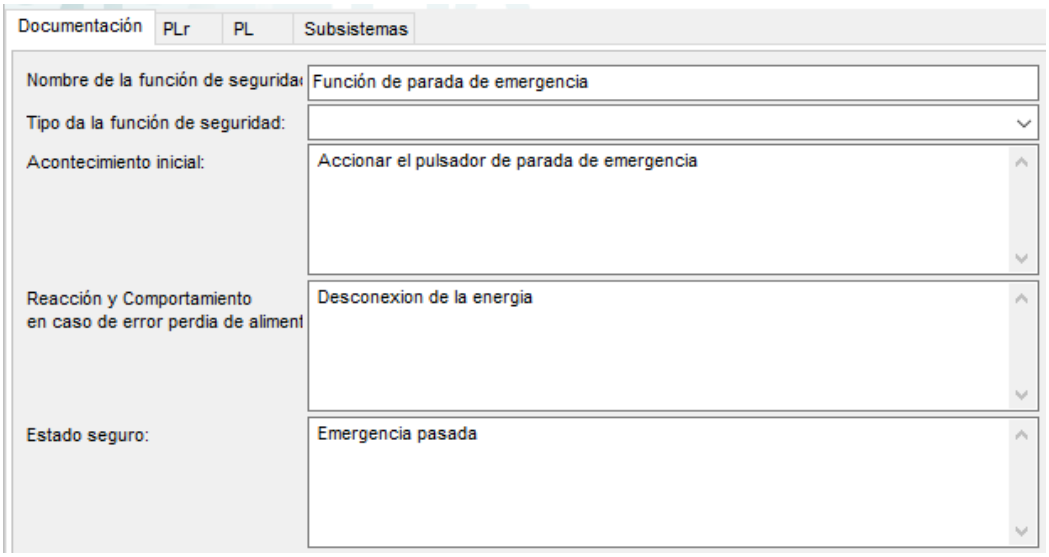


ILUSTRACIÓN 76. NOMBRE Y DESCRIPCIÓN DE LA FUNCIÓN DE SEGURIDAD

El siguiente paso es determinar el nivel de prestaciones requerido (PLr). Para ello el software proporciona el grafico de riesgos de tipo árbol de decisiones (ver ilustración 77). Como en este trabajo la función de parada de emergencia es una aplicación didáctica, y no protege de un peligro real, se ha supuesto una situación en la que:

S1 = Lesión leve (normalmente reversible)

F2 = Frecuente a continuo o tiempo de exposición largo

P1 = Posible bajo determinadas circunstancias

Obteniendo así un PLr b. Por lo tanto la función de parada de emergencia debe tener un PL mayor ó igual que b.

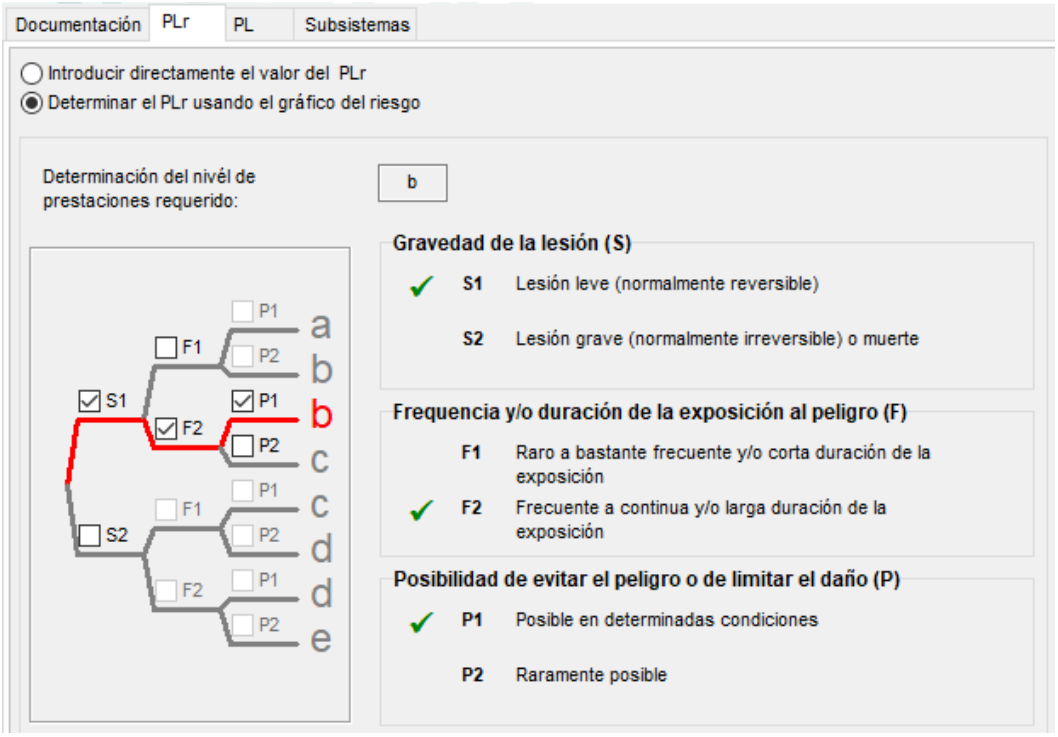


ILUSTRACIÓN 77. DETERMINACIÓN DEL PLR MEDIANTE GRÁFICO DE RIESGOS

Tras esto se introducen los subsistemas de los que está formada la arquitectura de la función de control. La herramienta cuenta con una amplia variedad de bibliotecas donde se encuentran innumerables componentes de diversas empresas. Estos componentes tienen predefinidos todos los valores necesarios para el cálculo del PL.

Nota: Las bibliotecas se pueden descargar gratuitamente desde la web de IFA. [10]

Una vez encontrados todos los componentes, se cargan y se cierra la biblioteca. Obteniendo así los subsistemas de la función de seguridad.

ILUSTRACIÓN 78. SUBSISTEMAS DE LA FUNCIÓN DE SEGURIDAD

Tras introducir toda esta información SISTEMA realiza automáticamente los cálculos pertinentes y arroja el nivel de prestación que ofrece la función de seguridad.

ILUSTRACIÓN 79. PL ALCANZADO POR LA FUNCIÓN DE SEGURIDAD

En este caso alcanza un PLe. Por lo que cumple PL > PLr, y por lo tanto la función de seguridad es válida.

6. Planificación

6.1. Descripción de las tareas

En este apartado se realizará la descripción del programa de trabajo que se ha seguido a la hora de realizar este proyecto.

T1. Documentación parte teórica

En esta fase se pretende realizar una búsqueda de la información relativa al estado del arte de la seguridad de máquinas. Para ello se buscan y se realiza una rápida lectura de documentos, normas, artículos y manuales de diversas fuentes; como las grandes empresas relacionadas con la automatización de procesos y seguridad de maquina industrial Pilz, Sick, ABB, Siemens o Rockwell.

Duración: 3 semanas.

T2. Análisis y estudio de la información

Tras reunir toda la información se comienza con un estudio profundo de toda la información para poder seleccionar la información que es realmente valiosa a la hora de realizar este proyecto.

Duración: 4 semanas.

T3. Documentación parte practica

Comprendido el estado del arte comienza la aplicación práctica del trabajo. Será necesario familiarizarse con la herramienta TIA Portal y, más en concreto, con el paquete de seguridad. Esto se realiza mediante pequeñas pruebas haciendo uso de dicha herramienta. Por otro lado, también se ha de comprender la parte física que se va a utilizar, el hardware. Para ello se realiza una búsqueda y lectura de los manuales de los dispositivos de las que se dispone.

Duración: 3 semanas.

T4. Programación

Una vez se conoce todo lo relativo a la aplicación práctica se dará comienzo a la realización de la programación de la función de seguridad. Mediante ensayo y error se ira conociendo más sobre el paquete de seguridad y como responde a las diferentes conexiones que se le practican. Hasta obtener el resultado final.

Duración: 4 semanas.

T5. Redacción del documento

En esta tarea se realiza la escritura del trabajo, de la manera más clara y detallada posible. Esto se realiza simultáneamente a algunas de las tareas anteriormente mencionadas.

Duración: 10 semanas.

6.2. Diagrama Gantt

Te:	Nombre de tarea	Duración	Comienzo	Fin
1	**Documentación parte teórica**	**3 sem.**	**lun 25/03/19**	**vie 12/04/19**
1.1	Busqueda de información	1 sem	lun 25/03/19	vie 29/03/19
1.2	Lectura superficial y organización	2 sem.	lun 01/04/19	vie 12/04/19
2	**Análisis y estudio de la información**	**4 sem.**	**lun 15/04/19**	**vie 10/05/19**
3	**Documentación parte práctica**	**3 sem.**	**lun 13/05/19**	**vie 31/05/19**
3.1	Busqueda de información	1 sem	lun 13/05/19	vie 17/05/19
3.2	Lectura superficial y organización	2 sem.	lun 20/05/19	vie 31/05/19
4	**Programación**	**4 sem.**	**lun 03/06/19**	**vie 28/06/19**
4.1	Hardware	2 sem.	lun 03/06/19	vie 14/06/19
4.2	Software	2 sem.	lun 17/06/19	vie 28/06/19
5	**Redacción del documento**	**10 sem.**	**lun 13/05/19**	**vie 19/07/19**

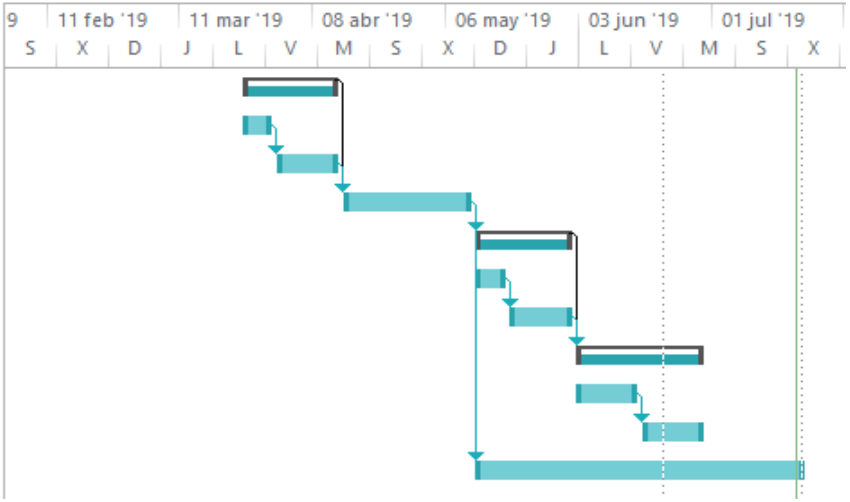


ILUSTRACIÓN 80. DIAGRAMA GANTT

7. Coste del proyecto

En este apartado se realizará un desglose de los gastos necesarios para la realización de este trabajo. No se presenta como un presupuesto ya que es un trabajo ya terminado y no uno por realizar.

Para detallar el coste, este se va a dividir en tres partidas: las horas internas, las amortizaciones y los gastos. Con estas partidas realizadas se calcularán los costes totales teniendo en cuenta los costes indirectos y los imprevistos.

Horas internas

En esta partida se tienen en cuenta el tiempo de trabajo invertido tanto por el alumno como por el director del TFG.

TABLA 8. COSTE HORAS INTERNAS

Concepto	Coste horario	Uds	Coste total
Director del TFG	50 €/h	15 horas	750 €
Autor del TFG	20 €/h	175 horas	3.500 €
		TOTAL	4.250 €

Amortizaciones

Se calcula el coste de amortización de las herramientas que se han utilizado a la hora de desarrollar el trabajo.

TABLA 9. COSTE AMORTIZACIONES

Concepto	Coste adquisición	Vida útil	Uso	Coste total
Componentes estandar	2.575 €	17.520 horas	50 horas	7,35 €
Componentes de seguridad	2.100 €	17.520 horas	40 horas	4,79 €
Ordenador	650 €	26.280 horas	175 horas	4,33 €
Licencia TIA Portal	2.450 €	8.760 horas	50 horas	13,98 €
Licencia Office	69 €	8.760 horas	100 horas	0,79 €
			TOTAL	31,24 €

Gastos

Tiene en cuenta los gastos que se han realizado en este trabajo y no pueden volver a ser utilizados.

TABLA 10. COSTE GASTOS

Concepto	Coste total
Pulsador de parada de emergencia	46 €
Cable	2 €
Material de oficina	5 €
Transporte	30 €
TOTAL	83 €

Costes totales

TABLA 11. COSTES TOTALES

Partidas	Coste total
Horas internas	4.250 €
Amortizaciones	31,24 €
Gastos	83 €
SUBTOTAL 1	4.364,24 €
Costes indirectos (4%)	174,57 €
SUBTOTAL 2	4.538,81 €
Imprevistos (5%)	226,94 €
TOTAL	4.765,75 €

8. Conclusiones

Tras la realización de este trabajo, donde se han analizado tanto la parte teórica como una parte de implementación de la seguridad en maquinaria, se puede concluir que:

La cada vez más rápida automatización del sector industrial, la revolución industrial 4.0, está trayendo consigo la necesidad de implementar más y mejores sistemas de seguridad. Estos sistemas están regulados y legislados por normativa europea y nacional cada vez más armonizada, destacando la Directiva de maquinaria.

Tras realizar el análisis de las pautas a seguir para llevar a cabo una correcta implementación de seguridad, se ha visto como es de gran importancia seguir los pasos tal y como los marcan las distintas normas. Esto es de especial importancia tanto en la estrategia de seguridad como a la hora de aplicar las normas de seguridad funcional. En caso contrario no se llegará a obtener el nivel de función de seguridad necesario.

De todas las funciones de seguridad existentes para maquinaria, en este trabajo se ha optado por aquella que más aplicación tiene en la maquinaria industrial: la función de parada de emergencia.

Al trabajar tanto en el hardware, haciendo uso de dispositivos de Siemens y Schneider, como en el software, programado en TIA Portal, se ha podido observar como es imprescindible conocer todos estos aspectos con mucho detalle., siendo necesario el uso de diversos manuales. De no ser así, seria complicado conseguir una función de parada de emergencia totalmente funcional y que cumpla con los requisitos de las normas que la regulan.

9. Bibliografía

[1] Cambridge Dictionaty. *Meaning of security.*
https://dictionary.cambridge.org/dictionary/english/security

[2] Merriam Webster Dictionary. *Definition of safety.*
https://www.merriam-webster.com/dictionary/safety

[3] Comisión Europea. Empresa e Industria. *Guía para la aplicación de la Directiva 2006/42/CE relativa a las máquinas.*
http://www.anmopyc.es/resources/archivos/noticias/915/edition_2.1_of_the_md_guide_final.pdf

[4] Unión Europea. *Normas armonizadas*.
https://europa.eu/youreurope/business/product/standardisation-in-europe/index_es.htm#shortcut-4-normas-armonizadas

[5] International Electrotechnical Commission (IEC). *Functional Safety.*
https://www.iec.ch/functionalsafety/explained/

[6] Siemens. *Sistema de periferia descentralizada ET 200S. Instrucciones de servicio.*
https://cache.industry.siemens.com/dl/files/348/1144348/att_33247/v1/et200S_operating_instructions_es_ES_es-ES.pdf

[7] Siemens. *Periferia descentralizada Técnica F Sistema de periferia descentralizada ET 200S. Manual de montaje y de manejo.*
https://support.industry.siemens.com/cs/document/12490437/simatic-periferia-descentralizada-t%C3%A9cnica-f-sistema-de-periferia-descentralizada-et-200s?dti=0&lc=es-WW

[8] Siemens. *Data sheet 3RT1015-1BB42.*
https://mall.industry.siemens.com/mall/es/es/Catalog/Product/3RT1015-1BB42

[9] IFA. *Software-Assistent SISTEMA.*
https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp

[10] IFA. *SISTEMA libraries.*
https://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/sistema-bibliotheken/index.jsp

DesignSpark - RS Components. *A brief history of industrial safety.*
https://www.rs-online.com/designspark/a-brief-history-of-industrial-safety

StaySafe. *The way we were: the evolution of health and safety.*
https://www.staysafeapp.com/history-workplace-health-safety/

Schneider Electric. *Manual de seguridad en maquinas.*
https://download.schneider-electric.com/files?p_enDocType=Specification+guide&p_File_Name=420134F10-manual-seguridad-maquinas.pdf&p_Doc_Ref=420134F10

Rockwell Automation. *Safebook sobre maquinaria 5.*
http://www.starautomation.es/fitxer/2527/Safebook%20sobre%20maquinaria%205.pdf

Pilz (pagina web). *Conocimientos técnicos.*
https://www.pilz.com/es-INT/knowhow

Siemens. *Barrera fotoeléctrica con función muting en la categoría de seguridad 4, conforme a la norma EN 954-1.*
https://cache.industry.siemens.com/dl/files/201/21331201/att_15588/v1/21331201_as_fe_i_005_v10_sp_lcurtain.pdf

Siemens. *Sequential Muting of a Light Curtain with S7-1500.*
https://support.industry.siemens.com/cs/document/58793869/sequential-muting-of-a-light-curtain-with-s7-1500?dti=0&lc=en-US

Siemens. *Safety Laser Scanner with Monitoring Case Switching on an S7-1500.*
https://support.industry.siemens.com/cs/document/58804919/safety-laser-scanner-with-monitoring-case-switching-on-an-s7-1500?dti=0&lc=en-WW

Rockwell Automation. *Pressure Sensitive Safety Mat System MatGuard™ Mat Manager.*
https://literature.rockwellautomation.com/idc/groups/literature/documents/um/440f-um001-en-p.pdf

Rockwell Automation. *Guardmaster® Safedge™ Pressure Sensitive Safety Edge System Installation and User Manual 440F.*
https://literature.rockwellautomation.com/idc/groups/literature/documents/um/440f-um002-en-p.pdf

Schneider Electric. *Safety Legislation and Standards.*
https://download.schneider-electric.com/files?p_enDocType=Catalog&p_File_Name=DIA3ED2150103EN.pdf&p_Doc_Ref=DIA3ED2150103EN

TÜV SÜD. *SIL or PL? What is the difference?.*
https://www.tuv-sud.co.uk/uploads/images/139722018023654425039 5/sil-or-pl.pdf

ReeR. *ISO 13849-1 PL*.
https://www.reersafety.com/ru/es/safety-guide/safety-in-the-working-environment/iso-13849-1-pl

ReeR. *IEC 62061 SIL - CONCLUSIONES.*
https://www.reersafety.com/ru/es/safety-guide/safety-in-the-working-environment/iec-62061-sil

Siemens. *Emergency stop up to SIL 3 / PL e with a fail-safe S7-1500 controller.*
https://support.industry.siemens.com/cs/document/21064024/em ergency-stop-up-to-sil- 3-pl-e-with-a-fail-safe-s7-1500-controller-?dti=0&lc=en-WW

Schneider Electric. *Soluciones de seguridad. Software SISTEMA.*
http://www.infoplc.net/files/descargas/schneider/infoPLC_net_Formacion_Software_Sistema.pdf