
# TELEDISPAROS Ó ESQUEMAS SUPLEMENTARIOS DE PROTECCIÓN DEL SISTEMA ELÉCTRICO (ESPS): PROPUESTA DE ESTUDIOS ADICIONALES

**ALBERTO RODRIGUEZ HERNANDEZ**

**CONSULTOR**

**Bogotá, diciembre de 2010**

# INDICE

## 1. INTRODUCCIÓN

El propósito de este documento es revisar la situación de los servicios de teledisparos ó esquemas suplementarios de protección en el sistema de potencia (ESPS), tanto para Colombia como para algunos otros países, como referencia para proponer estudios adicionales y reformas regulatorias, de encontrarlas necesarias.

Se analiza también la posibilidad de esquemas más seguros y extendidos de defensa del sistema contra situaciones de contingencia, incluyendo los apagones, con base en la interacción del sistema eléctrico con redes de información y comunicaciones, para constituir redes inteligentes.

Este análisis se lleva a cabo en cumplimiento de la agenda regulatoria de la CREG para 2010, la cual, en su punto 1.1.8, servicios complementarios, incluye el tema de la problemática de los servicios de arranque autónomo y teledisparos.

## 2. ¿SON LOS ESPS UN SERVICIO COMPLEMENTARIO?

Muy pocos autores consideran los teledisparos como un servicio complementario.

Entre ellos, Gjerde [1] analiza el estado del arte en el Mercado Nórdico y define que los servicios complementarios (SC) son aquellos necesarios para el transporte de la electricidad desde el productor hasta el consumidor y que a menudo sólo hay un comprador: el operador del sistema.

Su clasificación de los SC es como sigue:

a) Servicios de interconexión

   1. Servicios de respuesta de frecuencia
   2. Esquemas especiales de protección (SPS ó ESPS), para incrementar la capacidad de transferencia sin nuevas líneas

b) Servicio de balance entre generación y demanda

1. Respuesta de regulación ante el desbalance entre recursos y obligaciones
2. Seguimiento de carga, para responder a una señal de demanda programada
3. Reserva para contingencias o capacidad de respuesta ante eventos inesperados

c) Servicios locales

1. Servicios de reactivos para controlar y soportar el transporte de potencia activa por los sistemas troncales de transmisión
2. Black start o capacidad de arrancar de manera autónoma sin recurrir a fuentes externas

Este autor relaciona las siguientes formas de administración de los SC:

1) Comprarlos bajo principios de mercado (precio marginal o subastas)
2) Una combinación de métodos de mercado y una compensación fija. Una variante es un pago fijo más una compensación adicional cuando opera el SC.
3) Servicios obligatorios sin remuneración, cuando el suministro del servicio se fundamenta en el código de redes

## 3. ESPS: ESTADO DEL ARTE

XM [2] define los ESPS ***y*** hace un resumen del estado del arte**.**

Un ESPS es un conjunto de elementos de protección y control para detectar condiciones anormales de operación en el sistema y actuar con el fin de minimizar la extensión del evento y minimizar el colapso de la demanda atendida.

Su función principal es mitigar eventos que no son cubiertos mediante generación de seguridad o expansión del sistema, pues son de baja probabilidad de ocurrencia y no hay posibilidad de protegerse ante ellos o la protección es muy costosa.

Los ESPS usan elementos diferentes a los de las protecciones del sistema para no interferir con ellas ó porque estas no pueden actuar por los valores que toman las variables de operación durante el evento.

Un ESPS permite la detección de las variables de cada evento específico, determinando su severidad y actuando para mitigar su impacto sobre la atención de la demanda.

Las variables detectadas son voltajes en los nodos, corrientes y flujos por líneas y transformadores, cambios en la frecuencia, etc.

Los ESPS requieren comunicaciones entre diferentes instalaciones y diferentes agentes pueden ser propietarios de equipos que hacen parte de un mismo ESPS.

Por lo anterior, considera XM que se deben definir responsabilidades en el diseño, implementación, administración, operación y mantenimiento de los ESPS.

Los ESPS pueden actuar sobre la demanda, sobre la generación, sobre otros elementos de la red o sobre una combinación de los anteriores.

McCalley y otros [3] dicen que los SPS (Special Protection Systems), también llamados RAS (Remedial Action Schemes), se diseñan para determinar condiciones anormales del sistema, relacionadas con contingencias, y para iniciar acciones correctivas previamente planeadas, con el fin de mitigar las consecuencias de la condición anormal y dar un desempeño aceptable del sistema.

El SPS generalmente se refiere a controladores que tienen una o varias de las siguientes características:

- Se pueden armar o desarmar dependiendo de las condiciones del sistema
- Están normalmente "dormidos"; los eventos que los inicializan ocurren menos de una vez por año
- Usan leyes de control discretas
- En la mayoría de los casos, la acción de control está predeterminada
- Al menos una forma de comunicación hace parte de la acción de control

Los SPS dan acciones correctivas rápidas y pueden usarse para incrementar la capacidad de transferencia de la red. Se consideran una alternativa atractiva frente a construir nuevas facilidades de transmisión porque se puede poner en servicio relativamente rápido y a bajo costo.

Sin embargo, afirman que una dependencia excesiva de los SPS puede resultar en riesgos para la seguridad del sistema, que incluyen fallas para operar cuando se requieren, interacciones no planeadas con otros SPS y operaciones no previstas.

Las acciones de los SPS [4] pueden llevar a reducir cargas, cambiar generación o reconfigurar el sistema para mantener voltajes aceptables, el sistema estable y las cargas atendidas.

En [5] se ilustra el estado del arte en SPS en líneas largas, como la interconexión entre Canadá y California. Esta interconexión de la Costa Pacífica tiene controles de estabilidad que evitan costosos refuerzos de interconexión y fallas en cascada.

En [6] se propone una tecnología de sensores inalámbricos para evaluar la integridad mecánica de las líneas de transmisión, que es de utilidad en sistemas sometidos a sabotajes, como en el caso de la red en Colombia. Esta propuesta es complementada en [7] con una técnica para determinar el estado físico de una línea usando el concepto de estimación de estado mecánico.

Los SPS requieren una utilización cautelosa pues, a medida que continúan proliferando, parece que su confiabilidad será más difícil de asegurar [8]. Dado que los SPS sólo se arman normalmente bajo condiciones de estrés, si fallan hay severas consecuencias y el riesgo puede ser significativo.

Según su respuesta a un evento, la operación de los SPS se puede clasificar en una de las siguientes categorías [8]:

1) Operación deseable
2) Operación no deseable
3) No operación

Se dice que la operación del SPS es deseable si su resultado es menos severo que en el caso de que el SPS no hubiera operado. De lo contrario, se dice que es indeseable. Por ejemplo, cuando se dispara el SPS sin que haya ocurrido una falla en la red.

Si el SPS no opera ante un evento para el cual estaba diseñado, pudo haber ocurrido uno de los siguientes problemas:

1) Falla en el hardware
2) Error en el diseño lógico
3) Falla en el software
4) Error humano

Si el SPS opera correctamente puede mejorar significativamente la respuesta del sistema ante una contingencia. Sin embargo, si falla puede llevar a consecuencias muy graves y costosas.

Fuera del inconveniente de que no actúen cuando se requieren, los SPS también contribuyen al riesgo por operaciones no intencionales o interacciones con otros SPS, como ya se había dicho. En [3] se reportan 24 operaciones de SPS, 16 de las cuales fueron exitosas, mientras que en las 8 restantes hubo alguna falla. Las razones incluyen errores en el diseño lógico, fallas en el software ó en el hardware, calibración incorrecta, fallas en el armado y fallas en las comunicaciones ó en la telemetría.

Las consecuencias de estos problemas fueron bastante graves, como la pérdida de bloques de generación de hasta 1900 MW, la pérdida de carga de hasta 3950 MW y grandes apagones.

A los anteriores se agrega uno más reportado en [19] debido a la falla en el diseño de un SPS (apertura de un circuito en un nivel de corriente inferior al programado, posiblemente a causa de un desbalance de carga), causando caída en los voltajes y sobrecargas.

En [20] se cita un análisis del CIGRE para 93 esquemas de SPS en 18 empresas localizadas en diferentes países. Las operaciones reportadas para todos los esquemas en un período de siete años se resumen así.

Operaciones exitosas = 1093
Número de fallas = 36
Operaciones no exitosas = 20
Operaciones innecesarias = 306.

Las operaciones no exitosas ó innecesarias y las fallas que impiden que operen los SPS condujeron a importantes rechazos de generación ó de carga y a colapsos totales ó parciales.

## 4. De ESPS a SPID: ESTADO DEL ARTE

Un SPS es efectivo para escenarios específicos predeterminados pero no puede manejar situaciones inesperadas [9]. Se necesita un sistema más general de defensa, como SPID (Strategic Power Infrastructure Defense).

La función principal de SPID es prevenir apagones usando capacidades de reconfiguración adaptativa y autocuración (self-healing), que son características de las redes inteligentes. Un esquema de autocuración separa la red en islas, en las que se minimiza el problema de balance generación-carga.

Los orígenes de SPID están en que, a raíz de los atentados del 11 de septiembre de 2001, la Secretaría de Defensa de los Estados Unidos ha patrocinado estudios y proyectos para cuidar la seguridad de infraestructuras críticas como la eléctrica.

Un mecanismo de defensa básico es el deslastre de carga, pero hay otros más sofisticados, como los sistema de control de área amplia, con protección en tiempo real, con detección completa y capacidades en información y comunicaciones [10]. Uno de ellos es SPID, que hace análisis de fallas, evaluación de la vulnerabilidad y autocuración.

En la referencia [11] se describe una técnica para analizar la vulnerabilidad y proveer acciones de autocuración, basada en un sistema multiagente que utiliza tres capas: 1. Reactiva 2. De coordinación 3. Deliberativa. La reactiva controla subsistemas o

componentes locales. En la deliberativa se analiza o controla la red con un enfoque sistémico. Las dos pueden ser incoherentes, por lo que la capa de coordinación examina lo consistencia de las decisiones con el estado actual del sistema.

En la capa deliberativa se hace una estimación periódica de la vulnerabilidad y un grupo de agentes de reconfiguración da los controles preventivos y correctivos.

El propósito principal del sistema SPID es prevenir fallas catastróficas que puedan llevar a salidas de gran escala [12].

El sistema SPID tiene una aproximación probabilística, que incluye el concepto del riesgo y el concepto de protección adaptativa. El esquema tiene cuatro componentes: identificación del evento, cálculo del riesgo, análisis rápido de la red y análisis de decisiones.

Las estrategias de autocuración son opciones de control para llevar el sistema de potencia a una condición de operación más segura y menos vulnerable. Pueden ser preventivas o correctivas.

En [13] se propone un esquema basado en árboles de decisión y atributos críticos que permite identificar indicadores de seguridad y formular predicciones muy precisas sobre seguridad dinámica en tiempo real (Dynamic Security Assesment -DSA).

El DSA [14] se refiere al análisis requerido para determinar si el sistema de potencia puede cumplir criterios específicos de confiabilidad y seguridad, tanto en estado estable como transiente, para todas las contingencias posibles. En el nuevo ambiente competitivo, se requiere DSA en línea. Esta aproximación es un mecanismo tipo radar, que examina continuamente el sistema para detectar problemas potenciales de una contingencia N-1 o N-x.

En la Figura 1 del Anexo 1 se muestran los componentes de un sistema DSA online [14].

El DSA depende de métodos computacionales determinísticos complejos y que requieren tiempo (ciclos de 5 minutos en la red de China). Se puede unir a un sistema inteligente IS, que tiene el conocimiento acumulado de cálculos previos almacenados en una base de datos.

En la Figura 2 del Anexo 1 [14] se muestra que el Sistema Inteligente IS puede interactuar con el DSA y con el EMS (Energy Management System) para determinar acciones de control. De esta manera, el DSA online se convertirá en una herramienta importante contra los apagones del sistema.

Se propone en [15] que SPID tenga una red totalmente en fibra óptica basada en IP (Internet Protocol) sobre WDM (Multichannel Wavelength Division Mutiplexed Connection). Cada longitud de onda puede considerarse como una conexión dedicada.

En [16] se revisan estrategias para prevenir fallas en cascada y se introducen tecnologías para evitar apagones. Se advierte que, para prevenir apagones, se requieren centros de control más abiertos, estandarizados y flexibles (Grid Based Control Centers Architectures).

Adamiak y otros [17] analizan los sistemas de comunicaciones para los esquemas SPS, RAS y SPID. Se espera que, con los nuevos sistemas de medición de área amplia y las mediciones fasoriales sincronizadas, estos esquemas serán aún más efectivos.

Los sistemas de potencia modernos están haciendo un mayor uso de sensores, de sistemas de comunicación de alta velocidad y de redes distribuidas de computadores. Las estrechas interacciones entre redes de potencia, computadores y sistemas de comunicación conducen al concepto de una superinfraestructura.

Muchas empresas usan SONET (Syncronous Optical Network) con portadoras ópticas (OC), que transmite datos a tasas de Mbit y Gbit por segundo. SONET tiene comunicaciones redundantes mediante una configuración bidireccional en anillo. Si hay fallas, el sistema se restaura en 4 milisegundos.

La configuración se basa en IEDs (Intelligent Electronic Devices) conectados a SLAN (Substation Local Area Network) y las subestaciones se comunican con la WAN (Wide Area Network).

Este es el esquema de las redes inteligentes, que utiliza también PMUs (phasor measurement units), con altísima redundancia en la información recolectada, para hacer el sistema más confiable.

Finalmente, se hace énfasis en que la clave para la seguridad es la integración de la infraestructura con los sistemas de información y comunicaciones.

Aumentar la capacidad de transmisión no aumenta de manera inherente la seguridad ni reduce la probabilidad de apagones [18], porque la seguridad depende más bien de las reglas que gobiernan la operación.

Estos autores aseguran que tampoco ha cambiado la seguridad de los sistemas con la desregulación y en cambio sí ha aumentado la probabilidad de los apagones. Afirman que reglas como el criterio N-1 puede que no sean adecuadas y debieran reemplazarse por criterios probabilísticos que reflejen mejor el riesgo de un apagón.

## 5. SITUACIÓN EN COLOMBIA

En Colombia el Código de Redes clasifica como servicios complementarios los de control de frecuencia, los de control de voltaje y el arranque autónomo. En la Agenda Regulatoria 2010, la CREG menciona también los teledisparos como servicio complementario.

Con los apagones, en particular el del 26 de abril de 2007, se han incrementado las preocupaciones por la seguridad y la confiabilidad del sistema interconectado.

A continuación se examina el marco regulatorio para los teledisparos, y se registran las propuestas de XM para reformarlo.

XM informa que hay 20 esquemas ESPS habilitados en Colombia [2]: 7 actúan sobre la demanda, 8 sobre la generación y 5 sobre la red. No hay estadísticas o reportes sobre la operación de los denominados teledisparos. Según comentarios de XM, estos esquemas casi nunca operan y en general no presentan problemas, pero sí ha habido situaciones de operaciones erróneas ó de activación sin que se produzca el evento ante el cual debieran actuar.

Como ya se mencionó, XM cuestiona que no están definidas las responsabilidades de los agentes involucrados en estos esquemas. Ellos surgen en general por la iniciativa del operador, que busca un acuerdo con el ó los agentes sobre el diseño e instalación. A veces se implanta la solución y en ocasiones no. No están definidas las responsabilidades, en especial en casos de falla del esquema. Un problema subyacente es que XM solo actúa como coordinador de la operación y en estos casos no tiene atribuciones para que se adopte un esquema ó para asignar funciones ó responsabilidades. Este es un inconveniente adicional asociado a los teledisparos.

Por otra parte, XM en [2] hace el siguiente resumen sobre la reglamentación vigente:

En Colombia, desde el punto de vista legal, puede resaltarse lo establecido en el Artículo 12 de la Ley 143 de 1994:

"Artículo 12.- La planeación de la expansión del sistema interconectado nacional se realizará a corto y largo plazo, de tal manera que los planes para atender la demanda sean lo suficientemente flexibles para que se adapten a los cambios que determinen las condiciones técnicas, económicas, financieras y ambientales; que cumplan con los requerimientos de calidad, confiabilidad y seguridad determinados por el Ministerio de Minas y Energía; que

los proyectos propuestos sean técnica, ambiental y económicamente viables y que la demanda sea satisfecha atendiendo a criterios de uso eficiente de los recursos energéticos."

La regulación de la Comisión de Regulación de Energía y Gas – CREG – establece en el Código de Operación, los criterios técnicos para asegurar la confiabilidad y seguridad en la atención de la demanda, dentro de los cuales se determina la existencia del Esquema de Desconexión Automática, estableciendo además que: "En donde el esquema de desconexión nacional sea insuficiente, por ejemplo en áreas radiales o que a pesar de ser enmalladas se prevé su aislamiento del SIN, las empresas que estén localizadas en estas áreas deberán instalar esquemas suplementarios que permitan conservar parte de su carga y generación en condiciones de aislamiento. Estos esquemas suplementarios serán analizados entre el CND, los CRD´s y las empresas involucradas y aprobados por el CNO."

Así mismo, el Código de Conexión en su Anexo 4, Numeral 3.2, establece los requisitos técnicos de protecciones y define el requerimiento de relés de frecuencia en "puntos estratégicos de la red donde sea necesario implementar deslastres de carga para preservar la estabilidad del sistema", los cuales son solicitados por el CND a los transportadores.

De otra parte, la Resolución CREG 062 de 2000 establece los criterios de confiabilidad para la atención de la demanda, definiendo explícitamente la utilización del criterio del Valor Esperado de Racionamiento de Potencia de Corto Plazo en el despacho programado.

El Consejo Nacional de Operación, por su parte, aprobó, mediante Acuerdo número 330 la implementación de un Esquema Suplementario de Baja Frecuencia en la Costa Atlántica (Área Caribe), para permitir aumentar el límite de transferencia hacia esta área ante condiciones de emergencia o déficit de generación y con la indisponibilidad de un circuito a 500 kV.

Finalmente, el Ministerio de Minas y Energía emitió la Resolución MME 18 2148/07, por la cual se definen los criterios de seguridad y confiabilidad para los Sistemas de Transmisión Regional – STRs, la cual en su artículo primero establece que: "…la Comisión de Regulación de Energía y Gas – CREG deberá incorporar dentro de los criterios de remuneración las inversiones eficientes asociadas con las medidas necesarias para evitar que el Sistema de Transmisión Nacional – STN se afecte como resultado de una contingencia sencilla en líneas de los Sistemas de Transmisión Regionales – STR´s o en transformadores de conexión al STN." Esta recomendación es acogida en la Resolución CREG 097 de 2008.

Respecto a ESPS, se hacen las siguientes recomendaciones por parte de XM [2]:

Se recomienda a la CREG reglamentar la confiabilidad mínima requerida en la operación de los STR, de manera que se pueda determinar cuando se considera la actuación de los ESPS o cuando se programa generación de seguridad al cubrirse frente a alguno de los eventos para los cuales los ESPS han sido diseñados. En particular, los eventos sobre la transformación de conexión pueden ser objeto del análisis planteado.

Se recomienda realizar seguimiento periódico a la actuación de los esquemas y ejecución periódica de pruebas a fin de garantizar su operatividad y eficiencia.

Se recomienda a la CREG reglamentar la manera de remunerar el servicio de ESPS a los agentes que los representen. Como sugerencia se presenta el modelo argentino, en el cual se calculan los valores asociados a la implementación y gastos de AOM asociados a los ESPS y se reciben como ingresos mensuales (incluyen telecomunicaciones, mantenimientos preventivos, administración, reposición, etc.)

Se sugiere que la responsabilidad por el diseño y operación de los ESPS sea similar a la entregada a los agentes por la coordinación y operación de las protecciones de los elementos del sistema de potencia.

Se recomienda a la CREG reglamentar los niveles mínimos de confiabilidad en el largo plazo esperado para los STR y conexión, y ante fallas de baja probabilidad (diferentes a N-1) en el STN. De esta forma se obtendrán los criterios mínimos que se deben cumplir para evaluar alternativas de expansión.

## 6. ANÁLISIS DE LAS PROPUESTAS DE XM

Se resumen así las propuestas:

En cuanto a identificación y diseño, propone XM que la implementación de los ESPS sea recomendada por los OR ó por el CND para mantener los índices de confiabilidad de atención de la demanda. Los criterios de diseño deben ser iguales a los de las protecciones: seguridad y confiabilidad. Los ESPS deben contar con duplicidad de elementos, deben revisarse ante cualquier cambio, deben estar documentados en una base de datos en el CND y deben ser aprobados por el C.N.O.

En lo que se refiere a su implementación y operación, deben estar a cargo de los agentes propietarios de los elementos donde se hace la detección y/o la actuación del esquema. Debe haber coordinación en los casos de multipropiedad. Las pruebas se coordinan con el CND y deben realizarse periódicamente. La CREG debe recomendar la confiabilidad mínima en el STR para comparar con las opciones de generación de seguridad y expansión.

Recomienda XM remunerar el servicio de ESPS y que la responsabilidad por los ESPS sea similar a la entregada a los agentes por la coordinación y operación de las protecciones.

Ante estos planteamientos, se debe tener en cuenta que los ESPS entrañan riesgos en su funcionamiento y pueden convertirse más en un problema que en soluciones. Es preferible optar por recomendaciones de expansión y por soluciones más robustas e integrales para la defensa de la integridad del sistema.

En todo caso, las propuestas de ESPS deben pasar por la revisión de la UPME, que las sopese frente a sus planes de expansión y a las soluciones alternativas, con base en evaluaciones económicas y criterios de confiabilidad y costo.

Si finalmente una solución ESPS es temporalmente la mejor alternativa, su diseño e implementación deben sujetarse a las aprobaciones del CND y del C.N.O. y se pueden aplicar las recomendaciones de XM para las pruebas y la operación.

Por otra parte, retomando todo lo expuesto en los Capítulos 4 y 5, antes que a soluciones ESPS es recomendable dirigir los esfuerzos hacia el desarrollo de esquemas SPID, que son más integrales y consistentes, conduciendo a un sistema que puede prevenir y evitar situaciones de colapso, bajo el concepto de redes inteligentes. XM ha informado recientemente que está iniciando un proyecto denominado SIRENA (sistema de respaldo nacional ante eventos), que parece similar a un desarrollo SPID. XM considera que cuando el proyecto haya sido implementado hará innecesarios los teledisparos.

Ante la inquietud de que las propuestas de XM no son necesariamente acogidas por los agentes, se puede decir que en este caso una solución SPID, como la que se recomienda estudiar, se extendería a todo el sistema interconectado, pues es un esquema global tendiente a un sistema de información común, que sería aplicado en toda la red, de manera similar a como se implantó hace tres décadas la supervisión del sistema mediante el estimador de estado.

## 7. CONCLUSIONES y PASOS SIGUIENTES

Pocos autores consideran los teledisparos ó ESPS como servicios complementarios.

Se debe tener cuidado con el uso de los ESPS pues está sujeto a importantes riesgos.

Conviene considerar más bien la utilización de esquemas SPID tendientes a las redes inteligentes para prevenir colapsos en el sistema y mitigar el impacto de pérdidas importantes de generación ó demanda.

En muchos países se plantean soluciones basadas en técnicas modernas respecto al manejo de los sistemas de potencia, las mediciones, las comunicaciones y el control, con el uso de IEDs, PMUs, subestaciones automatizadas, información altamente redundante y centros de control descentralizados, todo lo cual conduce a redes inteligentes con capacidad de auto-

curación y de formación de islas, para protegerse de disturbios y evitar los apagones, mediante la detección temprana y las acciones correctivas.

Se recomienda adelantar estudios sobre la introducción de redes inteligentes en el sistema eléctrico colombiano, para determinar su oportunidad, definir las metas a cumplir y el plan de acción para alcanzarlas.

En el Anexo 2 se presenta un esquema simplificado de bases para los Términos de Referencia correspondientes.

Se recomienda tener en consideración el proyecto SIRENA que se propone adelantar XM, para unificar todos los esfuerzos.

## 8. BIBLIOGRAFÍA

[1] Ole Gjerde. State of the art in the Nordic Market. IEEE 2007.

[2] XM. Análisis y propuestas sobre esquemas suplementarios de protección y control del sistema de potencia (ESPS). Gerencia CND, mayo 2008.

[3] McCalley, J.D. and W. Fu. Reliability of special protection systems. Department of Electrical and Computer Engineering. Iowa State University. IEEE Transactions on Power Systems. Vol. 14, No. 4, November 1999, pp. 1400-1407.

[4] NERC Reliability Standards PRC- 012 through 017.

[5] C.W. Taylor. State of the art in SPS to prevent widespread blackouts: BPA and WSCC experience, 1999.

[6] Ramón A. León, Vijay Vittal, and G. Manimaran. Application of sensor network for secure electric energy infrastructure. IEEE Transactions on Power Delivery, Vol. 22, No. 2, April 2007, pp. 1021-1028.

[7] Poorani Ramachandran, Vijay Vittal, and Gerald T Heydt. Mechanical state estimation for overhead transmission lines with level spans. IEEE Transactions on Power Systems, Vol. 23, No. 3, August 2008, pp. 908-915.

[8] Fu, W. et.al. Risk assessment for special protection systems. IEEE Transactions on Power Systems, Vol. 17, No. 1, February 2002, pp. 63-72.

[9] Lim, S. et.al. Blocking of zone 3 relays to prevent cascaded events. IEEE Transactions on Power Systems, Vol. 23, No. 2, May 2008, pp. 747-754.

[10] Hao Li, et.al. Strategic Power Infrastructure Defense. Proceedings of the IEEE, Vol. 93, No. 5, May 2005, pp. 918-933.

[11] Chen-Ching Liu. APT Center. Department of Electrical Engineering. University of Washington. Strategic Power Infrastructure Defense (SPID): a wide area protection and control system. IEEE, 2002, pp. 500-502.

[12] Chen-Ching Liu, et.al. The Strategic Power Infrastructure Defense (SPID) System. A conceptual design. IEEE Control Systems Magazine. August 2000, pp. 40-52.

[13] Sun, et.al. An online dynamic security assessment scheme using phasor measurements and decision trees. IEEE Transactions on Power Systems, Vol. 22, No. 4, November 2007, pp. 1935-1943.

[14] Kip Morison, Lei Wang y Prasha Kandur. Power System Security Assessment. IEEE Power & Energy Magazine. September/October2004, pp. 30-39.

[15] Bin Qin et.al. Communication infrastructure design for strategic power infrastructure defense (SPID) system. IEEE 2002, pp. 672-677.

[16] Hou, Y. et.al. Blackout prevention: managing complexity with technology in China.

[17] Adamiak, M.G. et.al. Wide area protection technology and infrastructure. IEEE Transactions on Power Delivery. Vol. 21, No. 2, April 2006, pp. 601-609.

[18] Kirschen D. and Strbac, G. Why investments do not prevent blackouts. UMIST, Manchester, UK, 27 August 2003.

[19] NERC System Disturbance Reports 1986-1998

[20] Anderson P. M. and B.K. LeReverend. Industry Experience with Special Protection Schemes. IEEE Transactions on Power Systems, Vol. 11, No. 3, August 1996

# ANEXO 1

Figura 1

Componentes de un sistema DSA (Dynamic Security Assessment) en tiempo real [14]

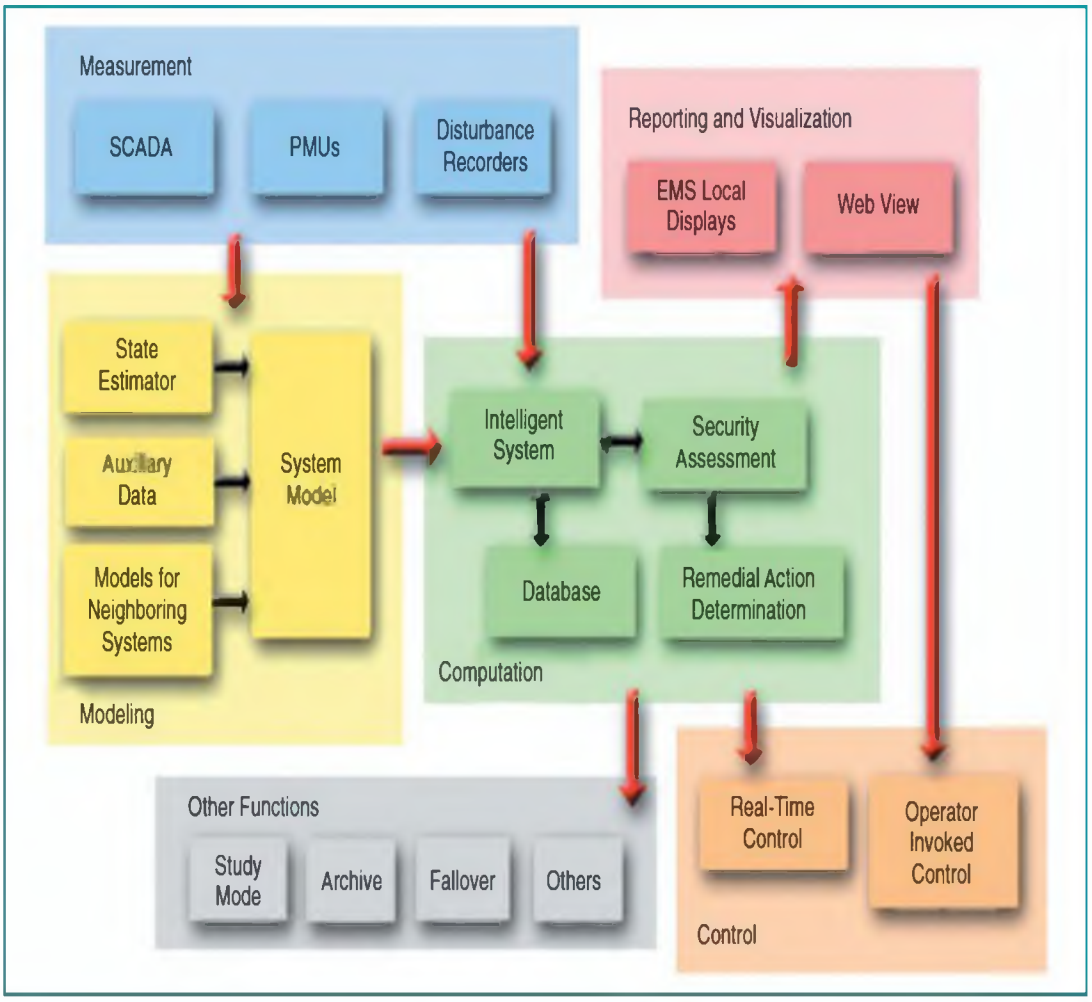
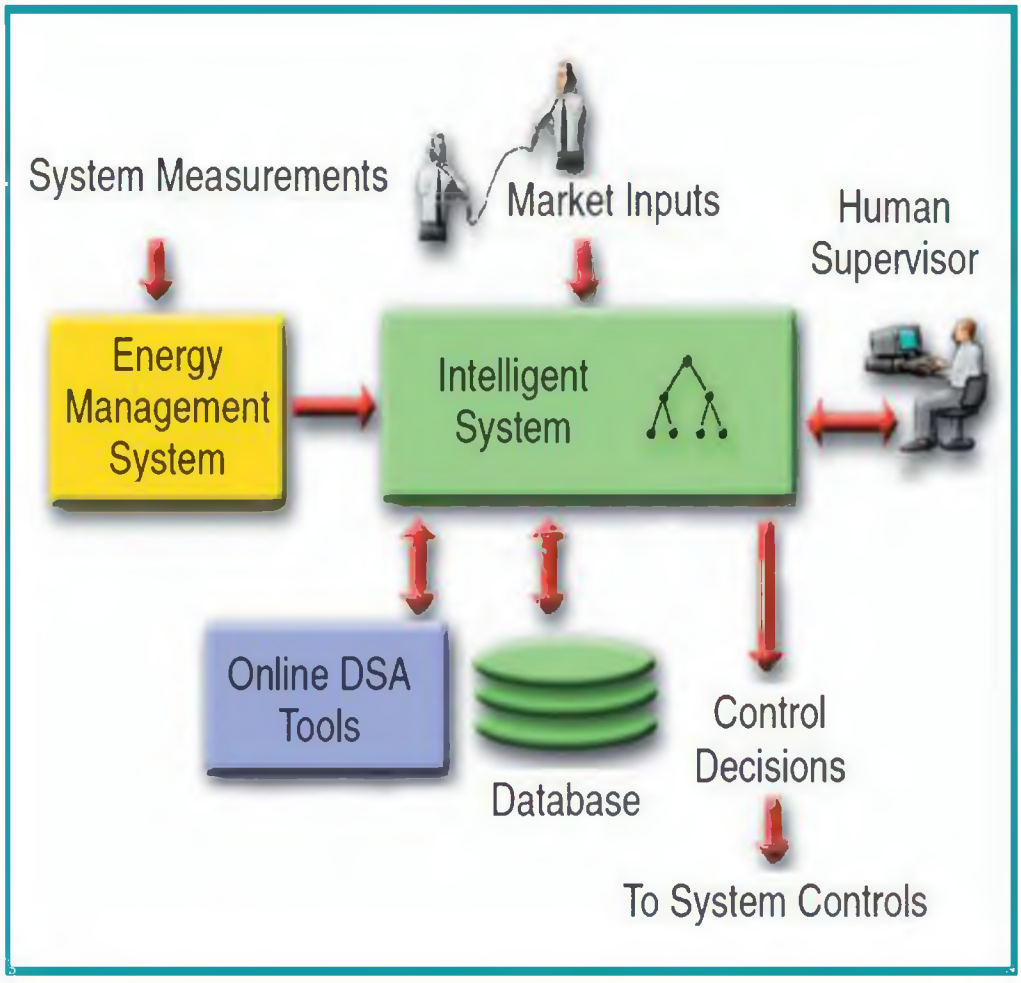


Figura 2

Estructura de un sistema DSA usando tecnologías inteligentes [14]



# ANEXO 2

## BASES DE TÉRMINOS DE REFERENCIA

## CONTRATACIÓN DE UNA ASESORÍA PARA DEFINIR INFRAESTRUCTURAS AVANZADAS DE REDES ELÉCTRICAS, DE INFORMACIÓN Y COMUNICACIONES EN EL SIN, QUE PROTEJAN EL SISTEMA DEL RIESGO DE APAGONES Y AUMENTEN LOS INDICES DE CALIDAD

### 1. ANTECEDENTES

Los sistemas eléctricos están expuestos a colapsos que pueden llegar a ser incluso apagones totales. Los orígenes de estos problemas están en muchos factores, pero los más importantes son la obsolescencia de los equipos por edad y/o configuración, la gran exposición de las redes de transmisión por su longitud y los errores humanos.

Para contrarrestarlos, se aplican diferentes soluciones. Entre las principales se cuentan la minimización de la necesidad del transporte de energía a grandes distancias utilizando la generación distribuida y el aumento de la confiabilidad mediante redes inteligentes.

En Colombia y en otros países se han utilizado los denominados esquemas suplementarios de protección del sistema (ESPS), considerados por algunos como servicios complementarios. Sin embargo, estos son esquemas muy puntuales para soluciones específicas que eviten inversiones en expansión y que pueden fallar, poniendo en riesgo la red.

En los sistemas más avanzados se están aplicando estrategias más robustas de protección para el sistema de potencia (SPID), que tienen una cobertura amplia, extensible a la red completa y que se basan en la combinación de infraestructuras de comunicaciones y de información, asociadas a la red eléctrica.

Los elementos básicos son los dispositivos electrónicos inteligentes y las unidades de medición fasorial, a partir de los cuales se obtienen datos sincronizados, confiables y de gran redundancia, que permiten optimizar la calidad, la seguridad y la confiabilidad del sistema eléctrico.

La función principal de SPID es prevenir apagones usando capacidades de reconfiguración adaptativa y autocuración (self-healing), que son características de las redes inteligentes. Un esquema de autocuración separa la red en islas en las que se minimiza el problema de balance generación-carga.

El propósito principal del sistema SPID es prevenir fallas catastróficas que pueden llevar a salidas de gran escala, como la ocurrida en Colombia el 26 de abril de 2007, evitándose incurrir en enormes costos económicos.

Por tanto, se considera de gran importancia analizar la incorporación de estas estrategias en el sistema eléctrico colombiano, para lo cual sería necesario desarrollar nuevos sistemas de medición y de intercambio de información.

Un análisis de SPID y redes inteligentes en el sistema eléctrico de Colombia es oportuno pues puede conducir a un desarrollo homogéneo que guíe las iniciativas de los agentes. De lo contrario, se pueden presentar compras de equipos y tecnologías en diferentes empresas bajo protocolos que pueden resultar incoherentes e incompatibles con los requerimientos de los centros de control.

## 2. OBJETIVO

Analizar la introducción de esquemas avanzados de infraestructuras eléctricas, de comunicaciones y de computadores en el SIN para prevenir colapsos en el sistema o minimizar su efecto.

## 3. ALCANCE.

El estudio debe cubrir los siguientes aspectos:

*Estado del arte

*Comparación de configuraciones y esquemas

*Recomendación para el caso colombiano

*Mapa de ruta

*Plan de acción

*Integración de los sistemas de redes inteligentes en las actividades de generación, transmisión y distribución

*Propuesta de interacción entre las infraestructuras de redes eléctricas, de comunicaciones y de computadores

*Conformación de las cadenas

PMU + PDC + SCADA (Unidades de Medición Fasorial más Concentradores de Datos Fasoriales más Sistema de Control y Adquisición de Datos).

IED + SLAN + WAN (Dispositivos Electrónicos Inteligentes más Redes de Área Local de las Subestaciones más Redes de Área Amplia), bajo el estándar IEC 61850.

DSA + IS + EMS (Estimación Dinámica del Sistema más Sistema Inteligente de Base de Datos más Sistema de Administración de la Energía).

*Efectuar un diagnóstico de la situación actual del SIN, hacia la perspectiva de las redes inteligentes

*Dentro del mismo, hacer el diagnóstico para una muestra seleccionada de empresas

*Proponer las bases de la configuración de los centros de control para las redes inteligentes en el SIN (GBCCA, Grid Based Control Centers Architecture, Arquitectura de los centros de control para la red inteligente).

## 4. EXPERIENCIA DE LOS PROPONENTES

Los proponentes deben tener experiencia comprobada en los siguientes temas:

a) Planeamiento y diseño de sistemas eléctricos de potencia
b) Centros de control
c) Automatización de redes eléctricas
d) Estimación de estado
e) Sistemas de información para redes inteligentes
f) Sistemas de comunicaciones para redes inteligentes

## 5. GRUPO DE PROFESIONALES

Grupo mínimo de especialistas:

Un experto en planeamiento y diseño de sistemas eléctricos de potencia

Un experto en comunicaciones

Un experto en sistemas de información para el control de redes eléctricas

Un experto con experiencia internacional en el diseño y puesta en marcha de redes eléctricas inteligentes y/o de sistemas SPID

## 6. PLAZO

Ocho meses.

## 7. EVALUACIÓN

Propuesta técnica (800 puntos)

Metodología (300 puntos) más la experiencia de los profesionales (500 puntos).

Propuesta económica

200 puntos.