

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO	
RAD: 13-284403- -2	FECHA: 2014-08-15 16:51:32
DEP: 2020 DIRECCION DE NUEVAS CREACIONES	EVE: 378 FASE NACIONAL INCLUIDO CAPITULO I
TRA: 11 PCT-PATENTE DE INVENCION CAPITULOS I Y II	FOLIOS: 17
ACT: 519 PRESENTACION	

DIRECCIÓN DE NUEVAS CREACIONES

2020
Bogotá, D.C.,

Abogado(a)/Señor(a)
LUZ CLEMENCIA DE PAEZ

Asunto: Radicación: 13-284403- -2
 Trámite: 11
 Evento: 378
 Actuación: 519
 Oficio: 10423
 Folios: 17

Patente de Invención	X			Patente de Modelo de Utilidad	
Vía Nacional					
Vía PCT (Fase Nacional)	X	Capítulo I	X	Capítulo II	
No. Solicitud Internacional	PCT/US2012/036611				
Fecha de Presentación Internacional	04/05/2012				

Como resultado del Examen de Fondo realizado, con fundamento en el artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se comunica:

1. Documentos estudiados

Descripción:	Rad. N° 13-284403-00000-0000	04/Diciembre/2013
Reivindicaciones:	Rad. N° 13-284403-00000-0000	04/Diciembre/2013
Dibujos:	Rad. N° 13-284403-00000-0000	04/Diciembre/2013
Prioridades:	US 61/482,538	04/Mayo/2011
	US 61/598,192	13/Febrero/2012

2. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, se tendrá en cuenta la tasa pagada por el solicitante al momento de comenzar el examen para las reivindicaciones adicionales; esto es que cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada. Por lo tanto, se estudiarán las reivindicaciones 1 a 22.

Título de la solicitud: “Análisis de riesgo de infraestructura energética y remediación” (Ver página 1 del radicado bajo el N° 13-284403-00000-0000).

El problema planteado en esta solicitud consiste en la necesidad de realizar de forma eficiente una evaluación, inspección y análisis de la infraestructura energética enterrada.

Para resolver este problema técnico, la solicitud en estudio proporciona sistemas, métodos y aparatos para analizar un sistema de infraestructura que incluye la medición de un parámetro asociado con el sistema de infraestructura, el registro electrónico del parámetro medido como un conjunto de datos, la transferencia de los datos a una unidad de infraestructura que puede ser remota del sistema de infraestructura, el análisis de los datos para generar un modelo de riesgo, y la predicción de una característica del sistema de infraestructura según el riesgo. Un plan de implementación puede ser generado, y/o servicios de mantenimiento pueden ser realizados según la característica que esté prevista.

El objeto de la presente Solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): G05B 9/02; G01N 17/00.

3 . De la Solicitud de Patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

Se sugiere al solicitante que incluya en las reivindicaciones independientes un preámbulo en donde se indican aquellas características técnicas conocidas en el estado de la técnica y una parte caracterizadora en donde se indican las características esenciales de la invención.

Se le sugiere al solicitante que indique al frente de la característica o del elemento, el número de referencia (X) guardando correspondencia con el capítulo descriptivo, las gráficas o dibujos y dicho capítulo reivindicatorio, con el objetivo de comprender mejor la invención al momento de hacer el análisis y distinguir los elementos de dicha invención.

Las reivindicaciones 1, 5 a 7, 16, 19 y 20 no son claras porque mencionan: “una herramienta de colección de datos”, “una unidad de infraestructura”, “una unidad de colección de datos”, “una unidad de implementación”, “una unidad de análisis del riesgo”, “una unidad de análisis comparativo”, “una unidad de análisis predictivo”, “una unidad de análisis relativo” y “una unidad de mitigación”, siendo frases de carácter general que sugieren de forma imprecisa que la protección se extiende a otras posibles variaciones o modificaciones.

Las reivindicaciones 1, 2, 5 a 8, 10, 15, 16, 19, 20 y 22 no son claras porque indican el uso que puede darse al producto reivindicado, el cual no es una característica técnica que defina a la invención. Lo anterior, según los siguientes fragmentos: “...configurada para soportar la línea de transmisión... configurada para recoger datos en la infraestructura de energía eléctrica... configurada para recibir datos estimando la infraestructura de energía eléctrica y su medio ambiente de la herramienta a partir de colección de datos... configurada para evaluar el riesgo relativo para la infraestructura de energía eléctrica y crear un plan de implementación para la remediación de la infraestructura de energía eléctrica.”, “...configurado para coleccionar los datos en la herramienta de colección de datos.”, “...configurada para evaluar una condición de degradación de cada una de las torres de transmisión basadas en los datos recibidos... configurada para comparar la condición de la degradación en cada una de las torres de transmisión para determinar un riesgo comparativo relativo de cada una de las torres de transmisión... configurada para determinar una función futura de las torres de transmisión.”, “...configurada para desarrollar un plan de implementación para mantener la integridad de una infraestructura de energía eléctrica teniendo una pluralidad de torres de transmisión... configurada para recibir datos con respecto a la infraestructura de energía eléctrica a partir al menos una herramienta de colección de datos... configurada para evaluar una condición de la degradación de cada una de las torres de transmisión

basadas en los datos recibidos... configurada para comparar la condición de degradación en cada una de las torres de transmisión para determinar un riesgo comparativo relativo de cada una de las torres de transmisión... configurada para determinar una función futura de las torres de transmisión... configurada para crear un plan de implementación para el mantenimiento de la infraestructura de energía eléctrica.”, “...configurada para determinar un estado de la corriente y un estado futuro de cada una de las torres de transmisión.”, “...en donde el plan de implementación es un horario de mantenimiento para cada pluralidad de las torres de transmisión.”, “...para acceder y manipular los datos en un momento futuro en el tiempo.”, “...para acceder y manipular estos datos en un momento futuro en el tiempo.”, “...configurada para transportar fluidos... configurada para recoger datos en la infraestructura de la tubería... configurada para recibir datos de la herramienta de colección de datos... configurada para recibir datos estimando la infraestructura de la tubería a partir de la herramienta de colección de datos... configurada para evaluar el riesgo relativo para la infraestructura de la tubería y crear un plan de implementación para la remediación de la infraestructura de la tubería.”, “...configurada para evaluar una condición de corrosión de la tubería basada en los datos recibidos... configurada para generar un informe de corrosión detallando la corrosión real, una probabilidad de una fuga actual de la tubería y una probabilidad de corrosión futura... configurada para determinar un tipo de trabajo de mitigación a ser realizada en la tubería.”, “...configurada para desarrollar un plan de implementación para mantener la integridad de una tubería... configurada para recibir datos estimando la tubería de herramientas de al menos una colección de datos... configurada para evaluar una condición de corrosión de la tubería basada en los datos recibidos... configurada para generar un informe de corrosión detallando la corrosión real, una probabilidad de una fuga actual de la tubería y una probabilidad de corrosión futura... configurada para determinar un tipo de trabajo de mitigación a ser realizada en la tubería... configurada para preparar un plan de implementación para el mantenimiento de la tubería.” y “...para acceder y manipular los datos en un momento futuro en el tiempo.” Se sugiere hacer la aclaración respectiva.

Las reivindicaciones 1 a 4, 6, 9, 12, 13, 16, 20, 21 no son claras porque el término: “al menos”, es impreciso, por lo cual no permite distinguir la invención del estado de la técnica. Se sugiere sustituirlo por un término preciso o un rango concreto.

De igual forma, se le recuerda a la solicitante que las características técnicas esenciales estructurales de carácter tangible son las que definen la invención en una reivindicación de producto, las que la hacen (o deberían hacerla) diferente del estado de la técnica y, por tanto, constituyen la solución al problema técnico que intenta resolver la invención. Para una mayor claridad, se definen los siguientes conceptos:

Las características que definen la invención son las características técnicas estructurales de carácter tangible (partes mecánicas, eléctricas, electrónicas y su relación o conexión). Las características funcionales son los elementos que conforman las invenciones, descritos en términos de su uso o su función. No definen la invención, pero explican la relación que hay entre sus diversas características estructurales, por lo tanto, dichas características funcionales no brindan novedad y/o nivel inventivo a la invención y no son tenidas en cuenta en el examen de patentabilidad.

De acuerdo con lo anterior, se sugiere a la solicitante que defina el producto por sus características técnicas esenciales estructurales tangibles.

Por lo anterior, el capítulo reivindicatorio de la solicitud en estudio no cumple con el requisito de claridad acuerdo con el artículo 30 de la Decisión 486. En consecuencia, el solicitante deberá presentar un nuevo capítulo reivindicatorio, donde se hayan modificado las objeciones anteriormente citadas; dichas modificaciones no deben ampliar el objeto inicialmente presentado por la presente solicitud.

Descripción (Art 28 D 486)

Se sugiere hacer la conversión de unidades (Pág. 12, Párr. 20; Pág. 13, Párr. 22; Pág. 14, Párr. 25; Pág. 15, Párr. 31 y Párr. 33; Pág. 20, Párr. 49 y figuras), al Sistema Internacional.

4. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de presentación de la solicitud de prioridad: mayo 04 de 2011 y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	Artículo 1	"Power System Survivability Increase with Intelligent Support Tools"	Julio/2009*
D2	US 2005/0183028	"System and method for acquisition and analysis of time and location-specific data"	18/Agosto/2005
D3	Artículo 2	"PRA for vulnerability assessment of power system infrastructure security"	Octubre/2005**
D4	US 2010/0088139	"Project management system adapted for planning and managing projects"	08/Abril/2010

* Power System Survivability Increase with Intelligent Support Tools. Power & Energy Society General Meeting, 2009. PES '09. IEEE. Calgary, Canadá. 23-30 Julio 2009. Dellwing, H.; Geretshuber, S.; Schwaegerl, C.; Seifert, O.

** PRA for vulnerability assessment of power system infrastructure security. Power Symposium, 2005. Proceedings of the 37th Annual North American. 23-25 Oct. 2005., Kang Lin; Holbert, K.E.

El documento D1¹ divulga que desde la liberalización del mercado energético un mayor número de actores con diferentes responsabilidades y el aumento de las transferencias de energía entre países, junto con una elevada proporción de generación dispersa y renovable están actualmente forzando a los sistemas de transmisión y distribución en Europa hasta sus límites. El aumento de la automatización crea una dependencia más alta en la infraestructura de las telecomunicaciones y aumenta la complejidad de las estructuras de dependencia y, como consecuencia el peligro de efectos en cascada, por ejemplo, causando apagones en toda la zona. Se requieren nuevas herramientas o una combinación inteligente de los enfoques existentes para aumentar la capacidad de supervivencia de las infraestructuras críticas. Este artículo describe algunos de los resultados de un proyecto de investigación europeo llamado IRRIS que fue dedicado a la reducción de riesgos críticos de las infraestructuras (Pág. 1, resumen).

El documento D2² divulga un sistema y un método que presenta un medio para acceder y revisar los datos registrados de una manera que apoye el análisis de la condición de los sistemas de infraestructura como la red de alcantarillado o en otros sistemas de tuberías. La presente invención proporciona además la posibilidad de ver una ubicación particular en un sistema de tuberías o conjunto de datos en diferentes puntos en el tiempo, apoyando así un análisis del deterioro y probablemente la prioridad de reparación de una sección particular de la infraestructura (Pág. 1, resumen).

El documento D3³ divulga que desde septiembre 11 de 2001, la seguridad de las grandes infraestructuras nacionales se ha convertido en una preocupación fundamental para el gobierno y la industria. Este artículo revisa los diferentes tipos de amenazas (físicas y cibernéticas) y las fuentes de estas amenazas en los sistemas de energía

1 <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5275602&contentType=Conference+Publications&>

2 <https://www.google.com/patents/US20050183028?dq=US+2005/0183028&hl=es-419&sa=X&ei=Q7vbU8-RIPDMsQSCmYHoAw&ved=0CB4Q6AEwAA>

3 <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=1560500&contentType=Conference+Publications&>

eléctrica, describe los proyectos emprendidos por el gobierno y la industria para hacer frente a los problemas de seguridad de la infraestructura del sistema de energía, y presenta una metodología de evaluación de la vulnerabilidad para las redes de potencia. Finalmente, este trabajo considera métodos de evaluación del riesgo probabilística (PRA) y los desafíos a la PRA, y propone el uso de la PRA en la evaluación de la vulnerabilidad del sistema de energía eléctrica (Pág. 43, resumen).

El documento D4⁴ divulga un método, que es practicado por un sistema informático, para la planificación y la gestión de planes de proyectos asociados con uno o más proyectos en un negocio, el sistema informático que incluye un procesador que es sensible a los datos de entrada, una grabadora o un dispositivo de visualización, y una memoria; la memoria almacena el software, que comprende: la ejecución por el procesador del software almacenado en la memoria del sistema computacional en respuesta a los datos de entrada que incluye datos de conocimiento y experiencia, y, en respuesta a la etapa de ejecución, la generación de una o más pantallas de salida adaptadas para la planificación y la gestión de los planes del proyecto de uno o más proyectos en el negocio; grabar o mostrar, por el dispositivo de grabación o visualización, la una o más pantallas de salida de la grabadora o dispositivo de visualización; en el que una o más pantallas de salida a ser grabadas o mostradas en la grabadora o dispositivo de visualización incluyen, vistas Line-of-Sight (LOS) de información relacionadas con el negocio, las vistas Line-of-Sight proporcionan a un usuario una vista del plan del proyecto de uno o más proyectos que se filtran según la disciplina o la responsabilidad en el proyecto del usuario y un nivel de detalle que sea apropiado para el papel del usuario en el uno o más proyectos (Pág. 1, resumen).

5 . Examen de Patentabilidad (Art 14 D 486)

Es importante mencionar que el siguiente análisis de patentabilidad se realizó teniendo en cuenta las objeciones del numeral 3 de la presente comunicación.

Novedad (Art 16 D486)

La reivindicación 1 consiste en “Un sistema de análisis de infraestructura, que comprende...” (Ver página 29 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D4	D1
Un sistema de análisis de infraestructura.	Un sistema de gestión de proyectos, conocido como el "Enterprise System Management Project (EPMS)", que está adaptado para la planificación y gestión de proyectos de diferentes tamaños y tipos en forma integrada e intuitiva para facilitar la colaboración entre los miembros del equipo relacionados con el proyecto y entre los miembros de una organización más grande (Pág. 1, Fl. 137, Párr. 1).	Una plataforma de comunicación sofisticada para el intercambio de información entre las infraestructuras críticas, y proporcionando componentes MIT add-on adecuados para gestionar esta información (Pág. 2, Col. Izq., Párr. 1).
Una infraestructura de energía eléctrica que comprende una línea de transmisión y una torre de transmisión.	No se menciona	El sistema experto CRIPS se basa en simulaciones de redes en estado de equilibrio realizadas con PSS TM SINCAL, una herramienta creada para apoyar el análisis y la planificación de las redes de energía eléctrica, de gas, agua o calor (Pág. 2, Col. Der., Párr. 2).

4 https://www.google.com/patents/US20100088139?dq=US20100088139&hl=es-419&sa=X&ei=lpbbU_ybHeHNSQSV-IDYCA&ved=0CB4Q6AEwAA

		Es conocido que las redes de energía eléctrica comprenden al menos una línea y una torre de transmisión.
Una herramienta de colección de datos.	Un centro de control operacional (157) puede asistir en la colección de los datos y tomar decisiones para intensificar las operaciones (Pág. 4, Fl. 140, Párr. 45).	Herramientas para extracción de estado funcional – una interfaz de datos simple para sistemas SCADA y de control (Pág. 2, Col. Izq., Párr. 2, MIT Components).
Una unidad de infraestructura, que comprende una unidad de colección de datos y una unidad de implementación.	El sistema computacional incluye un procesador que actúa en respuesta a los datos de entrada, un grabador o dispositivo de pantalla, y una memoria; la memoria almacena el software, que comprende: la ejecución por el procesador del software almacenado en la memoria del sistema computacional en respuesta a los datos de entrada que incluye datos de conocimiento y experiencia, y, en respuesta a la etapa de ejecución, la generación de una o más pantallas de salida adaptadas para la planificación y la gestión de los planes del proyecto de uno o más proyectos en el negocio; grabar o mostrar, por el dispositivo de grabación o visualización, la una o más pantallas de salida de la grabadora o dispositivo de visualización; en el que una o más pantallas de salida a ser grabadas o mostradas en la grabadora o dispositivo de visualización incluyen, vistas Line-of-Sight (LOS) de información relacionadas con el negocio, las vistas Line-of-Sight proporcionan a un usuario una vista del plan del proyecto de uno o más proyectos que se filtran según la disciplina o la responsabilidad en el proyecto del usuario y un nivel de detalle que sea apropiado para el papel del usuario en el uno o más proyectos (Pág. 1, Fl. 137, Párr. 5).	Los principales componentes desarrollados en IRRIS son: herramienta de comunicación MIT que permite a diferentes CI intercambiar información; estimador de riesgo (RE) el cual permite a los operadores procesar la información de los CI dependientes y enviar información crítica desde su propia red a los CI dependientes; la herramienta de apoyo de decisión CRIPS (“CRIsis management and Planning System”); y analizador de conocimientos de incidentes (Pág. 2, Col. Izq., Párr. 2, MIT Components).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 1 con la anterioridad D1, el sistema descrito en dicha reivindicación, ya era conocido en el estado de la técnica. Por lo tanto, la reivindicación 1 no es nueva.

Por otra parte, aunque el documento D4 no divulga en su totalidad las características técnicas esenciales de la reivindicación 1, es preciso indicar que dicha característica que no es divulgada hace referencia al uso de dicho sistema en un sistema particular, como un sistema de energía eléctrica. En este caso cabe mencionar, que la automatización de un método conocido de análisis de datos no brinda ningún efecto técnico inesperado.

De acuerdo al análisis anterior, las reivindicaciones dependientes son afectadas por novedad por las razones dadas a continuación:

- Reivindicaciones 2 y 3: Herramientas para extracción de estado funcional – una interfaz de datos simple para sistemas SCADA y de control (D1, Pág. 2, Col. Izq., Párr. 2, MIT Components).
- Reivindicación 5: Estimador de riesgo (RE) el cual permite a los operadores procesar la información de los CI dependientes y enviar información crítica desde su propia red a los CI dependientes (D1, Pág. 2, Col. Izq., Párr. 2, MIT Components). El RE combina y analiza la información de su CI principal, así como de CI dependientes. Estima el riesgo inmediato y el potencial en cascada y/o

efectos crecientes, teniendo en cuenta la información en tiempo real (evaluación interna), la información de estado de otro CI dependiente, planificación de la información en todo el área, el mantenimiento programado, el pronóstico del tiempo, las huelgas, los grandes eventos públicos, vulnerabilidad de software/hardware y otros recursos de información pública (D1, Pág. 2, Col. Izq., Párr. 5 a Col. Der., Párr. 1; Fig. 1). La herramienta de apoyo de decisión CRIPS (“CRIsis management and Planning System”) (D1, Pág. 2, Col. Izq., Párr. 2, MIT Components). CRIPS evalúa la situación actual de las redes de suministro de energía analizando los resultados de la simulación del comportamiento de la red física y toma las decisiones correspondientes para asistir al operador de red en la detección temprana y en la toma de decisiones en situaciones de emergencia (D1, Pág. 2, Col. Der., Párr. 2). Analizador de conocimientos de incidentes (D1, Pág. 2, Col. Izq., Párr. 2, MIT Components).

La reivindicación 6 consiste en *“Una unidad de infraestructura configurada para desarrollar un plan de implementación para mantener la integridad de una infraestructura de energía eléctrica teniendo una pluralidad de torres de transmisión, que comprende...”* (Ver página 30 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D1
Una unidad de infraestructura.	Una plataforma de comunicación sofisticada para el intercambio de información entre las infraestructuras críticas, y proporcionando componentes MIT add-on adecuados para gestionar esta información (Pág. 2, Col. Izq., Párr. 1).
Una unidad de colección de datos.	Herramientas para extracción de estado funcional – una interfaz de datos simple para sistemas SCADA y de control (Pág. 2, Col. Izq., Párr. 2, MIT Components).
Una unidad de análisis del riesgo.	Estimador de riesgo (RE) el cual permite a los operadores procesar la información de los CI dependientes y enviar información crítica desde su propia red a los CI dependientes (Pág. 2, Col. Izq., Párr. 2, MIT Components). El RE combina y analiza la información de su CI principal, así como de CI dependientes. Estima el riesgo inmediato y el potencial en cascada y/o efectos crecientes, teniendo en cuenta la información en tiempo real (evaluación interna), la información de estado de otro CI dependiente, planificación de la información en todo el área, el mantenimiento programado, el pronóstico del tiempo, las huelgas, los grandes eventos públicos, vulnerabilidad de software/hardware y otros recursos de información pública (Pág. 2, Col. Izq., Párr. 5 a Col. Der., Párr. 1; Fig. 1).
Una unidad de análisis comparativo.	La herramienta de apoyo de decisión CRIPS (“CRIsis management and Planning System”) (Pág. 2, Col. Izq., Párr. 2, MIT Components). CRIPS evalúa la situación actual de las redes de suministro de energía analizando los resultados de la simulación del comportamiento de la red física y toma las decisiones correspondientes para asistir al operador de red en la detección temprana y en la toma de decisiones en situaciones de emergencia (Pág. 2, Col. Der., Párr. 2).
Una unidad de análisis predictivo.	Analizador de conocimientos de incidentes (Pág. 2, Col. Izq., Párr. 2, MIT Components).
Una unidad de implementación.	Se compone de potentes herramientas necesarias para el examen de cualquier estado de la red y de la determinación de la estructura de red más adecuada en condiciones normales y en situaciones de emergencia. El impacto de las operaciones de conmutación puede ser analizada y las redes se pueden optimizar con respecto a las pérdidas y utilización (Pág. 2, Col. Der., Párr. 4).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 6 con la anterioridad D1, la unidad de infraestructura descrita en dicha reivindicación, ya era conocida en el estado de la técnica. Por lo tanto, la reivindicación 6 no es nueva.

De acuerdo al análisis anterior, las reivindicaciones dependientes son afectadas por novedad por las razones dadas a continuación:

Reivindicación 7: La documentación, por ejemplo, del análisis de hechos reales

(apagones) o de los resultados de ejercicios de gestión de crisis como una base de conocimiento que hace a este conocimiento automático utilizable y disponible de inmediato - un beneficio general del método de sistema experto. CRIPS proporciona los conocimientos para la evaluación de la situación y la toma de decisiones. La base de conocimiento no se limita a los datos técnicos, que se muestran en el ejemplo (tensión y la carga). Todos los indicadores disponibles de una situación crítica pueden ser tomados en cuenta (por ejemplo, a través de interfaces de los sistemas de comunicación). Todos los datos importantes están disponibles para la evaluación y la toma de decisiones correspondiente (D1, Pág. 5, Col. Der., Párrs. 5 y 6).

La reivindicación dependiente 8 no menciona alguna característica que haga nueva a la unidad de infraestructura de la reivindicación 6, dado que se encuentra redactada en términos de usos, funciones y/o resultados, por lo cual se considera que no es nueva.

La reivindicación 9 consiste en “*Un método para reparar una infraestructura de energía eléctrica teniendo al menos una torre de transmisión y al menos una línea de transmisión, donde el método comprende...*” (Ver página 30 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D3
Un método para reparar una infraestructura de energía eléctrica.	Durante las últimas décadas, la evaluación del riesgo probabilística (PRA) se ha convertido en una disciplina técnica capaz de lógica, sistemática y exhaustiva evaluación de las debilidades y vulnerabilidades de los sistemas complejos y las instalaciones que pueden afectar negativamente a la seguridad, la productividad y el éxito de la misión. Su utilidad ha sido probada en muchas industrias, incluyendo la aeroespacial [23], la generación eléctrica [24], petroquímica [25], y la defensa [26] (Pág. 45, Col. Izq. Párr. 2).
Recolección de datos con respecto a la infraestructura de energía eléctrica.	La identificación de los sucesos iniciadores es una tarea importante porque los perfiles de riesgo sólo se pueden obtener a través de la transformación de estos eventos en consecuencias. Los sucesos iniciadores son las interrupciones en el funcionamiento normal de la planta que requieren activación automática o manual de los sistemas de seguridad de la planta. Los eventos iniciadores debido a fallas de los sistemas activos y de apoyo también se incluyen. Un PRA completo maneja los sucesos iniciadores tanto internos como externos (Pág. 45, Col. Der., Párr. 6).
Introducción en la computadora de los datos en una unidad de infraestructura.	Dos métodos se pueden tomar para identificar sucesos iniciadores. El primero es una evaluación general de ingeniería, teniendo en cuenta la información de las evaluaciones previas de riesgo, la documentación que refleje el historial de funcionamiento y datos de diseño específicos de la planta. La información es evaluada y una lista de los sucesos iniciadores se compila. El segundo es un enfoque más formal. Esto incluye listas de control, como el análisis de riesgos preliminares, y los modos de fallo y análisis de efectos (Pág. 45, Col. Der., Párr. 7 a Pág. 46, Col. Izq., Párr. 1).
Comparación de los datos en la unidad de infraestructura.	Hay dos técnicas comunes de análisis que se utilizan en esta etapa: árboles de eventos y árboles de fallos (Pág. 46, Col. Izq., Párr. 5). El análisis de árboles de eventos (ETA) se utiliza para definir las secuencias de accidentes que involucran interrelaciones complejas entre los sistemas técnicos de seguridad, y están construidas utilizando la lógica hacia adelante. La probabilidad de accidentes se obtiene por la lógica hacia atrás (árbol de fallos). El análisis del árbol de fallos (TLC) es una técnica gráfica que proporciona una descripción sistemática de las combinaciones de posibles ocurrencias en un sistema, que puede resultar en un resultado indeseable. Este método puede combinar fallos de equipos y humanos. El resultado más grave (por ejemplo, explosión, liberación de tóxicos) es seleccionado como el evento más importante. Un árbol de fallas se construye entonces al relacionar las secuencias de acontecimientos, en forma individual o en combinación, que podrían llevar al evento superior. El evento no deseado aparece como el evento más importante que se relaciona con eventos de falla más básicos por las declaraciones de eventos y puertas lógicas (Pág. 46, Col. Izq., Párr. 6 a Col. Der., Párr. 1).
Provisión de un plan de	Una hoja de resumen puede ser preparada en la que los modos de fallo se

implementación a base de la condición de degradación.	enumeran en orden decreciente de códigos de prioridad de riesgo. El resumen también debe enumerar las medidas correctivas necesarias para reducir la frecuencia del fallo o para mitigar las consecuencias. Las acciones correctivas pueden incluir cambios en el diseño, procedimientos o modalidades de organización, tales como la adición de características redundantes y los métodos de detección, o puede ser sugerido un cambio en la política de mantenimiento Pág. 46, Col. Der., Párr. 3).
Ejecución del plan de implementación.	Las acciones correctivas pueden incluir cambios en el diseño, procedimientos o modalidades de organización, tales como la adición de características redundantes y los métodos de detección, o puede ser sugerido un cambio en la política de mantenimiento Pág. 46, Col. Der., Párr. 3).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 9 con la anterioridad D3, el método descrito en dicha reivindicación, ya era conocido en el estado de la técnica. Por lo tanto, la reivindicación 9 no es nueva.

De acuerdo al análisis anterior, la reivindicación dependiente es afectada por novedad por las razones dadas a continuación:

- Reivindicación 10: Dos métodos se pueden tomar para identificar sucesos iniciadores. El primero es una evaluación general de ingeniería, teniendo en cuenta la información de las evaluaciones previas de riesgo, la documentación que refleje el historial de funcionamiento y datos de diseño específicos de la planta. La información es evaluada y una lista de los sucesos iniciadores se compila. El segundo es un enfoque más formal. Esto incluye listas de control, como el análisis de riesgos preliminares, y los modos de fallo y análisis de efectos (D3, Pág. 45, Col. Der., Párr. 7 a Pág. 46, Col. Izq., Párr. 1).

La reivindicación 11 consiste en “Un método para analizar un sistema de infraestructura, que comprende los pasos de...” (Ver página 31 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D2
Un método para analizar un sistema de infraestructura.	El método de la presente invención presenta un medio para acceder y revisar los datos registrados de una manera que apoye el análisis de la condición de los sistemas de infraestructura (Pág. 2, Fl. 10, Párr. 12).
Medir un parámetro asociado con el sistema de infraestructura.	Como se ha descrito anteriormente en relación con las figuras 1 y 2, una inspección de un lugar físico prevé la adquisición y/o generación de datos, tales como observaciones, informes de defectos o videos de un elemento de infraestructura (305) (Pág. 3, Fl. 11, Párr. 26).
Registrar electrónicamente el parámetro medido como unos datos.	En la presente invención, dichos datos se correlacionan con la ubicación física de cada elemento que se está grabando, como un lugar de alcantarilla en un sistema de alcantarillado, y adicionalmente, se correlaciona (o asocia) con la fecha/hora de recogida de los datos (305). El sistema (300) también proporciona la transferencia (315) de datos heredados tales como cinta de vídeo o bibliotecas de CD/DVD a una o más bases de datos (310). El sistema (300) también proporciona la entrada y la vinculación de objetos de datos (320) que pueden comprender indicadores de estado, notas de inspección, datos de observación o de clasificación, o los resultados del análisis (Pág. 3, Fl. 11, Párr. 26).
Transferir los datos a una unidad de infraestructura remota de sistema de infraestructura.	Desde las bases de datos (310) la presente invención permite el enlace (325) de datos almacenados en las bases de datos (310) con elementos del sistema de información gráfica (GIS) tales como segmentos de tubería, válvulas, o pozos de registro. En un método de uso de la presente invención, un usuario selecciona una característica que se muestra en un esquema o mapa GIS para su revisión (330) (Figs. 4 y 5). Una lista de las fuentes de datos disponibles u opciones de medios se presenta a continuación junto con las propiedades de datos de estado/hora y representaciones gráfica y/o de código (por ejemplo, códigos de NASSCO), del elemento físico (por ejemplo, bocas de acceso, laterales, y defectos) (Fig. 6) y el usuario selecciona uno de los archivos multimedia con su límite de tiempo asociado (335). El usuario puede entonces

	seleccionar opcionalmente al menos uno de los elementos gráficos de función/código (340) para ver la representación de los medios (por ejemplo, vídeo) de ese elemento en ese punto en el tiempo (Fig. 7). El usuario puede entonces revisar la representación de los medios para determinar el estado físico del elemento representado en el archivo multimedia que corresponde a los elementos gráficos de función/código (345), y si el usuario lo desea, puede seleccionar un medio diferente y el calendario (335) o simplemente puede seleccionar otro código o característica que desea ver en la representación de los medios existentes (340) (Figs. 9 y 10) (Pág. 3, Fl. 11, Párr. 26).
Análisis de los datos.	En una realización de la presente invención, se utiliza una fuente de mapeo para crear relaciones entre las imágenes de vídeo y las representaciones de las secciones de tubería. El origen de asignación puede originarse a partir de cualquier número de herramientas de software asistidas por computador de ingeniería o diseño disponibles en el mercado, incluyendo, pero no limitado a ArcView, Arc Map, Pro-E o AutoCad. Tras el análisis de la representación de un mapa del sistema con segmentos de línea entre las ubicaciones de pozos, la presente invención asocia una o más representaciones en video de un segmento con su equivalente asignado (Pág. 4, Fl. 12, Párr. 34).
Predicción de una característica del sistema de infraestructura según el riesgo.	Cuando se detecta un posible defecto, los datos adquiridos previamente son consultados para la comparación de cambios en el tiempo, con un paso opcional para adquirir una representación de datos actual. El análisis entonces se traduce en la asignación de un recurso como un técnico, quien se despacha por la invención descrita y es guiado por la invención descrita a la fuente del problema potencial mediante técnicas tales como una pantalla en el vehículo junto a una unidad de GPS. A continuación, la invención descrita proporciona funciones de apoyo a la programación de un esfuerzo de mitigación tales como la excavación y reparación. El sistema acepta la tarea, asigna recursos, y proporciona la información de seguimiento a la tripulación de reparación para localizar el origen del problema de forma rápida y eficiente (Pág. 5, Fl. 13, Párr. 42).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 11 con la anterioridad D2, el método descrito en dicha reivindicación, ya era conocido en el estado de la técnica. Por lo tanto, la reivindicación 11 no es nueva.

De acuerdo al análisis anterior, las reivindicaciones dependientes son afectadas por novedad por las razones dadas a continuación:

- Reivindicaciones 12 a 15: Consideremos un escenario en el que un video de inspección revela una grieta en una sección de la tubería ubicada entre dos pozos de registro. Ingeniería selecciona la tubería sospechosa en el sistema GIS y encuentra que hay tres videos en archivo que corresponden a la sección de la tubería sospechosa. Un archivo de medios representa el estado después de que la tubería fue instalada, el segundo representa una inspección de rutina anterior y una tercera muestra los datos y medios de la inspección más actual. En la visualización del video más reciente, un ingeniero observa una decoloración inusual en el punto del defecto. La representación de la tubería indica un derecho lateral justo aguas arriba del defecto. Al seleccionar esta lateral el ingeniero visualiza la sección de vídeo para el lateral y encuentra que la decoloración se origina en ella. El ingeniero entonces abre una segunda ventana para comparar el vídeo actual con uno que fue grabado hace cinco años. Al seleccionar el mismo lateral el ingeniero puede instantáneamente ver y comparar el estado anterior al actual del lateral. El vídeo revela que no hay decoloración en el lateral y no hay señales de debilidad en el defecto actual. El ingeniero también ve el video como incorporado y no encuentra ninguna decoloración en el lateral y no hay señales de debilidad en el defecto actual. En cuestión de minutos el ingeniero ha sido capaz de ver todo el vídeo correspondiente al defecto actual y determinar un curso de acción. Únicamente con reparar el defecto no va a resolver el origen del problema. Una búsqueda de las licencias profesionales expedidas en los últimos cinco años para el área alimentada por el problema lateral dio como resultado, entre otros, un

negocio de venta de baterías y ácidos corrosivos. La investigación adicional reveló ácido, plomo, zinc y otros materiales de la batería situados en una boca de tormenta detrás del negocio y apoyó los esfuerzos de mitigación para prevenir más daños en el sistema de tuberías (D2, Pág. 3, Fl. 11, Párr. 32).

La reivindicación 16 consiste en “*Un sistema de análisis de la tubería, que comprende...*” (Ver página 32 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D2
Un sistema de análisis de la tubería.	El sistema de la presente invención presenta un medio para acceder y revisar los datos registrados de una manera que apoye el análisis de la condición de los sistemas de infraestructura, tales como tuberías de alcantarillado u otros sistemas de tuberías (Pág. 2, Fl. 10, Párr. 12).
Una infraestructura de la tubería que comprende una tubería.	Sistemas de infraestructura, tales como tuberías de alcantarillado u otros sistemas de tuberías (Pág. 2, Fl. 10, Párr. 12).
Una herramienta de colección de datos.	Medios de adquisición para los elementos de representación de datos de un sistema de infraestructura (Pág. 5, Fl. 13, reiv. 1).
Una unidad de infraestructura de la tubería que comprende una unidad de colección de datos y una unidad de implementación	Medios de selección para elegir una característica representada en un sistema de información gráfica; medios para seleccionar un archivo multimedia de un marco de tiempo asociado; medios para seleccionar al menos uno de un elemento de código/característica; y medios para la revisión de un estado físico de un objeto representado por un elemento de código/función (Pág. 5, Fl. 13, reiv. 1). Medios para presentar un indicio general de clasificación para la integridad de un elemento de un sistema de infraestructura (Pág. 5, Fl. 13, reiv. 5).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 16 con la anterioridad D2, el sistema descrito en dicha reivindicación, ya era conocido en el estado de la técnica. Por lo tanto, la reivindicación 16 no es nueva.

De acuerdo al análisis anterior, las reivindicaciones dependientes son afectadas por novedad por las razones dadas a continuación:

- Reivindicaciones 17 y 18: En aún otra realización de la presente invención, la adquisición de datos no sólo se toma de una fuente de datos y se correlaciona con las coordenadas espaciales y temporales, sino a partir de múltiples sensores y fuentes simultáneas. Por ejemplo, un robot, como se explica más arriba podría grabar una vista de 360 grados de la tubería, ya que atraviesa el sistema, eliminando así la necesidad de parar en los cruces laterales y realizar panorámicas de una cámara en las direcciones de los laterales. Gracias al registro de múltiples ángulos de visión, como una vista de 360 grados, la necesidad de parar y las panorámicas de una cámara se eliminan (D2, Pág. 4, Fl. 12, Párr. 41).

La reivindicación 20 consiste en “*Una unidad de infraestructura de la tubería configurada para desarrollar un plan de implementación para mantener la integridad de una tubería, que comprende...*” (Ver página 33 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D1
Una unidad de infraestructura de la tubería.	Una plataforma de comunicación sofisticada para el intercambio de información entre las infraestructuras críticas, y proporcionando componentes MIT add-on adecuados para gestionar esta información (Pág. 2, Col. Izq., Párr. 1).
Una unidad de colección de datos.	Herramientas para extracción de estado funcional – una interfaz de datos simple para sistemas SCADA y de control (Pág. 2, Col. Izq., Párr. 2, MIT Components).
Una unidad de análisis del riesgo.	Estimador de riesgo (RE) el cual permite a los operadores procesar la información de los CI dependientes y enviar información crítica desde su propia red a los CI dependientes (Pág. 2, Col. Izq., Párr. 2, MIT Components).

	El RE combina y analiza la información de su CI principal, así como de CI dependientes. Estima el riesgo inmediato y el potencial en cascada y/o efectos crecientes, teniendo en cuenta la información en tiempo real (evaluación interna), la información de estado de otro CI dependiente, planificación de la información en todo el área, el mantenimiento programado, el pronóstico del tiempo, las huelgas, los grandes eventos públicos, vulnerabilidad de software/hardware y otros recursos de información pública (Pág. 2, Col. Izq., Párr. 5 a Col. Der., Párr. 1; Fig. 1).
Una unidad de análisis predictivo.	La herramienta de apoyo de decisión CRIPS (“CRIsis management and Planning System”) (Pág. 2, Col. Izq., Párr. 2, MIT Components). CRIPS evalúa la situación actual de las redes de suministro de energía analizando los resultados de la simulación del comportamiento de la red física y toma las decisiones correspondientes para asistir al operador de red en la detección temprana y en la toma de decisiones en situaciones de emergencia (Pág. 2, Col. Der., Párr. 2).
Una unidad de mitigación.	Analizador de conocimientos de incidentes (Pág. 2, Col. Izq., Párr. 2, MIT Components).
Una unidad de implementación.	Se compone de potentes herramientas necesarias para el examen de cualquier estado de la red y de la determinación de la estructura de red más adecuada en condiciones normales y en situaciones de emergencia. El impacto de las operaciones de conmutación puede ser analizada y las redes se pueden optimizar con respecto a las pérdidas y utilización (Pág. 2, Col. Der., Párr. 4).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 20 con la anterioridad D1, la unidad de infraestructura descrita en dicha reivindicación, ya era conocida en el estado de la técnica. Por lo tanto, la reivindicación 20 no es nueva.

La reivindicación 21 consiste en “*Un método para enmendar una infraestructura de tubería que tiene al menos una tubería, donde el método comprende...*” (Ver página 33 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D3
Un método para enmendar una infraestructura de tubería.	Durante las últimas décadas, la evaluación del riesgo probabilística (PRA) se ha convertido en una disciplina técnica capaz de lógica, sistemática y exhaustiva evaluación de las debilidades y vulnerabilidades de los sistemas complejos y las instalaciones que pueden afectar negativamente a la seguridad, la productividad y el éxito de la misión. Su utilidad ha sido probada en muchas industrias, incluyendo la aeroespacial [23], la generación eléctrica [24], petroquímica [25], y la defensa [26] (Pág. 45, Col. Izq. Párr. 2).
Recolectar datos que estiman la infraestructura de la tubería.	La identificación de los sucesos iniciadores es una tarea importante porque los perfiles de riesgo sólo se pueden obtener a través de la transformación de estos eventos en consecuencias. Los sucesos iniciadores son las interrupciones en el funcionamiento normal de la planta que requieren activación automática o manual de los sistemas de seguridad de la planta. Los eventos iniciadores debido a fallas de los sistemas activos y de apoyo también se incluyen. Un PRA completo maneja los sucesos iniciadores tanto internos como externos (Pág. 45, Col. Der., Párr. 6).
Introducir en la computadora los datos en una unidad de infraestructura.	Dos métodos se pueden tomar para identificar sucesos iniciadores. El primero es una evaluación general de ingeniería, teniendo en cuenta la información de las evaluaciones previas de riesgo, la documentación que refleje el historial de funcionamiento y datos de diseño específicos de la planta. La información es evaluada y una lista de los sucesos iniciadores se compila. El segundo es un enfoque más formal. Esto incluye listas de control, como el análisis de riesgos preliminares, y los modos de fallo y análisis de efectos (Pág. 45, Col. Der., Párr. 7 a Pág. 46, Col. Izq., Párr. 1).
Comparar los datos en la unidad de infraestructura para determinar una porción dañada de la tubería.	Hay dos técnicas comunes de análisis que se utilizan en esta etapa: árboles de eventos y árboles de fallos (Pág. 46, Col. Izq., Párr. 5). El análisis de árboles de eventos (ETA) se utiliza para definir las secuencias de accidentes que involucran interrelaciones complejas entre los sistemas técnicos de seguridad, y están construidas utilizando la lógica hacia adelante. La probabilidad de accidentes se obtiene por la

	lógica hacia atrás (árbol de fallos). El análisis del árbol de fallos (TLC) es una técnica gráfica que proporciona una descripción sistemática de las combinaciones de posibles ocurrencias en un sistema, que puede resultar en un resultado indeseable. Este método puede combinar fallos de equipos y humanos. El resultado más grave (por ejemplo, explosión, liberación de tóxicos) es seleccionado como el evento más importante. Un árbol de fallas se construye entonces al relacionar las secuencias de acontecimientos, en forma individual o en combinación, que podrían llevar al evento superior. El evento no deseado aparece como el evento más importante que se relaciona con eventos de falla más básicos por las declaraciones de eventos y puertas lógicas (Pág. 46, Col. Izq., Párr. 6 a Col. Der., Párr. 1).
Proporcionar un plan de implementación.	Una hoja de resumen puede ser preparada en la que los modos de fallo se enumeran en orden decreciente de códigos de prioridad de riesgo. El resumen también debe enumerar las medidas correctivas necesarias para reducir la frecuencia del fallo o para mitigar las consecuencias. Las acciones correctivas pueden incluir cambios en el diseño, procedimientos o modalidades de organización, tales como la adición de características redundantes y los métodos de detección, o puede ser sugerido un cambio en la política de mantenimiento Pág. 46, Col. Der., Párr. 3).
Ejecución del plan de implementación.	Las acciones correctivas pueden incluir cambios en el diseño, procedimientos o modalidades de organización, tales como la adición de características redundantes y los métodos de detección, o puede ser sugerido un cambio en la política de mantenimiento Pág. 46, Col. Der., Párr. 3).

De acuerdo con la tabla anterior, donde se comparan las características técnicas de la reivindicación 21 con la anterioridad D3, el método descrito en dicha reivindicación, ya era conocido en el estado de la técnica. Por lo tanto, la reivindicación 21 no es nueva.

De acuerdo al análisis anterior, la reivindicación dependiente es afectada por novedad por las razones dadas a continuación:

- Reivindicación 22: La identificación de los sucesos iniciadores es una tarea importante porque los perfiles de riesgo sólo se pueden obtener a través de la transformación de estos eventos en consecuencias. Los sucesos iniciadores son las interrupciones en el funcionamiento normal de la planta que requieren activación automática o manual de los sistemas de seguridad de la planta. Los eventos iniciadores debido a fallas de los sistemas activos y de apoyo también se incluyen. Un PRA completo maneja los sucesos iniciadores tanto internos como externos (D3, Pág. 45, Col. Der., Párr. 6). Dos métodos se pueden tomar para identificar sucesos iniciadores. El primero es una evaluación general de ingeniería, teniendo en cuenta la información de las evaluaciones previas de riesgo, la documentación que refleje el historial de funcionamiento y datos de diseño específicos de la planta. La información es evaluada y una lista de los sucesos iniciadores se compila. El segundo es un enfoque más formal. Esto incluye listas de control, como el análisis de riesgos preliminares, y los modos de fallo y análisis de efectos (D3, Pág. 45, Col. Der., Párr. 7 a Pág. 46, Col. Izq., Párr. 1).

Nivel Inventivo (Art 18 D 486)

La reivindicación 4 consiste en “El sistema de análisis de infraestructura de la reivindicación 1...” (Ver página 29 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D1	D2
Al menos una herramienta de colección de datos comprende una herramienta escogida entre el grupo de herramientas consistente en una cámara, un dispositivo GPS, un dispositivo	No se menciona	En aún otra realización de la presente invención, la adquisición de datos no sólo se toma de una fuente de datos y se correlaciona con las coordenadas

de levantamiento de planos, un probador del suelo, una herramienta para medir un potencial electroquímico de una estructura, una herramienta para medir la corrosión del metal, un aparato de medición de la profundidad del hoyo, un escáner, un dispositivo de medida del recubrimiento, una herramienta de medida de acidez del suelo, una herramienta de medida de oxidoreduccion del suelo, una herramienta de resistividad del suelo, un examinación “NDE” de una estructura, y un medio para transducir una inspección visual.	espaciales y temporales, sino a partir de múltiples sensores y fuentes simultáneas. Por ejemplo, un robot, como se explica más arriba podría grabar una vista de 360 grados de la tubería, ya que atraviesa el sistema, eliminando así la necesidad de parar en los cruces laterales y realizar panorámicas de una cámara en las direcciones de los laterales. Gracias al registro de múltiples ángulos de visión, como una vista de 360 grados, la necesidad de parar y las panorámicas de una cámara se eliminan (Pág. 4, Fl. 12, Párr. 41).
---	--

Los documentos D1 y D2 se consideran el estado de la técnica cercano a la invención definida en la reivindicación 4 porque divulgan que desde la liberalización del mercado energético un mayor número de actores con diferentes responsabilidades y el aumento de las transferencias de energía entre países, junto con una elevada proporción de generación dispersa y renovable están actualmente forzando a los sistemas de transmisión y distribución en Europa hasta sus límites. El aumento de la automatización crea una dependencia más alta en la infraestructura de las telecomunicaciones y aumenta la complejidad de las estructuras de dependencia y, como consecuencia el peligro de efectos en cascada, por ejemplo, causando apagones en toda la zona. Se requieren nuevas herramientas o una combinación inteligente de los enfoques existentes para aumentar la capacidad de supervivencia de las infraestructuras críticas. Este artículo describe algunos de los resultados de un proyecto de investigación europeo llamado IRRIS que fue dedicado a la reducción de riesgos críticos de las infraestructuras (D1, Pág. 1, resumen); y un sistema y un método que presenta un medio para acceder y revisar los datos registrados de una manera que apoye el análisis de la condición de los sistemas de infraestructura como la red de alcantarillado o en otros sistemas de tuberías. La presente invención proporciona además la posibilidad de ver una ubicación particular en un sistema de tuberías o conjunto de datos en diferentes puntos en el tiempo, apoyando así un análisis del deterioro y probablemente la prioridad de reparación de una sección particular de la infraestructura (D2, Pág. 1, resumen).

La diferencia entre la invención, definida en la reivindicación 4 y el sistema de D1 consiste en que no especifica la herramienta de colección de datos.

La diferencia entre la invención, definida en la reivindicación 4 y el sistema de D2 consiste en que el sistema es utilizado en un sistema de tuberías y no en un sistema de energía eléctrica.

El incluir la especificación de la herramienta de colección de datos no brinda ningún efecto técnico.

Sin embargo, la especificación de la herramienta de colección de datos, ya está divulgada en el documento D2 que se refiere a que en aún otra realización de la invención, la adquisición de datos no sólo se toma de una fuente de datos y se correlaciona con las coordenadas espaciales y temporales, sino a partir de múltiples sensores y fuentes simultáneas. Por ejemplo, un robot, como se explica más arriba podría grabar una vista de 360 grados de la tubería, ya que atraviesa el sistema, eliminando así la necesidad de parar en los cruces laterales y realizar panorámicas de una cámara en las direcciones de los laterales. Gracias al registro de múltiples ángulos de visión, como una vista de 360 grados, la necesidad de parar y las panorámicas de una cámara se eliminan (D2, Pág. 4, Fl. 12, Párr. 41).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la especificación de la herramienta de colección de datos de D2 en el sistema de D1 para llegar así al objeto de la reivindicación 4 de la solicitud. Por lo cual se considera obvia.

La reivindicación 19 consiste en “El sistema de análisis de la tubería según la reivindicación 16...” (Ver página 32 del radicado N° 13-284403-00000-0000).

Comparación de las características técnicas esenciales, con las del Estado de la Técnica:

Características esenciales	D2	D1
Una unidad de análisis del riesgo.	No se menciona	Estimador de riesgo (RE) el cual permite a los operadores procesar la información de los CI dependientes y enviar información crítica desde su propia red a los CI dependientes (Pág. 2, Col. Izq., Párr. 2, MIT Components). El RE combina y analiza la información de su CI principal, así como de CI dependientes. Estima el riesgo inmediato y el potencial en cascada y/o efectos crecientes, teniendo en cuenta la información en tiempo real (evaluación interna), la información de estado de otro CI dependiente, planificación de la información en todo el área, el mantenimiento programado, el pronóstico del tiempo, las huelgas, los grandes eventos públicos, vulnerabilidad de software/hardware y otros recursos de información pública (Pág. 2, Col. Izq., Párr. 5 a Col. Der., Párr. 1; Fig. 1).
Una unidad de análisis predictivo.	No se menciona	La herramienta de apoyo de decisión CRIPS (“CRIsis management and Planning System”) (Pág. 2, Col. Izq., Párr. 2, MIT Components). CRIPS evalúa la situación actual de las redes de suministro de energía analizando los resultados de la simulación del comportamiento de la red física y toma las decisiones correspondientes para asistir al operador de red en la detección temprana y en la toma de decisiones en situaciones de emergencia (Pág. 2, Col. Der., Párr. 2).
Una unidad de mitigación.	No se menciona	Analizador de conocimientos de incidentes (Pág. 2, Col. Izq., Párr. 2, MIT Components).

Los documentos D1 y D2 se consideran el estado de la técnica cercano a la invención definida en la reivindicación 19 porque divulgan que desde la liberalización del mercado energético un mayor número de actores con diferentes responsabilidades y el aumento de las transferencias de energía entre países, junto con una elevada proporción de generación dispersa y renovable están actualmente forzando a los sistemas de transmisión y distribución en Europa hasta sus límites. El aumento de la automatización crea una dependencia más alta en la infraestructura de las telecomunicaciones y aumenta la complejidad de las estructuras de dependencia y, como consecuencia el peligro de efectos en cascada, por ejemplo, causando apagones en toda la zona. Se requieren nuevas herramientas o una combinación inteligente de los enfoques existentes para aumentar la capacidad de supervivencia de las infraestructuras críticas. Este artículo describe algunos de los resultados de un proyecto de investigación europeo llamado IRRIS que fue dedicado a la reducción de riesgos críticos de las infraestructuras (D1, Pág. 1, resumen); y un sistema y un método que presenta un medio para acceder y revisar los datos registrados de una manera que apoye el análisis de la condición de los sistemas de infraestructura como la red de alcantarillado o en otros sistemas de tuberías. La presente invención proporciona además la posibilidad de ver una ubicación particular en un sistema de tuberías o conjunto de datos en diferentes puntos en el tiempo, apoyando así un análisis del deterioro y probablemente la prioridad de reparación de una sección particular de la infraestructura (D2, Pág. 1, resumen).

La diferencia entre la invención, definida en la reivindicación 19 y el sistema de D2 consiste en que no especifica que la unidad de infraestructura comprende una unidad de análisis del riesgo, una unidad de análisis predictivo y una unidad de mitigación.

La diferencia entre la invención, definida en la reivindicación 19 y el sistema de D1 consiste en que el sistema es utilizado en un sistema de energía eléctrica y no en un sistema de tuberías.

El efecto que logra el incluir especificar que la unidad de infraestructura comprende una unidad de análisis del riesgo, una unidad de análisis predictivo y una unidad de

mitigación es que permite evaluar una condición de corrosión, generar un informe de dicha corrosión y determinar un tipo de trabajo de mitigación.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D2 para evaluar una condición de corrosión, generar un informe de dicha corrosión y determinar un tipo de trabajo de mitigación?”.

Sin embargo, el especificar que la unidad de infraestructura comprende una unidad de análisis del riesgo, una unidad de análisis predictivo y una unidad de mitigación, para evaluar una condición de corrosión, generar un informe de dicha corrosión y determinar un tipo de trabajo de mitigación, ya está divulgado en el documento D1 que se refiere a un estimador de riesgo (RE) el cual permite a los operadores procesar la información de los CI dependientes y enviar información crítica desde su propia red a los CI dependientes (D1, Pág. 2, Col. Izq., Párr. 2, MIT Components). El RE combina y analiza la información de su CI principal, así como de CI dependientes. Estima el riesgo inmediato y el potencial en cascada y/o efectos crecientes, teniendo en cuenta la información en tiempo real (evaluación interna), la información de estado de otro CI dependiente, planificación de la información en todo el área, el mantenimiento programado, el pronóstico del tiempo, las huelgas, los grandes eventos públicos, vulnerabilidad de software/hardware y otros recursos de información pública (D1, Pág. 2, Col. Izq., Párr. 5 a Col. Der., Párr. 1; Fig. 1). La herramienta de apoyo de decisión CRIPS (“CRIsis management and Planning System”) (D1, Pág. 2, Col. Izq., Párr. 2, MIT Components). CRIPS evalúa la situación actual de las redes de suministro de energía analizando los resultados de la simulación del comportamiento de la red física y toma las decisiones correspondientes para asistir al operador de red en la detección temprana y en la toma de decisiones en situaciones de emergencia (D1, Pág. 2, Col. Der., Párr. 2). Analizador de conocimientos de incidentes (D1, Pág. 2, Col. Izq., Párr. 2, MIT Components).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría el especificar que la unidad de infraestructura comprende una unidad de análisis del riesgo, una unidad de análisis predictivo y una unidad de mitigación de D1 en el sistema de D2 para llegar así al objeto de la reivindicación 19 de la solicitud. Por lo cual se considera obvia.

6. Conclusión

Los requisitos de patentabilidad de la presente solicitud están afectados de acuerdo a las objeciones del numeral 3 y así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	Artículo 1	1 a 3, 5 a 8 y 20 4 y 19	Novedad/Nivel Inventivo Nivel Inventivo
D2	US 2005/0183028	11 a 18 4 y 19	Novedad/Nivel Inventivo Nivel Inventivo
D3	Artículo 2	9, 10, 21 y 22	Novedad/Nivel Inventivo
D4	US 2010/0088139	1	Nivel Inventivo

En cumplimiento del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir del día siguiente de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Se invita al solicitante se sirva indicar, si así lo considera, su renuncia al término faltante de sesenta (60) días para dar respuesta a este requerimiento y presentarla por escrito.

Finalmente, se le recuerda al solicitante que si como respuesta a este requerimiento llegara a modificar el capítulo reivindicatorio y éste contenga más de diez (10) reivindicaciones, no pagará la tasa de modificación voluntaria pero sí la correspondiente al pago por reivindicación adicional.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única No. 10 de 2001.



JOSÉ LUIS SALAZAR LÓPEZ
Director de Nuevas Creaciones (c)

El anterior requerimiento fue notificado por fijación en lista, de fecha 2014-08-19

Elaboró: Angelica Maria Ramirez
Revisó: Rosa Patricia Tellez Chavarro

Power System Survivability Increase with Intelligent Support Tools

Dellwing, H.¹; Geretshuber, S.¹; Schwaegerl, C.²; Seifert, O.²

Abstract — Since deregulation of the energy market an increased number of stakeholders with different responsibilities and increased cross-national power transfers along with high shares of dispersed and renewable generation are currently forcing European transmission and distribution systems to its limits. Increased automation creates a higher dependency on telecommunication infrastructure and enlarges the complexity of dependency structures and as a consequence the danger of cascading effects, e.g. causing area-wide blackouts.

New tools or an intelligent combination of existing approaches are required to increase the survivability of critical infrastructures. This paper describes some outcomes of a European research project called IRRIS that was dedicated to risk reduction of critical infrastructures. One promising application is the assessment and decision support tool CRIPS – realized as an expert system; it is based on network simulations realized with PSSTMSINCAL, an established tool to support the analysis and planning of electrical power, gas, water or heat networks. CRIPS assesses the current situation in power supply networks analyzing the simulation results of the physical network behavior and makes corresponding decisions; a possible common use-case is outlined and benefits of this application are shown.

Index Terms — Network simulation, situation assessment, critical infrastructure protection, decision making, emergency management, expert system

I. INTRODUCTION

With open access to deregulated markets increased power transfers are currently forcing European transmission systems to its limits. Renewable and dispersed generation supported with priority interconnection and access to the network according to legislation in almost all European countries additionally leads to network congestions, especially by large wind farms that are located i.e. in the North Sea far from load centers or by high shares of dispersed generation units in distribution networks that may reverse power flows. To achieve higher economic objectives the systems are also operated closer to their limits partly supported by increased network automation (monitoring and control) also known as 'smart grids'. As a result unexpected events, weak interconnections, high loading of lines, protection malfunction or problems with data transmission may cause the systems to loose stability – possibly leading to catastrophic failures or

black-outs as can be seen by the increased number of blackouts during the last years.

An increased number of stakeholders since deregulation of the energy markets with different responsibilities along with high shares of dispersed and renewable generation units also raise the danger of blackouts in distribution systems; thus intelligent software solutions are required also on distribution level.

In parallel, increased automation creates also a higher dependency on telecommunication infrastructure that vice versa relies on a secure electricity supply. Due to competition only a limited data exchange between neighbored utilities takes place.

Although many control and simulation systems for transmission and partly distribution systems already exist to secure electricity supply – special systems for control and systems which can be used as a “further support”, such as static and dynamic security assessment or the use of phasor measurement units (PMU). But, these systems are only dedicated to a special task, i.e. the estimation of power flows in the networks, or evaluation of the most recent dynamic behavior of the network. Current solutions don't consider dependencies from other critical infrastructures or neighbored utilities also involved in energy supply tasks. New tools or an intelligent combination of existing approaches are required to increase the survivability of interdependent critical infrastructures (CI).

II. THE EUROPEAN RESEARCH PROJECT IRRIS

Aims of the Project

To overcome this problem to increase the survivability of interdependent critical infrastructures a European research project called IRRIS (Integrated Risk Reduction of Information-based Infrastructure Systems) [1] was launched in February 2006 within the 6th Framework Program. The aim of IRRIS - that will end in July 2009 - is to develop methodologies, models and tools for the analysis, simulation and improved management of dependent and interdependent Critical Infrastructures. Middleware Improved Technology (MIT) will provide new communication and information processing facilities in order to manage CI dependencies and thus to mitigate the danger of blackouts in these networks.

¹ S. Geretshuber and H. Dellwing are with IABG, Germany, Einsteinstr. 20, 85521 Ottobrunn (dellwing@iabg.de).

² C. Schwaegerl and O. Seifert are with Siemens AG, Germany, P.O. 3220, 91050 Erlangen (christine.schwaegerl@siemens.com).

Today, Critical Infrastructures need highly sophisticated information and communication technologies for their management and control. But, though we encounter a growing importance of dependencies from and to other Critical Infrastructures there is nothing comparable on the control level. MIT shall close this gap: by providing a sophisticated communication platform for exchange of information between Critical Infrastructures, and by providing appropriate MIT add-on components to manage this information [2].

MIT Components

The main MIT components developed in IRRIS are

- MIT Communication Tool allowing different CI to exchange information;
- Risk Estimator (RE) which enables the operators to process information from depending CI and to send critical information from its own network to depending CI;
- the CRIPS decision support tool (“CRIsis management and Planning System”).
- Tools for Extraction of functional status – a simple data interface to SCADA and control systems; and
- Incident Knowledge Analyzer.

All MIT components are integrated into the simulation platform SimCIP (Simulator for Critical Infrastructure Protection applications). This is an agent-based simulation system based on the LAMPS (Language for Agent-based Simulation of Processes and Scenarios) language and the LAMPSYS agent simulation framework. These agents represent the components of critical infrastructures, their attributes and their behavior. Their connections can also be of different types allowing the description of different kinds of dependencies and thus the simulation of different scenarios on different CI models. Experiments on scenarios with SimCIP will validate how well MIT fit the needs of improved communication between depending Critical Infrastructures [2].

Communication between depending Critical Infrastructures is an essential element for improved dependency management and increased dependability – either for interdependencies between different infrastructures such as telecommunication and electricity network operators or between different stakeholders in electricity supply chain. The MIT communication backbone was designed and implemented for this purpose. Each CI has its own interface to the backbone and is enabled to send and receive messages from/to depending CI and process this information for their own purposes.

A key assumption for developing the risk estimator is that specific conditions within one CI may not be critical by themselves, but that they become critical in combination with other situations. Therefore, the RE combines and analyses information from its home CI as well as further dependent CI. It estimates the immediate risk and potential cascading and/or

escalating effects taking into account real-time information (internal assessment), status information from other depending CI, wide-area planning information, scheduled maintenance, weather forecast, strikes, major public events, software/ hardware vulnerability and other public information resources (Fig. 1).

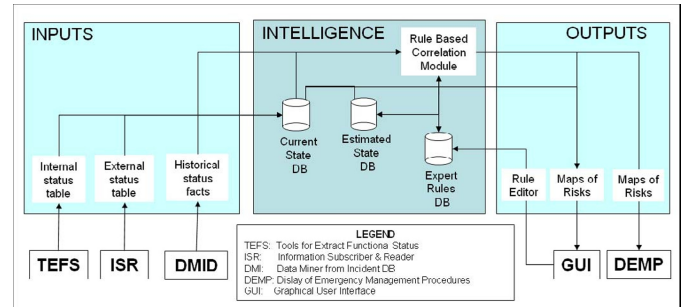


Fig. 1 Principle function of the Risk Estimator

III. THE EXPERT SYSTEM CRIPS

General Overview

The expert system CRIPS is based on steady-state network simulations realized with PSSTMSINCAL [3], an established tool to support the analysis and planning of electrical power, gas, water or heat networks. It calculates power flows in these networks based on the data of the components corresponding to physical laws. CRIPS assesses the current situation in power supply networks analyzing the simulation results of the physical network behavior and makes corresponding decisions to assist the network operator in early detection of and decision making in emergency situation. CRIPS does not use directly physical engineer-knowledge, its knowledge base represents the experience resulting from the operating of the system and corresponding crisis management exercises [4].

Simulation with PSSTMSINCAL

PSSTMSINCAL is well suited for the needs of both industry and utility companies. Typical user groups include municipal power companies, regional and national system operators, industrial plants, power stations and engineering consulting companies.

PSSTMSINCAL provides the system planner with high-performance tools for planning and design of supply networks for a variety of critical infrastructures – for gas, district heating, electrical power and water. It comprises powerful tools necessary for examining any network states and determining the most suitable network structure in normal and in emergency situations. The impact of switching operations can be analyzed and networks can be optimized with regard to losses and utilization.

Input data of the networks to be calculated, equipment data and graphics data for true-location or schematic network representation, as well as results of the various calculation methods - all data necessary for system planning - are stored in a commercial data base, thus data access by the expert

system is possible by standard methods. Vice versa, PSSTMSINCAL is easy to integrate in any data environment because it is a data base application.

Various steady-state and dynamic calculation methods such as power flow, short circuit, stability (RMS), Eigenvalues/modal analysis, harmonics, protection simulation, contingency analysis, reliability or cost analysis are available that allow the determination of weak points in the network, even under difficult circumstances, such as when several infeeds, transformer taps and poor supply voltages are involved. It is also possible to simulate the effect of time series (e.g. load curves) or time events (e.g. open circuit) on the network.

Calculation results can be depicted in different ways (e.g. tables, screen forms, diagrams and reports) and evaluated in the network diagram by means of coloring in accordance to predefined criteria. For instance, “traffic-light colors” can indicate the state of system elements, what is also taken as additional information for CRIPS.

Aim and Method of CRIPS

The basic assumption for CRIPS is that the operation of a power system is based on physical laws, but not every problem in the power networks can be described by physical laws.

The goal is to mitigate the danger of blackouts power networks by support of the

- **strategic assessment** of the current situation taking into account the dependency structure in the sense of “Can identified risks be accepted or not with regard to the goal?”;
- **strategic decision making** based on the assessment of the current situation; *strategic* means, that a local outage is not part of the goal.

CRIPS stores the experiences of experts in a knowledge base and so it makes sure, that this knowledge is immediately available in critical situations by the automatic evaluation (inference machine of the expert system). This knowledge is to support the assessment: “is a situation in the power supply critical with respect to danger of a blackout” and the corresponding decision making – as described above. Such knowledge usually is a *heuristic knowledge* and the canonical representation of this is accomplished by *if-then-else-rules*. So the core of CRIPS is an *expert system*, and the rule based representation of the knowledge takes into account the following observation ([4], [5], and [6]):

“..... knowledge bases from the real world often only include restricted clauses, so-called horn clauses ...”

$$A1 \wedge A2 \wedge A3 \wedge \dots \wedge An \Rightarrow B \quad (1)$$

A “horn clause” is a construction of the formal logic and the logical expression (1) is the most understandable way to describe it. It is a very simple formalism to describe

knowledge and the question arises “is this simple knowledge representation sufficient with respect to the goal”. Of cause, there may be some restrictions concerning the knowledge representation, but this formalism ensures e.g. a very effective and consistent maintenance of the knowledge base, which is necessary when there are essential changes in the networks. So the basic structure of rules about critical situations and decision is:

If data of components = value then critical situation is given

If critical situation is given then decision is recommended

This is a very basically description of the rule system but it describes the paradigm of the knowledge base. Taking into account the experience of other expert system developments we assume

With a set of such easy structured rules a sufficient support of the assessment of the current is possible (very good relationship “simplicity – efficiency”

Now what is a “given critical situation”? One possibility to define it is as “abnormal current data of indicator components”. An “indicator component” may be a power line, which caused a blackout in the past. But this is only one possibility. Already happened blackouts show that a critical situation can not be identified only by the evaluation of the current network data: A sequence of events – together with appropriate data – has to be taken into account.

And what is a “recommended decision”? It is assumed that the decision making takes place in control centers. A recognized critical situation forces a decision of the operators. The possible decisions have to be predefined, i.e. through emergency plans which contain a set of decision options or during crisis management exercises possible decisions had been identified.

The modeling of the knowledge base will be the task of a knowledge engineer. Prototypical experimentations support the thesis that a modeling of the assessment and decision support problem by simple structured horn clauses is possible, which guarantees sure and consistent maintenances of the knowledge base.

CRIPS – this is the current prototypical realization – is working in the background, no special user interface is necessary: The results can easily be integrated into already existing monitoring screens. The scanning rules are permanently applied the data of the corresponding grid for assessment.

Interaction CRIPS - PSSTMSINCAL

The structure of the interaction with PSSTMSINCAL is [4]:

- Caused by a special event or periodically operators in control centers start a simulation with PSSTMSINCAL, e.g. check of compliance with (n-1)-criterion in total grid or of a part of it, a loading analysis of lines, etc.
- Via interface the resulting values of the power flow simulation are available to CRIPS – no physical load flow results are transferred, only data which are indicators for a critical situation.
- CRIPS contains rules about so called “indicator components” for critical situations. The evaluation of the simulation data may indicate a critical situation. Currently only these components are used to make the assessment. The use of further criteria – independent from the status of indicator components – is in work.
- Depending on the critical situations different decisions are recommended.

CRIPS is working like a virus scanner to find critical data in a computer system. It evaluates permanently the result-tables of PSSTMSINCAL – or in real networks additionally the data of SCADA system – in order to find a critical situation. In this case, CRIPS generates a corresponding message and the proposed decisions.

The operator only receives a message about the situation and proposed, recommended, or possible decisions but, he makes “final decision”.

The Scanning Procedure of CRIPS

Fig. 2 demonstrates a scanning procedure of CRIPS that is displayed on the monitor of the CRIPS-Guard. This kind of output – to show all steps of the whole scanning process – shall only demonstrate the functionality. CRIPS should work in the background and only significant results are presented.

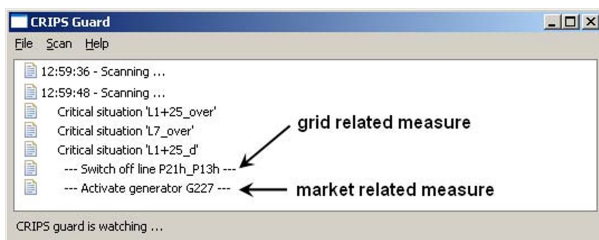


Fig. 2: Assessment and Decision Support with CRIPS

The CRIPS-Guard shown in Fig. 2 displays:

- At the beginning of the scanning (12:59:36) there is no critical situation identified, and so there are no recommended decisions.
- Then – because of changes in the grid – CRIPS finds a critical situation (and can give further explanations if wanted).

- Decisions are recommended, in this case one “grid related measure” and one “market related measure”.
- Scanning continues: The critical situations and the recommended measures are indicated until there is a change in the grid (e.g. by an operator).

Assessment of critical situations with fuzzy logic

A methodical benefit will be the use of *fuzzy logic*, especially for the evaluation of critical situations. Let us assume, that “load of a line” and “voltage at a busbar” are indicating data for a critical situation. There is no sharp switch e.g. at a certain value of the “load” from “100 % normal” to “100 % overload”; furthermore it’s more realistic to introduce so called “linguistic variables” (e.g. “normal” and “overloaded”), with degrees between 0 and 1. Such a *fuzzification* of “load”, “voltage” and the “assessment of the situation” is shown in Fig. 3.

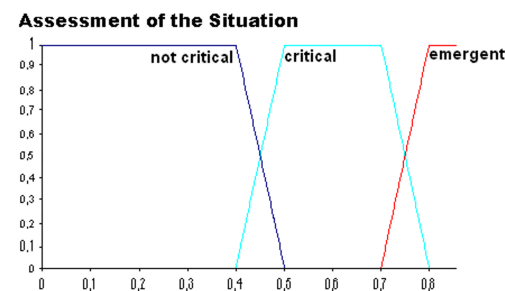
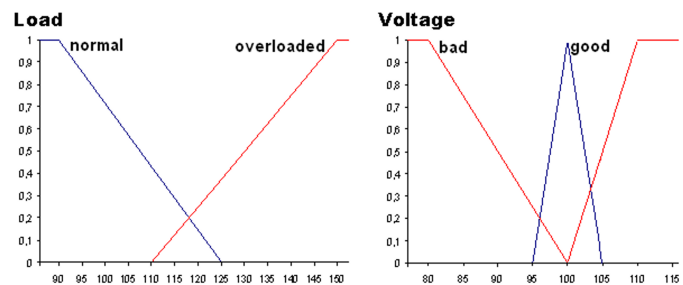


Fig. 3: Fuzzification

The method is demonstrated by a simple example:

Let us assume only one “fuzzy rule”:

$$\text{Load}=\text{overloaded} \wedge \text{Voltage}=\text{bad} \Rightarrow \text{Situation}=\text{critical}$$

Further we assume the input values

$$\text{Load} = 120 \wedge \text{Voltage} = 105$$

The evaluation of the corresponding fuzzy rule (inference) with fuzzified load and voltage inputs, to assess the current situation in the network e.g. as “not critical”, “critical” or “emergency” is shown in Fig. 4.

The “degree of criticality” is represented by the grey trapezium”. To get a numeric values – e.g. as input value for other rules – a “defuzzification” is to be done: Usually the center of gravity of the trapezium resp. of all resulting areas is calculated.

The use of fuzzy logic reduces the number of rules and it is the appropriate way to deal with “uncertainties” in the assessment and decision making processes.

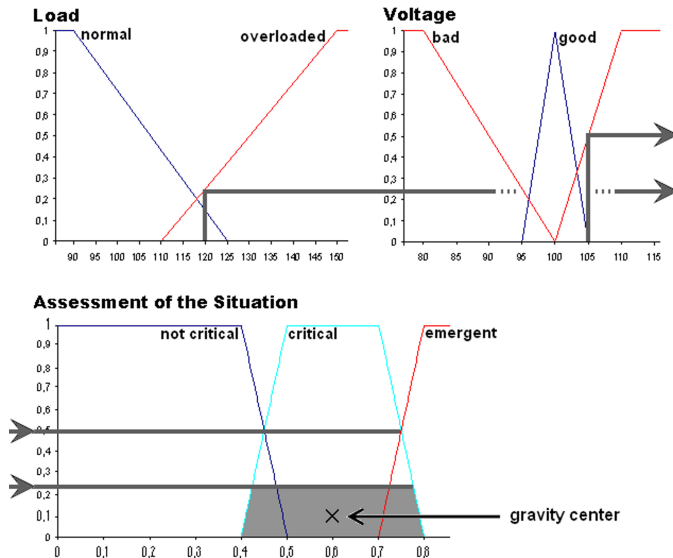


Fig. 4: Inference and defuzzification

IV. APPLICATION OF CRIPS

A possible common use-case for this application is outlined in this chapter and benefits for the network operator using this MIT-add-on-component are shown.

CRIPS is scanning in real time all relevant data (e.g. provided by SCADA systems, and the other MIT components described above to assess the current situation in order to identify critical situations which can be the beginning of a blackout and to give a decision support to decrease the criticalness. In case of an identified critical situation by the rule system appropriate messages about details of the situation and possible decision options occur on the monitors in the operation center.

As an example, the application is demonstrated with a 150 kV network as shown in Fig. 5, using PSSTMSINCAL as simulation tool.

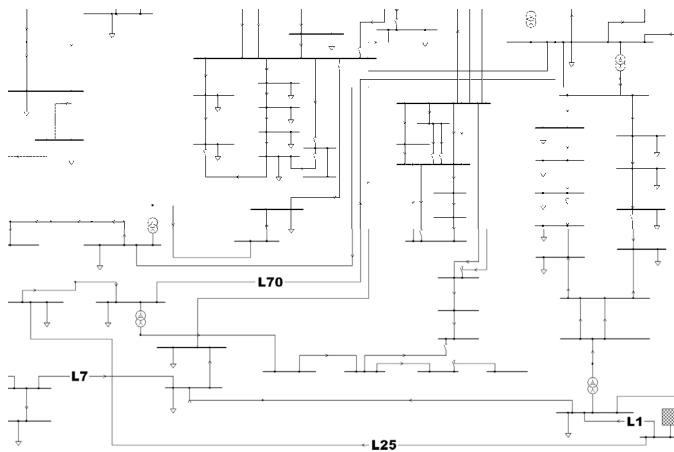


Fig. 5 Application of CRIPS - Example

Have a look at the Fig. 5:

- There may be a situation (e.g. caused by a natural catastrophe) of overloaded or dropped lines (L1, L25, L7 and others). The assessment of experts is – e.g. as a result of lessons learned – that a wide area blackout can be the result of this situation. Of course, not in any case – this is taken into account – this situation leads to a blackout.
- Let us assume that there is some experience – e.g. as a result of real events – with such a situation, and this experience is, that the described situation of overloaded or dropped lines is a critical situation in any case. So this knowledge becomes part of the knowledge base of CRIPS as corresponding rules. If such a situation occurs CRIPS detects a “critical situation”.
- After the drop of lines L1 and L25, there may be a decrease of the situation by topology measure (like the switching off line L7), but after the drop of line L7 the experience is, that in this situation only a drop of loads is the only possibility to avoid the blackout. This knowledge about “possible decision options” is part of the knowledgebase of CRIPS, too.
- Based on this knowledge base CRIPS is scanning the network data (and other information e.g. coming via MIT-components). If an overload or drop of the described lines is detected, the critical situation and possible decisions options are displayed.

Benefits for the operator resp. operation center are:

- The documentation e.g. of the analysis of real events (blackouts) or of the results of crisis management exercises as a knowledge base makes this knowledge automatic usable and so immediate available – a general benefit of the expert system method. CRIPS provides knowledge for the assessment of the situation and decision making.
- The knowledge base is not restricted to technical data as it is shown in the example (voltage and load). All available indicators from a critical situation can be taken into account (e.g. via interfaces to communication systems). All important data are available for the assessment and the corresponding decision making.
- As it is mentioned before – see the passage about “Horn clauses” – it is possible to create a “simple structured knowledge base”, which is an important condition for the maintenance of the knowledge.

V. CONCLUSIONS

New tools are required to increase the survivability of interdependent critical infrastructures, especially as modern 'intelligent' electricity networks depend highly on automation and communication solutions to cope with an increased number of participating stakeholders and high shares of renewable and dispersed generation.

It could be shown that with intelligent solutions that evaluate not only the results available and displayed in control centers, but also from other infrastructure operators i.e. from telecommunication or neighboring electricity networks the danger of blackouts in the networks can be mitigated. A good example for this is the application of CRIPS that provides benefits for the operator and increases the survivability of modern power systems.

CRIPS combines the physical analysis of a power network with an assessment and with a decision support in case of critical situations. Thus the whole spectrum of the operating of power networks can be covered. The physical analysis of the network is completed by an automatic provision of the knowledge of experts, resulting from experience and lessons learned concerning the management of critical situations ([4]).

VI. ACKNOWLEDGEMENT

The research described in this paper was partly funded by the EU commission within the 6th IST Framework Program in the IRRIS Integrated Project under contract No 027568. The authors thank the project partners for many interesting discussions which greatly helped to achieve the results described.

VII. REFERENCES

- [1] IRRIS: Integrated Risk Reduction of Information-based Infrastructure Systems, EU 6th framework research program, www.irris.org
- [2] R. Klein, et. al., Information Modeling and Simulation in large dependent Critical Infrastructures - an Overview on the European Integrated Project IRRIS, CRITIS 2008, Rome

- [3] PSSTMSINCAL system manual, description of the program, www.siemens.com/systemplanning (follow link software solutions)
- [4] Christine Schwaegerl, Olaf Seifert, Robert Buschmann, Hermann Dellwing, Stefan Geretshuber, Claus Leick, Increase of power system survivability with the Decision Support Tool CRIPS based on Network Planning and Simulation Program PSSTMSINCAL, CRITIS 2008, Rome
- [5] Hermann Dellwing and Walter Schmitz, J. Lopez and B. Hämmerli (Eds.): Expert system CRIPS: Support of Situation Assessment and Decision Making, CRITIS 2007, LNCS 5141, © Springer-Verlag Berlin Heidelberg 2008
- [6] Russel, S., Norvig, P.: Künstliche Intelligenz - Ein moderner Ansatz. Prentice-Hall, Englewood Cliffs (2004)

VIII. BIBLIOGRAPHIES

Hermann Dellwing studied from 1969 to 1976 mathematics and physics at the university of Saarbrücken, Germany; he received the diploma in mathematics in 1976. After an employment at the institute of applied mathematics at the university of Saarbrücken he was employed by IABG at 1980. His main field of work is "crisis management" with various subject areas. One of these subject areas is the concept and the realization of the computerized support of decision making in crisis situations using rule based methods (expert system).

Stefan Geretshuber received his Masters Degree in Systems Engineering in 2003 and his Diploma in Computer Sciences in 2000 both at the University of Applied Sciences Munich. Since 2001 he works as an IT consultant and systems engineer at IABG for a wide range of customers from public administration and the German defense area to the EU. His main areas of research activities there are the design and development of simulation systems and simulation models for critical infrastructures in the power and telecommunication domain.

Christine Schwaegerl received her Diploma in Electrical Engineering at University of Erlangen, Germany, in 1996, and her PhD from Dresden Technical University, Germany, in 2000, where she has been working in the field of energy management and dispersed generation. In 2000 she joined Siemens AG with development of substation automation. Since 2002 she works as consultant with Siemens Power Technologies International, responsible for the several national and international research and development activities on power transmission and distribution networks.

Olaf Seifert received his Diploma in Electrical Engineering at Dresden Technical University, Germany, in 1997 and was working there at Institute of Electrical Power Systems and High Voltage Engineering as research Engineer at the field of distribution grid planning and earth fault compensation. Since 2003 he is with Siemens AG where he works as consultant with Siemens Power Technologies International in the field of strategic planning of distribution networks, power quality and insulation coordination.

PRA for Vulnerability Assessment of Power System Infrastructure Security

Kang Lin, *Student Member, IEEE*, and Keith E. Holbert, *Senior Member, IEEE*

Abstract—Since September 11, 2001 the security of major national infrastructures has become a critical concern to government and industry. This paper reviews different types of threats (physical and cyber) and sources of these threats in electric power systems, describes the projects undertaken by the government and industry to address the security issues of the power system infrastructure, and presents a vulnerability assessment methodology for power networks. Finally, this paper considers probabilistic risk assessment (PRA) methods and the challenges to PRA, and proposes the use of PRA in electric power system vulnerability assessment.

Index Terms—Vulnerability assessment, PRA, Monte Carlo methods, event tree analysis, fault tree analysis.

I. INTRODUCTION

SINCE September 11, 2001, terrorist attacks have been considered a significant threat to the U.S. economy. Almost all economic and social functions depend on energy sources, telecommunication services, transportation, etc. An attack on these infrastructures would bring destructive effects on the economy and in people's lives [1,2].

Security of electricity supply networks has always been a key point in the development of the power industry. In recent years, the increasing development of supervisory control and data acquisition (SCADA) systems and energy management systems (EMS), the growing number of market participants, and the development of more complex market schemes have been increasingly reliant on information technologies (IT) and sensing equipment. Power networks are critically dependent on information and sensing equipment for system reliability, operation, protection and maintenance. In today's environment, utilities are increasingly concerned with intentional intrusions, and individuals and entities that are dedicated to bringing the system down. Such an environment is the type that has been expected by war planners, but not that anticipated by utility engineers. Hence, a rethinking is appropriate in trying to address such problems.

II. POWER SYSTEM INFRASTRUCTURE SECURITY STUDIES

A. Security and Vulnerability in Electric Power Networks

In the U.S. and elsewhere, the trend in the electricity

infrastructure is from a vertically integrated system to a horizontally integrated system. New markets have been developed relying upon more modern and aggressive models, requiring complex interaction between an increasing number of agents (generating companies, transmission companies, distribution companies, independent system operators, etc.). The decentralization of the property and the decision-making process rely on more complex and evolving IT. In parallel to the increase in the number of market participants, the electric industry has faced an increase in the number of SCADA/EMS systems, thereby raising the interdependency between the operation of the entire electric grid and the operation of the wholesale electric market. The electric power system and market are more closely tied and the operation of one depends on the continuous and reliable functioning of the other [3].

1) Threat definitions

Threats are defined as a potential for security violation, which exists when there is a circumstance, capability, action, or event that could compromise the well being of a network. A threat presents itself when an attacker/hacker has the ability to take advantage of existing security weaknesses or loopholes within a network. A threat that eventuates through cyber means into an offense can be regarded as a *cyber attack*, that is, an attacker accesses the system network from remote sites of the network. Similarly, a threat that results through physical ways into a violation can be regarded as a *physical attack*. Physical attacks occur as a result of an attacker physically accessing the system network and sabotaging the system either directly or through cyber methods [4].

2) Categories of cyber attacks

Today, the vulnerability of the power system is not simply a matter of the operation of the bulk electric power system, but increasingly a matter of cyber security. A market participant unable to accurately observe the market or a SCADA/EMS unable to properly control the facilities could be as disastrous as a terrorist attack to critical substations or transmission towers. As pointed out in [5-7], there are seven types of cyber attacks which are: denial of service (DoS), information leakage, regular file access, misinformation, database or special file access, remote arbitrary code execution, and elevation of privilege.

3) Threat actions and sources

A *threat action* is an assault on system security which could be an intentional behavior or an accidental event. The

K. Lin and K. E. Holbert are with Arizona State University, Department of Electrical Engineering, Tempe, AZ 85287-5706 (email: kang.lin@asu.edu and holbert@asu.edu).

intentional behaviors often include [4]: *masquerade*—the attacker, whether an insider or outsider, adopts the identity of a legitimate peer; and *interception*—the invader gains access to network information that is considered sensitive.

Terrorists and hostile nation-states pose a realistic threat to the electric energy sector. In 1997, the President's National Security Telecommunications Advisory Committee's Information Assurance Task Force determined that "Physical destruction is still the greatest threat facing the electric power infrastructure [8]." This still holds true as it is in accordance with known terrorist tactics, and high-yield targets in the electric energy sector lend themselves to physical assault; however, cyber threats have been mounting, especially if viewed in the context of compound attacks combining physical and cyber strikes.

Cyber threats could come from one of several groups [9]. *Hostile nation-states* have the resources, capabilities, and knowledge of management and control systems necessary to pose the most serious threat to electric energy sector. U.S. government officials assume that *cyber terrorists* are developing cyber attack capabilities, perhaps aided by hostile nation-states that share their beliefs and goals [10]. A small group of technically cognizant *hackers* with detailed knowledge of energy systems and networks, and experience in network penetrations and unauthorized intrusions, create a real threat to energy systems. Disgruntled or ex-employees (*i.e.*, *insiders*) with technical knowledge of control systems could also jeopardize the smooth functioning of energy systems.

B. Industry Initiatives

After September 11, 2001, many efforts have been initiated to protect the secure and reliable operation of electricity, gas, telecommunication, transportation, and financial infrastructures. The strong interdependence of these infrastructures can produce a cascading effect when one network is affected by a disturbance [1]. The goal of the industry and government initiatives is to develop new tools and techniques that will enable large national infrastructures to withstand threats, material failures, and other destabilizing factors. Some of these efforts are briefly presented below.

The Electric Power Research Institute (EPRI) has been conducting research in collaboration with electric utilities for increasing the security of the North American electric power infrastructure. EPRI's Infrastructure Security Initiative (ISI) research efforts focus on four key areas of concern [11,12]: (1) secure communications, (2) vulnerability assessment, (3) strategic spare parts inventory, and (4) "Red Team" attacks. Further, EPRI proposed to undertake a phased approach to develop advanced sensors and sensory networks (transducers, detectors, and data transmission paths) for use in transmission networks [13].

The North American Electric Reliability Council (NERC) has been responsible for the reliability of the interconnected grid since 1968. NERC plays a major role in protecting the electric system by serving as the focal point for coordinating

information exchange on critical infrastructure issues between the electricity industry and the federal government. NERC has undertaken several key initiatives (many of which began well before September 11) to focus attention on security matters and to encourage electric power industry participants to act. The missions commenced by NERC include [14]: (1) Electricity Sector Information Sharing and Analysis Center, (2) Critical Infrastructure Protection Committee, (3) security guidelines for the electricity sector, (4) cyber security standards, and (5) public key infrastructure.

With the increased focus on physical and cyber security, NERC created a compendium of best practices for protecting critical facilities against a spectrum of threats. A *critical facility* is defined as any facility or combination of facilities that if severely damaged or destroyed would [15]: have a significant impact on the ability to serve large quantities of customers for an extended period of time; have a detrimental impact to the reliability or operability of the energy network; or cause significant risk to public health and safety. The main components of the security guidelines are the following [16,17]: vulnerability assessment, threat response capability, emergency management, continuity of business processes, communications, physical security, IT/cyber security, employment screening, and protecting potentially sensitive information. The threat response guideline is based on the Threat Alert System of NERC [18,19].

In recognizing the national energy supply as vital to a strong economy and national security, the U.S. Department of Energy (DOE) established the Energy Security and Assurance (ESA) program. This program aims at protecting the nation against severe energy supply disruption. This is accomplished in close collaboration with the private sector, by providing technical expertise to [20]: identify system critical components and interdependencies; identify threats to the systems; recommend actions to correct or mitigate vulnerabilities; plan for response and recovery to system disruptions; and provide technical response support during energy emergencies. The ESA program is the initiative of DOE to develop and maintain a strategy for energy assurance in support of the President's National Energy Policy and to provide intradepartmental energy assurance activities.

III. VULNERABILITY ASSESSMENT FOR POWER NETWORKS

A power system can become vulnerable for various reasons, such as intrusion by external agents. These sources are either internal or external to the power infrastructure (see Fig. 1). As illustrated in Fig. 1, diverse causes from natural calamities to uncertain information in decision making can lead to catastrophic failures. The potential sources of system vulnerability are categorized in [21] as follows: natural calamities and weather conditions, major power system component failure, control and protection system failure, information/communication system failure, power system instability, human errors, inadequacy/error in system modeling and assessment, vulnerability in a competitive environment, and inability to obtain, synthesize, and use

reliable information.

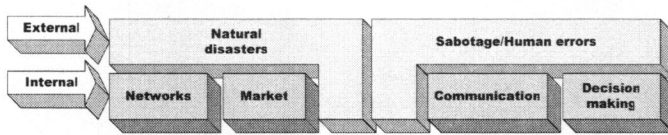


Fig. 1. Sources of vulnerability [21].

Fig. 2 provides an overview of the assessment methodology by DOE's Office of Energy Assurance (OEA). As shown, the methodology is divided into three basic phases: pre-assessment, assessment, and post-assessment. Each phase consists of a series of elements or tasks that have been designed to ensure comprehensiveness and confidentiality of the assessment results. Lessons learned are captured and used to enhance and, when appropriate, expand the technique. The specific elements or tasks associated with each assessment phase can be tailored to meet the assessment objectives. Although the methodology has incorporated unique elements that leverage the expertise of the national laboratories, the approach can be adapted for self-assessment.

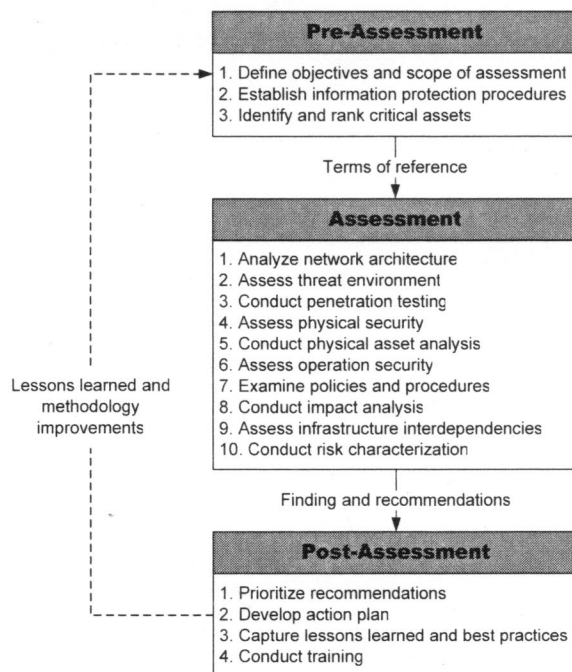


Fig. 2. Vulnerability assessment phases [22].

IV. PROBABILISTIC RISK ASSESSMENT IN VULNERABILITY ASSESSMENT

A. Probabilistic Risk Assessment

Over the last several decades, probabilistic risk assessment (PRA) has evolved into a technical discipline capable of logically, systematically, and comprehensively assessing the weaknesses and vulnerabilities of complex systems and facilities that can adversely impact safety, productivity and mission success. Its usefulness has been tested in many industries including aerospace [23], electrical generation [24], petrochemical [25], and defense [26]. The most useful

applications of PRA have been in complex systems subject to low-probability high-consequence scenarios or to complex scenarios consisting of chains of events that lead to adverse conditions or other impacts on the systems. Impacts may include those that appear to be slight or insignificant but collectively can interact to cause high severity consequences.

Risk is defined as the possibility of injury/damage or death/destruction to people/property. A general mathematical expression for risk is [27]

$$\text{risk} \left[\frac{\text{consequence}}{\text{time}} \right] = \text{frequency} \left[\frac{\text{events}}{\text{unit time}} \right] \times \text{magnitude} \left[\frac{\text{consequence}}{\text{event}} \right] \quad (1)$$

The risk analysis approach is only valid when dealing with a large database, which invokes the classical concept of long-run relative frequencies.

From a risk-analysis standpoint there can be no bad ending if there is a good beginning; however, there are a variety of bad beginnings in real life. In PRA, bad beginnings are called *initiating events* or *accident initiators* [28]. PRA is a methodology that transforms initiating events into *risk profiles*.

Fig. 3 shows a plant with four risk-mitigation features, which are normal control systems, emergency safety systems, physical barriers, and onsite and offsite emergency countermeasures. Initiating events are denoted as a *challenge*. Risk profiles for the plant result from correlating the *damage* done with the frequency of accident occurrence.

Identification of initiating events is an important task because risk profiles can only be obtained through transformation of these events into consequences. Initiating events are any disruptions to normal plant operation that require automatic or manual activation of plant safety systems. Initiating events due to failures of active and support systems are also included. A full PRA deals with both internal and external initiating events.

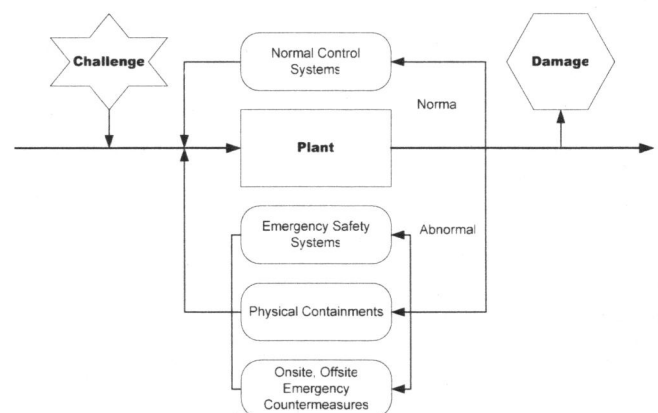


Fig. 3. Protection configuration for plant with catastrophic risks [34].

Two methods can be taken to identify initiating events [28]. The first is a general engineering evaluation, taking into consideration information from previous risk assessments,

documentation reflecting operating history, and plant-specific design data. The information is evaluated and a list of initiating events is compiled. The second is a more formal approach. This includes checklists, such as preliminary hazards analysis, and failure modes and effects analysis. Initiating-event studies vary among industries and among companies. Unless specific government regulations dictate the procedure, industrial practice and terminology will vary widely.

1) Preliminary hazards analysis

The only guideposts in achieving an understanding of initiators are sound engineering judgment and a detailed grasp of the environment, the process, and the equipment. Knowledge of toxicity, safety regulations, explosive conditions, reactivity, corrosiveness, and flammability is fundamental.

Initiating events lead to accidents in the form of uncontrollable releases of energy or toxic materials. Certain parts of a plant are more likely to pose risks than others. Checklists are used to identify uncontrollable releases and to decompose the plant into subsystems to recognize sections or components that are expected sources of an accident or initiating event.

If a checklist study is extended in a more qualitative manner to include consideration of the event sequences that transform a hazard into an accident, the study is called a *preliminary hazards analysis* (PHA). After identification, the hazards are characterized according to their effects. A common ranking scheme is [27]: Class I–negligible effects, Class II–marginal effects, Class III–critical effects, and Class IV–catastrophic effects.

2) Event trees and fault trees

There are two common analytical techniques: *event trees* and *fault trees* that are used in this stage. Consider the reactor safety study as an example [27]. It was determined that the critical portion of the nuclear reactor system is the reactor cooling system, so the risk study begins by following the potential course of events beginning with “pipe break”, the initiating event having a probability of P_A in the event tree (see Fig. 4). The numerical value of P_A is obtained by backward logic using fault tree techniques that will be discussed later. By working through the entire event tree, a spectrum of release magnitudes and their probabilities for the various accident sequences can be produced.

Event tree analysis (ETA) is used to define accident sequences that involve complex interrelationships among engineered safety systems, and are constructed using forward logic. The accident probability is obtained by backward (fault tree) logic. Fault tree analysis (FTA) is a graphical technique that provides a systematic description of the combinations of possible occurrences in a system, which can result in an undesirable outcome. This method can combine equipment and human failures. The most serious outcome (e.g., explosion, toxic release) is selected as the *top event*. A fault tree is then constructed by relating the sequences of events, which

individually or in combination, could lead to the top event. The undesired event appears as the top event which is linked to more basic fault events by event statements and logic gates.

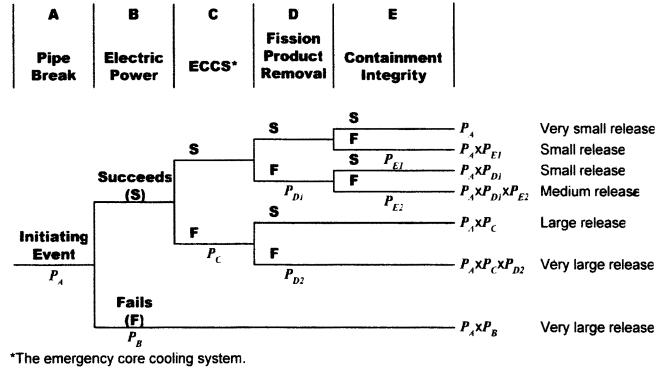


Fig. 4. The event tree for a nuclear reactor loss of coolant accident [27].

3) Failure modes and effects analysis and criticality analysis

Failure modes and effects analysis (FMEA) is an analytical technique that explores the effects of failures or malfunctions of individual components in a system. First, the system under consideration must be defined, so that system boundaries are established. Thereafter, the essential questions are [29]:

- How can each component/part fail?
- What might cause these modes of failure?
- What could the effects be if the failures occur?
- How serious are these failure modes?
- How is each failure detected?

A practical application of the FMEA technique would involve the completion of a worksheet in which the failure modes of individual components, such as relays and switches, are identified, evaluated and risk priority codes identified. A summary sheet can then be prepared in which failure modes are listed in declining order of risk priority codes. The summary should also list the corrective measures required to reduce the frequency of failure or to mitigate the consequences. Corrective actions could include changes in design, procedures or organizational arrangements, such as the addition of redundant features and detection methods, or a change in maintenance policy may be suggested.

FMEA is used for single point failure modes but can be extended to cover concurrent failure modes. FMEA can be a costly and time consuming process but once completed and documented it is valuable for future reviews and as a basis for other risk assessment techniques such as FTA and ETA.

Criticality analysis (CA) is the next step after a FMEA. Component rankings can be achieved by computing a *criticality number* C_r [27]:

$$C_r = \sum_{n=1}^N \beta \alpha \lambda_G t \quad (2)$$

where C_r is the criticality number for the system component in losses per million trials, n is the critical failure modes in the system component that fall under a particular loss statement, N is the last critical failure mode in the system component

under loss statement, λ_G is the generic failure frequency of the system component under loss statement, t is the operating time in hours or number of operating cycles of the component per mission, α is the failure mode ratio of critical failure mode, which is the fraction of λ_G attributable to the critical failure mode, β is the conditional probability that the failure effects of the critical failure mode will occur, given that the critical failure mode has occurred.

4) Summary and comparison of techniques

Table I is a summary of the various risk analysis techniques presented above. Note that FMEA, CA, and FTA are well-standardized and documented techniques, which are listed within the table in order of increasing sophistication. FTA is complex logic structures and its construction and quantitative analysis involves, minimally, a sound knowledge of Boolean algebra, set theory, and other advanced mathematical topics.

TABLE I
SUMMARY AND COMPARISON OF RISK STUDY TECHNIQUES [23]

Method	Characteristics	Advantages	Disadvantages
Preliminary hazards analysis	- Defines the system hazards and identifies elements for FMEA and FTA. - Overlaps with FMEA and CA.	A required first step.	None.
Failure modes and effects analysis	- Examines all failure modes of every component. - Hardware oriented.	- Easily understood. - Well accepted, standardized approach; non-controversial, non-mathematical.	- Examines non-dangerous failures. - Time consuming. - Often, combinations of failures and human factors not considered.
Criticality analysis	Identifies and ranks components for system upgrades.	- Well-standardized technique. - Easy to apply and understand. - Non-mathematical.	- Follows FMEA. - Frequently does not take into account human factors, common cause failures, system interactions
Fault tree analysis	Starts with initiating event and finds the combination of failures which cause it.	- Well-accepted technique. - Very good for finding failure relationships. - Fault oriented: looking for ways system can fail.	- Large fault trees are difficult to understand, bear no resemblance to system flow sheet, and are not mathematically unique. - Complex logic is involved.
Event tree analysis	Starts with initiating event and examines alternative event sequences.	Can identify (gross) effect sequences and alternative consequences of failure.	- Fails in case of parallel sequences. - Not suitable for detailed analysis.

B. PRA in the Nuclear Power Industry

The first PRA was the Reactor Safety Study (WASH-1400) [30], undertaken by a team headed by Prof. Norman Rasmussen under the sponsorship of the U.S. Nuclear Regulatory Commission (NRC), originally the Atomic Energy Commission. The NRC's responsibility is centered on ensuring that there is no undue risk to the health and safety of the public associated with the operation of commercial nuclear power plants or other facilities that it licenses. It does this by the application and enforcement of a set of technical requirements on plant design and operations.

PRA is a systematic process for examining how engineered systems, built and operated based on these requirements and practices, and human interactions with these systems work together to ensure plant safety. This process is quantitative, in that probabilities of events with potential public health consequences are calculated, as are the magnitudes of these potential health consequences. The risk of such events is the product of the event probabilities and their consequences. Information on this risk, and what failures contribute most to the risk, are of great value to the NRC in helping to determine the acceptability of a licensed facility's overall design and operation, as well as in focusing the agency's and the regulated industry's resources on those aspects of design and operation that are most risk-important.

PRA as an analytical tool includes consideration of the following [31]: identification and delineation of the combinations of events that, if they occur, could lead to an accident (or other undesired event); estimation of the chance of occurrence for each combination; and estimation of the consequences associated with each combination. As practiced in the field of nuclear power, PRAs generally focus on accidents that can severely damage the power plant's reactor core (containing the largest amount of radioactive material in the plant) and can also challenge the surrounding containment structures, since such events pose the greatest potential risk to the public. This technique, or related risk assessment techniques, can be used in the evaluation of all aspects of the fuel cycle, from fuel fabrication to high-level waste disposal. The PRA integrates into a uniform assessment tool the relevant information about plant design, operational practices, operating history, component reliability, human performance, the physical progression of accidents, and the potential consequences in as realistic a manner as practical.

PRA accounts for certain processes and phenomena that may have never occurred, or may occur infrequently, and may involve severe conditions that are difficult to replicate in experiments. Similarly, data on component or human behavior may not be available in sufficient quantities or for the circumstances of concern. Therefore, the results are inherently uncertain. PRA illuminates these uncertainties and

provides a way of considering them in regulatory decisions. The degree to which a detailed uncertainty analysis may be required will vary with the nature of the regulatory decision involved. Thus, analyses that depend only on the ability to separate the important from the obviously unimportant (e.g., prioritizing inspection efforts) may require only a general understanding of the magnitude of the uncertainty. Other applications, such as decisions regarding plant back fits, may require detailed uncertainty analyses.

C. Monte Carlo Methods

1) Introduction

Numerical methods that are known as Monte Carlo (MC) methods can be loosely described as statistical simulation methods, where statistical simulation is defined in quite general terms to be any method that utilizes sequences of random numbers to perform the simulation. MC methods have been used for centuries, but only in the past several decades has the technique gained the status of a full-fledged numerical method capable of addressing the most complex applications.

In many MC applications, the physical process is simulated directly, and there is no need to even write down the formulae that describe the system behavior. The only requirement is that the physical (or mathematical) system be described by probability density functions (pdfs). Once the pdfs are known, the MC simulation can proceed by random sampling from the pdfs. Many simulations are then performed and the desired result is taken as an average over the number of observations (which may be a single observation or perhaps millions of observations). In many practical applications, one can predict the statistical error (variance) in this average result, and hence an estimate of the number of MC trials that are needed to achieve a given error.

2) MC methods for system quantification—an example

The MC technique consists of building, usually with a computer program, a probabilistic model of the system under investigation. A trial run of the model is repeated many times, and each time the performance of the synthesized system is recorded. For example, suppose that it is desired to find the percentage of downtime for a system. It has been determined that the time between failures and repair time for the system follow, respectively, an exponential distribution with an expected time of 300 hours, and a normal distribution with an expected time of 24 hours and a standard deviation of 4 hours. The simulation can be designed to examine 30 independent periods of 10,000 hours each and report the percentage of downtime for each time period. A simple MC simulation is programmed here using these pdfs. There are only two states (normal and failed) of the system as shown in Fig. 5.

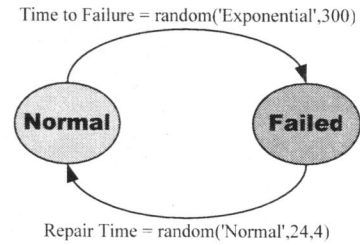


Fig. 5. The two states of the system.

The simulation starts when the system is Normal. After an operation period, generated according to an exponential distribution, the system changes to Failed. Afterward the system undergoes a time span of restoration produced from the normal distribution to return the system to the Normal state. The system moves alternately from one state to the other. The simulation time of each trial is the summation of all operation periods and restoration durations, while the total downtime of each trial is the summation of every restoration duration. Each trial ends when the simulation time equals or exceeds 10,000 hours.

Fig. 6 shows the percentage downtime for each of 30 trials. Fig. 7 presents the histogram (distribution plot) of the percentage downtime for 30 trials. Fig. 8 shows the distribution of the percentage downtime generated by increasing the total trials of the simulation by a factor of a hundred. From Fig. 8, it can be seen that the distribution looks more like a normal distribution than Fig. 7 does. This phenomenon agrees with the *central limit theorem* that states the sum of n independently distributed random variables will tend to be normally distributed as n becomes large [32]. A comparison between the MC results can be made. For 30 MC trials, the estimated downtime is $7.67 \pm 1.3\%$; for 3,000 trials the estimate is $7.42 \pm 1.25\%$.

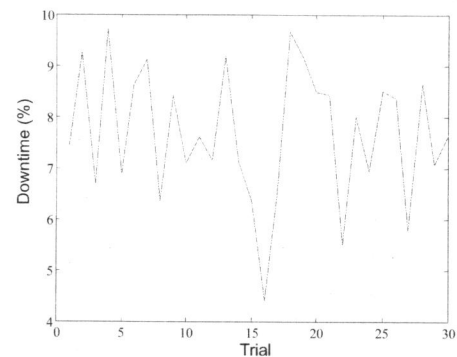


Fig. 6. The percentage downtime of each MC trial.

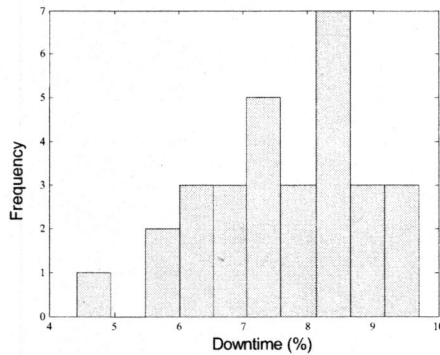


Fig. 7. Histogram of the percentage downtime for 30 MC trials.

D. Challenges to Probabilistic Risk Assessment

The approach taken in PRA is to decompose the system as a whole into subsystems and components (e.g., pumps and valves), stopping the decomposition at a point where substantial amounts of data are available for most of the components of the resulting model. Thus, for instance, although very few actual core melt accidents have been observed, it can be expected to find significant data on the frequencies of pump and valve failures, both during operation and routine testing. Using such data to estimate component failure rates, the resulting failure rates can then be aggregated according to the PRA model to derive an estimate of the overall frequency of accidents for the system.

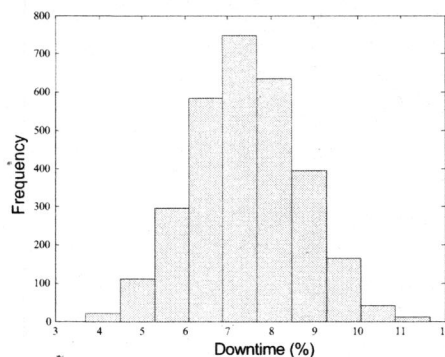


Fig. 8. Histogram of the percentage downtime for 3000 MC trials.

Apparently, the accuracy of the resulting estimated accident frequency depends decisively on the accuracy of the PRA model itself. If crucial failure modes have been neglected, the resulting estimate can be considerably lower than the actual accident frequency (i.e., a non-conservative result). Similarly, the model must make assumptions about such factors as the success criteria for the system, and about whether particular components fail independently or, conversely, whether failure of one component makes the others more likely to fail. Significant errors in any one of these assumptions can affect the accuracy of the resulting PRA estimates.

In addition to the model completeness issue, there are two major challenges to PRA [33]: the reliance on subjective judgment, and the difficulty of accounting for human performance in PRA models. Each of these issues is discussed below.

1) Use of subjective judgment

When individuals have different opinions, but must reach a common decision, it is unclear whose opinion is better or how the various opinions should be combined. This is not only a theoretical question, but one with both significant policy implications for how to effectively use PRA results in risk-based regulation and technical implications for how to choose the prior distributions used in PRA [33].

As described in [33], because of the complexity of the facilities being analyzed and the developing PRA models, even verifying or validating a PRA is a lengthy and costly task, comparable in scope to the level of effort required to perform the analysis in the first place, so the regulator is generally dependent on risk analyses carried out by facility owners/operators. Ignoring for purposes of argument the possibility of outright abuse or deliberate misrepresentations, the differing goals and incentives of the regulator and licensees, combined with the reliance on subjective judgment in PRA models, creates ample opportunity for licensees to shade PRA results in a favorable direction.

In addition to the difficult policy questions raised by the subjectivity of PRAs, there are also some technical issues. In particular, although analysts should ideally have good mechanistic reasons for their selection of distributional forms, PRA practitioners have sometimes treated the subjectivity of their inputs somewhat cavalierly [34]. Momentous guidance exists regarding the elicitation of subjective prior distributions from experts [35]. Similarly, the practice of pre-posterior analysis [36] can help to prevent the selection of unreasonable prior distributions. However, this guidance is complex and expensive to apply and is therefore sometimes ignored in practice [31]. Consequently, Bier [31] concluded that it makes sense to develop less resource-intensive methods of choosing prior distributions for use in PRA.

2) Human errors and human performance

Human error has been a causal factor in many large industrial accidents, including those at Three Mile Island [35] and Chernobyl [37], as well as others. Human errors are conventionally divided into two groups [33]: (1) *errors of omission*—neglecting to perform one or more steps of a well-defined procedure; and (2) *errors of commission*—deliberately undertaking an action not specified in procedures, with undesirable consequences. Errors of omission are relatively straightforward to model, since such errors can be explicitly enumerated based on a thorough understanding of the procedures to be performed by plant personnel at any given point in time. However, errors of commission have historically been considered difficult or impossible to analyze due to the infinite variety of actions that a person could conceivably undertake.

Recently, the majority of errors of commission have been recognized as “rational actions based on the operators’ understanding and perceptions of the plant status,” [38] and fall into a few reasonably well-defined categories. In particular, people are unlikely to undertake actions that do not

seem reasonable to them at the time, so most errors of commission are likely to reflect factors such as short-cuts, competing goals and incentives, and misdiagnoses [39]. While these causal mechanisms cannot be analyzed as easily as errors of omission, the recognition that most errors of commission do in fact have a rational basis makes them more amenable to analysis than was previously thought, and there have been several pilot studies incorporating errors of commission into PRAs [38].

Another issue that has been of concern to PRA practitioners is the effect of management and organizational (M&O) factors on risk, which is broader than just the influence of such factors on human error. At least for the commercial nuclear power plants (NPPs) in the U.S., corporate culture may have a stronger influence on risk than does the design of the plant itself. For instance, some of the worst mistakes at American NPPs have been blamed on a series of relatively minor foul-ups that plague poorly managed plants. Moreover, badly run plants also shut down more frequently, produce more contaminated waste, expose workers to more radiation, and produce less electricity [40].

V. SUMMARY

This paper presents reviews of power system infrastructure security and PRA methods and the challenges to the acceptance of PRA. PRA has been performed for naturally-occurring risks and for evaluating the safety of nuclear power plants, but not extensively applied for the type of risks imposed by other sources discussed in this paper. Therefore, we propose utilizing the PRA technique to address risks caused by those newborn threats in electric power systems.

VI. REFERENCES

- [1] A. Massoud, "Towards self-healing energy infrastructure systems," *IEEE Computer Applic. in Power*, vol. 14, no. 1, pp. 20-28, Jan. 2001.
- [2] A. Massoud, "Modeling and control of complex interactive networks," *IEEE Control Systems Magazine*, vol. 22, no. 1, pp. 22-27, Feb. 2002.
- [3] Comments of the North American Electricity Council, Nov. 2002. [Online] Available: www.nerc.com/~filez/cipfiles.html.
- [4] J. Fisher, *Vulnerability Assessment of Information Communication Networks in Power Engineering*, Thesis (M.S.), Arizona State University, Tempe, AZ, 2004.
- [5] S. Northcutt, M. Cooper, M. Fearnow, and K. Frederick, *Intrusion Signatures and Analysis*, New Riders Publishing, Indianapolis, 2001.
- [6] M. Ahmad, I. Dubrawsky *et al.*, *Hacking Proof Your Network*, Syngress Publishing, Rockland, 2002.
- [7] M. Bishop, *Computer Security: Art and Science*, Addison Wesley, Boston, 2003.
- [8] The President's National Security Telecommunications Advisory Committee, "Electric power information assurance risk assessment," March 1997 [Online]. Available: www.aci.net/kalliste/electric.htm.
- [9] E. Goetz, "Cyber security of the electric power industry," *Investigative Research for Infrastructure Assurance Group and Institute for Security Technology Studies Report*, Dec. 2002 [Online]. Available: www.ists.dartmouth.edu/library.
- [10] B. Gellman, "Cyber-Attacks by Al Qaeda Feared," *Washington Post*, p. A01, Thursday, June 27, 2002.
- [11] EPRI, "Infrastructure security initiative (ISI): promoting security for the electric power grid report," Oct. 2003 [Online]. Available: www.epri.com/OrderableItemDesc.asp?product_id=1009203.
- [12] EPRI, "Infrastructure security initiative under way," Nov. 2001 [Online]. Available: www.epri.com/journal/default.asp.
- [13] EPRI, "Advanced sensor system assessing vulnerability of power system—phase I," Sept. 2003 [Online]. Available: www.epriweb.com/public.
- [14] NERC, "Industry-government interface," [Online]. Available: www.nerc.com/cip.html.
- [15] G. Michael and C. Lynn, "Reflections on security," *IEEE Power & Energy Magazine*, vol. 1, no. 1, pp. 46-52, Jan.-Feb. 2003.
- [16] NERC, "Security guidelines for the electricity sector: version 1.0.," June 2002 [Online]. Available: www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf.
- [17] D. Watts, "Security & vulnerability in electric power systems," *Proc. of 35th North American Power Symp.*, pp. 559-66, Rolla, MO, Oct. 2003.
- [18] NERC, "Threat alert system and physical response guidelines for the electricity sector," Oct. 2002 [Online]. Available: www.nerc.com/~filez/cipfiles.html.
- [19] NERC, "Threat alert system and cyber response guidelines for the electricity sector," Oct. 2002 [Online]. Available: www.nerc.com/~filez/cipfiles.html.
- [20] DOE, "Energy security and assurance," [Online]. Available: www.mbe.doe.gov/budget/03budget/content/otherdef/esa.pdf.
- [21] C.-C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A. G. Phadke, "The strategic power infrastructure defense (SPID) system," *IEEE Control Systems Magazine*, vol. 20, no. 4, pp. 40-52, Aug. 2000.
- [22] DOE, "Vulnerability assessment and survey program. Overview of assessment methodology," Sept. 2001 [Online]. Available: www.esisac.com/publicdocs/assessment_methods/OEA_VA_Methodology.pdf.
- [23] J. Perera and J. Holsomback, "Use of probabilistic risk assessments for the space station program," *Proc. of IEEE Aerospace Conference*, vol. 1, pp. 512-517, March 2004.
- [24] Z. Pei, S. T. Lee, and D. Sobajic, "Moving toward probabilistic reliability assessment methods," *Proc. of 8th Intern. Conf. on Probabilistic Methods Applied to Power Systems*, Ames, IA, pp. 906-913, Sept. 2004.
- [25] F. I. Khan and T. Husain, "Risk assessment and safety evaluation using probabilistic fault tree analysis," *Human and Ecological Risk Assessment*, vol. 7, pp. 1909-1927, 2001.
- [26] R. W. Price, "Managing weapon system R&M in the post Cold-War environment," *Proc. of Reliability and Maintainability Symposium*, pp. 96-99, Jan. 1993.
- [27] E. J. Henley and H. Kumamoto, *Probabilistic Risk Assessment*, IEEE Press, pp. 8-43, New York, 1991.
- [28] H. Kumamoto and E. J. Henley, *Probabilistic Risk Assessment for Engineers and Scientists*, IEEE Press, pp. 95-115, New York, 1996.
- [29] The Institution of Electrical Engineers (IEE), "Quantified Risk Assessment Techniques - Part 1," Sept. 2004.
- [30] NRC, *Reactor Safety Study: An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants (WASH-1400)*, Washington, DC, 1975.
- [31] NRC, "Fact sheet on probabilistic risk assessment," June 2003 [Online]. Available: www.nrc.gov/reading-rm/doc-collections/fact-sheets/probabilistic-risk-asses.pdf.
- [32] D. C. Montgomery and G. C. Runger, *Applied Statistics and Probability for Engineers*, John Wiley & Sons, p. 690, New York, 2003.
- [33] V. M. Bier, "Challenges to the acceptance of probabilistic risk analysis," *Risk Analysis*, vol. 19, no. 4, pp. 703-710, 1999.
- [34] C. M. Thompson *et al.*, "The application of ATHEANA: A technique for human error analysis," *Proc. of IEEE Sixth Conference on Human Factors and Power Plants*, pp. 8-13, Orlando, Florida, June 1997.
- [35] A. Moselhi, V. M. Bier, and G. E. Apostolakis, "Methods for the elicitation and use of expert opinion in risk assessment," *Reliability Engineering & System Safety*, vol. 20, pp. 63-85, 1988.
- [36] J. Kemeny, *The Need for Change: Report of the President's Commission on the Accident at Three Mile Island*, Pergamon Press, New York, 1979.
- [37] P. P. Read, *Ablaze: The Story of the Heroes and Victims of Chernobyl*, Random House, New York, 1993.
- [38] J. Julius, E. Jorgenson, G. W. Parry, and A. M. Mosleh, "A procedure for the analysis of errors of commission in a probabilistic safety assessment of a nuclear power plant at full power," *Reliability Engineering & System Safety*, vol. 50, pp. 189-201, 1995.
- [39] K.-S. Hsueh and A. M. Mosleh, "The development and application of the accident dynamic probabilistic risk assessment of nuclear power plants," *Reliability Engineering & System Safety*, vol. 52, pp. 297-314, 1996.

- [40] D. Wessel, "Study in contrasts: Pilgrim and Millstone, two nuclear plants, have disparate fates. Different management styles cause the first to be shut while the second thrives—Matter of 12,000 little things," *The Wall Street Journal*, vol. 1, pp. 14, July 28, 1987.

VII. BIOGRAPHIES

Kang Lin was born in Tainan, Taiwan. He received his B.S. in 1999 from National Sun Yat-Sen University, Kaohsiung, Taiwan and M.S. from Arizona State University, Tempe, USA. He is currently a Ph.D. student at Arizona State University.

Keith E. Holbert is currently an Associate Professor in the Electrical Engineering Department of Arizona State University. He earned his Ph.D. in nuclear engineering from University of Tennessee in 1989. His research interests focus on power plant instrumentation, signal processing, and fuzzy logic applications for power plants. Dr. Holbert is a registered professional engineer. He has published more than 50 journal and conference papers.