

J. A. Cabrera 4621	Tel (54)	(11) 4833 0020	SistemasDACS S.A.
Buenos Aires (C1414BGI)	Fax (54)	(11) 4833 0019	
Argentina	E-mail:	dacs@dacs.com.ar	

Protección de Calderas - Sistemas BMS (Burner Management Systems)

ARTÍCULO "BMS-SIL-PDF" (mayo 2001)

por Ing. **Roberto Fernández Blanco**
FUNCTIONAL SAFETY EXPERT

Toda Caldera requiere, para su funcionamiento, de la implementación de dos Sistemas Automáticos de Control: el **Sistema de Control Regulatorio**, responsable del **Funcionamiento** de la Caldera, y el **Sistema BMS**, responsable de la **Seguridad Operativa** de la misma.

El objeto de este trabajo es el de analizar los Sistemas BMS para su uso en Calderas de Plantas Industriales con Nivel SIL 2, Safety Integrity Level 2, según IEC 61508 (**de aplicación rigurosa**, como se indica más adelante).

❖ **Definición de Riesgo Aceptable**

Nada es absolutamente seguro. Toda operación industrial, por sencilla que sea, por rutinaria que sea, o por "segura" que parezca, envuelve un riesgo, ya sea **riesgo de daño a los equipos**, **riesgo de perder la producción** o, lo que es peor aún, **riesgo de dañar la integridad física de quienes operan el proceso**. No existe operación que no envuelva riesgo, y **la única manera de que el riesgo sea nulo, es no realizar la operación**.

Es decir, el **riesgo depende de una acción y/o de su ocurrencia en el tiempo**, por lo cual **definiremos el riesgo como la probabilidad estadística de que un hecho peligroso ocurra**.

El riesgo se determina en términos del número probable de accidentes por unidad de tiempo. Ejemplo: el número probable de ocurrencias por año (un accidente cada 100, 1.000 ó 10.000 años, o bien 0,01 accidentes por año, etc.).

Podemos definir **riesgo aceptable**, como el **nivel de riesgo** que permite establecer **hasta qué punto se puede aceptar que una operación pueda causar eventuales daños y qué nivel de gravedad es aceptable para ese daño**.

El riesgo aceptable se podría definir también como "después de cuánto tiempo se puede aceptar que ocurra un accidente" (¿1.000 años, tal vez?)

En la industria en general, el riesgo aceptable es determinado por las Normas generadas por los Gobiernos, por las Corporaciones, por las Compañías de Seguros o por la misma Empresa en la cual tienen lugar las operaciones de riesgo.

No obstante e independientemente de cuál sea el organismo que genere dicha normativa, **toda la responsabilidad recae sobre la Empresa en la cual se desarrollan las operaciones**, razón por la cual es ésta quien debe tener en cuenta, a la hora de fijar el riesgo aceptable, factores tales como:

- Seguridad de los empleados
- Seguridad de la comunidad
- Responsabilidad Civil
- Pérdidas materiales
- Imagen de la empresa

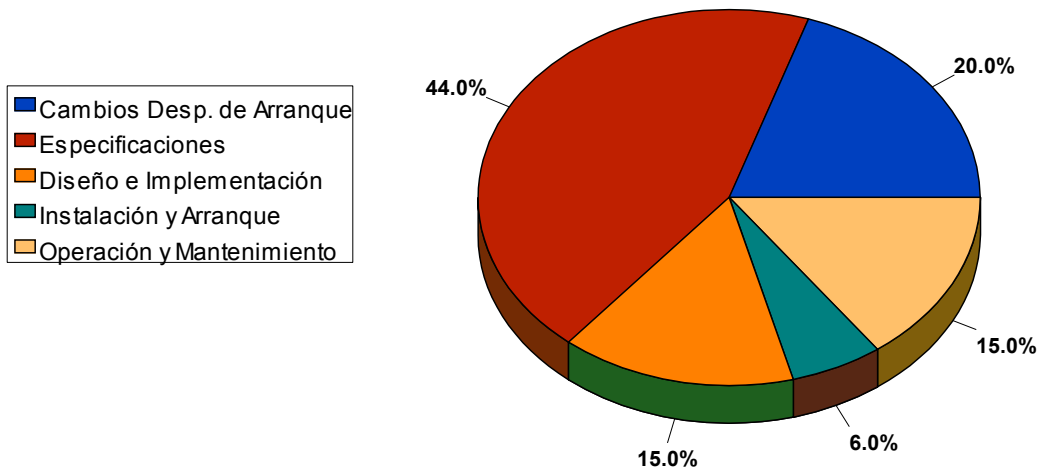
Una vez definido el nivel de riesgo aceptable, se deberá evaluar el nivel de riesgo de cada operación, y determinar si éste está por debajo o por encima del valor de riesgo aceptable.

J. A. Cabrera 4621	Tel (54)	(11) 4833 0020	SistemasDACS S.A.
Buenos Aires (C1414BGI)	Fax (54)	(11) 4833 0019	
Argentina	E-mail:	dacs@dacs.com.ar	

Para todas aquellas operaciones en las cuales el nivel de riesgo sea superior al aceptable, se deberá utilizar algún **método de reducción del factor de riesgo**, muchos de los cuales se hallan definidos en la normativa arriba mencionada.

El siguiente gráfico nos da una idea de las pérdidas producidas a nivel mundial por accidentes causados por no tener en cuenta la implementación de Normas de Seguridad para reducir el nivel de riesgo. Esta estadística, obtenida para la Industria Petrolera en general, sirve como ejemplo claro de la importancia de cumplir con los requerimientos de las Normas de Seguridad.

Pérdidas Mundiales por Siniestros en la Industria Petrolera (Los Culpables)



En el caso concreto de Argentina, existe una gran zona gris, en lo referente a las normativas, lo que muchas veces nos lleva a asumir que tales normativas no existen...

En el caso de las Calderas, la Empresa deberá adoptar algún tipo de modelo de Normas a seguir, basándose en la experiencia de otros países o de otras Empresas, lo que nos lleva a plantear la necesidad de contemplar las siguientes Normas de Seguridad.

Normas de Seguridad para Sistemas BMS

La **IEC 61508** es de **aplicación obligatoria** para todo **Sistema de Seguridad en Procesos de Alto Riesgo**, y **exige** utilizar equipamiento **Homologado** y **Certificado** para su uso en el **Nivel SIL preestablecido**, esto es, **aprobado por TÜV o FM para su aplicación en Plantas de dicho Nivel SIL de Alto Riesgo**. Además se deberá cumplir con las normas correspondientes a cada tipo de aplicación (**NFPA 85** y **FM 7605** en el caso de las Calderas), asegurando el Nivel de Integridad del Sistema (Nivel SIL) y la Operación Segura de la Planta.

El **Nivel SIL** define el Grado de Reducción de Riesgo que la Planta o Proceso requiere para una operación adecuadamente segura (riesgo aceptable) y éste, a su vez, impone el **Nivel de Integridad** exigido al **Sistema Instrumentado de Seguridad** (Sistema BMS para el caso de las Calderas), el

J. A. Cabrera 4621	Tel (54)	(11) 4833 0020
Buenos Aires (C1414BGI)	Fax (54)	(11) 4833 0019
Argentina	E-mail:	dacs@dacs.com.ar

SistemasDACS S.A.

que deberá ser provisto con un **Certificado o Approval** (de TÜV, FMRC u otra institución equivalente), que lo garantice como apto para ser aplicado en dicho Proceso con el Nivel SIL requerido.

La norma **IEC 61508** impone este procedimiento (que **no debe ser soslayado**) para **todo tipo de industrias donde se requiera un Alto Nivel de Seguridad**, a fin de garantizar la Protección adecuada para resguardo de la Integridad de las Personas, del Medio Ambiente y de los Bienes de Producción, permitiendo además una mayor y más eficiente Continuidad Operativa del Proceso.

Los **Sistemas BMS deben cumplir** con las siguientes Normas:

IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems.

FM 7605 Programmable Logic Control Based Burner Management Systems

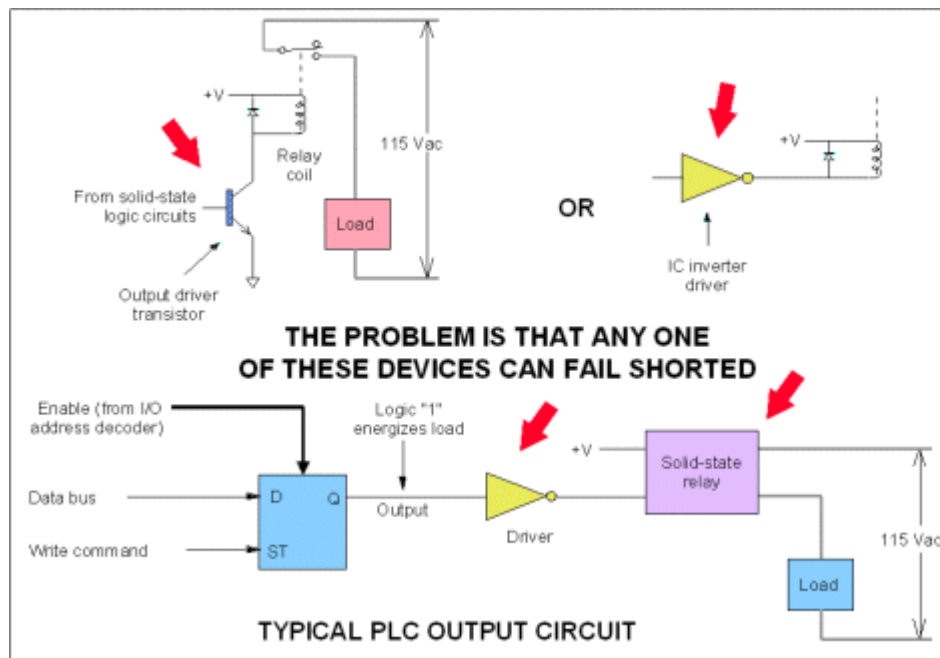
NFPA 85 Boiler and Combustion Systems Hazards Code

El elemento principal de este Equipamiento Certificado de Seguridad es el **SIS** (Safety Instrumented System) o **PES** (Programmable Electronic -Safety Related- System), definido así por la IEC61508 **para diferenciarlo de los Controladores Lógicos Programables (PLCs)**, que **NO pueden ser utilizados en Aplicaciones de Seguridad, pues éstos tienen una alta probabilidad de “fallar en forma peligrosa”**.

Por qué los PLCs convencionales pueden fallar en forma peligrosa

Un sistema eléctrico/electrónico está sujeto a la probabilidad de falla de sus componentes.

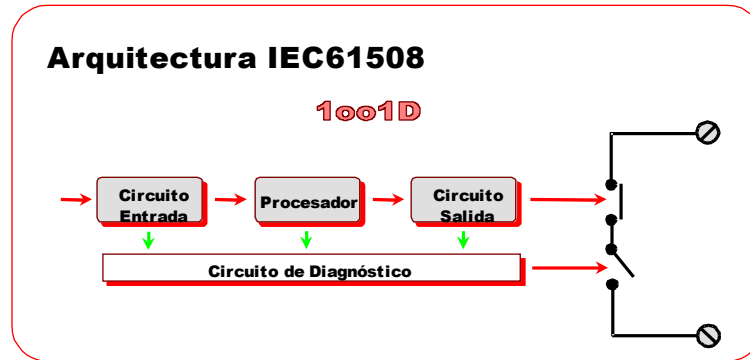
De los siguientes esquemas se puede inferir que la probabilidad de falla peligrosa es bastante alta en equipamiento standard.



J. A. Cabrera 4621	Tel (54)	(11) 4833 0020
Buenos Aires (C1414BGI)	Fax (54)	(11) 4833 0019
Argentina	E-mail:	dacs@dacs.com.ar

SistemasDACs S.A.

La única forma de impedir que esto suceda, es proveer a los circuitos electrónicos de la cobertura de diagnóstico necesaria para que, ante la probabilidad de una falla, el sistema de diagnóstico actúe llevando el circuito a condición segura (fail-safe). (Ver Artículo "Design of Fail-safe control systems" adjunto).



Tipos de Falla

Un sistema siempre puede fallar y cuando lo hace, esta falla puede producirse de dos maneras:

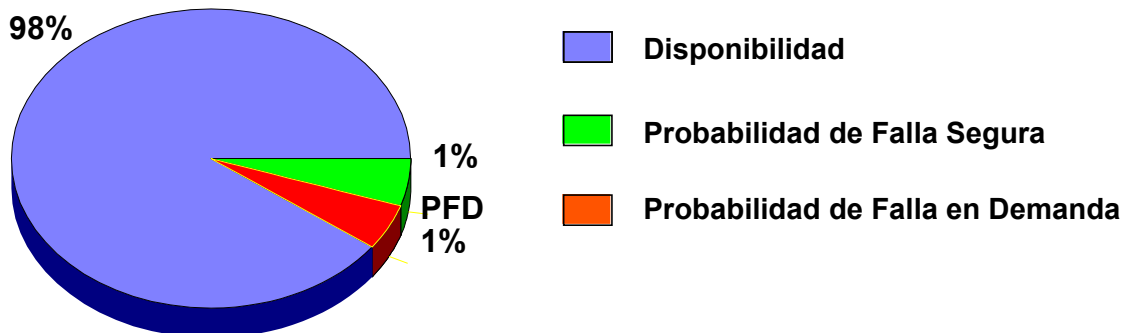
- A. Falla Segura
- B. Falla Peligrosa

En una Caldera, una falla segura sería el caso, por ejemplo, del corte de la tensión de alimentación del Sistema de Control. En este caso, las válvulas de alimentación de combustible se cerrarán, apagando la Caldera ante la imposibilidad de poder controlarla (como consecuencia de la falla en el circuito de tensión).

Una **falla peligrosa se generará**, por ejemplo, cuando ante el requerimiento del Sistema de Control de cerrar una válvula de combustible, ésta quede abierta, **poniendo en peligro de explosión a la Caldera**.

La IEC61508 define la Probabilidad de Falla en Demanda (PFD, **Probability Of Failure on Demand**), como la probabilidad estadística de que un Sistema **falle en forma peligrosa**.

Las PFD son utilizadas para la fijación y determinación de los **Niveles SIL (Safety Integrity Levels)** o **Niveles de Integridad**, para los cuales corresponderá un **Factor de Reducción de Riesgo o FRR** ($FRR = 1/PFD$).



J. A. Cabrera 4621	Tel (54)	(11) 4833 0020	SistemasDACS S.A.
Buenos Aires (C1414BGI)	Fax (54)	(11) 4833 0019	
Argentina	E-mail:	dacs@dacs.com.ar	

Para Alcanzar un Nivel de Seguridad SIL	Necesitamos una PFD (Average)	Necesitamos un FRR
1	0.1 - 0.01	10 - 100
2	0.01 - 0.001	100 - 1.000
3	0.001 - 0.0001	1.000 - 10.000
4	0.0001 - 0.00001	10.000 - 100.000

Cómo se determina el Nivel SIL

Para la determinación del Nivel SIL, la Norma IEC61508 utiliza las recomendaciones de la Norma DIN19250 "Fundamental Safety aspects to be considered for Measurement and Control Equipment". Ésta establece una colección de criterios que nos permitirán establecer el nivel de riesgo del equipamiento a proteger.

Escapa al objetivo de este Curso el realizar un análisis profundo de los niveles de riesgo y operabilidad de una Caldera (HAZAN/HAZOP), pero de acuerdo con estos criterios de evaluación, para una Caldera Industrial de un sólo quemador, podemos estimar un nivel de riesgo igual a AK4, según DIN 19250.

Una vez establecido este nivel, la Norma IEC61508 nos dice cuál es el Nivel SIL correspondiente.

Y, finalmente, elegir el Controlador de Seguridad (PES) necesario para el nivel de riesgo evaluado. (Ver Sistemas de Seguridad Certificados, más adelante).

Qué es el Factor de Reducción del Riesgo (FRR)

Todo elemento utilizado para el control de un sistema actúa como elemento de reducción de riesgo. El Sistema de Control Regulatorio de la Caldera, por ejemplo, monitorea en forma permanente las variables de proceso, manteniendo segura la operación de la Caldera.

Es decir, cuando la presión de vapor aumenta por encima de cierto nivel, el Sistema regula el poder calórico de la mezcla de combustible para mantener la presión dentro de ciertos límites, como se ve en el siguiente gráfico.

En caso que esto no fuera suficiente, y la presión siguiera aumentando, el Sistema provee las Alarmas necesarias como para que una rápida intervención del Operador pueda proveer la protección adecuada, volviendo la Caldera a su operación segura.

Pero, ¿qué sucedería si esto no fuera suficiente?. La respuesta parece obvia: la Caldera podría explotar.

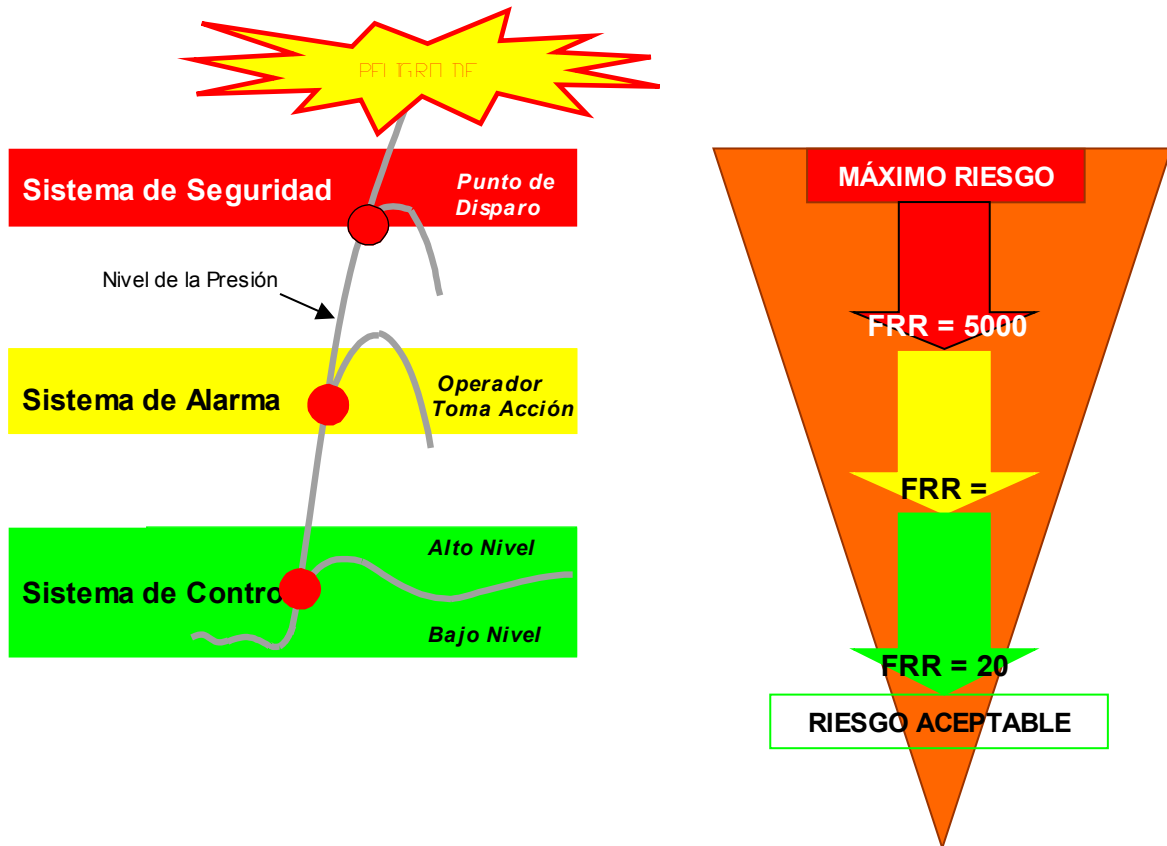
Para evitar esto, se hace necesaria la utilización de otro Sistema adicional de Seguridad.

Cada uno de estos elementos actúa como Factor de Reducción de Riesgo.

La capacidad de reducción de riesgo de cada uno de ellos dependerá de su Nivel SIL, tal como se vió más arriba.

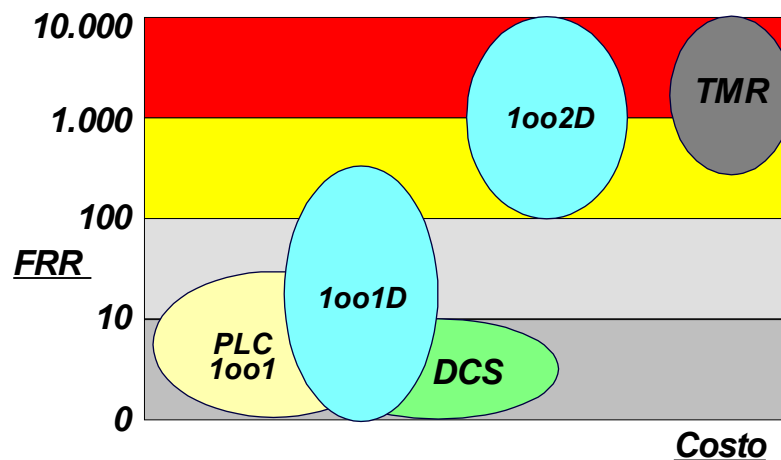
J. A. Cabrera 4621	Tel (54)	(11) 4833 0020
Buenos Aires (C1414BGI)	Fax (54)	(11) 4833 0019
Argentina	E-mail:	dacs@dacs.com.ar

SistemasDACS S.A.



Sistemas de Seguridad Certificados

El corazón del **Sistema de Seguridad** según IEC 61508 **debe ser un PES** (Programmable Electronic Safety Related System) el cual poseerá un Nivel SIL 2 (FRR = 100 a 1.000) para esta Caldera en particular.



J. A. Cabrera 4621	Tel (54)	(11) 4833 0020	SistemasDACS S.A.
Buenos Aires (C1414BGI)	Fax (54)	(11) 4833 0019	
Argentina	E-mail:	dacs@dacs.com.ar	

En los PES, Las configuraciones válidas de las Unidades Centrales de Procesamiento son las siguientes:

- Una sólo CPU con Diagnóstico (1001D)
- Dos CPUs con Diagnóstico (1002D)
- Tres CPUs con Diagnóstico (1003D ó 3003 ó 2003)

Se incluyen en el gráfico los PLCs convencionales y otros Sistemas de Control. Para poner en evidencia la necesidad de utilizar un PES en aplicaciones de alto riesgo (Nivel SIL 2 o superior).

El PES elegido para esta aplicación es el KT93S de ABB (1001D).

Las Unidades de Entrada/Salida **poseen el mismo grado de seguridad o Nivel SIL del PES al que responden** y realizan las funciones de verificación de la integridad de los cables y de las señales de cada dispositivo.

Por su parte, el Bus de comunicación (CS31) utilizado para comunicar los módulos de Entrada/Salida con la CPU **tiene el mismo Nivel SIL especificado para todo el sistema, contando con una adecuada Cobertura de Diagnóstico** (Diagnostics Coverage).

Todas las acciones de Seguridad (Detección, Bloqueo, Activación, Desactivación, etc.) **son ejecutadas en forma segura (FAILSAFE) por el PES.**

SistemasDACS S.A.
Mayo 2001