

1er. Congreso Latinoamericano y 3ro. Nacional de Seguridad y Salud Ocupacional en la industria del Petróleo y del Gas.

Gestión de la Seguridad Funcional

Importancia e implementación

Aplicación de las normas IEC61508 e IEC 61511

Preparado por: Guillermo Leanza

Gerente: Centro de Ejecución de Proyectos de Seguridad

ABB Argentina

Email Guillermo.leanza@ar.abb.com

1 Sinopsis:

La Seguridad Funcional es una rama de la industria que se encarga garantizar del correcto funcionamiento de los Sistemas de protección de proceso,

Se habla, "Seguridad Funcional" cuando la seguridad depende del funcionamiento correcto de un sistema eléctrico (E), electrónico (E) y electrónico programable (PE) (abreviado: sistema E/E/PE). También conocidos como Sistemas Instrumentados de Seguridad (SIS)

La Seguridad Funcional nos permite afrontar los "Riesgos Mayores" inherentes a un proceso determinado y ha significado un importante avance, tanto en la metodología, como en la filosofía para tratar el problema del riesgo tecnológico.

El correcto funcionamiento de un sistema de seguridad no solo depende del hardware y el software propiamente dicho, sino también, de cómo ha sido desarrollado. Es decir: especificación, diseño, construcción, operación y mantenimiento.

No importa lo bueno que hoy o en el futuro sean los productos diseñados para seguridad, ya que poco podrán hacer si no se los usa correctamente.

El desarrollo en la empresa de "La cultura de la seguridad" es un hecho clave para la sustentabilidad de los negocios. Incluyendo las disciplinas de Seguridad y Salud Ocupacional como así también la Seguridad Funcional de los sistemas de proceso.

El presente trabajo intenta mostrar la importancia del desarrollo de un sistema de gestión de la Seguridad Funcional, siguiendo los lineamientos normas IEC 61508/ IEC 61511. Asimismo se describen las experiencias del proceso de certificación del mismo por un ente independiente como el TUV. Permitiendo asegurar que los proyectos son realizados con los procesos adecuados, los profesionales competentes y en el tiempo correcto.

2 Introducción

Según un estudio del HSE sobre un conjunto de explosiones en industrias químicas¹, el 71% se debió a la ausencia de un sistema de gestión de seguridad o a falencias en el mismo (el otro 29% se reparte entre fallas de equipos, equipos faltantes y problemas de mantenimiento).

Por lo tanto, resulta importante considerar la Gestión de Seguridad entre las prioridades más altas de una planta industrial.

Las Normas IEC 61508² e IEC 61511³, son consideradas en la actualidad como las mejores prácticas para garantizar la seguridad en los procesos industriales. Su principal fortaleza radica en el concepto de la gestión del ciclo de vida, ya que permite un enfoque sistemático

¹ Health and Safety Executive, UK, 1997

² IEC61508 "Functional safety of electrical/electronic/programmable electronic safety-related Systems"

³ IEC 61511³ "Functional safety - Safety instrumented systems for the process industry sector"

basado en el desempeño de las organizaciones. Asimismo describen requerimientos técnicos en cuanto a Hardware y Software que deben tenerse en cuenta.

2.1 Importancia de la Seguridad Funcional

Con el fácil acceso a la información que nos posibilita Internet, las noticias se difunden con rapidez en todo el mundo. Basta con poner la palabra BP es su buscador preferido e inmediatamente aparecen miles de enlaces mostrando las consecuencias catastróficas del accidente de la plataforma de petróleo en el golfo de México.

Aparte de las consecuencias del accidente propiamente dicho, al medio ambiente, pero también por las fatalidades ocasionadas y las pérdidas materiales en la plataforma, las acciones de la compañía han bajado en el orden del 50% y se estima un costo de USD 2.000 millones para compensar los daños ocasionados.



Figura 1: Valor de las acciones de BP (Fuente www.bp.com)

Muchos más casos han ocurrido en la industria, como por ejemplo Flixborough, UK, 1974; Seveso, Italia, 1976; Bhopal, India, 1984; Piper Alpha, UK, 1988; Pasedena, USA, 1989; Texas City, USA 2005. etc. En todos estos casos han demostrado falencias en la gestión de la seguridad.

Es interesante la lectura del llamado “Baker panel report”, preparado, después del accidente de Texas City, por un comité independiente de reconocidos especialistas, liderado por James Baker:

http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/SP/STAGING/local_assets/assets/pdfs/Baker_panel_report.pdf

De las doce conclusiones principales destaca las graves falencias en el sistema de gestión de la seguridad.

A partir de estos casos catastróficos, parecería obvio que se debería prestar especial atención a los sistemas de protección de los procesos de planta.

Sin embargo, actualmente, algunos factores culturales y económicos, hacen que la seguridad funcional, no sea implementada correctamente.

Frases tales como: “A mi no me va a pasar”, “Siempre funcionó así”, “Un sistema de protección es muy costoso para mi empresa”, “La empresa no está preparada aún para implantar la gestión de la seguridad funcional”, “No tenemos gente” etc. Son muy comunes de escuchar.

Por otra parte las demandas de mayor producción, hacen que la seguridad muchas veces sea comprometida.

Sin embargo, los costos de un accidente de proporciones mayores, puede dejar a la compañía en la bancarrota.

Actualmente en la Argentina, tenemos un grupo de profesionales altamente capacitados, tecnologías sofisticadas y a la vez confiables para ser usadas en seguridad, sin embargo falta la dirección política de tomar a la seguridad de procesos como una especialidad en si misma.

Es bueno citar una frase del científico español Santiago Ramón y Cajal, para demostrar lo que cuesta aprender de los errores del pasado:

“Lo peor no es cometer un error, sino tratar de justificarlo, en vez de aprovecharlo como aviso providencial de nuestra ligereza o ignorancia.”

Ejemplos de los errores ya los tenemos ¡¿Qué esperamos para poner en práctica lo aprendido?!

3 Gestión de la Seguridad Funcional. ¿Qué necesitamos?

Uno de sus principales requerimientos de las normas IEC 61508/IEC61511, es que la organización instale un Sistema de Gestión de Seguridad Funcional (Functional Safety Management System, en adelante FSMS)⁴ que asegure que cuando se use un SIS (Safety Instrumented Systems) éstos mantengan el proceso en un estado seguro. La organización debe definir una política y una estrategia de seguridad⁵, comunicarla a sus empleados, y determinar la forma de evaluar su cumplimiento.

Esto implica identificar las personas, departamentos u otras unidades responsables de llevar a cabo y revisar las fases del ciclo de vida de seguridad, informarlas de sus responsabilidades y asegurar su competencia. La organización debe definir los roles y responsabilidades de cada integrante del equipo, y a quién reporta.

La gestión de la seguridad incluye la evaluación y gestión de riesgos, planificación de las actividades, implementación, seguimiento, evaluación y revisión de los sistemas de seguridad. Esto requerirá la conformación de un equipo que tenga la competencia técnica⁶ para llevar a cabo las actividades de cada fase, y que incluya como mínimo un miembro competente independiente (interno o externo) no involucrado en el equipo de diseño para asegurar la objetividad⁷.

El equipo debe asegurar que al menos se haga una evaluación de seguridad funcional, (Functional Safety Assessment)⁸ confirmando que se hizo un análisis de riesgo, se aplicaron las recomendaciones resultantes, se cumplen las especificaciones de requerimientos de seguridad, se validaron los sistemas y se entrenó al personal, etc. El nivel de independencia para efectuar la evaluación depende de cuanto sea el nivel SIL (safety Integrity Level) de la función de seguridad y pueden ser individuos, departamentos u organizaciones.

También deben definirse procedimientos de auditoría del sistema⁹ (incluyendo frecuencia, independencia de los auditores y registro), y procedimientos para modificaciones y cambios.

4 Ciclo de vida de la seguridad

Uno de los conceptos más importantes de la IEC 61511 (Indicada para la industria de procesos) es el de ciclo de vida de seguridad: las actividades involucradas en la implementación de funciones instrumentadas de seguridad (SIF, safety Instrumented

⁴ IEC61508-1 Capítulo 6, IEC 61511-1 Capítulo 5 - Management of functional safety.

⁵ IEC 61511-1 5.2.1.1 The policy and strategy for achieving safety shall be identified together with the means for evaluating its achievement and shall be communicated within the organization.

⁶ IEC 61511-1 5.2.2.2 Persons, departments or organizations involved in safety life-cycle activities shall be competent to carry out the activities for which they are accountable.

⁷ IEC 61511-1 5.2.6.1.2 The membership of the assessment team shall include at least one senior competent person not involved in the project design team.

⁸ IEC 61508-4 3.8.3 functional safety assessment investigation, based on evidence, to judge the functional safety achieved by one or more E/E/PE safety-related systems and/or other risk reduction measures

⁹ 5.2.6.2 Auditing and revision

Function) que comienzan con la fase de conceptualización y terminan cuando las SIF ya no se usan. La norma requiere que las actividades se organicen en un ciclo de vida y que se definan las fases y requerimientos de las mismas. Cada fase debe tener sus objetivos, entradas, salidas y actividades de verificación.

4.1 Fases del ciclo de vida de Seguridad

Las fases típicas para el desarrollo, operación y mantenimiento de un SIS mencionadas por la norma son:

1. Análisis de peligrosidad y riesgos.
2. Asignación de las funciones de seguridad a capas de protección.
3. Especificación de requerimientos del SIS.
4. Diseño e ingeniería del SIS
5. Instalación, puesta en servicio y validación del SIS
6. Operación y mantenimiento del SIS
7. Modificaciones al SIS
8. Retiro de servicio del SIS

Existe además una fase en paralelo a las previamente mencionadas, que es la de verificación para asegurar que cada fase provea los resultados requeridos.

Todas estas actividades deben ser planificadas y documentadas desde el principio, como así también las personas que participarán en cada fase y verificación. No menos importante es documentar qué debe verificarse y cómo manejar las no conformidades.

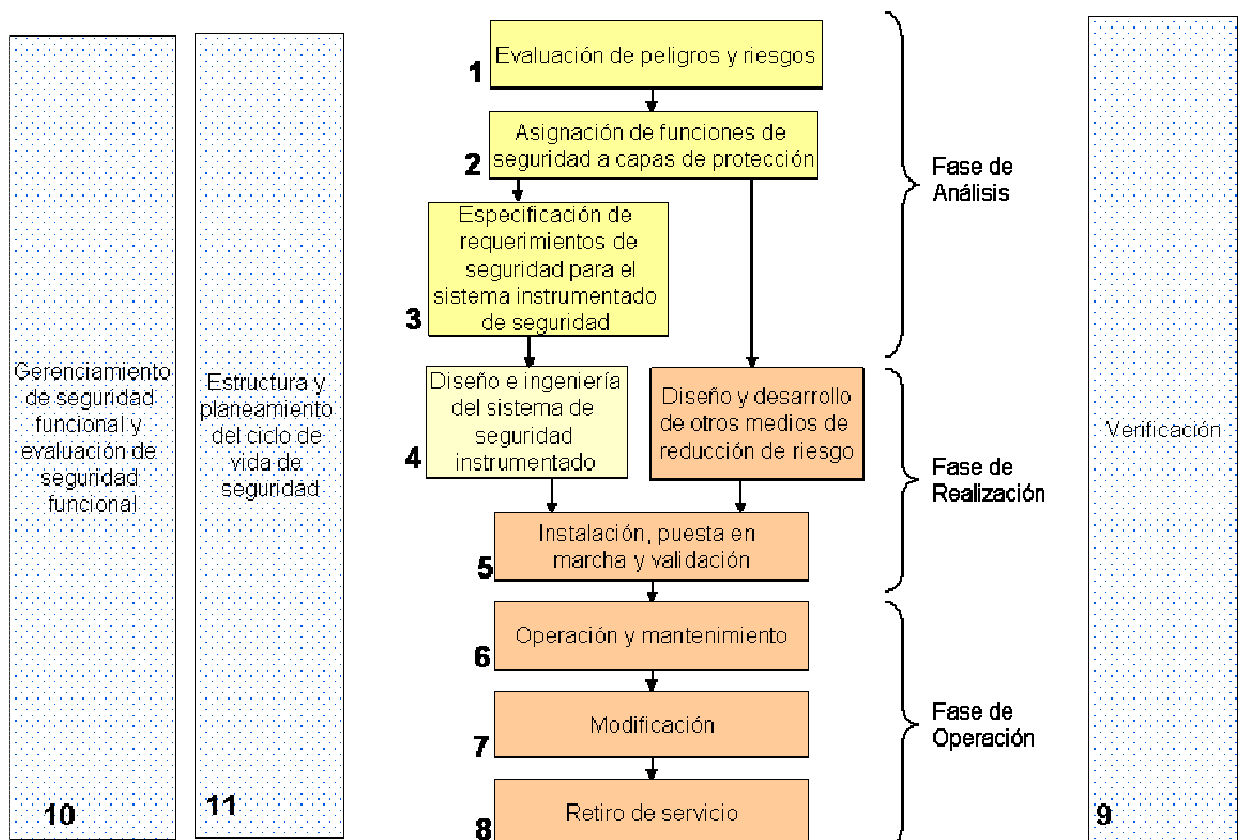


Figura 2 Ciclo de vida de la seguridad

5 Desarrollo de un Sistema de Gestión certificado

5.1 ¿Por qué certificar?

Así como las normas de calidad ISO9001, o de seguridad OSHA 18001 o de medio ambiente ISO 14001, pueden ser auditadas y certificadas por un ente independiente, también corresponde con la implementación de las normas IEC61508 e IEC61511. Son numerosas e importantes las ventajas de tener un sistema certificado, entre ellas se puede mencionar las siguientes:

- Permite demostrar el cumplimiento de los estándares.
- Garantizar la competencia de la organización y de los individuos.
- Permite desarrollar buenas prácticas en la ejecución del proyecto, operación y mantenimiento.
- Permite el uso de una metodología común, y de uso internacional, que puede repetirse en otras instalaciones.
- Reduce la exposición de las posibles demandas, demostrando que se han usado las buenas prácticas de ingeniería.
- Permite una reducción de costos por el hecho de tener acotado los riesgos y con la posibilidad de obtener beneficios en menores primas en las reaseguradoras.

6 Proceso de desarrollo implementación y certificación del FSMS

El proceso de la implementación del sistema de gestión de la seguridad funcional, que se describe a continuación, ha sido llevado a cabo en la Argentina. El mismo, es el primero en América que logrado la certificación del TUV Rheinland de Alemania.

6.1 Decisión corporativa y liderazgo

Todo proceso de implementación de un sistema de gestión debe tener una firme decisión corporativa para llevarlo adelante. Esto es plasmado en la política de la seguridad funcional de la compañía. Dicha política debe ser escrita y firmada por la dirección.

Ello permite asignar los recursos necesarios, el desarrollo de las actividades del día a día y asignando las prioridades para que el sistema siga adelante, a pesar de las adversidades.

Considerando los beneficios que conlleva dicha actividad, pero asumiendo un costo inicial que prontamente pueda ser amortizado con una reducción del riesgo operativo dado por las buenas prácticas y el alineamiento a las normas.

Definitivamente, es muy difícil que un sistema de gestión pueda ir adelante sin esta decisión corporativa. Los esfuerzos individuales sin este apoyo generalmente terminan usualmente en una frustración.

Tomada la decisión se debe identificar las personas que por sus capacidades puedan liderar el proceso.

6.2 Capacitación

Como medida inicial es importante entender claramente los requerimientos de las normas IEC61508 e IEC61511, por lo que es altamente importante la capacitación de los involucrados a llevar a cabo el proceso de certificación. Por otra parte, como la norma requiere demostrar la competencia de las personas, es importante certificar un grupo de ingenieros en seguridad funcional por TUV Rheinland ya que permite demostrar la competencia de las personas.

6.3 Definición de alcance

Como se mostró en el ciclo de vida de seguridad, comprende diferentes fases, con diferentes objetivos y capacidades. Las mismas pueden ser desarrolladas por diferentes tipos de organizaciones tales como, usuarios finales, empresas de ingeniería, integradores, operadores, etc.

Por ejemplo una asignación típica de responsabilidades puede ser la siguiente (ver Fig., 2):

- Fases 1, 2 ,3 Usuario final u operador
- Fases 4 y 5 Empresa de ingeniería o integrador
- Fases 6, 7, 8 Usuario final u operador
- Fase 7 Empresa de ingeniería o integrador (Opcional)

Por consiguiente, cada organización puede establecer un sistema de gestión para afrontar sus responsabilidades según la fase del ciclo de vida que deba desarrollar.

En este caso, por tratarse de una organización de ingeniería, el alcance de la certificación definido son las siguientes fases:

IEC 61508 E/E/PES Safety Related Systems Integration.

IEC61511 SIS Integration.

6.4 Evaluación de la situación actual

Una vez capacitados los profesionales y formados los equipos de trabajo, con el alcance de aplicación claramente definido, es necesario saber que grado de cumplimiento existe respecto a las normas. Es interesante comentar que aunque no se esté trabajando de acuerdo a las normas IEC61508/11, muchos de los requerimientos de las mismas, eventualmente pueden estar cumpliéndose, ya que como sistema de gestión, una parte de ellos pueden estar cubiertos por el sistema de calidad ISO9001.

La técnica utilizada para saber que hacemos y que debemos hacer es la de “Gap análisis” donde se procede a elaborar un listado con los requerimientos de las normas y por otro lado sustentar que se hace actualmente para cada requerimiento.

Target of Evaluation	Purpose of TOE	Ref. 61508 Clauses / Tables	Assessment Notes	61511 Clauses and Purpose
1 Verification Documentation <i>Life Cycle Phase – Always applies for each phase identified</i>	To demonstrate for each phase of the lifecycle, by review, analysis or test documentation, that the outputs for the phase meet the specified requirements. 61511 Phase 4, 61508 Phase 8 for System Integrator	1/7, 10	No formal planning of verification is undertaken, however verification deliverables are produced, ie test records. <i>It is recommended that the safety lifecycle management plan be used for planning the verification activities.</i> <i>It is recommended that a formal review and configuration management procedure is used</i>	7.1 Objective Demonstrate by review, analysis and/or testing that the required outputs satisfy the defined requirements for an appropriate phase of the safety life cycle identified by the verification plan

Que deberíamos hacer

Referencia en IEC 61508

Que estamos haciendo

Referencia en IEC 61511

Figura 3 Ejemplo de Gap Análisis

Considerando lo que hacemos y determinando lo que debemos hacer, podemos establecer un plan para cubrir las áreas donde las actividades no son satisfactorias para los requerimientos de las normas.

6.5 Planeamiento de FSMS.

Ahora que se conoce lo que hay que debemos hacer, de deben planificar los puntos más relevantes para formar una organización de seguridad funcional.

- Política de la seguridad funcional.
- Estructura organizativa.
- Actividades y responsables.
- Decidir cómo vamos a ejecutar proyectos de seguridad.
- La identificación de nuevos procedimientos.
- La identificación de nuevas actividades.

Es importante destacar que aparte de la estructura organizacional en si misma, debe pensarse que las funciones de evaluación (assessment) y auditorias que deben ser independientes de la ejecución. Por lo tanto se va a necesitar soporte de otros departamentos u organizaciones con la suficiente independencia.

6.6 Desarrollo de una metodología para el ciclo de vida de seguridad

El desarrollo de un modelo de ciclo de vida de seguridad, nos ayuda a resolver en forma metódica y sistemática, los requerimientos de las normas IEC61508/IEC61511. La generación de procedimientos, su interrelación y las definiciones de las tareas y actividades sustentan la base organizacional del FSMS. Las evaluaciones y auditorias, nos permiten que los errores puedan ser minimizados en forma temprana y evitar la propagación durante la ejecución del proyecto o peor aún si el SIS está en operación. Los puntos principales a cubrir del modelo son:

- Gestión de la Seguridad Funcional.
 - Auditoría.
 - Evaluación (assessment).
 - Control de cambio.
 - Técnicas y métodos.
- Estructura y planificación.
 - Plan de manejo del ciclo de vida de la seguridad.
 - Registros de producción.
- Requisitos y Diseño.
 - Especificación funcional.
 - Diseño de detalle.
- Verificación y Validación.
 - Revisión del Código.
 - Prueba de integración.
 - SIL logrado.
 - FAT.
 - SAT.

Si bien este modelo ha sido concebido para la fase de realización de un SIS, un modelo de similar características, pero con otras actividades podría implementarse para cualquier parte del ciclo de vida de seguridad.

El uso de actividades genéricas, permite facilitar las mismas y reducir costos. De todas formas, deben desarrollarse de forma tal que se contemplen todos los requerimientos necesarios de las normas, por lo que deben ser lo suficientemente estrictos para garantizar que se logra la seguridad funcional. Para dichas actividades, deben especificarse los criterios de aceptación, responsabilidades y su salida.

Activity Number	Business Process Model Reference	Activity	Activity Related Procedure or Document	Acceptance Criteria	Prime Responsibility for Activity	Activity Deliverable	Inspection Schedule		
							ABB	Client	VB
2 Design and Engineering									
2.1 Hardware and Software									
2.1.1		Preparation, Submission, Review and update of Functional Design Specification	Safety Requirements Specification Safety Execution Centre Local Procedures Review and Configuration Management Procedure	Conformity in contract specifications and quality system requirements Review of Safety Manual Requirements	SIS Lead Engineer Independent Verification Body	Client Approved Functional Design Specification Design Review Report	A	A	R

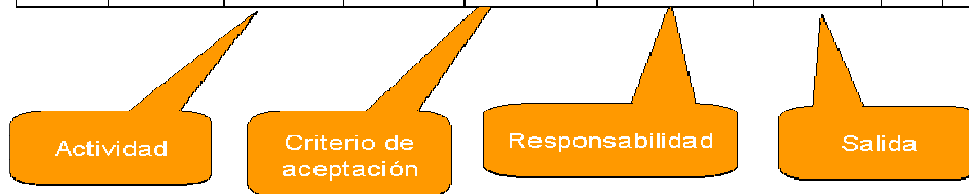


Figura 4 Actividades genéricas.

6.7 Desarrollo de la documentación

El desarrollo del FSMS requiere de la elaboración de nuevos documentos que amplíen el sistema de gestión de la calidad con los requerimientos de la seguridad funcional. Por lo que es necesaria la elaboración de nuevos procedimientos documentados o proveer de mayor rigor a parte de los procedimientos existentes. Como parte de las adecuaciones que fueron necesarias, se mencionan:

- Nuevos procedimientos.
- Gestión del Cambio.
- Gestión de la Configuración.
- Técnicas y mediciones.
- SIL logrado.
- Documentos marco.
- Safety Lifecycle Management (Calidad).
- Plan de pruebas.
- Esqueletos de documentos (Directrices).
- Especificaciones funcionales de diseño.
- Especificaciones de diseño detallad.



Figura 5 Elaboración del FSMS

Es importante destacar que si bien los sistemas de gestión de calidad como ISO9001, consideran el control de cambio, para las normas IEC61508/11 dicho control es mucho más riguroso y debe hacerse un análisis de impacto en la seguridad de cada cambio propuesto a fin de evitar la incorporación de nuevos errores.

6.8 Certificación

Una vez concluido la elaboración del FSMS como sistema, podemos certificarlo por una organización independiente, a fin de comprobar el alineamiento a las normas IEC61508 e

IEC61511. Para ello la opción debía basarse en una organización independiente y de reconocido liderazgo internacional.

La selección ha sido TÜV Rheinland de Alemania. (www.tuvsi.com), Organización que es ampliamente reconocida por las certificaciones de equipamiento de seguridad funcional como así también de FSMS.

El proceso Consiste en tres fases:

- Pre-Auditoría.
- Puesta en funcionamiento. (demostrable por medio de un proyecto piloto.)
- Auditoría final.

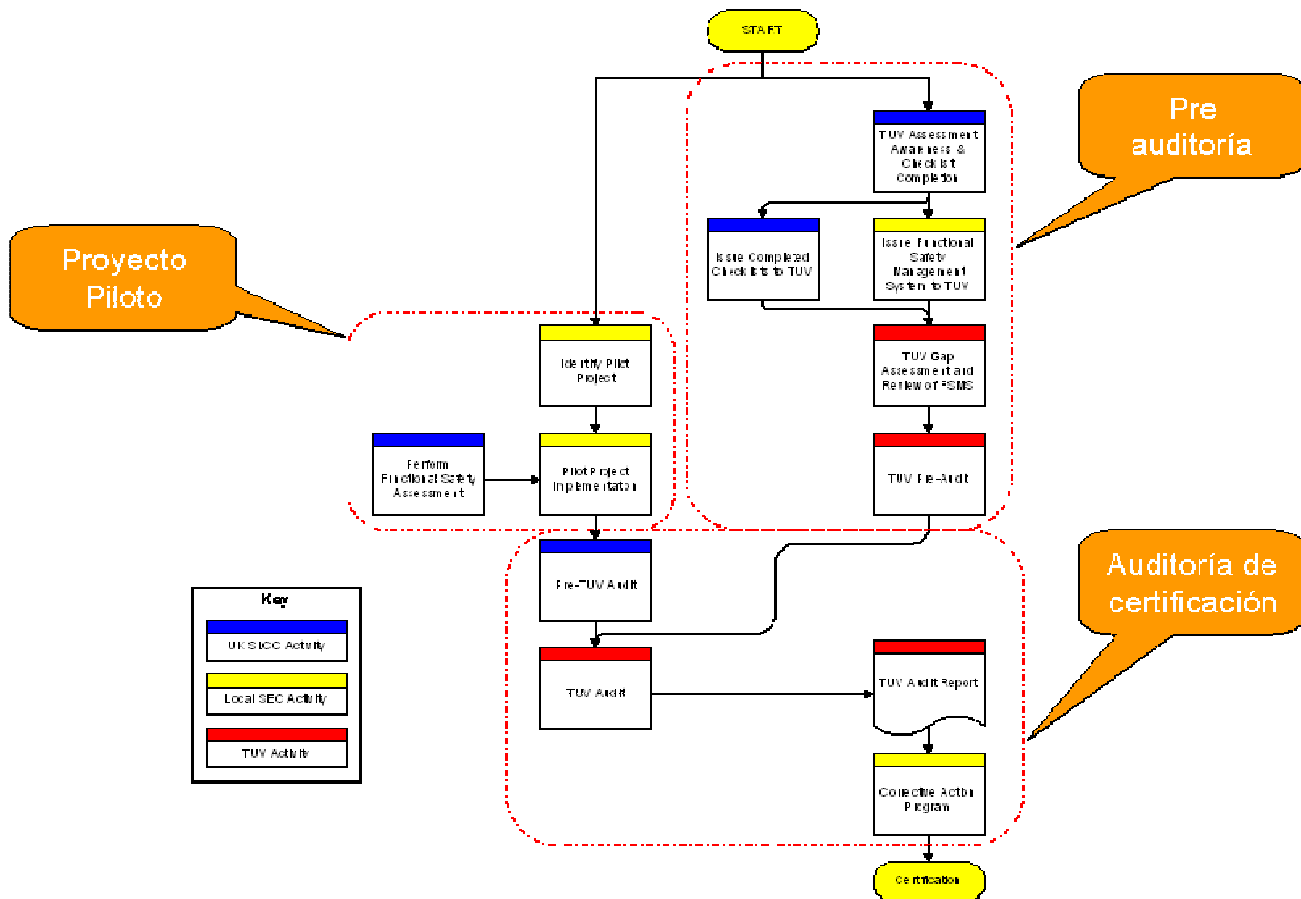


Figura 6 Proceso de certificación

6.9 Pre-Auditoría.

La pre-auditoría consiste en asegurar que el sistema FSMS cumple con los requerimientos de las normas, el mismo está dividido en fases a cumplir

1. Completar las Listas de verificación (checklist) enviados por TÜV.
La función de los mismos es verificar que el sistema de gestión se ajusta a la norma. En cada punto se indica un requerimiento de la norma y se debe demostrar, con evidencia, como se cumple con dicho requerimiento.

Functional Safety Management IEC61511-Checklist:

Management of Functional Safety			References:
No.:	Topic and special items of interest	Standard-Reference Note 1	Referenced Procedures Referenced Work Instructions Referenced Templates
MFS 1	Overall quality description: • Strategy • Policy	5.2.1.1 5.2.1.2	- Functional Safety Management System Strategy and Policy is described in the FSMS Overview, 3BAR004075. - The FSMS Policy, 3BAR004070A0001, states that the SEC (Safety Execution Centre) Manager and the PA (Process Automation) Industrial Systems General Manager is responsible for communicating the FSMS policy throughout the SEC. - The FSMS Overview, 3BAR004075, shows the relationship between the SEC and QMS (Quality Management System) management systems, FSMS (Functional Safety Management System).

Requerimiento del standard

Referencia SEC FSMS

Figura 7 Checklist TÜV.

- Enviar los procedimientos a TÜV para su comprobación de escritorio “desk check”
En esta actividad se verifica la consistencia e interrelación de los procedimientos definidos, asimismo que se comprueba el alineamiento con la norma.
- En Base a las listas de verificación y la comprobación de escritorio, surgen una serie de no cumplimientos con la norma que deben ser solucionados antes de continuar con el uso del sistema de gestión. TÜV emite un documento Lista de ítems abiertos (Open Items List. OIL) donde se expresan todas las desviaciones encontradas. Sobre este documento de deben indicar las correcciones necesarias al sistema, responsable y fecha prevista de solución.

Open Items			To be done by / until	Confirmed by / at
No	ID			
		Item: PAS Project Query Handling supplemental 3BGB 000228 Scope: "This document relates to the processing of Queries using the ABB Lotus Notes/web based Charge Management Tool Version 1.4" KP-Q: What could be a worst case if a 'query' that may be safety critical is lost/deleted or corrupted within the Lotus Notes/web based system? Also, it is further implied the 'impact analysis' is incorporated within 'Lotus notes'. What if a critical analysis is lost/deleted Action: The AEB Lotus Notes servers are under the control of ABE's rigorous backup and archive regimes, ensuring that secure daily backups, and regular archives of the PQ data, including impact analysis and other attachments are stored securely. Catastrophic loss of the Lotus notes server would not cause total loss of the PQ and attachments, as these can be recovered from either the daily backup or archive material.	3 weeks before the final audit date	kg, kg
1	D-1			
		Done: KP		

Procedimiento

Open Item

Respuesta del SEC

Figura 8 Open Item List

6.10 Puesta en marcha (Proyecto Piloto)

El éxito de un sistema de gestión es que pueda ponerse en práctica y que sea aceptado como metodología de trabajo. Es por ello, que debe aplicarse a un proyecto piloto y probar su funcionamiento. Es de destacar que muchas veces se tiende a realizar sistemas de gestión que son impracticables de llevarlos a funcionamiento.

Una vez identificado el proyecto piloto, debemos demostrar que el sistema de gestión, funciona y que lo usamos correctamente. Para ello las actividades de auditoria y de evaluación (assessment), son la clave para asegurar su cumplimiento.

6.11 Auditoría de certificación

Antes de realizar la auditoría final de certificación, se acuerda el plan con la entidad certificadora. Durante la auditoría se examina la eficacia del sistema de gestión. Los documentos y actividades realizadas son el punto de partida para la evaluación.

La tarea fundamental es demostrar la aplicación práctica del FSMS, en el proyecto piloto. Para esta actividad, la clave es proveer evidencia de cada actividad, y que consideraciones se efectúan a la hora de garantizar la seguridad funcional. La capacitación del personal involucrado, es una de las partes donde más se hace hincapié, ya que las normas dan gran importancia a las capacidades para realizar cada actividad.

Como resultado del proceso de auditoría se generan nuevas desviaciones, por lo que se produce un nuevo documento con la Lista de Ítems Abiertos, (OIL). Para lo cual se deben plantear las correcciones necesarias.

Si las acciones correctivas satisfacen los criterios de aceptación. La autoridad de certificación decide, sobre el informe de auditoría y la documentación que la sustenta, la certificación del sistema de gestión FSMS.

7 Conclusiones

La experiencia nos demuestra que la mayoría de las catástrofes en la industria han sido debidas a fallas de procedimientos. La implementación de un sistema de Gestión de la Seguridad Funcional, nos permite reducir el riesgo a valores aceptables.

Es común creer que la implementación de las Normas IEC61508/IEC61511 se limita a tener un hardware SIL3 certificado por TÜV.

Si bien es importante que las partes de hardware a utilizar en seguridad sean aptas, si no se gestiona la seguridad estamos propensos a incurrir en errores que podrían ser fatales. Ya que por su naturaleza los errores sistemáticos se propagan sin darnos cuenta

También se cree que la Seguridad Funcional, es costosa, sin embargo, es todo lo contrario ya que muchas veces se incurre en sobre dimensionamiento con mayores costos de implementación o peor aún en sub dimensionamiento donde el riesgo no es mitigado correctamente. Esto ocurre por la ignorancia de desconocer cuanta seguridad es necesaria. Finalmente cabe mencionar, tal como se ha demostrado que el cumplimiento de las normas IEC61508/IEC61511 es posible, y que puede ser certificado y por lo tanto se puede exigir a la hora de implementar un sistema de protección de planta

8 Agradecimiento

El autor desea agradecer a las perronas que han participado en este emprendimiento ya sea por su decisión en el rumbo a seguir, como así también a los colaboradores que aportaron lo mejor se sí, para llevar adelante el proceso de certificación

Stuart Nuns
Alejandro Calissano

Gaspar Urman
Guillermo Vergara
Pablo Daneri
Augusto Bezzola
Pablo Kalis
Jorge Bourdette

9 Referencias

IEC61508 "Functional safety of electrical/electronic/programmable electronic safety-related Systems"

² IEC 61511 "*Functional safety - Safety instrumented systems for the process industry sector*"

3 Functional Safety Managemet Explained M. Houtermans, T. Huber, W. Velten- Philip ISA Safety Division

4 Safety Management Tools and Techniques, M.J.M. Houtermans Published online at the ISA Safety Division.

5 Functional Safety A straightfoward qude to applying IEC61508 and the related standards. David J Smith & Kenneth G Simpson. ISBN: 0750662697

6 Review of Process Safety Management Systems at BP North American Refineries for the BP U.S. Refineries Independent Safety Review Panel. James Baker and others