De como escapar la trampa del HIPS
Optimizando la reducción de riesgo en proceso

SIEMENS

1

Presentado por:

luisgarcia@siemens.com

Luis M F Garcia G

- Siemens Digital Industries
  - Process Safety Consultant para Las Américas
- 35+ años experiencia
- Voting member – ISA S84 Safety and Security Committee
- ISA course developer & instructor
- CFSE – Certified Functional Safety Expert
- (CFSEGB & TÜV).
- B Eng. Metallurgy and Material Science - Liverpool University
- Técnico Mecánico - Colegio Salesiano San José

Luis Garcia

https://bcert.me/sirpfkhst

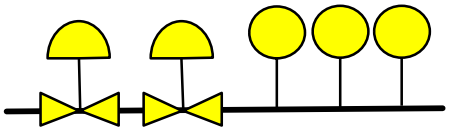
SIEMENS

2

Lo real de "La Realidad"

Cuanto más funcionalmente seguro, menos confiable.

Razón por la cual la gente evita Funciones Instrumentadas de Seguridad **SIL 3**.



Muchos instrumentos que pueden "**fallar**".

Válvulas → Usualmente el eslabón más débil

Puede que sean **más seguras,** pero son **menos fiables**

Solución: Optimice la reducción de riesgo **cuando esto sea posible**, usando capas Independientes de Protección **(Independent Protection Layers** o IPL)
(No ponga muchos huevos en una sola canasta) – IEC 61511-3 Anexo C

Autoridad con Jurisdicción

El Tango del HIPS

SIEMENS

3

SIL 3 debe usarse como último recurso – Cuando otra IPL no sea posible utilizar

De IEC 61511-3 Anexo C

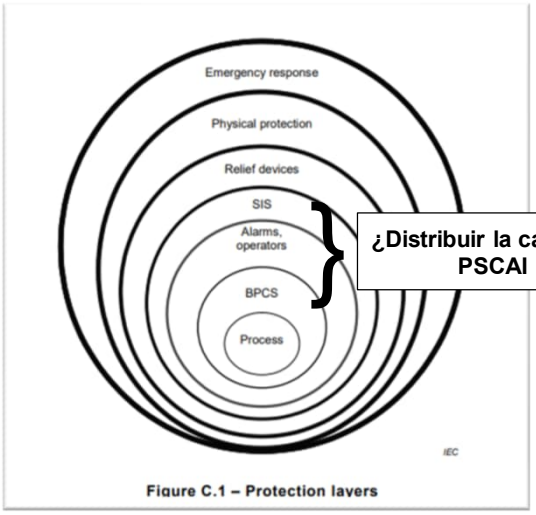


Figure C.1 – Protection layers

El concepto de IPL se basa en 3 principios

1 – Es un grupo de equipos de control o de procedimientos

2 – Cumplimiento de los siguientes criterios:
- Reduce el riesgo **al menos ¡10 veces!**
- Tiene las siguientes **características**
  - Especificidad (a un peligro)
  - Independencia (de otras IPL)
  - confiabilidad (para reducir riesgo)
  - Auditabilidad (indicación de rendimiento)

3 – Cumplir con clausula 3.2.69
  - Definición de SIL de una SIF

¿Cuánta reducción de riesgo puede ser distribuida entre el SIS y otras IPL?

SIEMENS

4

Para el BPCS (de ANSI/ISA 61511-1, 2018 - V2.1 – Pagina 49)

9.3.2 The risk reduction claimed for a BPCS protection layer shall be ≤10.

NOTE Consideration can be given to the fact that a BPCS may also be an initiating source for the demand on the protection layer.

9.3.3 …en the BPCS shall be des…

¿Permitido? → ¡Si, pero NO automáticamente!
Es necesario seguir un proceso → ISA 84.91.03

9.3.4 …hen:

- no more than one BPCS protection layer shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is the initiating source for the demand on the protection layer; or
- no more than two BPCS protection layers shall be claimed for the same sequence of event leading to the hazardous event when the BPCS is not the initiating source of the demand.

NOTE The identified BPCS protection layer can consist of one BPCS as the initiating source for the demand (see 8.2.2) and a second independent BPCS protection layer (see 9.3.2 and 9.3.3) or up to two independent BPCS protection layers when the initiating source is not related to BPCS failure.

SIEMENS

5

ISA 84.91.03 – Borrador en votación del Comité en pleno. Proyectado para inicio del 2025.

Seguridad Functional:
Process Safety Controls, Alarms, and Interlocks (PSCAI) como capas de proteccion.

Modelado en el concepto de “ciclo de vida IEC61511”

ISA 84.91.03

1 Scope

1.1 This standard applies to a wide variety of industries within the process sector, for example, chemicals, oil and gas, pulp and paper, pharmaceuticals, food and beverage, and non-nuclear power generation.

1.2 This standard specifies requirements for achieving functional safety using process safety controls, alarms, and interlocks (PSCAI) as protection layers that are not intended to conform to the ANSI/ISA 61511-1:2018 requirements for safety instrumented systems (SIS).

…quirements for safety …ers in ANSI/ISA61511.

Tabla1: Aplicabilidad de estándares de seguridad funcional a PSCAI

Tipo de PSCAI	Crédito por Reducción de Riesgo	Estándar aplicado
Safety Instrumented Functions SIF	RR ≥ 10	ANSI/ISA 61511
Low Integrity Protection Layers LI-PL	1 < RR ≤ 10	ANSI/ISA 84.91.03
Salvaguardas no clasificadas como capas de protección	Sin Reducción de Riesgo	ANSI/ISA 84.91.01

→ **Dos advertencias**

SIEMENS

6

1ra advertencia: BPCS como IPL (IEC 61511-3, 2018 - V2.1 – Page 51)

BPCS? → ?Se requiere intervención humana?

Anexo F (informativo) - Layer of Protection Analysis (LOPA)

Table F.4 – Typical protection layers (prevention and mitigation) PFD_{avg}

Protection layer	PFD_{avg}
Control loop	$1,0 \times 10^{-1}$
Human performance (trained, no stress)	$1,0 \times 10^{-1}$ to $1,0 \times 10^{-2}$ → **Parece ser el caso**
Human performance (under stress)	0,5 to 1,0
Operator response to alarms	$1,0 \times 10^{-1}$ → **¿Requiere intervención humana?**
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-4} or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule)

NOTE The figures in Table F.4 are illustrative of the range of values that could appear in assessments. These values cannot be taken as generic probabilities and used in specific assessments. Human error probabilities can be appropriately assessed on a case by case basis.

SIEMENS

7

1ra advertencia: BPCS como IPL (IEC 61511-3, 2018 - V2.1 – Page 51)

Cuando se trata de aceptar Alarmas IPL, hay dos facciones opuestas

- Una facción no acepta Alarmas de Seguridad como IPL debido a la intervención humana. Solo se aceptan como RAGAGEP. **(Recognized And Generally Accepted Good Engineering Practices)**
- Otros aceptan "Alarmas IPL" como algo posible, y se basan en IEC 61511
  - **A pesar de ser clarificado como "solo un ejemplo": 13.7 Anexo F, IEC 61511-3; 2016:**

    "*… La alarma puede tomar crédito como una capa de protección puesto que está localizada en un controlador diferente al del lazo de control de temperatura …*"
- Nosotros proponemos que la aplicación misma determina si el crédito a la alarma es:
  - ***Considerado como aceptable*** *(refiérase a ANSI/ISA 18.2)*

SIEMENS

8

1ra advertencia: BPCS como IPL (IEC 61511-3, 2018 - V2.1 – Page 51)

Alarmas

1. **IEC 61511,** *clausula 9.2.7 reconoce alarmas como otro método para reducir riesgo, disminuyendo, como IPL, los chances de que el evento peligroso ocurra (safety alarms).*
2. **IEC 62682,** *clausula 3.1.78. Una "Alarma de Seguridad" es aquella clasificada como critica apara la seguridad del proceso, la protección de vidas humanas y del ambiente. Generalmente son Alarmas HMA – (ver más adelante).*
   - ❑ *Por ejemplo: Alarmas con una reducción de riesgo de 10 ó más.*
3. **Tel sistema de alarmas debe estar bien "Racionalizado".**
   - ❑ *Un sistema que no este racionalizado, tiende a tener muchas alarmas, prioridades equivocadas, y sin respuesta del operador. Todo esto impacta la habilidad del operador para detectar, diagnosticar y responder a las alarmas.*
4. **El sistema de alarmas debe de poder ser evaluado y considerado apropiado.**
   - ❑ *Un sistema no auditado esta propenso a tener falsas alarmas, inundaciones de alarmas, sobrecargas de alarmas además de repetición de alarmas ya atendidas.*

SIEMENS

9

1ra advertencia: BPCS como IPL (IEC 61511-3, 2018 - V2.1 – Page 51)

Alarmas (continuación)

5. **IEC 62682, Alarmas HMA (Highly Managed Alarms)**

6.2.9 Highly managed alarms

Highly managed alarm (HMA) classes are classes of alarms that require more administration and documentation than others. Since the criteria can vary by process, industry or location, the alarm philosophy shall define the criteria for assigning alarms to HMA classes, if HMA are used. The designation of alarm classes as highly managed should be based upon one or more of the following:

a) alarms critical to process safety for the protection of human life (e.g., safety alarms),
b) alarms for personnel safety or protection,
c) alarms for environmental protection,
d) alarms for current good manufacturing practice,
e) alarms for commercial loss,
f) alarms for product quality,
g) alarms for process licensor requirements, and
h) alarms for company policy.

If HMA classes are used, this section of the alarm philosophy shall document the requirements for these alarm classes.

SIEMENS

10

2da advertencia: BPCS como IPL

Debe haber suficiente independencia entre IPLs

¿Independencia?

1. ¿Separación?
2. ¿Asincronismos?
3. ¿Divergencia tecnológica?
4. ¿ Todo lo anterior?

- La idea es tener un valor de causa común (b) suficientemente bajo, para la falla de una IPL no afecte a otra IPL.
  - Hardware libre de interferencia
  - Firmware libre de interferencia
  - Software libre de interferencia

→ ***Probabilidad Multiplicación***

SIEMENS

11

¿Qué dicen los usuarios? – NAMUR NE 165

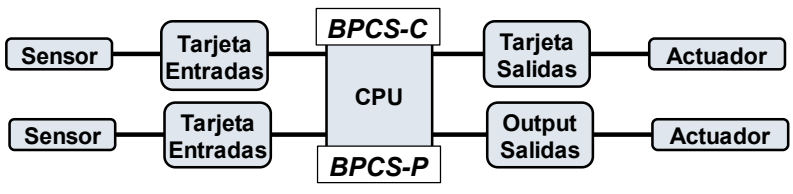
Clausula 8

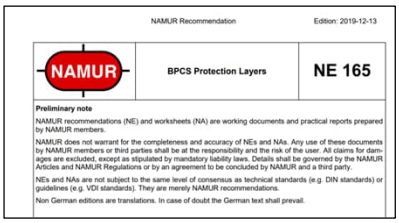
8 Allocation of safety functions to protection layers

The regulations mentioned in section 6 define either independently or by cross-reference the BPCS-P as a possible safety-related device with a risk reduction up to and including factor 10 (RRF <= 10)[3]. The special peculiarity here is the acceptance of the implementation as part of the general BPCS.

BPCS-P can have a switching character (i.e. interlocks), but if necessary, can also be linked via an alarm with a suitable operating instruction (e.g. operator handles the actuator in response to the alarm). In both cases, however, the safe state condition must be achieved by triggering the BPCS-P (and, if applicable, the associated suitable operating instructions).

Anexo A & B **– Una arquitectura entre figura 5 y 6**




NAMUR Recommendation Edition: 2019-12-13

NAMUR | BPCS Protection Layers | NE 165

Preliminary note

NAMUR recommendations (NE) and worksheets (NA) are working documents and practical reports prepared by NAMUR members.

NAMUR does not warrant for the completeness and accuracy of NEs and NAs. Any use of these documents by NAMUR members or third parties shall be at the responsibility and the risk of the user. All claims for damages are excluded, except as stipulated by mandatory liability laws. Details shall be governed by the NAMUR Articles and NAMUR Regulations or by an agreement to be concluded by NAMUR and a third party.

NEs and NAs are not subject to the same level of consensus as technical standards (e.g. DIN standards) or guidelines (e.g. VDI standards). They are merely NAMUR recommendations.

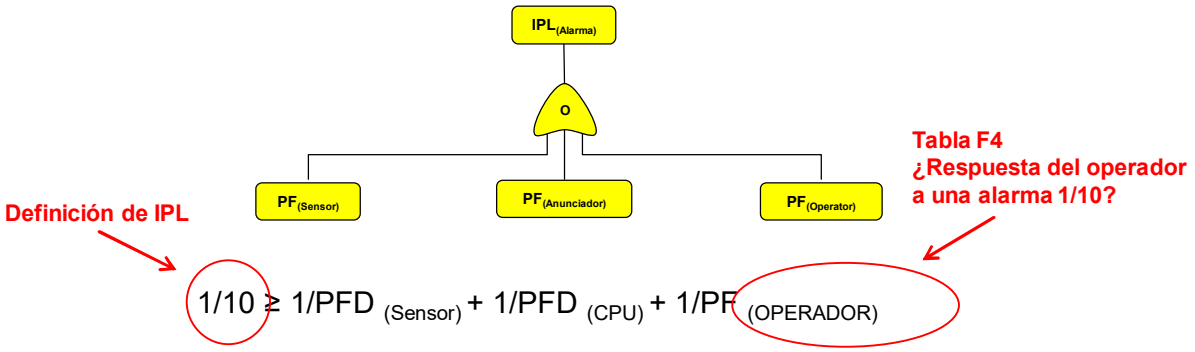
Non German editions are translations. In case of doubt the German text shall prevail.

SIEMENS

12

Cálculos – IPL ó LIPL

Consideremos la probabilidad de de una HMA IPL. En el limite;



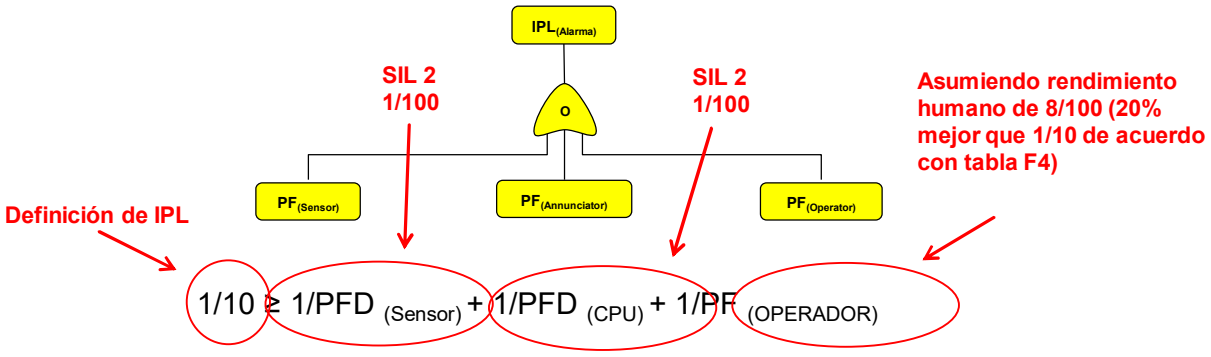
¿Es que el Sensor y el anunciados deben ser **PERFECTOS**?
… O todas las Alarmas son LI-PLs

SIEMENS

13

Cálculos – IPL ó LIPL

Consideremos una falla humana (compatible con la tabla F4) un 20% mejor.
(Rendimiento de un humano → De 1/100 a 1/10)



Sensor y CPU:

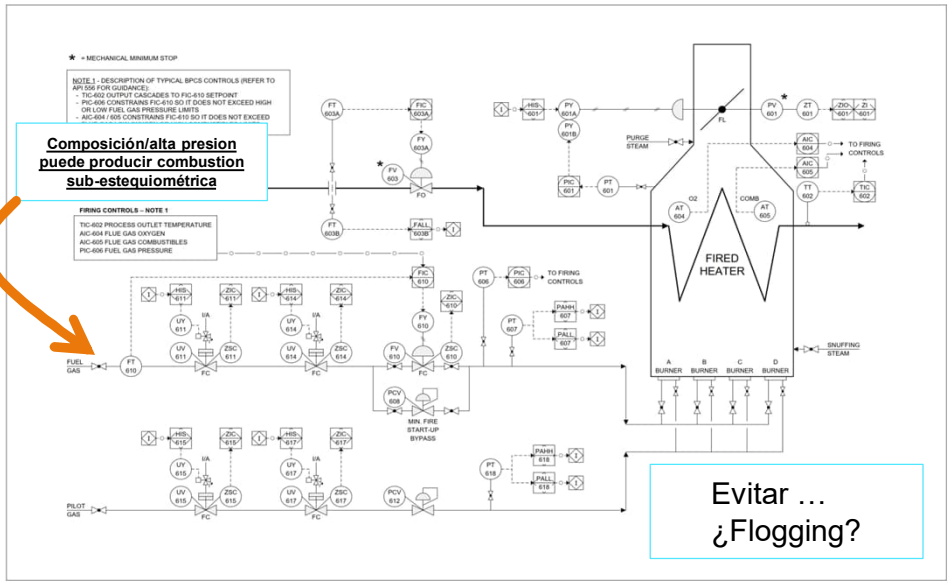
Deben de contribuir con dos órdenes de magnitud de reducción de riesgo.

O sea… Necesita utilizar instrumentación ***SIL 2***

SIEMENS

14

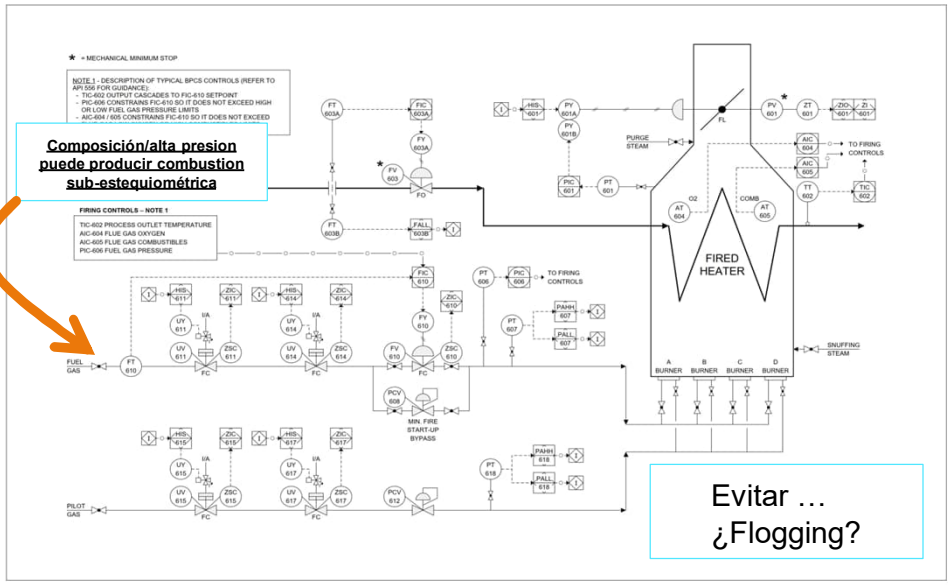
Ejemplo de aplicación #1: API 556 (Nota: ejemplo solamente. Sistema de PSM debe ser implementado primero)



SIEMENS

15

Ejemplo de aplicación #1: API 556 (Nota: ejemplo solamente. Sistema de PSM debe ser implementado primero)



SIEMENS

16

Ejemplo de aplicación: API 556

Definición de zonas:
A. Diseño Aceptable – Sin cambios
B. Considere protecciones adicionales
C. Requiere protecciones adicionales
D. Rediseñe

BPCS

Consecuencias	Frecuencia Categorías - Años				
	>10.000	10.000 - 1.000	1.000 - 100	100 - 10	10 - 1
1	A	A	A	B	B
10	A	A	B	B	C
100	A	B	B	C	C
1.000	B	B	C	C	D
10.000	B	C	C	D	D

SIL 3 (HIPPS)

No recomendable → Muchos disparos en falso

¿Manejable? → Mucho mantenimiento

1oo2 (SC SIL 3) Valves → En promedio dos disparos por año

Diseño → Rechazado

Categorías de Consecuencias
1 - Sin heridos – Primeros auxilios
10 – Heridos leves no incapacitados
100 – Heridos incapacitados sin muertes que lamentar
1.000 - Al menos una fatalidad
10.000 - Múltiple fatalidades

SIEMENS

17

Ejemplo de aplicación: API 556

Definición de zonas:
A. Diseño Aceptable – Sin cambios
B. Considere protecciones adicionales
C. Requiere protecciones adicionales
D. Rediseñe

Alarma IPL | BPCS

Consecuencias	Frecuencia Categorías - Años				
	>10.000	10.000 - 1.000	1.000 - 100	100 - 10	10 - 1
1	A	A	A	B	B
10	A	A	B	B	C
100	A	B	B	C	C
1.000	B	B	C	C	D
10.000	B	C	C	D	D

SIL 2

Aconsejable → Con Alarmas IPL. Si se considera apropiado →
Necesita probar especificidad, Independencia, fiabilidad y auditabilidad.

¿Manejable? → Si las alarmas están racionalizadas.
Se sugieren "Alarmas de seguridad" - HMA

Diseño → Primera alternativa

Categorías de Consecuencias
1 - Sin heridos – Primeros auxilios
10 – Heridos leves no incapacitados
100 – Heridos incapacitados sin muertes que lamentar
1.000 - Al menos una fatalidad
10.000 - Múltiple fatalidades

SIEMENS

18

Ejemplo de aplicación: API 556

Definición de zonas:
- A. Diseño Aceptable – Sin cambios
- B. Considere protecciones adicionales
- C. Requiere protecciones adicionales
- D. Rediseñe

BPCS-C/P

Consecuencias	Frecuencia Categorías - Años				
	>10.000	10.000 - 1.000	1.000 - 100	100 - 10	10 - 1
1	A	A	A	B	B
10	A	A	B	B	C
100	A	B	B	C	C
1.000	B	B	C	C	D
10.000	B	C	C	D	D

SIL 2

Aconsejable → Con Alarmas IPL. Si se considera apropiado → Necesita probar especificidad, Independencia, fiabilidad y auditabilidad.

¿Manejable? → Si las alarmas están racionalizadas. Se sugieren "Alarmas de seguridad" - HMA

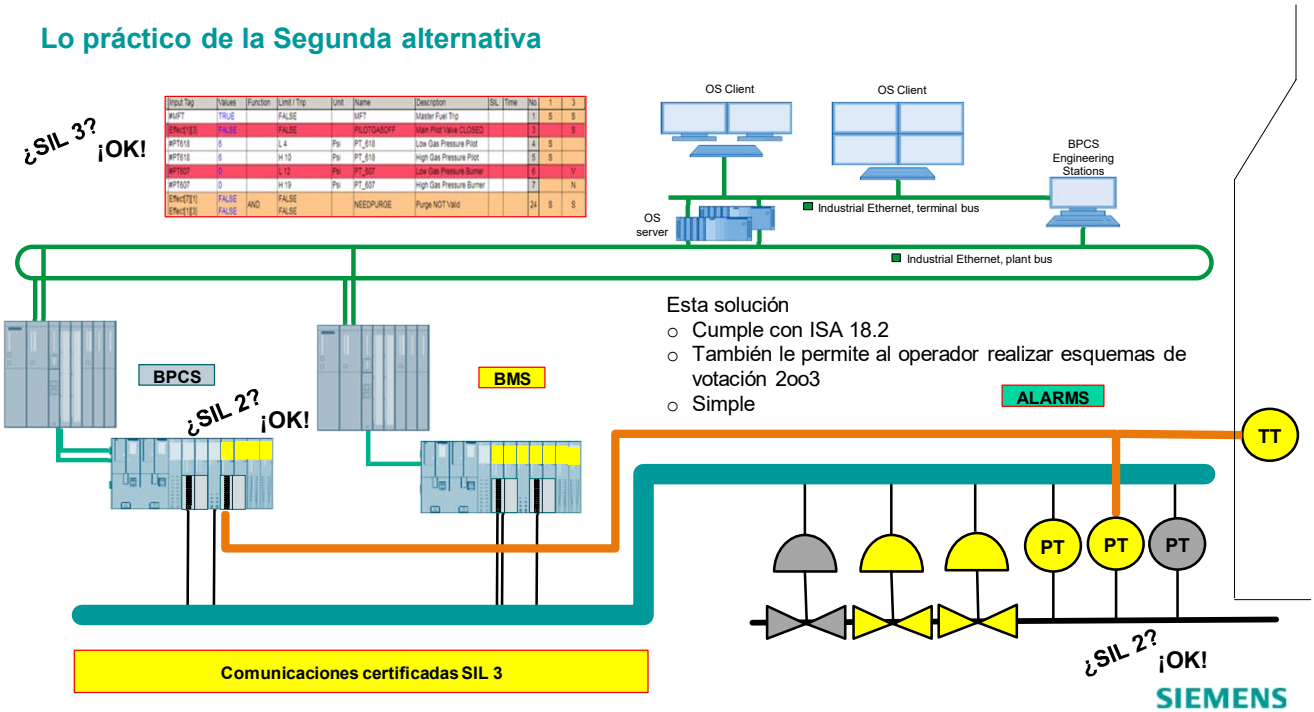
Diseño → Segunda alternativa → Más practica

Categorías de Consecuencias
1 - Sin heridos – Primeros auxilios
10 – Heridos leves no incapacitados
100 – Heridos incapacitados sin muertes que lamentar
1.000 - Al menos una fatalidad
10.000 - Múltiple fatalidades

SIEMENS

19

Lo práctico de la Segunda alternativa



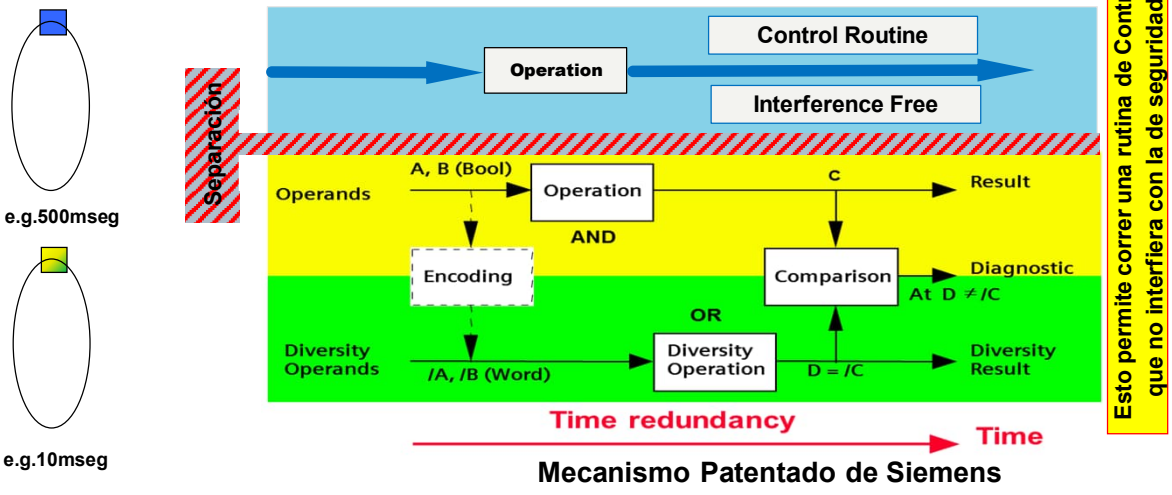
Esta solución
- Cumple con ISA 18.2
- También le permite al operador realizar esquemas de votación 2oo3
- Simple

SIEMENS

20

Ejemplo SIMATIC (Tecnología basada en diagnostico)

En vez de usar dos CPU (Redundancia Estructural) como lo hacen otros sistemas, SIMATIC S7-400F/FH utiliza un novedoso mecanismo de *Redundancia en el Tiempo* con *Software Divergente (ASIC)*

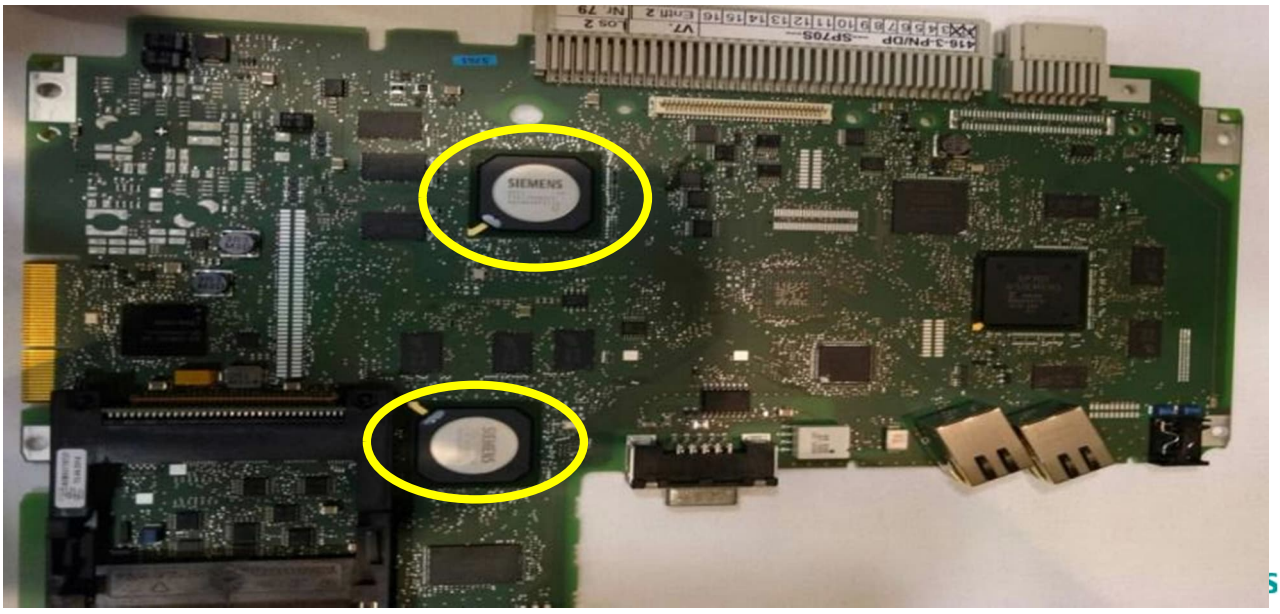


Mecanismo Patentado de Siemens

SIEMENS

21

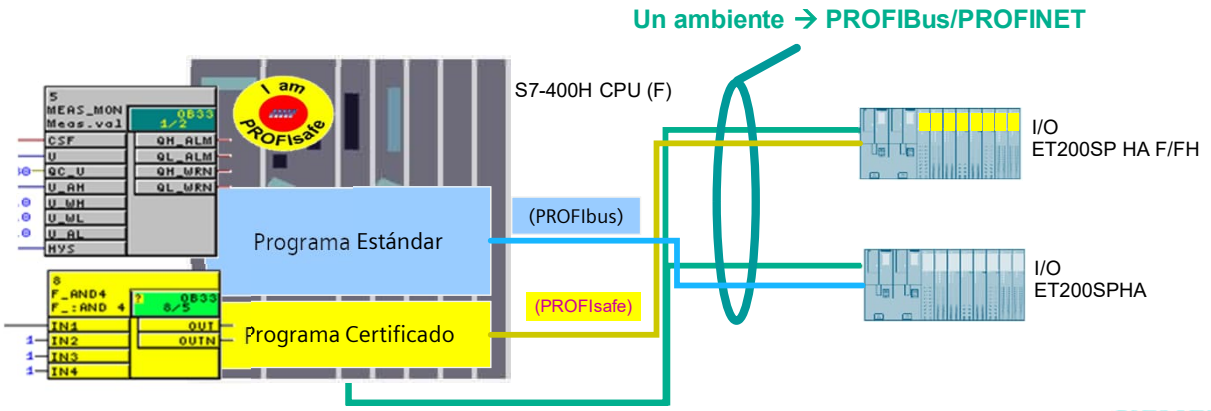
Ejemplo SIMATIC (Tecnología basada en diagnostico)



22

Ejemplo SIMATIC (Tecnología basada en diagnostico)

- Programa estándar y Falla Segura (o “Falla A Seguro”) en un controlador.
- Comunicación con módulos estándar y Falla Segura vía protocolo PROFIsafe
- Extensa cobertura en diagnósticos de fallas (RAM/CPU etc.)

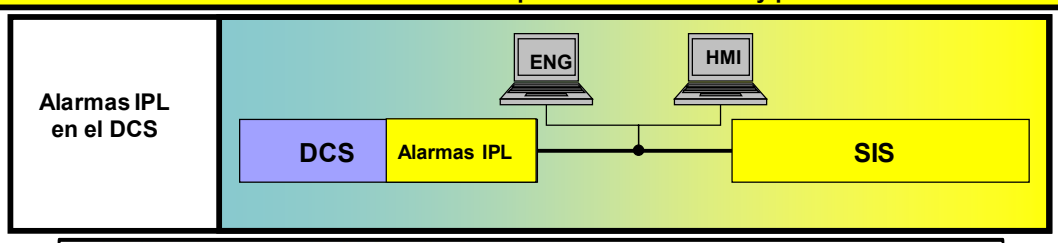


SIEMENS

23

Ejemplo SIMATIC (Tecnología basada en diagnostico)

La certificación IEC 61508 de SIMATIC S7-400 F/FH permite hacer control y protección en un controlador



9.4.2 The assessment shall consider the following:

- independence between protection layers;
- diversity between protection layers;
- physical separation between different protection layers;
- common cause failures between protection layers and between protection layers and BPCS.

NOTE 1 Common causes from the process can be addressed. Plugging of relief valves may cause the same problems as plugging of sensors in a SIS.

NOTE 2 Independence and physical separation can be addressed. A Human Machine Interface, SIS/BPCS networks or bypass means can cause common cause failure.

SIEMENS

24

Ejemplo SIMATIC (Tecnología basada en diagnostico)

La certificación IEC 61508 de SIMATIC S7-400 F/FH permite hacer control y protección en un controlador

El reporte del certificado de TÜV del S7 400 F/FH indica que sus componentes estándar no interfieren con su función de seguridad por lo que pueden ser implementados en el mismo controlador.
La clausula habla no solo de conmopentes de Hardware y Firmware …

2.2 Hardware/Firmware Components under Certification

The system components which are certified 'safety-related' are listed in the current revision of the applicable Annexes to this report. This allows the components to be used to process safety critical signals and functions.

All other components of the S7 -400 and S7-300 family are 'interference-free' and allowed to be used; however, they are not certified for process safety critical signals and functions. Using these components does not interfere with the proper functioning of the safety-related modules.

For details on architectural, configuration and implementation requirements please refer to the manuals (see chapter 2.4).

SIEMENS

25

Ejemplo SIMATIC (Tecnología basada en diagnostico)

La certificación IEC 61508 de SIMATIC S7-400 F/FH permite hacer control y protección en un controlador

El reporte del certificado de TÜV del S7 400 F/FH indica que sus componentes estándar no interfieren con su función de seguridad por lo que pueden ser implementados en el mismo controlador.
La clausula habla no solo de conmopentes de Hardware y Firmware … sino también de Software

2.3.1 Safety-related Software Components

The following software components have been certified 'safety-related' allowing the software components to be used for processing safety critical signals and executing critical functions:

- Add-on option package S7 F Systems
- F-FBs

For the specific versions see the current revision of the Annexes to this report.

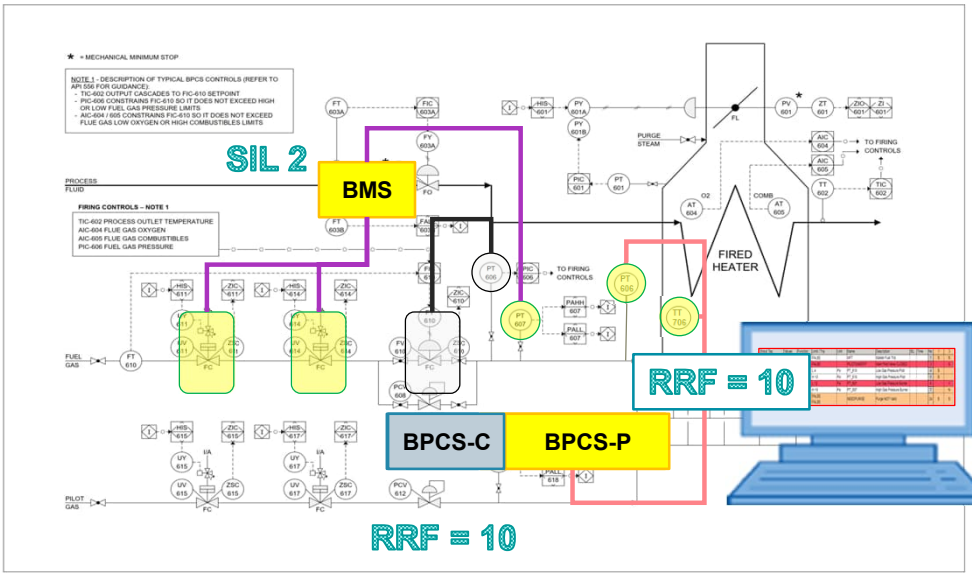
2.3.2 Interference-Free Software Components

Other software components than those mentioned in 2.3.1 are not the subject of this certification. Absence of impact of non certified components on 'safety-related' components is enforced due to the intrinsic safety features provided by the diverse logic implementation followed by the 1oo2 F-I/O modules.

SIEMENS

26

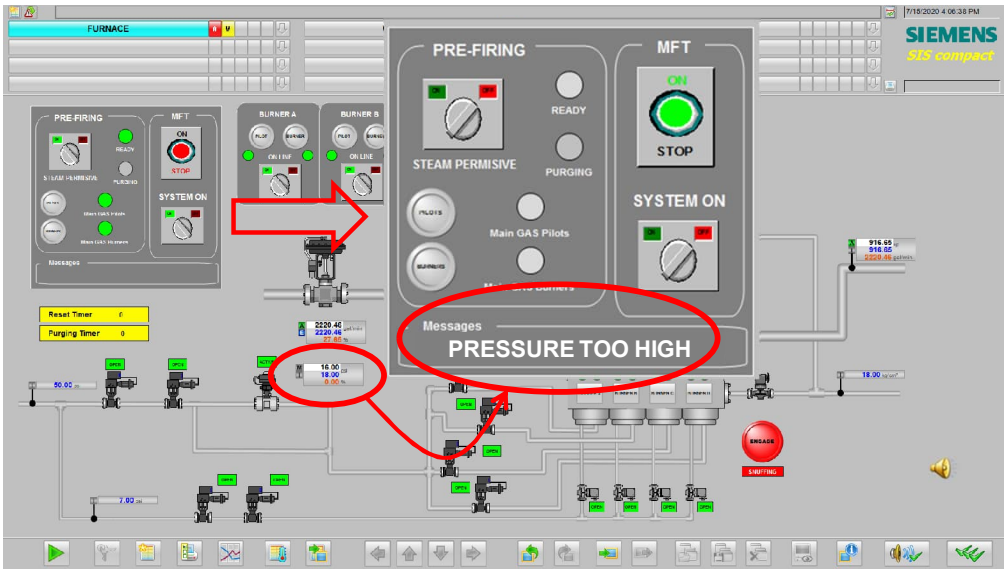
Conclusión – Solución sugerida



SIEMENS

27

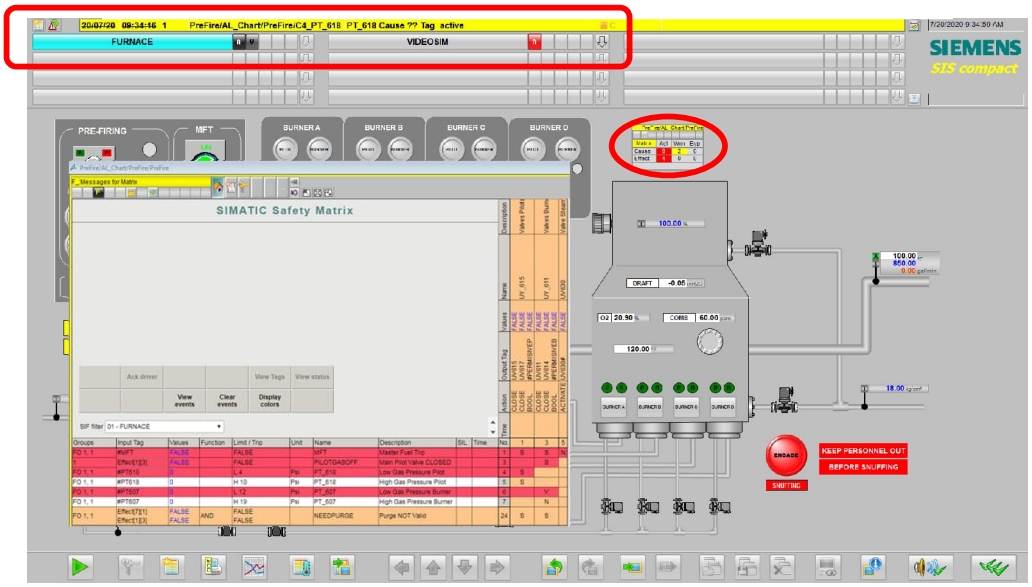
Mensajes a partir de Simatic Safety Matrix son posibles



SIEMENS

28

Mensajes a partir de Simatic Safety Matrix son posibles



SIEMENS

29

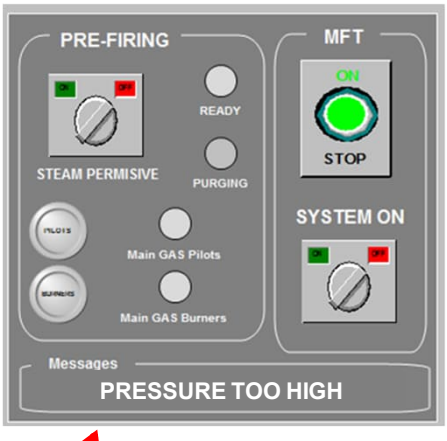
Mensajes a partir de Simatic Safety Matrix son posibles

Seniales traídas a SIMATIC Safety Matrix©

- Asegura disparo de alarma mensaje en la HMI
- **Utiliza las alarmas empotradas en SSM (SIL 3)**

Input Tag	Values	Function	Limit / Trip	Unit	Name	Description	SIL	Time	No	1	3
#MFT	TRUE		FALSE		MFT	Master Fuel Trip			1	S	S
Effect[1][3]	FALSE		FALSE		PILOTGASOFF	Main Pilot Valve CLOSED			3		S
#PT618	6		L 4	Psi	PT_618	Low Gas Pressure Pilot			4	S	
#PT618	6		H 10	Psi	PT_618	High Gas Pressure Pilot			5	S	
#PT607	0		L 12	Psi	PT_607	Low Gas Pressure Burner			6		V
#PT607	0		H 19	Psi	PT_607	High Gas Pressure Burner			7		N
Effect[7][1]	FALSE	AND	FALSE		NEEDPURGE	Purge NOT Valid			24	S	S
Effect[1][3]	FALSE		FALSE								

- Los efectos pueden ser configurados para generar mensajes para el operador.



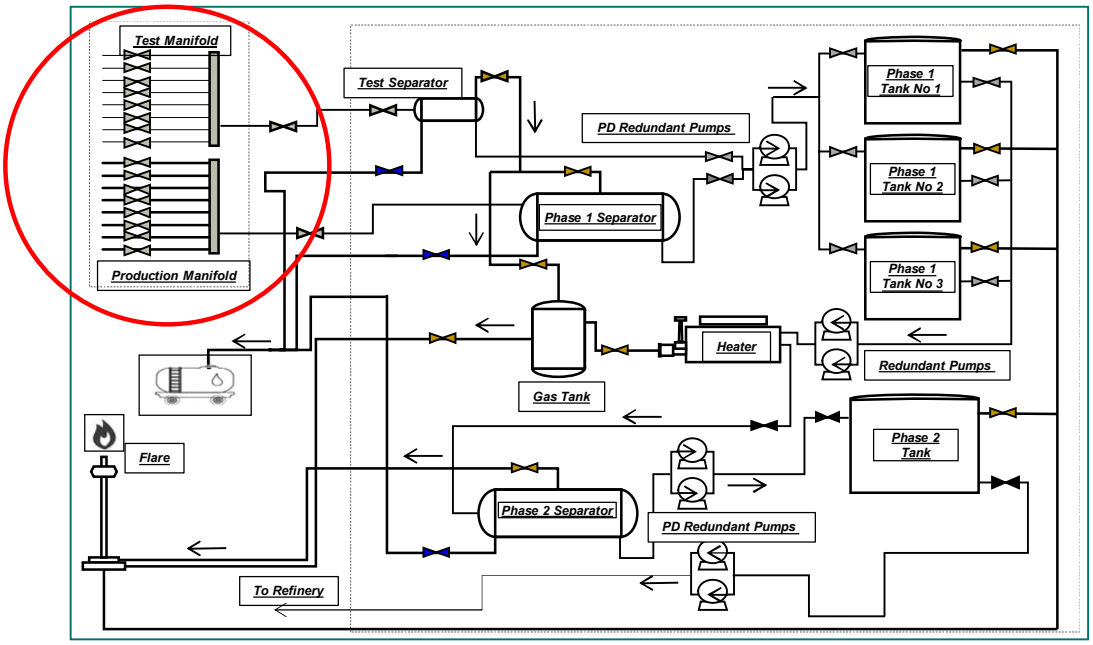
Ventajas

- **La meta es obtener suficiente independencia de instrumentos, para reclamar Alarmas IPL**
- **La meta es balancear la reducción de riesgo lo más posible**

SIEMENS

30

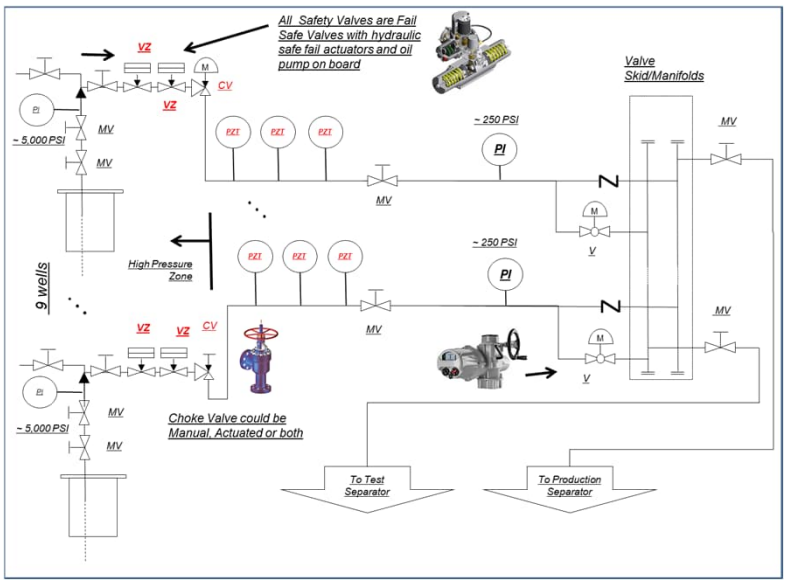
Ejemplo de aplicación #2: Cabezal de Pozos de Alta Presión. (Se requiere de PSM)



SIEMENS

31

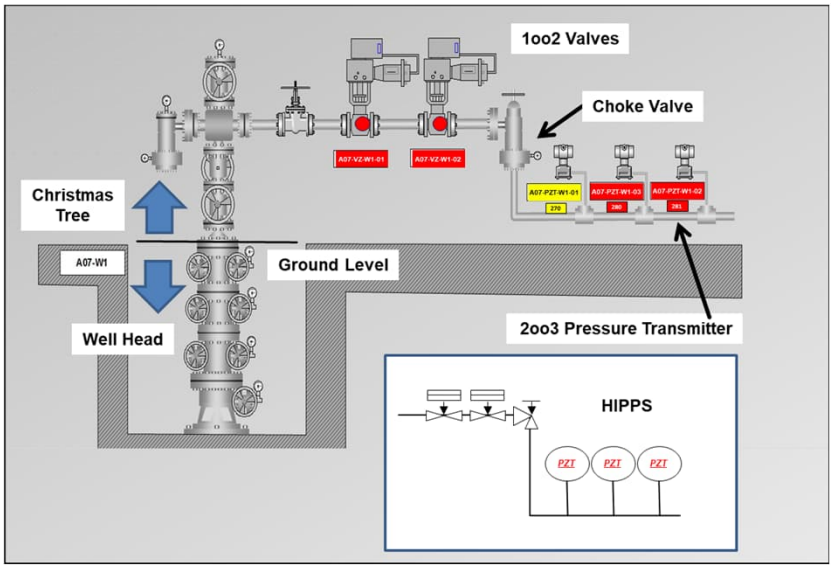
Ejemplo de aplicación #2: Cabezal de Pozos de Alta Presión. (Se requiere de PSM)



SIEMENS

32

Ejemplo de aplicación #2: Cabezal de Pozos de Alta Presión. (Se requiere de PSM)



SIEMENS

33

Ejemplo de aplicación #2: Cabezal de Pozos de Alta Presión. (Se requiere de PSM)

¿Es possible cambiar esto …?

BPCS

Consecuencias	Frecuencia Categorías - Años				
	>10.000	10.000 - 1.000	1.000 - 100	100 - 10	10 - 1
1	A	A	A	B	B
10	A	A	B	B	C
100	A	B	B	C	C
1.000	B	B	C	C	D
10.000	B	C	C	D	D

SIL 3 (HIPPS)

¿Por esto …?

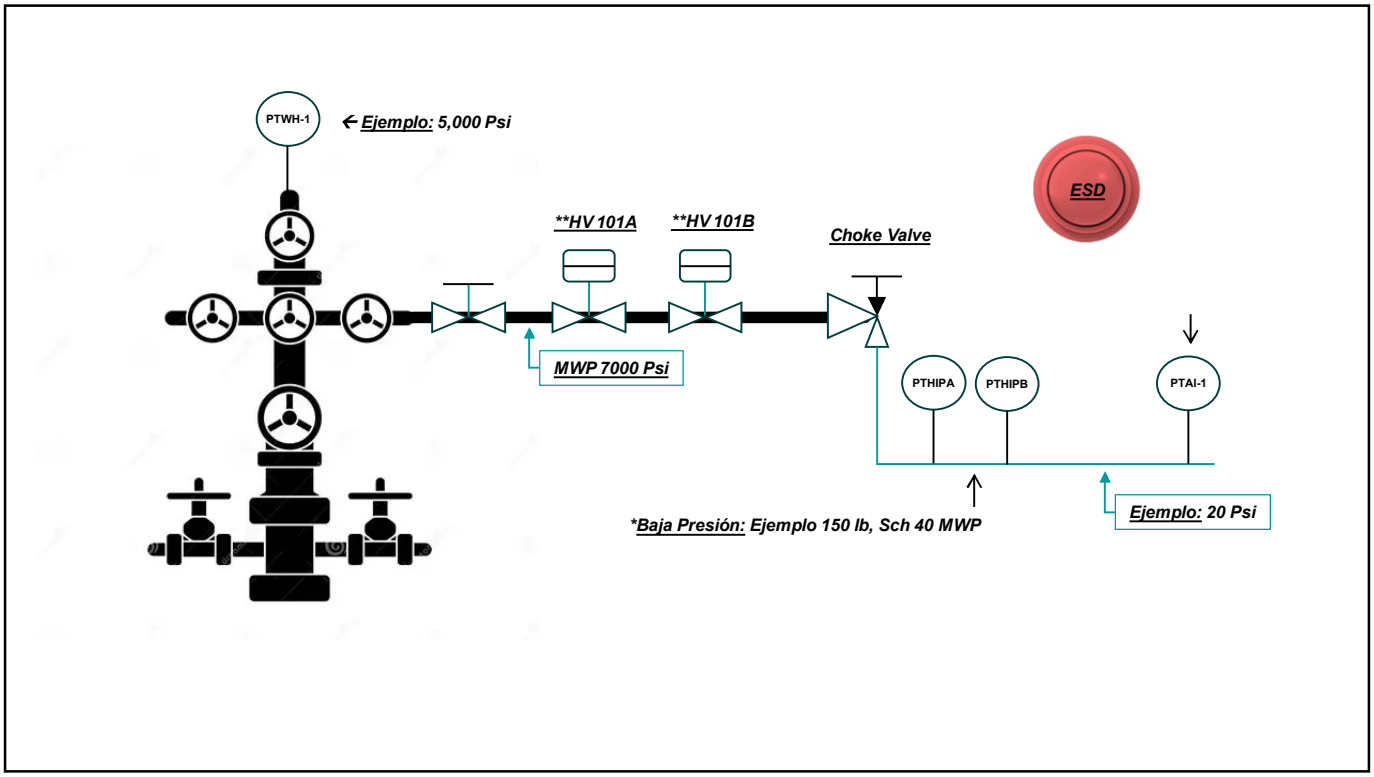
BPCS-C/P

Consecuencias	Frecuencia Categorías - Años				
	>10.000	10.000 - 1.000	1.000 - 100	100 - 10	10 - 1
1	A	A	A	B	B
10	A	A	B	B	C
100	A	B	B	C	C
1.000	B	B	C	C	D
10.000	B	C	C	D	D

SIL 2

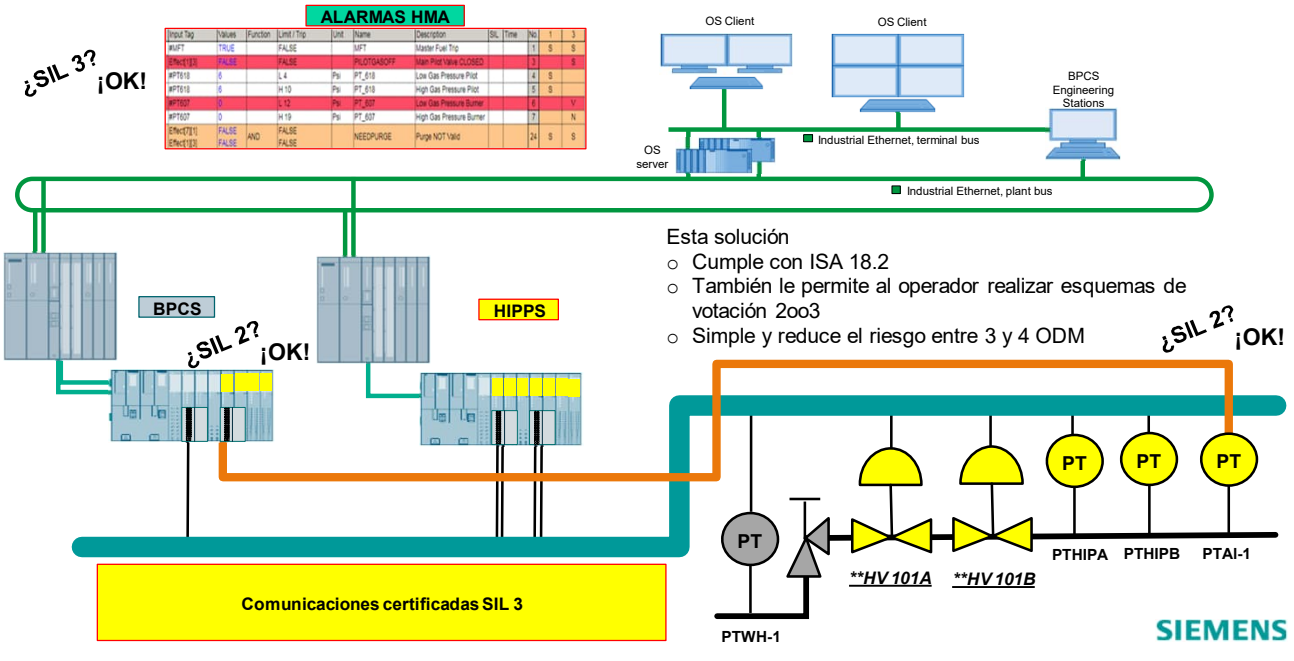
SIEMENS

34



35

¿Optimizando la reducción de riesgo?



Esta solución
- Cumple con ISA 18.2
- También le permite al operador realizar esquemas de votación 2oo3
- Simple y reduce el riesgo entre 3 y 4 ODM

36

Conclusión

1. **Si** se considera aceptable que una Alarma IPL ó LI-PL que este racionalizada sea acreditada para reducir riesgo de un peligro en especifico
2. **Si** necesita optimizar el rendimiento de una SIF disminuyendo el SIL objetivo
3. **Se puede lograr** con un sistema que independientemente pueda realizar funciones de protección que estén libre de interferencia del control … tanto para **IPL** como para **LIPL**

Entonces:

- Tomar crédito por **Alarmas IPL** por un orden de magnitud es posible en un DCS con las características de SIMATIC S7-400 F/FH siempre y cuando se administren como **Alarmas HMA**.
- La gestión de alarmas como **LI-PL** o como **IPL,** se simplifica significativamente

SIEMENS

37

Preguntas?

SIEMENS

38

Contact

Published by Siemens Industry

Luis M F Garcia G
Process Safety Consultant
Process Safety Americas
Houston, TX
USA

Phone +11 (281) 687-8369

E-mail luisgarcia@siemens.com

usa.siemens.com/processsafety

SIEMENS

39