SISTEMAS INTEGRADOS, CALIDAD Y SERVICIO AL USUARIO

Norberto Santiago

Índice

Introducción

Actualmente la tecnología digital está siendo implementada de forma decidida en las subestaciones eléctricas. No ha sido un proceso fácil ni rápido.

Las compañías eléctricas fueron pioneras en la utilización de las computadoras para gestión y por supuesto las han venido empleando de forma intensiva en labores administrativas, financieras, así como en el manejo de la información de su sistema.

Sin embargo en las subestaciones la evolución ha sido "lenta" y es ahora en los 90 cuando se está aplicando la informática de una forma generalizada en los equipos de protección, control y medida.

Entorno

Alguien podría pensar que este fenómeno se debe a que las empresas eléctricas en nuestro país están padeciendo los efectos de un retraso tecnológico, y que en otros países la situación es diferente.

Podemos asegurar, por nuestra experiencia con compañías eléctricas de todo el mundo, que las compañías españolas gozan de una reputación técnica de primerísimo orden, siendo algunas de ellas pioneras, en practicas como el telecontrol de instalaciones, la telemedida, etc., etc.

En un país del que nadie tiene dudas sobre su modernidad, tal como Estados Unidos, y en un reciente congreso celebrado en abril de este año había compañías eléctricas que explicaban sus recientes experimentos en el telemando de subestaciones y su futura aplicación a su estrategia de "instalaciones abandonadas", practica adoptada en España desde los años 70.

Luego si las compañías, y sobre todo sus técnicos, son favorables a la evolución tecnológica ¿Porqué estamos empezando recientemente la era de la "digitalización" de las subestaciones?.

El sector ha sido tradicionalmente muy conservador ante cualquier innovación tecnológica, dada la repercusión de estos temas en la fiabilidad del sistema, la calidad del servicio, etc. Sin embargo, se han realizado experiencias más o menos importantes, que por desgracia han dado resultados variados, dando a los escépticos razones para reforzar sus argumentos de "no hacer" en aras de la "máxima seguridad" requerida en el tipo de instalaciones que nos ocupa.

Sin duda el factor que más ha influido en el desarrollo de este proceso, es la aparición del software como parte fundamental, y en cierta forma obscura, de unos equipos cuyas características repercuten de forma inmediata y directa en la seguridad, la calidad de servicio, etc. de todo el sistema.

Referencias históricas

La evolución tecnológica, y sus repercusiones en áreas consideradas de máxima seguridad, no es exclusiva de nuestros tiempos, y por desgracia la actitud humana hacia el cambio tampoco.

En un artículo aparecido en la revista IEEE COMPUTER sobre la problemática de la industria del software, se analizaban las semejanzas históricas entre la implantación del software en los procesos de alta seguridad en la industria, y la introducción de la alta presión en las máquinas de vapor, o de la alta tensión en la generación y transporte en la industria eléctrica.

En 1786 James Watt trabajando como instrumentista en la universidad de Glasgow fue encargado de reparar un modelo del motor de Newcomen que era usado en la clase de filosofía natural.

Watt, por una de esas casualidades que tanto abundan en la historia, era el único de los que por aquella época estaban trabajando en las máquinas de vapor, que tenía frecuentes contactos con científicos que estudiaban el calor, incluido su .amigo Joseph Black, que le comentó su reciente descubrimiento sobre el calor latente.

Watt pensó que podía mejorar el motor de Newcomen y patentó unas cuantas ideas importantes, como un condensador separado y el diseño de un motor que produce un movimiento rotativo. Al mismo tiempo, y debido a la revolución industrial, se genera una demanda de energía sin precedentes en la historia.

Con la colaboración del industrial Matthew Boulton, Watt generó un diseño de "máquina de vapor" que protagonizó el cambio tecnológico en la última parte del siglo XVIII. Podemos decir que la aplicación de este invento en la industria y en el transporte supuso uno de los cambios históricos más importantes en la sociedad.

Sin embargo, rápidamente, los usuarios se percatan que la eficiencia y economía de la máquina están en función de la presión de vapor utilizada (entre 5 y 15 libras por pulgada cuadrada) y que el aumento de dicha presión (por encima de la presión atmosférica) aumentaba significativamente su rendimiento y sus posibles aplicaciones.

Watt y Boulton se opusieron totalmente a la modificación de su diseño , argumentando que el aumento de presión significaba un aumento inaceptable del riesgo de explosión.

Tan pronto sus patentes expiraron en 1800, casi simultáneamente, Oliver Evans en Estados Unidos y Richard Trevithick en Inglaterra, diseñaron máquinas con una presión de vapor bastante más alta que la atmosférica, que accionaba el pistón directamente.

Las predicciones de Watt fueron correctas y múltiples accidentes con víctimas salpicaron todas las aplicaciones de dichas máquinas. Las primeras máquinas se componían de materiales no adecuados utilizados sin unos requisitos precisos por personal sin la suficiente preparación, ni experiencia. Por supuesto no se sabía que era el control de calidad.

En Estados Unidos el Comisionado de Patentes estimó que entre 1816 y 1848 unos 233 barcos de vapor explotaron, ocasionando la muerte de 2562 personas y heridas a otras 2097 con unos daños materiales de 3 millones de dólares (de la época) aproximadamente.

Sin embargo, el uso de las máquinas de vapor no se detuvo, ya que los ingenieros, presionados por el mercado, desarrollaron distintos aditamentos y modificaciones que poco a poco fueron aumentando el nivel de seguridad, y fundamentalmente con el aumento del conocimiento del fenómeno por la experiencia se terminó por conseguir una máquina con los niveles de seguridad requeridos.

Otro ejemplo de avance imparable de la tecnología lo tenemos en la alta tensión.

Prácticamente al mismo tiempo que la naciente industria eléctrica se enfrentaba a un problema similar con la alta tensión, otro inventor Tomas Edison, criticaba el empleo de la alta tensión por ser compleja, poco fiable, y sobre todo por atentar contra la seguridad de los usuarios. Comenzó una campaña alertando al público del peligro y defendiendo que un sistema basado en una baja tensión sería más rápidamente aceptado por los consumidores.

Como Watt, sólo tuvo un éxito pasajero.

Otro inventor, el ingeniero Elihu Thomson, que estaba de acuerdo con el peligro de la alta tensión, en lugar de oponerse a ella y hacer campaña contra su utilización, dedicó sus esfuerzos a encontrar una tecnología que controlara el riesgo, definiera diseños seguros, y así resolviera sus problemas de forma aceptable, tanto técnica y económicamente.

Watt y Edison trataron de limitar el riesgo frenando la evolución de la tecnología y por supuesto renunciando a su vez a sus ventajas y beneficios.

Cualquier responsable de una empresa sabe que la actitud de Thomson es la que tarde o temprano se impone, la diferencia está en que si por las razones que sea, en su empresa los argumentos tipo Watt (que siempre tienen algo de base y razón) son los que predominan, el tiempo pasará y serán otras empresas las que se aprovechen (a trancas y barrancas) de los beneficios de las nuevas tecnologías.

Edison argumentaba en su campaña la poca formación y conocimiento de los operarios en el manejo de la alta tensión, y Watt resaltaba la responsabilidad moral de los ingenieros al dejar predominar los intereses económicos (mayor rentabilidad) a la seguridad de las personas. Cualquier preocupación debe de ser tenida en cuenta y emplearse como punto de partida o como problema a resolver, pero nunca debe de ser la razón para "no hacer", o no avanzar. La evolución seguirá con o sin nosotros.

Si tiene suerte podrá coger el tren en marcha, pero siempre con los riesgos y esfuerzos añadidos que eso supone.

El software factor innovador y de riesgo

Esta es la era de los computadores, y de nuevo nos enfrentamos a una situación en la que la tecnología ofrece grandes ventajas haciendo cosas nuevas, o resolviendo situaciones que hasta ahora no tenían solución.

Si tratamos de aprender de la historia y comparamos los distintos casos, veremos que casi siempre el peligro no viene de la tecnología en si , sino de la forma y el como la aplicamos.

Por lo general muchos proyectos o implementaciones de soluciones innovadoras, adolecen de tener muchos y buenos expertos en la tecnología utilizada como herramienta (informática, microelectrónica, software, computadoras etc.) pero pocos o ningún experto en los procesos o fenómenos básicos que queremos mejorar o como en nuestro caso controlar y proteger.

Los conocimientos en electrotecnia no están muy de moda en este momento, y menos entre las ultimas promociones de ingenieros. Además con frecuencia las ganas de innovar de algunos se suman al ímpetu del gremio informático acostumbrado a tener que implementar cosas que rompen drásticamente con las practicas tradicionales y juntos a menudo se olvidan de un principio básico de la ingeniería:

Mantener las cosas lo más simples posibles, y aumentar su complejidad en la misma medida que aumentamos nuestro conocimiento gracias a nuestra experiencia.

Un ejemplo: Ontario Hydro ha sido la primera compañía eléctrica en Canadá en obtener recientemente una licencia de explotación de un sistema de desconexión completamente computarizado de una planta nuclear.

El programa consiste en unas 6.000 líneas de código empleando las más simples y directas técnicas de programación.

El software incluye principios de diseño aplicados y probados en sistemas electromecánicos y aceptados como "estándar" hasta ahora. Además Ontario Hydro implementó sistemas adicionales propios de verificación de seguridad, tanto por hardware como por software, haciendo posible la aplicación de técnicas de prueba formales e informales que han aumentado la confianza en la fiabilidad del sistema.

Por el contrario la primera experiencia similar, en evaluación en este momento, en Inglaterra para el reactor de Sizewell B, tiene 100.000 líneas, requiere entre 300 y 400 microprocesadores, y contiene las funciones de control y desconexión.

El sistema supera la capacidad de prueba de cualquier herramienta, por muy sofisticada que sea, y además infringe un principio básico en la industria nuclear, que es la independencia entre los sistemas de control y seguridad.

El ser humano trabaja bien cuando tiene un profundo conocimiento de lo que está haciendo, comprende el modelo y puede predecir las consecuencias y resultados de sus acciones.

Sistemas integrados

La historia de los "sistemas integrados" de protección y control, está teniendo una evolución con bastantes semejanzas a las mencionadas anteriormente.

Si analizamos el impacto de los cambios tecnológicos anteriores, en los diferentes equipos de protección y control de una subestación, veremos como en su mayoría, las funciones básicas han seguido siendo las mismas, sin que apenas hayan aparecido principios de detección de falta o prácticas de control novedosas. Esto es válido incluso para toda la evolución sufrida a partir del paso de relés directos a indirectos.

Los principios de detección de falta desarrollados con elementos electromecánicos, fueron emulados con electrónica analógica primero, y posteriormente con electrónica digital discreta sólo se afrontaron soluciones parciales a funciones de lógica de sistema, reenganche etc. siempre como elementos aislados.

Sin embargo, la tecnología digital actual ha facilitado dos cambios significativos, por un lado la concentración de funciones en un único elemento y por otro la aparición de funcionalidades nuevas, casi todas alrededor de la posibilidad que incorporan de registrar, proporcionar e intercambiar información sobre sus actuaciones y características.

La disponibilidad de este intercambio de información entre los equipos de una subestación, y la posibilidad de acceder a la misma variando sus características remotamente a través de un único canal, si fuera necesario, es lo que determina que hablemos de sistemas integrados.

El termino integrado se comenzó a aplicar en las subestaciones al control. Eran tiempos en que al irse abandonando las instalaciones se implementaban sistemas que integrando convertidores, captadores y accionadores en cada posición, concentraban toda la información y la capacidad de proceso en un puesto central que actuaba como cerebro de todo el conjunto.

Se realizaba una integración "física".

En el área de las protecciones, dadas las exigencias de rapidez y fiabilidad, siempre se ha asumido que la capacidad de proceso debe de estar cuanto más cerca de la captación y la actuación.

Sin embargo, la evolución tecnológica ha propiciado la aparición de la capacidad de comunicación, con lo que se empieza a pensar en sistemas de protecciones comunicadas, capaces de mejorar o aumentar sus prestaciones en función de la información recibida de otras, apareciendo incluso nuevas funciones de protección de un nivel superior.

El concepto de integrado se aplica desde el punto de vista " funcional".

Actualmente, podremos decir que tenemos un sistema integrado de protección, control y medida, cuando desde un nivel superior podamos acceder a todos sus elementos (su información, ajuste de parámetros, etc.) de una forma simple, con un único programa de comunicaciones y de una forma armónica, como si fueran partes de un todo, independientemente de la topología y comunicaciones de la subestación.

Además la tecnología ha facilitado que las unidades de protección dispongan, de una capacidad de proceso que posibilita el desempeño de las funciones de control local y captación de datos con lo que la configuración física ha experimentado una simplificación definitiva.

Al disponer los equipos terminales de protección y control de múltiples formas de comunicación, la información entre ellas no se pasa por cableado convencional de contactos, sino por fibra óptica, par telefónico etc., con lo que el coste de los cableados tradicionales se ha reducido espectacularmente, y si comparamos las posibles alternativas, esta claro porque se está apostando decididamente por esta solución.

Siendo realistas tendremos que mencionar que las primeras experiencias piloto no fueron lo suficientemente positivas, ya que todas las ventajas tecnológicas quedaron ensombrecidas por la sensación de perdida de control del proyecto por parte del usuario, y la inmadurez de los fabricantes al introducir excesivas modificaciones (versiones) en sus equipos, algunas veces no compatibles entre sí, sin tener en cuenta la imagen de inseguridad que quedaba en el usuario.

El Espíritu del gremio

El hecho de que se empiecen a utilizar de forma generalizada (relativamente) los equipos digitales en la subestación, no debe darnos la idea de que todos esos problemas se han resuelto, ya que aún quedan bastantes factores a resolver por ambas partes.

Existe entre los expertos de las compañías un sentimiento de que con los sistemas integrados se pierde parte del "espíritu tradicional" en los equipos de protección y control.

Los equipos de protección han sido tratados por todos, históricamente, desde el fabricante hasta el usuario de una forma específica (espíritu del gremio), y en algunas de las instalaciones actuales de sistemas de protección y control integrados parece que este se puede perder, o al menos el usuario siente que las cosas son muy distintas.

Este espíritu, como casi todos, es difícil de concretar pero podríamos identificar algunas de las cosas que están cambiando y que sin duda son los factores que generan esa sensación de inseguridad.

Tradicionalmente los equipos de protección respondían a principios de operación perfectamente comprendidos por el usuario medio.

La documentación disponible facilitaba no sólo la implementación del equipo en una instalación, sino que ayudaba a comprender sus limitaciones.

Eran equipos de vida larga, partiendo de un diseño muy estable que estaba en fabricación durante mucho tiempo y era instalado en muy diversas instalaciones durante muchos años.

Los equipos estaban diseñados para funcionar de forma razonable a lo largo de toda la vida de la instalación.

El personal de las compañías eléctricas se sentía capaz de garantizar el funcionamiento del equipo aún después del periodo de garantía del fabricante, y con poca colaboración del mismo, al dominar las prácticas de mantenimiento preventivo y correctivo necesarias.

Puede que no estemos de acuerdo en que todas estas condiciones sean necesarias también en el futuro, pero si es cierto que algunas han sido muy importantes a la hora de hablar de calidad de servicio, costes de mantenimiento, actualización de instalaciones, etc. , por lo que sería lógico que entre fabricantes y usuarios tomemos las acciones necesarias para conservar las más importantes.

Fabricante

Si analizamos la evolución de los equipos de protección y control, podemos ver fácilmente como el cambio tecnológico ha ido acompañado de una sofisticación / aumento de las funciones por equipo, y a la vez de una disminución de la información facilitada por el fabricante sobre el producto, muy especialmente en lo relativo al software.

En el pasado los fabricantes facilitaban información sobre sus equipos, los que lo hacían, confiados en que los elementos electromecánicos de que estaban compuestos, requerían grandes inversiones para su fabricación con lo que se limitaba la posible competencia a grandes empresas que al estar perfectamente identificadas no podían limitarse a copiar.

Los usuarios eran personas con conocimientos eléctricos, que asimilaban perfectamente esa información y eran capaces de determinar las ventajas y limitaciones de cada equipo, por ser tecnologías muy directamente ligadas al sistema eléctrico.

Con los electrónicos, la situación empezó a cambia , coincidiendo el aumento de recelo por parte del fabricante, al ser más fácil la copia de sus productos por cualquiera, produciéndose a su vez un distanciamiento entre la tecnología empleada y los conocimientos de los usuarios.

La introducción de equipos basados en microprocesadores o similares ha determinado un agravamiento en todos los factores, produciendo la situación que nos preocupa, que obviamente no es buena ni para el usuario ni para el fabricante.

La diferencia más importante nace de la incorporación del software al producto como algo intrínseco, pero a su vez separable y con una vida independiente.

La forma más clara de analizar el problema quizá sea distinguir entre Hardware y Software, como si fueran dos productos distintos conviviendo a la vez (formando un sistema), de forma que tienen personalidad propia e independiente de cara a revisiones, experiencia, vida etc.

Con este principio en mente, podemos empezar a analizar las prácticas actuales en todo el proceso y nos daremos cuenta que en lo que se refiere al Hard. las cosas siguen casi de acuerdo a las practicas tradicionales, pero en lo relativo al Soft. simplemente no existen., o se ha producido una ruptura total en la continuidad de las prácticas.

En los catálogos se dan características del hardware, que el usuario puede contrastar y comparar entre varios fabricantes antes de comprar, pero poco o nada sobre el software.

Algunas veces podemos ver descripciones funcionales de los distintos módulos, casi siempre más con intenciones comerciales que de divulgación técnica, también se suelen incluir descripciones de la lógica que liga el funcionamiento de todos estos módulos y que da forma al sistema, pero

rara vez, y siempre de forma limitada, se incluye una descripción comprensible de los algoritmos de medida u operación, etc.

Parece claro que el miedo a que la competencia mejore sus diseños mediante el análisis de esta información puede ser una de las razones , ya que al no existir una practica común, el que lo haga puede ponerse en una situación de inferioridad si no es seguido por el resto, y por supuesto sería difícil identificar una copia de un algoritmo si el plagiador no facilita suficiente información.

Por otra parte, tampoco existen formas acordadas de facilitar información objetiva sobre las características del soft en cuanto a sus características generales como dimensión, complejidad, estructura, lenguaje, etc., de forma que el usuario pueda hacer una valoración previa o una comparación de las características entre varios fabricantes.

Se tiende a pensar que el soft. de las protecciones es algo "especial" o apartado del mundo del soft en general, cuando en realidad los expertos de las unidades de desarrollo de los fabricantes están inmersos en la evolución general, y tratan de optimizar su trabajo con el uso de las ultimas herramientas y procesos existentes en el área de su competencia.

La industria del soft ha alcanzado tal dimensión y protagonismo en la economía mundial que por fuerza surgen métodos para la medida de su calidad y prestaciones que ayuden a usuarios y responsables de los proyectos a evaluar los "productos" fruto de dicha tecnología. Un ejemplo del estado del arte en este campo puede ser el número de septiembre de 1994 de la revista COMPUTER editada por la IEEE COMPUTER SOCIETY dedicada a este tema con el titulo de METRICS in SOFTWARE.

Usuario

Sería fácil pensar que con un "reciclado" del personal de las compañías eléctricas se solucionaría el problema, pero aunque por supuesto esto se tendrá que dar, antes de definir el perfil profesional del experto en protecciones habrá que pensar en el entorno organizativo dentro de la compañía, definiendo su sinergia con otras áreas como comunicaciones, explotación del sistema, etc.

La actitud de las compañías eléctricas es muy variable, dependiendo de su tradición y de sus planes de futuro.

En el pasado, con los equipos electromecánicos, también había compañías que se limitaban a ser meros observadores de los equipos que instalaban, dejando al fabricante o al personal subcontratado las tareas de evaluación y mantenimiento. Por supuesto, este tipo de compañías son las menos preocupadas por el tema que nos ocupa, ya que en el futuro su conducta no variará con las protecciones digitales.

Sin embargo, es en las compañías en que todas esas actividades eran desempeñadas por su personal, y particularmente por expertos profundos del tema, en las que esta actividad era tenida como labor básica no delegable, o fundamental para el control de la calidad del servicio, donde esta situación ha suscitado mas problemas, llegando incluso a reconsiderar sus estrategias de futuro, o al menos a retrasarlas hasta que sus técnicos no se sientan mas seguros, o lo que es lo mismo hasta que no dominen mejor la situación.

Si a este sentimiento añadimos las experiencias con sistemas cerrados con protocolos propietarios del fabricante , entenderemos fácilmente la situación de recelo existente.

Las compañías que han decidido salir de esta situación han comenzado a identificar cuales pueden ser los primeras acciones internas, como estandarización de instalaciones, definición de los componentes, especificación de las funciones en cada componente, definición de los protocolos de comunicaciones o en su defecto ser propietarios de los mismos, etc. (PROCOME).

Fabricante y usuario en equipo

Es cierto que en general el producto se ha convertido en una caja de sorpresas para el usuario., lo que conlleva un recelo ,e inseguridad en sus planes que le frenan a la hora de tomar decisiones de alcance. Esto origina que algunas compañías se estén planteando incluso un cambio de sus practicas, no se sabe si influenciados por sus planes de optimización de dedicarse a "lo suyo", o simplemente como la respuesta mas fácil ante la dificultad que supone reciclarse y aprender del tema (soft), y además enfrentarse con los proveedores para que les proporcionen la información y acepten los compromisos necesarios de cara al futuro.

La contribución de los fabricantes a la solución no puede ser sólo un aumento en la información facilitada , ya que en el pasado otros factores como la corta vida de los productos, generaciones no compatibles, entornos rodeados de secretismo, etc., etc., han sido en ocasiones las auténticas generadoras del problema.

Todo esto sugiere que la solución pasa por que todos los involucrados cambien de alguna forma sus formas de pensar y hacer, y es por lo que se necesitarán acuerdos entre las partes que garanticen la rentabilidad del esfuerzo.

Por una parte se podrá invertir en formación si es que el producto es "estable", y se podrá dar más información si hay confianza de que no se divulgue, o quizás las prácticas de venta deben de cambiar incluyendo en la venta parte de la propiedad del software, de forma que sea criterio del usuario seguir empleando una versión aunque el fabricante cambie de hardware.

Los fabricantes deben de ser fieles a sí mismos manteniendo siempre la compatibilidad entre los nuevos equipos y los anteriormente desarrollados e instalados, de forma que los usuarios puedan decidir incluso seguir utilizando UN SOFTWARE YA IMPLEMENTADO Y PROBADO EN UN EQUIPO existente, aunque el fabricante cambie por las razones que sea el hardware por otro más moderno.

Convendría definir y aceptar las características y criterios de calidad del software, ya empleados en otras áreas, de modo que se publiquen , se homologuen y puedan usarse para evaluación antes y después de comprar, y distinguir de alguna forma lo "bueno" de lo "malo".

Calidad

Si nos atenemos a la definición de "bueno" en lo relativo al Software. "Un programa no tiene errores en tanto en cuanto responde a los requisitos del usuario en la forma especificada". Comprendemos ahora como la especificación se convierte en fundamental, tanto en su vertiente

previa al desarrollo, como en la realimentación con la información proveniente de la instalación / uso (fig. 1).

Los primeros equipos digitales tuvieron fallos, lo cual dio argumentos a los de la teoría del "no hacer".

En una nota técnica presentada a la CIGRE un grupo japonés mostró unos datos que adjuntamos al final, basados en una experiencia de más de 11.000 relés durante 13 años.

Se puede apreciar como la tasa de fallos ha descendido en 10 veces y como si lo comparamos con otros tipos de equipos es muy favorable (fig. 4).

El análisis de los fallos encontrados es muy interesante y demuestra cómo a pesar de tener un marco definido de relaciones fabricante usuario, las especificaciones siguen siendo la base de la calidad de un producto (figs. 3 y 5).

Existen dos formas distintas de como un usuario puede conseguir un equipo, por muy complicado que sea, totalmente ajustado a sus practicas y necesidades:

a) Mediante una especificación absolutamente detallada, o en su defecto después de varias pruebas en campo (por aproximaciones) de forma que el fabricante finalmente acierte.

b) Con un equipo muy versátil que disponga de la posibilidad de ser configurado por el propio usuario.

Parece claro que desde el punto de vista del coste ninguna de las dos formas es la buena, ya que por experiencia sabemos que la primera es casi imposible y conlleva mucho tiempo, y la segunda genera productos muy complejos para algunos usuarios y más caros de lo necesario para todos. Es obvio por tanto que, cuanto más mejoremos la comunicación entre usuario y fabricante en la fase de especificación, mejor será para todos.

En los últimos tiempos, algunos usuarios han puesto sus esperanzas en las homologaciones según las normas ISO 9000, como la forma de conseguir más control sobre la calidad de lo que compran, pero por desgracia, en el estado actual de dicha normativa, todo lo relativo al software es suficientemente genérico como, en mi opinión, no garantizar absolutamente nada.

Un proceso de desarrollo, fabricación, etc., puede estar perfectamente documentado y controlado por el fabricante, pero si no se definen y acuerdan entre el comprador y el suministrador que información se intercambia (como parte del contrato de compra), quien es el propietario, o que derechos de propiedad sobre que documentación se adquieren, etc., podemos tener un marco muy bonito para una foto en blanco (fig. 2).

Si analizamos los apartados de la norma ISO 9003, teniendo en mente un equipo de protección y control integrado, seguro que se nos ocurren bastantes cosas que se podrían concretar y que serían un buen marco legal (los únicos validos a nivel comercial, o entre dos empresas) que contribuirían a despejar todos estos recelos de una forma práctica y aceptable por todos.

Cualquier fabricante de prestigio mantiene un sistema de documentación de soft que le puede permitir facilitar sin ningún problema cualquier información a su usuario.

Las homologaciones ISO 9003 debidamente concretadas pueden ser una referencia., pero cualquier conocedor de las homologaciones sabe que la solución no es muy práctica a no ser que nos pusiéramos de acuerdo en materializar / concretar dichas normas para nuestro tema concreto de los equipos de protección y control de subestaciones.

El tema sugiere incluso la creación de grupos de trabajo conjuntos entre fabricantes y usuarios, que con la presencia de expertos en normalización puedan llegar a concretar los aspectos específicos y definir así un marco de relaciones que facilite el trasvase de información.

Experiencias como el SPICE (Software Process Improvement and Capability Determination), proyecto del ISO, demuestran que en bastantes áreas se están enfocando las cosas de la misma forma.

Esta sería a nuestro juicio la forma más practica para conseguir que el futuro de los equipos de protección y control integrados continúe siendo fiel al espíritu tradicional del gremio.

Servicio

El concepto de servicio al usuario ha ido cambiando con el tiempo, y está claro que en el área de protección y control integrados se requiere una revisión de ciertas prácticas.

De la experiencia acumulada hasta ahora podríamos destacar los siguientes puntos donde el Servicio al usuario podría mejorarse.

Mejor y más completa información.

El usuario es un técnico, y como tal gusta de comprender lo que instala y de lo cual él va ha ser responsable en el futuro.

La información relativa al Software o no se da o es excesivamente básica.

Producto estable.

Los fabricantes han pecado de excesivo afán de introducción de nuevos productos, que, en ocasiones, sustituían a sus mismos equipos en unos tiempos no acordes con las practicas de las compañías. No habían terminado los técnicos de dominar un equipo, cuando el mismo fabricante anunciaba la aparición de uno mejor y no compatible.

Los productos se dejan de fabricar en tiempos muy cortos, imposibilitando que en una instalación sus ampliaciones o modificaciones sean coherentes con lo existente.

Control de versiones.

Distintos envíos de un mismo producto pueden ser totalmente distintos si se modifica la versión de software implementada.

Estas modificaciones se hacen por lo general sin consultar al usuario, se supone que se hacen porque son para bien, pero en realidad estamos instalando un producto que puede ser distinto al que hemos probado y homologado.

En el futuro cuando la compañía invierta fuertemente en sistemas de comunicación y de tratamiento de la información a distancia de los equipos, es elemental que se deberá contar con su permiso antes de que, mejorando un producto por su bien, le anulemos todo su sistema.

La definición de las prácticas en las modificaciones del software es una de las áreas donde más urgente es la definición de posibles normas o practicas.

Como ejemplo, podemos exponer la práctica seguida en nuestro caso para definir cuando se trata de una Actualización o de una Revisión de un programa.

Los tipos de cambios puede ser:

a) Corrección.- Por que no cumple con la especificación original o se ha detectado la necesidad de modificar dicha especificación.

b) Mejora en alguna función, que ya era válida, por si misma, o por encajar mejor en el sistema completo, ampliar un rango optimizar el código, etc.

c) Adición, de una función nueva, usada o no en ese modelo, un rango nuevo, rutinas de comprobación, protocolo, etc.

d) Reordenación, de todo el sistema, o de alguna función, por uniformizar modelos, etc.

Las funciones a las cuales puede afectar un cambio pueden ser :

1- Fundamentales (esenciales para la función básica)

2- Auxiliares (MMI, etc.)

3- "Background" (rutinas generales, como autotest, comunicaciones, etc.)

4- No usadas (en el modelo de que se trate)

Podemos decir que se genera una actualización de versión, es decir pasaremos por ejemplo de la 1.5 a la 1.6, en los casos a) y b) de funciones 2, 3, y 4, dejando los cambios de versión ó sea pasar de a la 2.0 a los c) y d) de todas las funciones y a los a) y b) de las Fundamentales.

En este momento el usuario solo participa, generalmente, cuando la modificación ha añadido alguna función y el fabricante pretende cobrar algo adicional.

Lógicamente debería de ser la opinión del usuario la que definiera el carácter de la función y la importancia del cambio.

Sin información detallada eso es imposible.

El contrato de compra se supone que es privado entre las partes, con lo que la confidencialidad de la información facilitada debería estar garantizada, las compras dentro de los ámbitos de calidad concertada y de homologaciones ISO 9000 deberían ser el marco adecuado.

Conclusiones

La evolución tecnológica seguirá adelante.

De nosotros depende que dicha evolución sea "controlada " y coherente con todas las practicas tradicionales.

La colaboración entre fabricantes y usuarios es la única forma práctica de que ese control se haga de forma eficaz .

En el estado actual de la normativa internacional tenemos la oportunidad de liderar ese proceso, con la ventaja que supone para nuestras compañías y para nuestra sociedad.

Figuras

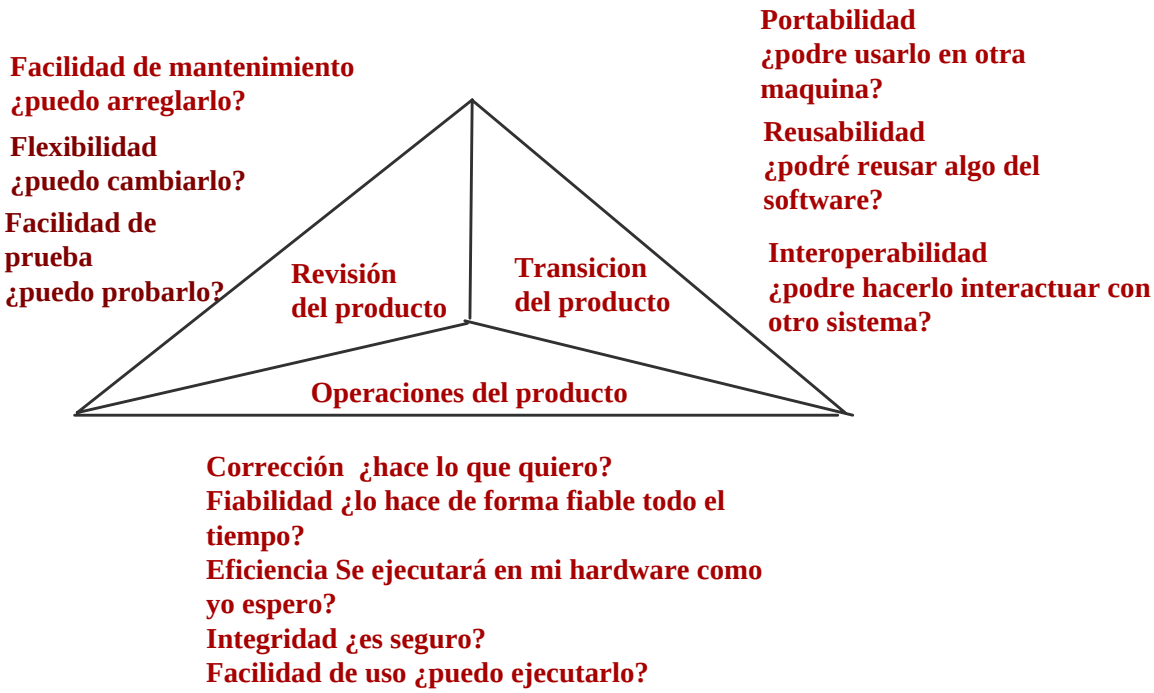


fig. 1 **Factores que determinan la calidad del Software**

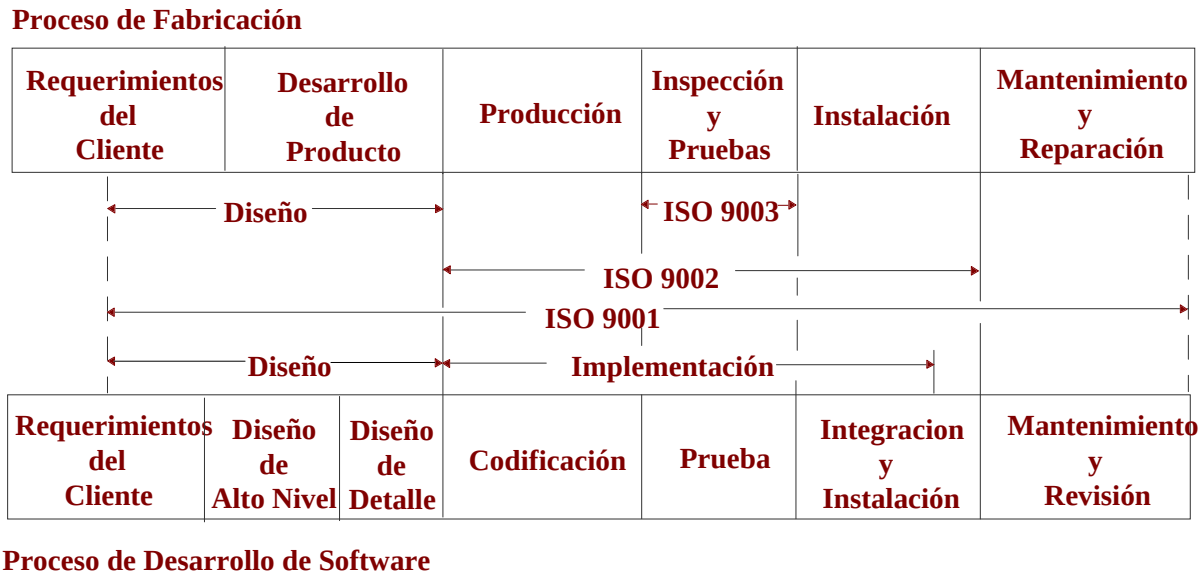


fig. 2 **Relación entre las normas ISO 9000 y los Procesos**

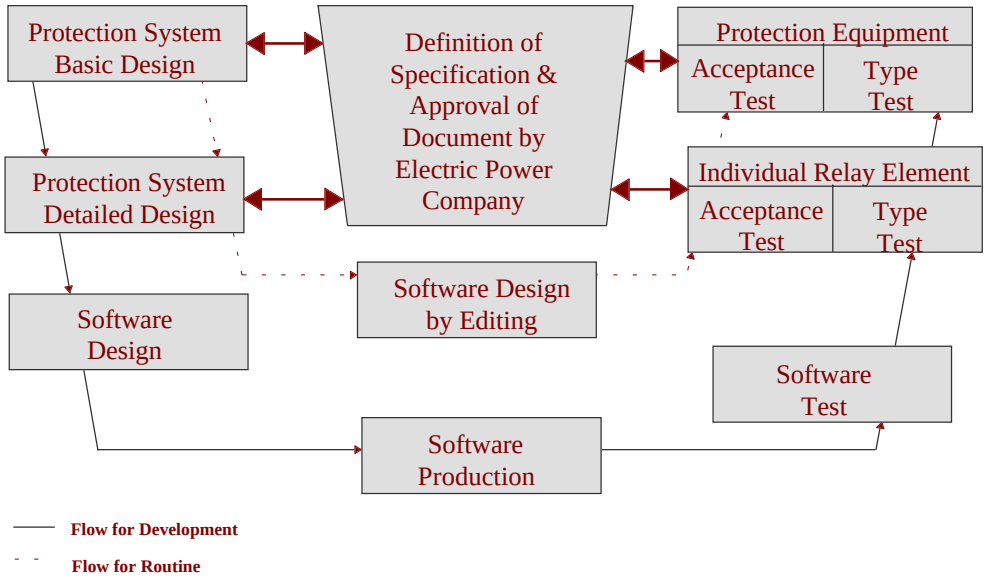


fig. 3 **Flow Chart or Relatinship Manufacturing-Electric Power Companies for Digital Protection**
Power Systems Dept.,Wadasaki-cho, Hyogo-ku, Kobe 652, JAPAN (1995 SC 34 Stockholm)

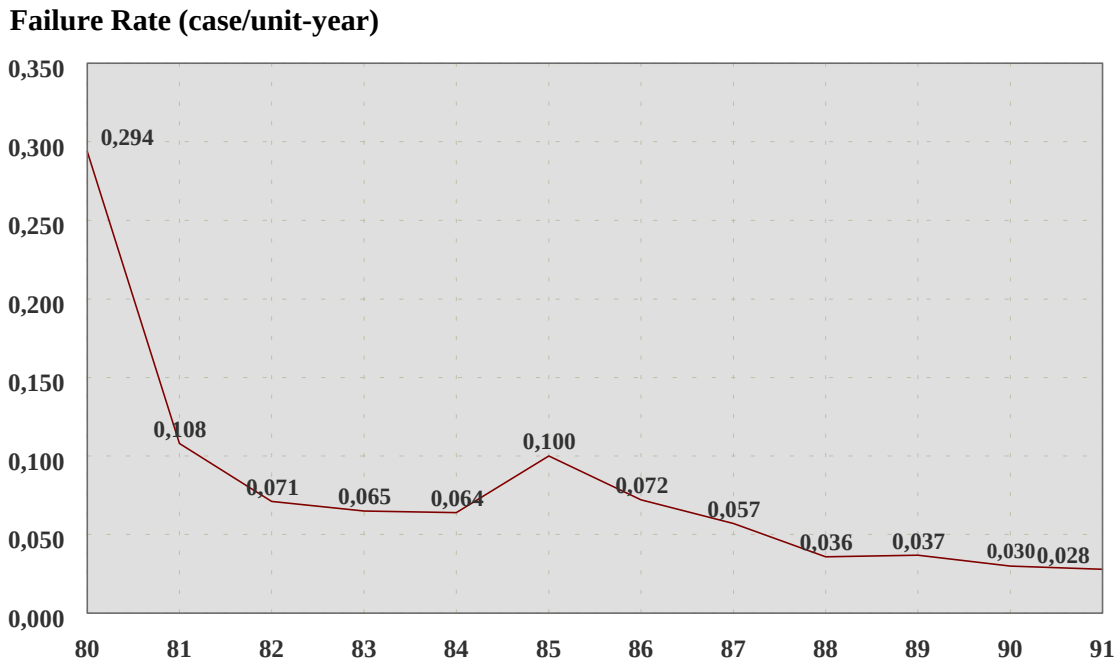
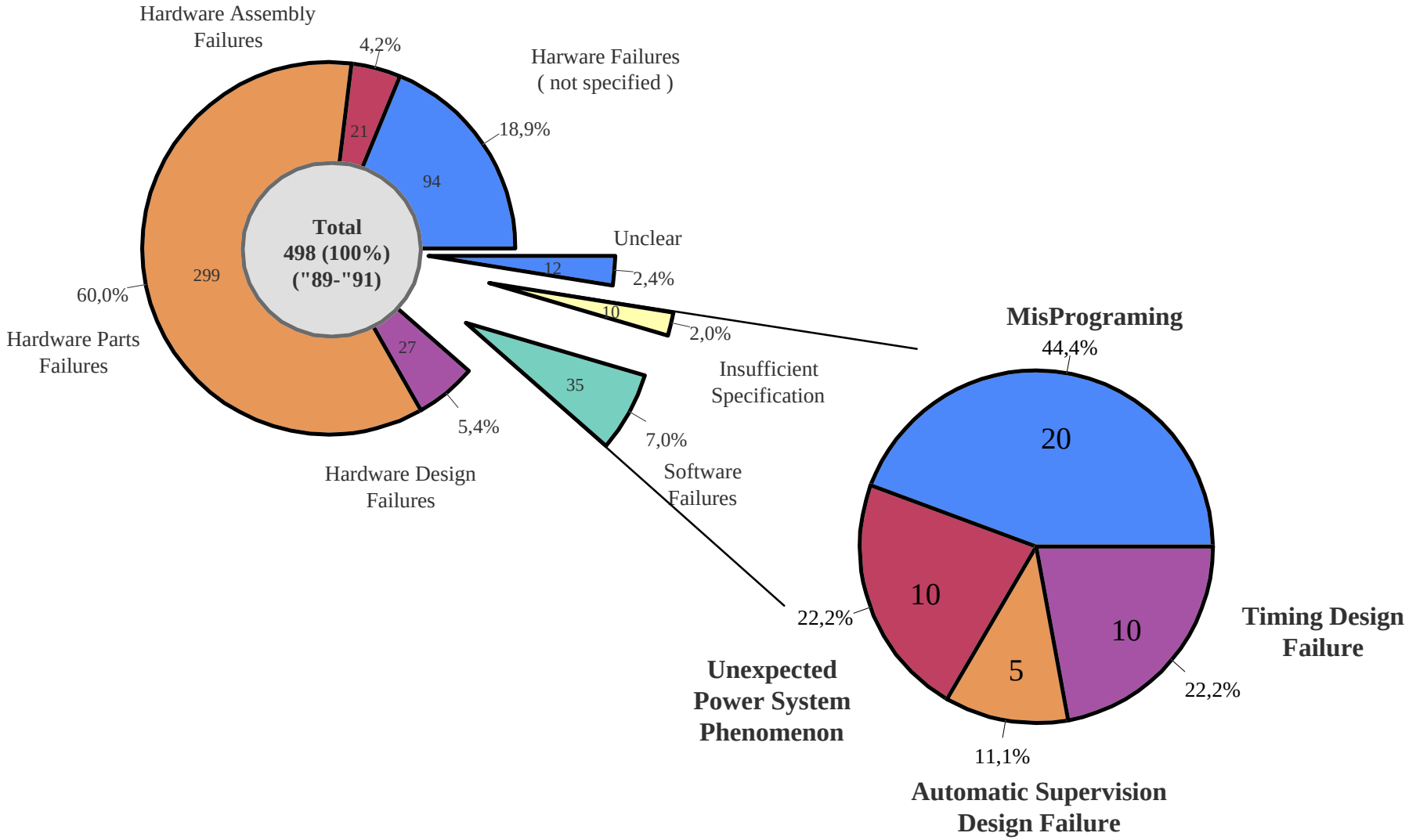


fig. 4 **Change of Failure Rate Of Digital Protection Equipment**



Análisis de las causas de fallo de 498 averias en equipos de protección durante el periodo 89-91.
Sobre un total de aproximadamente 9.000 unidades digitales.
Power System Dept., Wadasaki-cho, Hyogo-ku, kobe 652 JAPAN (1995 SC 34 Stockholm)

fig. 5