MODELO Y CUANTIFICACIÓN DEL VAR OPERATIVO EN EL AREA TECNOLOGICA DE LAS REDES DE TRANSMISIÓN ELECTRICA.

ING.JUAN PABLO VÉLEZ URIBE

Director
Ph.d Santiago Medina Hurtado

Trabajo de grado presentado como requisito
para optar al título de Magister en Ingeniería Administrativa

Universidad Nacional de Colombia
Sede Minas
Medellín
2013

RESUMEN

Esta investigación presenta 2 modelos para la cuantificación de fallas de producto en los sistemas SCADA, para el monitoreo de la líneas de transmisión de energía, en esta se caracterizan las fallas más frecuentes presentadas que son las de infraestructura y software, la cuales son muy relevantes para las empresas de transmisión debido a que la información que estas entregan es de gran importancia para la toma de decisiones de la demanda de energía que deben suministrar.

De la exploración del estado del arte acerca de las fallas en las líneas de transmisión se aprecia que los estudios para determinarlas han sido por medio de redes neuronales, Smart grid y SCADA, sin embargo todos las investigaciones se han basado en resultados generales y cualitativos que dejan por fuera elementos que pueden ser de gran importancia y cuantificables. Por tal motivo utilizamos el análisis de las fallas en SCADA en específico de software y de infraestructura tomando una serie de tiempo de 694 y procesándola por medio de tratamientos estadísticos para obtener resultados numéricos que nos permitan simular por medio de @ Risk los datos y así obtener de forma clara y ordenada la información de las frecuencias de fallas y la duración de cada una de estas en el periodo en que se presentan, así como también se puede proyectar un número n de simulaciones para predecir el comportamiento de las fallas en el futuro.

Esto le permite a las compañías que transmiten energía, tomar decisiones más precisas antes y durante el momento que se presenta una falla en las líneas de transmisión con el fin de minimizar los riesgos y evitar sobrecostos innecesarios.

ABSTRACT

This research presents two models for quantification of product flaws in SCADA systems for monitoring of power transmission lines , with the most frequent failures are presented and the software infrastructure are characterized , which are the relevant for transmission companies because the information they deliver is of great importance for decision making of energy demand to be supplied .

Exploration of the state of art about the faults in transmission lines shows that the studies were to determine them by means of neural networks, SCADA and Smart Grid , but all investigations have been based on general results and qualitative leave out items that may be of great importance and quantifiable . Therefore we use the analysis of the flaws in SCADA software specific infrastructure and taking a time series of 694 and processing it through statistical treatments to obtain numerical results that allow us to simulated using @ Risk data and to obtain in a clear and orderly information failure frequencies and duration of each of these in the period in which they occur, also can also project n number of simulations to predict the behavior of failures in the future.

This allows companies that transmit energy, make more accurate before and during the time that a fault in the transmission lines in order to minimize the risks and avoid making unnecessary costs is presented.

DEDICATORIA

A DIOS quien me ha dado la fuerza y la tenacidad para afrontar cada uno de los retos que he tenido en mi vida, a mi familia que es mi más grande motivación para alcanzar mis metas y a todas aquellas personas que día a día me brindan su apoyo y solidaridad para hacer de mí una persona exitosa.

AGRADECIMIENTOS

Deseo expresar mis más sinceros agradecimientos al Doctor Santiago Medina Hurtado quien me oriento y me apoyo en todo el proceso de realización de la maestría como tutor.

También agradezco a las siguientes personas quien con sus aportes y consejos me ayudaron a desarrollar este trabajo de la mejor manera posible.

Profesor: Luis Diego Vélez
Ingeniera: Jakeline Lopera Jaramillo

Y a quien me brindó su apoyo incondicional y me formo como ingeniero, a quien considero parte de mi familia y mi punto de referencia para seguir luchando como persona y profesional.
Ingeniero: Guillermo León Mesa Betancur

A todos los que de una u otra forma estuvieron conmigo y me brindaron sus conocimientos para alcanzar esta gran meta.

Contenido

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE GRAFICOS

CAPITULO I

1.1 INTRODUCCIÓN

El valor del riesgo operativo, está asociado a las fallas que se pueden presentar en el funcionamiento normal de cualquier empresa por un sin número de razones. La gestión y cuantificación de estos se ha centrado en el sector financiero, sin embargo cualquier empresa del sector real está expuesta a estos riesgos y no se gestionan ni se cuantifican los costos de estas fallas y sus efectos sobre las utilidades de las empresas, además no hay un sistema, o metodología de monitoreo y control que integre todas las posibles fallas clasificadas e identificadas en el sector de la energía eléctrica, así como tampoco existe un modelo especifico que permita integrar la incidencia de todas las variables críticas para predecir y evitar fallos o accidentes en los sistemas de transmisión, lo cual permitiría detectar la ubicación de estas y así disponer de los recursos físicos, de infraestructura y de personal para asistir el tramo que presente el problema y dejarlo habilitado en el menor tiempo posible.

La disponibilidad de energía en un país es un factor crítico, ya que está ligada al funcionamiento y desarrollo de empresas, colegios, hospitales, entidades gubernamentales, educativas y financieras que son las que impulsan el desarrollo sostenible de estos y le permiten posicionarse a nivel global, por tal motivo se debe ver con detenimiento los efectos que causarían el corte de energía parcial en un sector determinado.

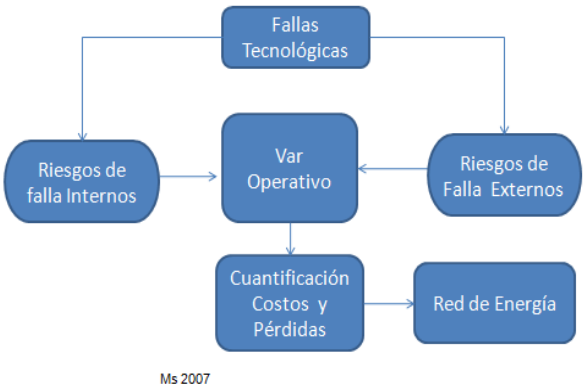
Por este motivo se estudia y analiza esta área con la finalidad de darle solución a este tipo de problemas y minimizar el riego de ocurrencia dentro del sistema interconectado de energía.

1.2 ANTECEDENTES

El VaR operativo es incluido en el sector energético como una herramienta de análisis de datos para la toma de decisiones en tiempo real, pero su estructuración

es generalizada y no han podido hallar un modelo único que de certeza y precisión para determinar los incidentes, como respuesta se desarrolla la implementación del VaR en el área Tecnológica de las redes de Transmisión, para determinar los costos económicos y financieros de las posibles fallas asociadas y la conexión entre áreas para lograr un diagnostico eficaz y crear un modelo que facilite la toma de decisiones y genere confiabilidad en la operación del sistema.

Figura 1. Esquema de VaR en Fallas Tecnológicas



Se entiende por Riesgo Operativo la probabilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o acontecimientos externos.[1] y por VaR (Valor en Riesgo): VaR nos Permite medir la máxima perdida potencial, expresada en unidades monetarias ($) que puede experimentar el valor futuro de un portafolio o cartera de inversión dado un cierto nivel de confianza y dentro de un periodo de tiempo determinado [2], [3].

El riesgo operativo está asociado a las fallas que se pueden presentar en el funcionamiento normal de cualquier empresa por errores humanos, caídas en el sistema, fallas en procesos, mal manejo de clientes, etc. [1], [2], [3]. La gestión y cuantificación de estos riesgos se ha centrado en el sector financiero sin embargo

cualquier empresa del sector real está expuesta a estos riesgos y por lo general no se gestionan ni se cuantifican. Para el sector eléctrico es de vital importancia caracterizar los diferentes tipos de variables que pueden afectar el mercado y operación del sistema y sus efectos financieros; mediante indicadores que permitan medir la vulnerabilidad del sistema mostrando el nivel de riesgo [4] y sus efectos financieros. El desconocimiento y mala gestión de riesgos puede ocasionar altos costos para la empresa por ejemplo hasta septiembre de 2010 la demanda no atendida en Colombia fue de 3.9 GWh, de la cual el 74.40% correspondió a causas no programadas asociadas a eventos operativos o de falla [5] en el sistema de generación, transmisión y distribución, que en algunos casos terminaran en un blackout. Los costos de estas fallas y sus efectos sobre las utilidades de las empresas no están cuantificados [6], la demanda no atendida genera pérdidas para todos los entes del mercado, por otra parte las empresas generadoras se exponen a tener que pagar multas, sanciones o se ven involucradas en procesos legales de los entes reguladores.

1.3 MOTIVACION

Las redes de transmisión de energía eléctrica hacen parte de la infraestructura fundamental para el desarrollo económico, social, político y cultural de un país. Estas redes cumplen la función de llevar la energía desde los centros de generación hacia las ciudades principales y los pueblos con el objetivo de suministrar energía a las compañías, entidades, universidades, colegios, hospitales, empresas, hogares y otras instituciones que dependen en gran parte del suministro continuo de esta para el funcionamiento de la maquinaria, equipos y el desempeño de sus actividades, estas redes en ocasiones se ven afectadas e interrumpidas por factores tales como :

Los técnicos

Los tecnológicos

Los ambientales

Los humanos

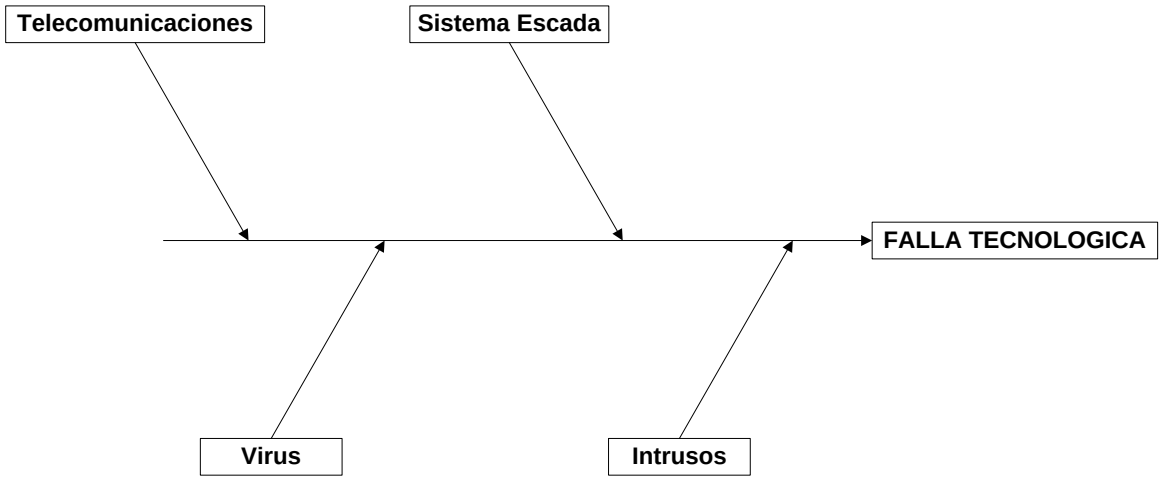
Ocasionando inestabilidad en el flujo eléctrico y en el peor de los casos apagones súbitos que generan un impacto negativo sobre todos los usuarios, trayendo esto como consecuencia, pérdidas económicas, retrasos y demandas contra las empresas que prestan los servicios de transmisión y distribución de energía. Aunque las empresas poseen gran cantidad de información de las anormalidades, fallas, apagones y todos los eventos asociados a estos, no han caracterizado las variables críticas y la relación que existe entre la información cualitativa y la cuantitativa para predecir que se presentara un evento fortuito a corto o a largo plazo.

Los factores tecnológicos de las redes de energía son un punto crítico ya que por medio de estos se puede determinar, predecir o anticipar que un evento de falla se presente. Existen diversos métodos para la captura, transmisión y reporte de datos en las redes, algunos de estos están basados en inteligencia artificial, lógica difusa, redes neuronales, redes bayesianas, sin embargo no hay una metodología que pueda cuantificar los eventos cualitativos y arrojar resultados precisos o exactos para determinar el riesgo. Estos métodos se integran con las redes de comunicación y los sistemas para interactuar con las centrales de control y por medio de una interfaz mostrarle a los controladores las anormalidades o comportamientos atípicos que está presentando la red, esto determina la toma de decisiones para prevenir los riesgos y genera un mejoramiento continuo en la operación. El uso del modelo basado en redes de petri, tiene como objetivo cuantificar la información cualitativa y procesarla para reducir los riesgos y tomar acciones preventivas que eviten fallas o apagones súbitos en el sistema.

1.4 PLANTEAMIENTO DEL PROBLEMA

En el trabajo de esta tesis nos ocupamos del modelamiento y la cuantificación del Var Operativo asociado a los factores tecnológicos en redes de transmisión eléctrica, en especial en los mencionados a continuación:

Figura 2. Espina de pescado del planteamiento del problema



Las fallas tecnológicas se pueden producir por cualquiera de los siguientes motivos:

1.4.1 SISTEMA SCADA [7]

Los sistemas SCADA originalmente se diseñaron para cubrir las necesidades de un sistema de control centralizado, sobre procesos o complejos industriales distribuidos sobre áreas geográficas muy extensas. Tal es así que en la definición clásica de un sistema SCADA se hace referencia a esta característica. Hoy en día con el desarrollo de las redes digitales, la definición se tiene que modificar para incluir esta nueva forma de conectividad.

Definición

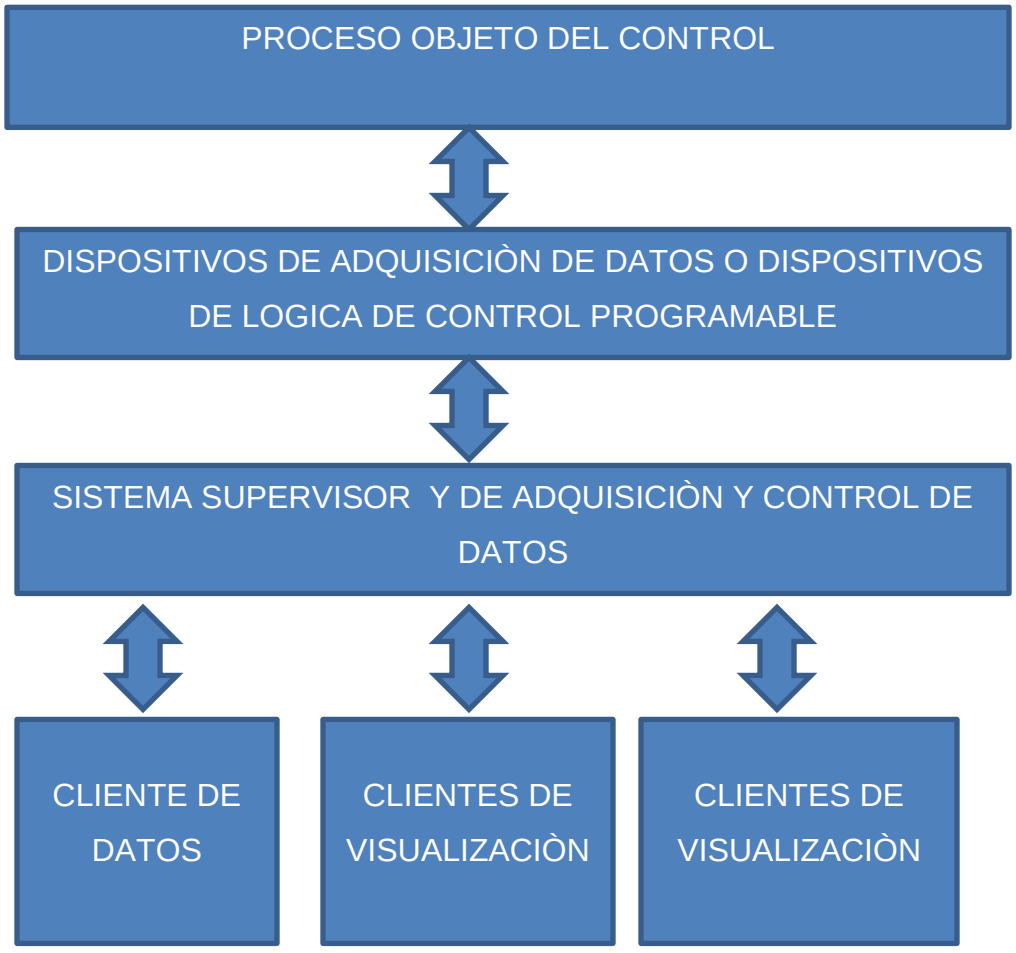
SCADA viene de las siglas “Supervisory Control And Data Acquisition”, es decir: hace referencia a un sistema de adquisición de datos y control supervisor. Tradicionalmente se define un SCADA como un sistema que permite supervisar una planta o proceso por medio de una estación central que hace de Master (llamada también estación maestra ò unidad terminal maestra, MTU) y una o

varias unidades remotas (generalmente RTUs) por medio de las cuales se hace el control/ adquisición de datos hacia/ desde el campo.

Si bien las topologías sobre las que se sustentan los sistemas SCADA se han adecuado a los servicios de los sistemas operativos y protocolos actuales, las funciones de adquisición de datos y supervisión no han variado mucho respecto a lo que proponían en sus inicios.

Esquemáticamente un sistema SCADA conectado a un proceso automatizado consta de las siguientes partes:

Figura 3. Esquema de un sistema SCADA



1. Proceso objeto de control: Es el proceso que se desea supervisar. En consecuencia es el origen de los datos que se requiere colectar y distribuir.
2. Adquisición de datos: Son un conjunto de instrumentos de medición dotados de algunas interfaces de comunicación que permiten su interconexión.
3. SCADA: Combinación de Hardware y Software que permita la colección y visualización de los datos proporcionados por los instrumentos.
4. Clientes: Conjunto de aplicaciones que utilizan los datos obtenidos por el sistema SCADA

Un término clave en la definición, al que muchas veces no se le da adecuada atención, es el de supervisión, que significa que un operador humano es el que al final tiene la última decisión, generalmente críticas. La importancia de esta definición está en que se contrapone a la idea generalizada, que a veces si se hace, de que en la unidad Master se hace control automático del proceso supervisado.

Es cierto que puede hacerse control automático pero debe evaluarse suficientemente su implementación, tomando sobre todo en consideración la confiabilidad de los enlaces (en particular si son de larga distancia) que transportan los datos y comandos desde y hacia el campo. Una falla de comunicación, significaría dejar fuera de control el proceso. Esto explica por qué ahora la industria favorece a los sistemas de control distribuidos. [8]

Tipos de sistemas SCADA

A. Sistemas SCADA Monolíticos

Los primeros sistemas SCADA ejecutaban todas las operaciones en una sola computadora, por lo general un ordenador central. Se ejercía poco control y la mayoría de las funciones de los primeros sistemas SCADA se limitaban a los sensores de control y el marcar las operaciones que superaban los niveles de

alarma programados. Estos sistemas eran todos programas de propiedad del proveedor y por lo general se limitaban a una sola planta o instalación. Al igual que los programas, los equipos SCADA de un proveedor rara vez se podían utilizar en el sistema SCADA de otro proveedor.

B. Sistemas SCADA distribuidos

Más tarde, los sistemas SCADA se conocieron como sistemas distribuidos, ya que solían compartir las funciones de control a través de varios ordenadores más pequeños (generalmente PC) conectadas por redes de área local (LAN). Usando redes LAN, las estaciones individuales compartían información en tiempo real y a menudo realizaban pequeñas tareas de control, además de alertar a los operadores de los posibles problemas o niveles de alarma disparados.

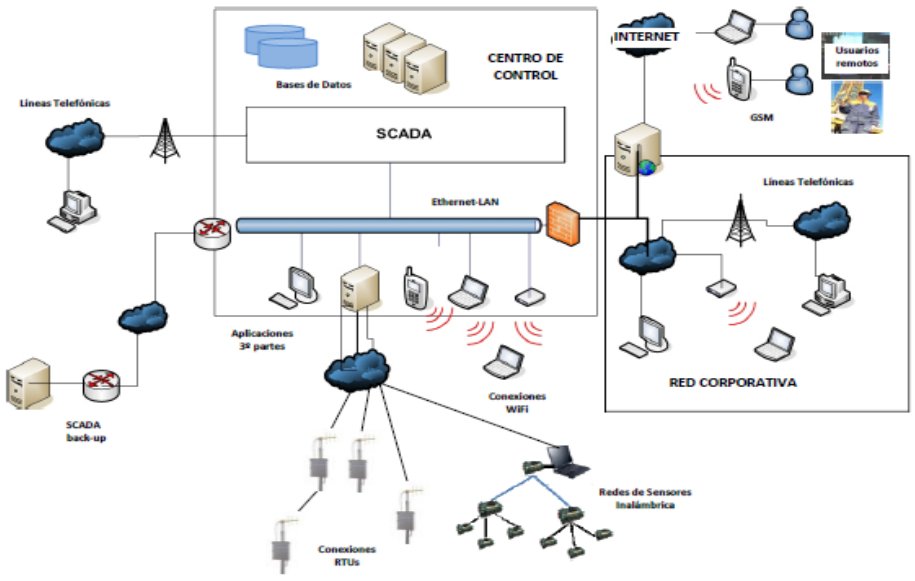
C. Red de sistemas SCADA

Los sistemas SCADA actuales están generalmente conectados en red. Se comunican a través de sistemas de redes de área amplia (WAN), a través de líneas telefónicas o de datos y a menudo transmiten datos entre los nodos a través de Ethernet o conexiones de fibra óptica. Los sistemas SCADA en red hacen un uso intensivo de los Controladores Lógicos Programables (PLC) para monitorear y hacer ajustes de rutina de los procesos, sólo marcando y avisando a los operadores cuando se requieren tomar decisiones importantes. A diferencia de versiones anteriores de los sistemas SCADA, que utilizaban principalmente programas del proveedor y algunas veces sus equipos, los sistemas actuales se basan más en los programas de uso general. Los equipos tienden a ser más intercambiables, ya que los proveedores de PLC y otras subunidades tienen sistemas de comunicación y protocolos estandarizados para permitir al usuario elegir el mejor componente para sus necesidades en lugar de estar atado a la línea de productos de un sólo proveedor. Mientras que los sistemas SCADA anteriores se limitaban a un solo edificio o algunas veces a redes individuales en un sólo sitio, muchos de los sistemas SCADA actuales se conectan a Internet, lo que aumenta los riesgos de seguridad, lo cual no se veía en los sistemas más antiguos o "sellados".[9],[10]

Problemas presentados en los sistemas SCADA

- Grandes cantidades de Información
- Incertidumbre en la Información
- Correlación de Múltiples variables Complejas
- Entrenamiento difícil y costoso
- Deficiencias en las conclusiones sobre las secuencias y detalles de los eventos.

Figura 4. Estructura de Comunicaciones de un Sistema SCADA [11]



1.4.2 TELECOMUNICACIONES [12]

El concepto de telecomunicación abarca todas las formas de comunicación a distancia. La palabra incluye el prefijo griego tele, que significa “distancia” o “lejos”. Por lo tanto, la telecomunicación es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional

de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones.

Dentro del ámbito de las telecomunicaciones es importante que se conozca la importancia de la variedad del material físico que se utiliza en las mismas. De él, de su calidad y de sus prestaciones, depende el éxito del proceso y en este sentido ello conlleva a que sea necesario el estudio de una serie de pautas y criterios para apostar por el material más adecuado. En concreto, los expertos en dicha área tienen que proceder a analizar concienzudamente lo que son los costos, la seguridad, la capacidad que tiene, los errores que puede traer consigo o también la facilidad de uso que tiene.

La historia de las telecomunicaciones comenzó a desarrollarse en la primera mitad del siglo XIX, con el telégrafo eléctrico (que permitía enviar mensajes con letras y números). Más adelante apareció el teléfono, que agregó la posibilidad de comunicarse utilizando la voz. Con las ondas de radio, la comunicación inalámbrica llegó para completar una verdadera revolución en los hábitos de la humanidad.

Por supuesto, las innovaciones tecnológicas en el campo de la telecomunicación nunca se detuvieron. El módem posibilitó la transmisión de datos entre computadoras y otros dispositivos, en lo que constituyó el punto de inicio para el desarrollo de Internet y otras redes informáticas.
Los elementos que integran un sistema de comunicación son:

- Emisor
- Receptor
- Lenguaje o protocolos de transmisión
- Mensaje
- Canal o Medio

El Emisor: Es el sujeto que envía el mensaje. Es el que prepara la información para que pueda ser enviada por el canal, tanto en calidad (adecuación a la

naturaleza del canal) como en cantidad (amplificando la señal) La transmisión puede realizarse:

a) En banda base, o sea, en la banda de frecuencia propia de la señal, el ejemplo más claro es el habla.

b) Modulando, es decir, traspasando la información de su frecuencia propia a otra de rango distinto, esto nos va a permitir adecuar la señal a la naturaleza del canal y además nos posibilita el multiplexar el canal, con lo cual varios usuarios podrán usarlo a la vez.

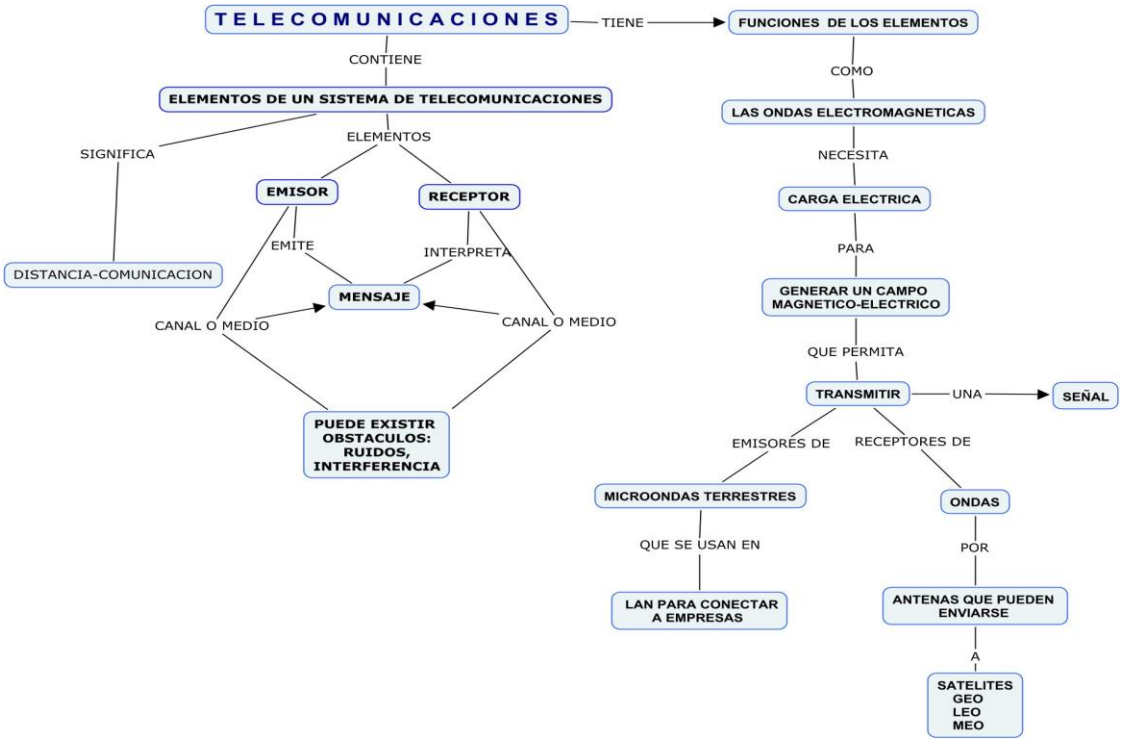
El Receptor: Es la entidad a la cual el mensaje está destinado, puede ser una persona, grupo de personas, un dispositivo artificial, etc.

Lenguaje o protocolos de transmisión: Son el conjunto de códigos, símbolos y reglas que gobiernan la transmisión de la información. Por ejemplo, en la transmisión oral entre personas se puede usar el español, el inglés.

El mensaje: Es la información que tratamos de transmitir, puede ser analógica o digital. Lo importante es que llegue íntegro y con fidelidad.

El Medio: Es el elemento a través del cual se envía la información del emisor al receptor.

Figura 5. Esquema de un Sistema de Telecomunicaciones [13]

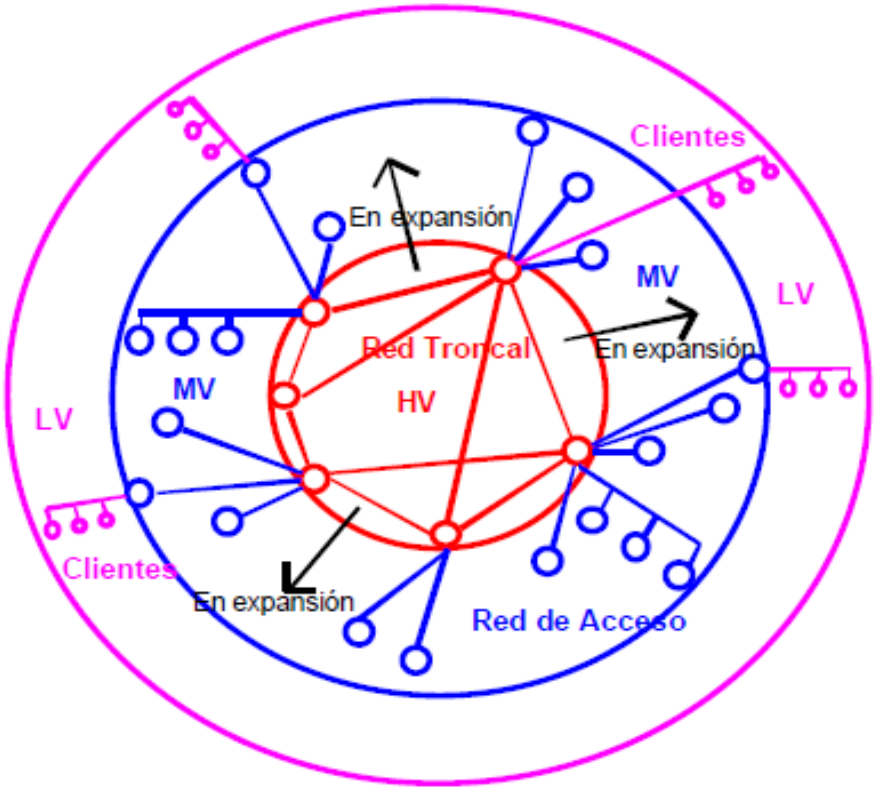


Estructuras de las redes de comunicaciones de los sistemas de telecontrol de redes eléctricas [14], [15]

En la red de comunicaciones de un sistema de telecontrol de una red eléctrica existen 2 niveles de jerarquía: La Red Troncal, centrada básicamente en las instalaciones de alta tensión (HV) y en los centros de control; y la Red de Acceso usada para comunicar las instalaciones de media (MV) y baja (LV) tensión, e incluso en los mismos clientes.

Dicha Estructura se muestra en la siguiente figura:

Figura 6. Estructura de las redes de comunicaciones de los sistemas de telecontrol de redes Eléctricas.



Estructura jerárquica de las redes de comunicaciones de los sistemas de telecontrol de redes eléctricas.

Arquitectura y protocolos tradicionales

Las redes y protocolos de comunicaciones de los sistemas tradicionales de telecontrol de redes eléctricas presentaban las siguientes características.

Bajas velocidades de transmisión (entre 200 y 1200 bps)

Arquitecturas de red simples (punto a punto, punto a multipunto y anillo)

Medios físicos y protocolos de comunicación privados

Estructura jerárquica en la que la información viaja a baja velocidad desde las remotas a los centros de control de distrito, que concentran la información y la pasan a los centros de control regionales que, a su vez, la transmiten a un centro de control principal.[16]

Daños más comunes en las telecomunicaciones [17]

- Interfaces Inadecuadas o poco amigables
- Dificultad para acoplarse entre diferentes sistema de comunicación
- Dificultades para localizar las fallas ocurridas en el sistema
- Cortes, interrupciones o Interferencias
- Mal manejo de los equipos

1.4.3 VIRUS

Es un pequeño programa escrito intencionalmente para instalarse en la computadora de un usuario sin el conocimiento o el permiso de este. Decimos que es un programa parásito porque el programa ataca a los archivos o sector es de "booteo" y se replica a sí mismo para continuar su esparcimiento. Algunos se limitan solamente a replicarse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas. Nunca se puede asumir que un virus es inofensivo y dejarlo "flotando" en el sistema. Tienen diferentes finalidades: Algunos sólo 'infectan', otros alteran datos, otros los eliminan, algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: PROPAGARSE.

Es importante destacar que el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.

La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

Es dañino

Es autorreproductor

Es subrepticio

Son programas, realizados por personas. Además de ser programas tienen el fin ineludible de causar daño en cualquiera de sus formas. Asimismo, se pueden distinguir tres módulos principales de un virus informático:

Módulo de Reproducción

Módulo de Ataque

Módulo de Defensa

El módulo de reproducción se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

El módulo de ataque es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus.

El módulo de defensa tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

Daños de los virus.

Definiremos daño como acción indeseada, y los clasificaremos según la cantidad de tiempo necesaria para reparar dichos daños.

Existen seis categorías de daños hechos por los virus, de acuerdo a la gravedad.

Daños triviales.

Daños menores.

Daños moderados.

Daños mayores.

Daños severos.

Daños ilimitados.

Efectos de los virus:

Bloqueo de los equipos
Pérdida de Información
Procesamiento de la información más lento
Pérdida de eficiencia en los equipos
Daños en el software y en los equipos
Bloqueo de las redes [18]

1.4.4 INTRUSOS [19]

- Robo de Información
- Bloqueo del hardware o el software
- Alteración del funcionamiento de los sistemas y equipos
- Implantación de Virus y corrupción de Archivos

Los objetivos principales de esta tesis son:
Modelar y Simular los parámetros y Variables de los riesgos operativos de una red de energía para prevenir y evitar blackout.
Identificación de la diversidad de riesgos que generan blackout

Clasificación de los riesgos Operativos
Selección y caracterización de datos históricos y eventos de falla
Selección y estructuración del modelo
Integración de los procesos de riesgos, los datos y el modelo
Simulación

1.5 PREGUNTAS DE INVESTIGACIÓN

¿Cómo Integrar en un modelo los proceso de riesgos operativos en las redes de energía eléctrica?

¿Cómo cuantificar el valor del riesgo operativo en las fallas tecnológicas de una red de transmisión de energía?

1.6 OBJETIVOS

1.6.1 Objetivo General

Modelar y Simular los parámetros y Variables de los riesgos operativos de una red de energía para prevenir y evitar blackout.

1.6.2 Objetivos Específicos

- Identificar la diversidad de riesgos que generan blackout
- Clasificar los riesgos Operativos
- Seleccionar y caracterizar los datos históricos y eventos de falla
- Seleccionar el modelo
- Integrar los procesos de riesgos y los datos
- Cálcular el VaR operativo utilizando simulación Monte Carlo.

1.7 ORGANIZACIÓN

La tesis es constituida por 6 capítulos los cuales están organizados de la siguiente forma:

Capítulo 1. Se describe la introducción, los antecedentes, la motivación, el planteamiento del problema, las preguntas de investigación y los objetivos

Capítulo 2. Conceptos básicos de las redes de transmisión de energía eléctrica, también se dan las nociones básicas de Var

Capítulo 3. Se analizan los avances que existen en detección de fallas tecnológicas en las redes de Transmisión de energía eléctrica.

Capítulo 4. Se realiza el tratamiento de datos con las series de tiempo de las fallas más críticas en las redes de transmisión de energía eléctricas.

Capítulo 5. Conclusiones

CAPITULO II

MARCO TEORICO

En este capítulo se describen todos los conceptos teóricos que relacionan las fallas en las líneas de transmisión de energía y la detección de estas por medio de herramientas tecnológicas, tomando como foco los sistemas SCADA para determinar los tipos de fallas.

2.1 REDES DE TRANSMISIÓN DE ENERGIA ELECTRICA

La red de transporte de energía eléctrica es la parte del sistema de suministro eléctrico constituida por los elementos necesarios para llevar hasta los puntos de consumo y a través de grandes distancias la energía eléctrica generada en las centrales eléctricas.

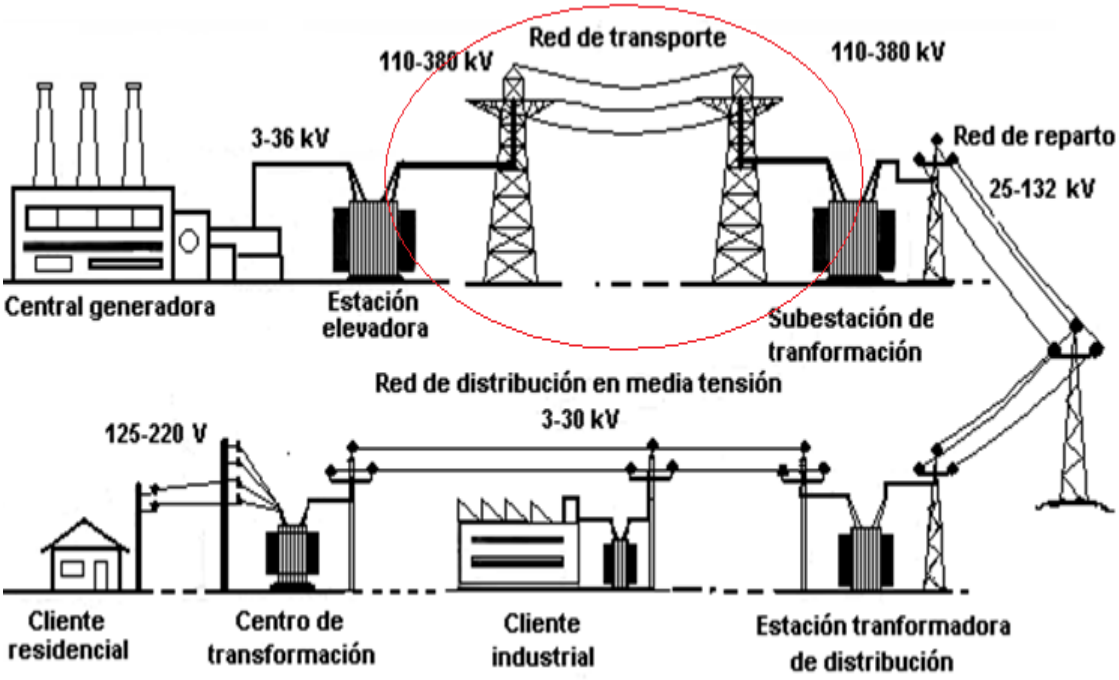
Para ello, los niveles de energía eléctrica producidos deben ser transformados, elevándose su nivel de tensión. Esto se hace considerando que para un determinado nivel de potencia a transmitir, al elevar la tensión se reduce la corriente que circulará, reduciéndose las pérdidas por Efecto Joule. Con este fin se emplazan subestaciones elevadoras en las cuales dicha transformación se efectúa empleando transformadores, o bien autotransformadores. De esta manera, una red de transmisión emplea usualmente voltajes del orden de 220 kV y superiores, denominados alta tensión, de 400 o de 500 kV.

Parte de la red de transporte de energía eléctrica son las líneas de transporte.

Una línea de transporte de energía eléctrica o línea de alta tensión es básicamente el medio físico mediante el cual se realiza la transmisión de la energía eléctrica a grandes distancias. Está constituida tanto por el elemento

conductor, usualmente cables de acero, cobre o aluminio, como por sus elementos de soporte, las torres de alta tensión. Generalmente se dice que los conductores "tienen vida propia" debido a que están sujetos a tracciones causadas por la combinación de agentes como el viento, la temperatura del conductor, la temperatura del viento, etc. [20]

Figura 7. Red de transmisión de Energía Eléctrica



Existen una gran variedad de torres de transmisión como son conocidas, entre ellas las más importantes y más usadas son las torres de amarre, la cual debe ser mucho más fuertes para soportar las grandes tracciones generadas por los elementos antes mencionados, usadas generalmente cuando es necesario dar un giro con un ángulo determinado para cruzar carreteras, evitar obstáculos, así

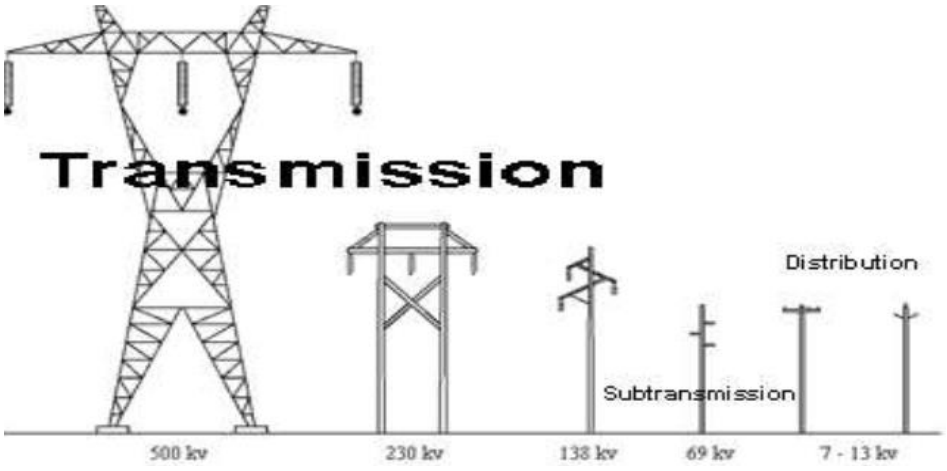
como también cuando es necesario elevar la línea para subir un cerro o pasar por debajo/encima de una línea existente.

Existen también las llamadas torres de suspensión, las cuales no deben soportar peso alguno más que el del propio conductor. Este tipo de torres son usadas para llevar al conductor de un sitio a otro, tomando en cuenta que sea una línea recta, que no se encuentren cruces de líneas u obstáculos.

La capacidad de la línea de transmisión afecta al tamaño de estas estructuras principales. Por ejemplo, la estructura de la torre varía directamente según el voltaje requerido y la capacidad de la línea. Las torres pueden ser postes simples de madera para las líneas de transmisión pequeñas hasta 46 kilovoltios (kV). Se emplean estructuras de postes de madera en forma de H, para las líneas de 69 a 231 kV. Se utilizan estructuras de acero independientes, de circuito simple, para las líneas de 161 kV o más. Es posible tener líneas de transmisión de hasta 1.000 kV.

Al estar estas formadas por estructuras hechas de perfiles de acero, como medio de sustentación del conductor se emplean aisladores de disco y herrajes para soportarlos. [21]

Figura 8. Estructuras de Soporte para las líneas de Transmisión de Energía Eléctrica.



2.2 FALLAS EN LOS SITEMAS ELECTRICOS DE POTENCIA

Un SEP esta balanceado cuando la magnitud de la corriente y voltaje en sus tres fases presentan un nivel similar, y los ángulos entre estas es de 120º. El ángulo entre la corriente y voltaje en cada fase depende del flujo de potencia en el instante en que se mide. Asimismo se puede decir que un SEP se encuentra en estado estable si las variables eléctricas del sistema permanecen constantes con el tiempo y en un rango de valores aceptable.

Cuando se presenta una falla en un SEP, generalmente las subestaciones más cercanas al punto de falla tienen aumento de corriente y una caída de voltaje en las fases que presentan el problema, que depende de la impedancia en la subestación, lo que conlleva cambios en los flujos de potencia y el ángulo de transferencia entre las dos subestaciones que están interconectadas, además de posibles oscilaciones de frecuencia y presencia de armónicos de corriente y voltaje

En un SEP se pueden presentar varios tipos de falla que pueden ocasionar perturbaciones en el sistema, entre las cuales se destacan por su frecuencia de ocurrencia las fallas monofásicas a tierra, presentes en aproximadamente 90% de eventos totales de falla [22]. También existen otras no menos importantes como las fallas bifásicas a tierra, fallas bifásicas aisladas, fallas trifásicas a tierra y fallas trifásicas aisladas, todas con diferentes niveles de impedancia de falla.

2.2.1 Fallas Monofásicas a tierra

Este tipo de falla únicamente afecta una sola fase del SEP, presentándose un aumento de corriente y caída de voltaje en la fase que presenta el problema. La falla puede ser de baja impedancia (falla franca) con valores cercanos a 0 ohmios, de media-alta ó de alta impedancia (FAI) con valores mayores a 30 y 60 ohmios,

respectivamente. Las fallas de alta impedancia no presentan gran variación en la variable corriente de la fase fallada por lo que a veces no se detecta fácilmente ya que pueden ser vistas como un aumento en la demanda energía del SEP. En contraste las fallas francas presentan un importante aumento de la corriente, lo cual facilita su detección.

Las Fallas de Alta Impedancia, son producidas normalmente por árboles, cometas, fuego bajo la línea, flámeos de aisladores, entre otros.

2.2.2 Falla Bifásica a tierra. (L-L-G)

En esta falla se afectan dos fases del SEP, generalmente por la caída de una de las fases, haciendo contacto con otro cable y con elemento externo que conduce a tierra. Cuando se presenta esta falla aumenta la corriente en ambas fases y disminuye el voltaje.

2.2.3 Falla Trifásica aislada (L-L-L)

Se presenta cuando las tres fases entran en contacto, con caídas de voltaje y aumento de corriente similar para las tres fases. No obstante esta falla tiene poca frecuencia de ocurrencia en los SEP.

2.3 CLASIFICACIÒN DEL SISTEMA DE TRANSMISIÒN EN COLOMBIA

En transmisión las redes de transporte se dividen en el sistema de transmisión nacional (STN), el sistema de transmisión regional (STR) y el sistema de distribución local (SDL), las cuales se clasifican por los niveles de tensión asi:

STN: mayor o igual a 220 KV (Para Colombia son redes de 220KV a 500KV)

Nivel 4: mayor o igual a 57.5 KV y menor a 220 KV

Nivel 3: mayor o igual a 30 KV y menor de 57.5 KV

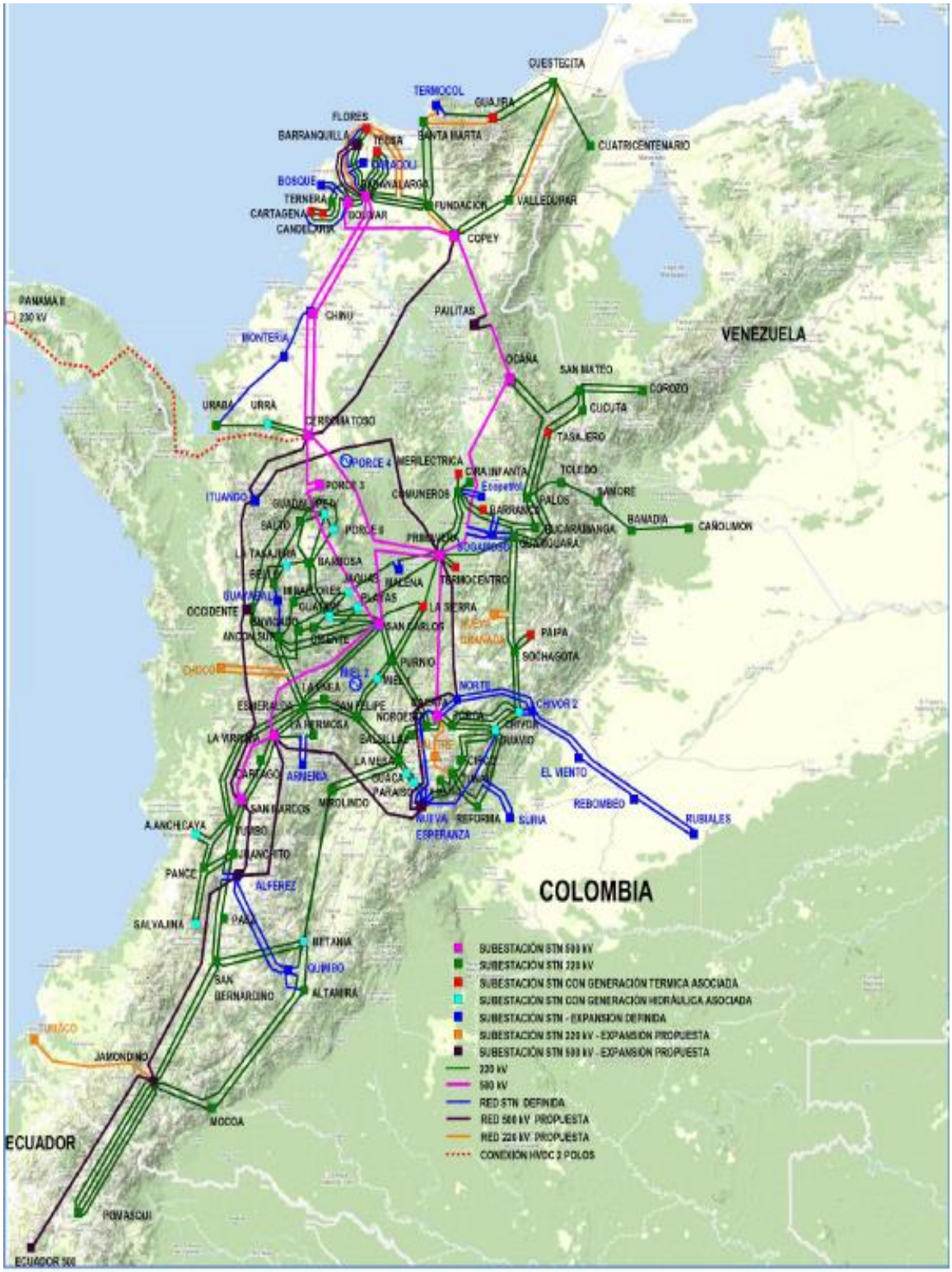
Nivel 2: mayor o igual a 1 KV y menor de 30 KV

Nivel 1: menor a 1 KV.

El STN cobra gran importancia dado que el operdor a niveles de tensión superiores permite transmitir grandes cantidades de energía a grandes distancias desde las centrales de generación hasta los centros de distribución y consumo. Adicionalmente permite el intercambio de energía entre áreas excedentarias y deficitarias. En otras palabras, el STN se constituye en la red troncal del país que actualmente cuenta con mas de 11.654 Km de redes a 220 KV, mas de 2646 Km de redes a 500KV, con sus respectivas subestaciones, equipos de conexión, control y protecciones. [23]

Figura 9. Mapas de la infraestructura actual y futura del STN

Figura 10. Sistema de Transmisión a 2015 en Colombia



2.3.1 Líneas de Transmisión por empresa [24]

Tabla 1. Líneas de Transmisión por Empresa a 2007

LINEAS DE TRANSMISION POR EMPRESAS A 2007		
EMPRESAS PROPIETARIAS	CIRCUITOS (Km)	%
Centrales Eléctricas Del Caribe S.A ESP	458,5	4,6
Centrales Eléctricas de Nariño S.A ESP	552,7	5,6
Cementos Diamante S.A	10,5	0,1
Centrales Eléctricas del Norte de Santander S.A ESP	344,9	3,5
Central Hidroeléctrica de Caldas S.A ESP	446,8	4,5
Codensa S.A ESP	977,8	9,8
Concrecem	1,7	0
Empresa de Distribución del Pacifico S.A ESP	331,8	3,3
Empresa de Energía de Boyacá S.A ESP Empresa de Servicios	685,8	6,9
Empresa De Energía del Quindío S.A ESP	17	0,2
Empresa de Energía de Cundinamarca S.A ESP	96,1	1
Empresa de Energía de Pereira S.A ESP	31,1	0,3
Empresas Publicas de Medellín ESP	832	8,4
Electrificadora del Caribe S.A ESP	658,7	6,6
Electrificadora de la Costa Atlántica S.A ESP	758,5	7,6
Electrificadora del Huila S.A ESP	400,9	4
Electrificadora del Tolima S.A ESP (En liquidación)	487,5	4,9
Electrificadora del Meta S.A ESP	173	1,7
Empresa de Energía de Arauca ESP	60	0,6
Empresa de Energía Eléctrica del departamento del Guaviare S	187	1,9
Empresa de Energía del Pacifico S.A ESP "Epsa ESP"	984,7	9,9
Electrificadora de Santander S.A ESP	438,9	4,4
Etaservicios S.A ESP	417,5	4,2
International Colombia Resource Corporation	304	3,1
Interconexión Eléctrica S.A ESP	108,7	1,1

Ministerio de Minas y Energía	102	1
Nd	30	0,3
Siderúrgica de Boyacá S.A	2,4	0
Termoflores S.A ESP	3,2	0
Termo yopal Generaciòn 2 S.A ESP	13,7	0,1
Transelca S.A ESP	12,6	0,1
TOTAL	**9930**	**43,79**

Tabla 2. Líneas de Transmisión de 138 KV

TRANSMISION A 138 KV		
Empresa Propietaria	***Circuitos (Km)***	***%***
Interconexión Eléctrica S.A ESP	15.5	100
TOTAL	**15.5**	**0,07**

Tabla 3. Líneas de Transmisión de 220 – 230 KV

TRANSMISION 220 - 230KV		
Empresa Propietaria	***Circuitos (Km)***	***%***
Distansa S.A ESP	27,3	0,2
Empresa de Energía de Bogotá ESP	684	6,2
Empresas Publicas de Medellín ESP	791,8	7,2
Empresa de Energía del Pacifico S.A ESP "Epsa ESP"	269,8	2,5
Electrificadora de Santander S.A ESP	122,9	1,1
Interconexión Eléctrica S.A ESP	7,478,3	68,1
Termoflores S.A ESP	14,8	0,1
Transelca S.A ESP	1,595,5	14,5
TOTAL	**10,984,3**	**48,4**

Tabla 4. Líneas de Transmisión a 500 KV

TRANSMISION A 500KV		
Empresa Propietaria	***Circuitos (Km)***	***%***
Interconexión Eléctrica S.A ESP	1,774,6	100
TOTAL	**1,774,6**	**7,69**

2.4 RIESGO OPERATIVO

Se entiende por riesgo operativo a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

2.4.1 Fuentes de riesgo operativo

Procesos Internos

Posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, o con políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y presupuestos planeados.

Personas

Posibilidad de pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores. Se puede también incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación.

Tecnología de Información

Posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

Las instituciones pueden considerar de incluir en ésta área, los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas TI, a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología y fallas para alinear la TI con los objetivos de negocio, con entre otros aspectos. Otros riesgos incluyen la falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

Eventos Externos

Posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información. Entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros. Otros riesgos asociados con eventos externos incluyen: el rápido paso de cambio en las leyes, regulaciones o guías, así como el riesgo político o del país.

2.4.2 Categorización de eventos de pérdida por riesgo operativo

En coordinación con el sector financiero, el Comité de Basilea ha identificado los siguientes tipos de eventos que pueden resultar en pérdidas sustanciales por riesgo operativo. [25]

Fraude Interno

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicada, al menos, una parte interna a la empresa; no se consideran los eventos asociados con discriminación en el trabajo. Esta categoría incluye eventos como: fraudes, robos (con participación de personal de la empresa), sobornos, entre otros.

Fraude Externo

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero. Esta categoría incluye eventos como: robos, falsificación, ataques informáticos, entre otros. Relaciones laborales y seguridad en el puesto de trabajo. Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con discriminación en el trabajo.

Clientes, productos y prácticas empresariales

Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

Daños a activos materiales

Pérdidas derivadas de daños o perjuicios a activos físicos como consecuencia de desastres naturales u otros eventos de fuentes externas.

Interrupción del negocio y fallos en los sistemas Pérdidas derivadas de incidencias o interrupciones en el negocio y de fallas en los sistemas.

Ejecución, entrega y gestión de procesos

Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores.

Esta categoría incluye eventos asociados con: captura de transacciones, ejecución y mantenimiento, monitoreo y reporte, entrada y documentación de clientes, gestión de cuentas de clientes, contrapartes de negocio, vendedores y proveedores.

2.4.3 Gestión del riesgo operativo: Identificación, Evaluación, Medición, Monitoreo y Control

Como principio general, las entidades financieras deben contar con una estrategia aprobada por el Directorio estableciendo principios para la identificación, medición, control, monitoreo y mitigación del riesgo operativo.

Las estrategias y políticas deberían ser implementadas por la Función de Gestión de Riesgo, responsable de identificar y gestionar todos los riesgos. La Función de Gestión de Riesgo puede incluir sub-unidades especializadas por riesgos específicos. Las entidades financieras deberían desarrollar su propio enfoque y metodología para la gestión de riesgos, de acuerdo con su objeto social, tamaño, naturaleza y complejidad de operaciones y otras características. La implementación del sistema de gestión de riesgo operativo debería considerar todas las etapas de gestión de riesgo, incluyendo la identificación, evaluación, medición, monitoreo y control.

Identificación

La identificación efectiva del riesgo considera tanto los factores internos como externos que podrían afectar adversamente el logro de los objetivos institucionales.

Evaluación

Para todos los riesgos operativos materiales que han sido identificados, la entidad debería decidir si usa procedimientos apropiados de control y/o mitigación de los riesgos o asumirlos. Para aquellos riesgos que no pueden ser controlados, el banco debería decidir si los acepta, reduce el nivel de actividad del negocio expuesta o se retira de esta actividad completamente.

Todos los riesgos materiales deberían ser evaluados por probabilidad de ocurrencia e impacto a la medición de la vulnerabilidad de la entidad a este riesgo.

Los riesgos pueden ser aceptados, mitigados o evitados de una manera consistente con la estrategia y el apetito al riesgo institucional. Cuando sea posible, la entidad debería usar controles internos apropiados u otras estrategias de mitigación, como los seguros.

Medición

Las entidades financieras deberían estimar el riesgo inherente en todas sus actividades, productos, áreas particulares o conjuntos de actividades o portafolios, usando técnicas cualitativas basadas en análisis expertos, técnicas cuantitativas que estiman el potencial de pérdidas operativas a un nivel de confianza dado o una combinación de ambos.

Monitoreo

Un proceso efectivo de monitoreo es esencial para una gestión adecuada del riesgo operativo.

Un monitoreo regular de las actividades puede ofrecer la ventaja de detectar rápidamente y corregir deficiencias en las políticas, procesos y procedimientos de gestión del riesgo operativo. El monitoreo regular también fomenta la identificación temprana de cambios materiales en el perfil de riesgo, así como la aparición de nuevos riesgos. El alcance de las actividades de monitoreo incluye todos los aspectos de la gestión del riesgo operativo en un ciclo de vida consistente con la naturaleza de sus riesgos y el volumen, tamaño y complejidad de las operaciones.

Control

Después de identificar y medir los riesgos a los que está expuesta, la entidad financiera debería concentrarse en la calidad de la estructura de control interno. El control del riesgo operativo puede ser conducido como una parte integral de las operaciones o a través de evaluaciones periódicas separadas, o ambos. Todas las deficiencias o desviaciones deben ser reportadas a la gerencia.

Reporte

Debe existir un reporte regular de la información pertinente a la alta gerencia, al directorio, al personal y a partes externas interesadas, como clientes,

proveedores, reguladores y accionistas. El reporte puede incluir información interna y externa, así como información financiera y operativa.

2.5 VALOR AL RIESGO

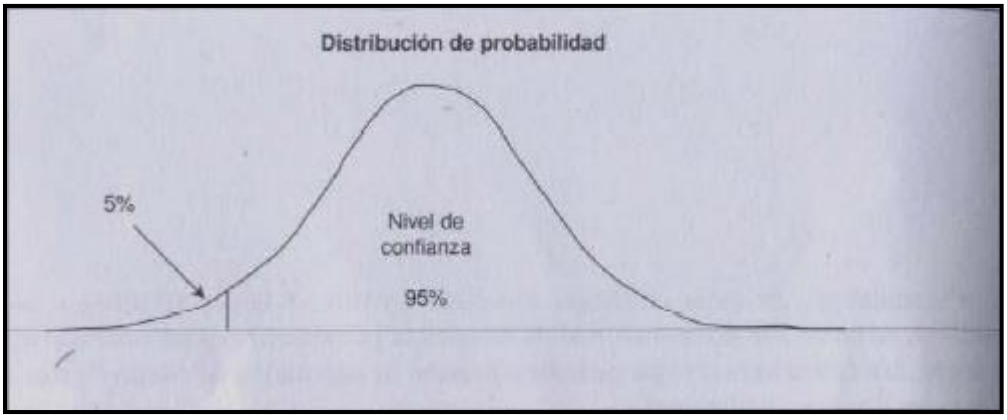
El valor en riesgo (VaR) es un método para cuantificar exposición al riesgo de mercado por medio de técnicas estadísticas tradicionales.

“El valor en riesgo es una medida estadística de riesgo de mercado que estima la pérdida máxima que podría registrar un portafolio en un intervalo de tiempo y con cierto nivel de probabilidad o de confianza “

Es importante destacar que la definición de valor en riesgo es válida únicamente en condiciones normales de mercado, ya que en momentos de crisis y turbulencias la perdida esperada se define por pruebas de stress o valor extremo.

Dos aspectos fundamentales para el cálculo del VAR: *El nivel de confianza* que desean tener para determinar el VAR, el horizonte de tiempo con que se va a medir.

Figura 11: Distribución de Probabilidad



Las metodologías para el cálculo del VaR son las siguientes:

1. Métodos Parametricos
2. Métodos No-parametricos

2.5.1 Métodos Paramétricos

Tienen como características el supuesto de que los rendimientos del activo en cuestión se distribuyen de acuerdo con una curva de densidad de probabilidad normal. Sin embargo en la práctica se ha observado que la mayoría de los activos no siguen un comportamiento estrictamente normal, si no que son aproximados a la curva normal y, por tanto, los resultados que se obtienen al medir el riesgo son una aproximación.

El valor en riesgo de un Activo Individual

Bajo el supuesto de normalidad y de media de rendimiento igual a cero, el modelo para métrico que determina el valor en riesgo de una posición es:

$$VaR = F \times S \times \sigma \times \sqrt{t}$$

F=factor que determina el nivel de confianza del cálculo. Para un nivel de confianza del 95% , F=1.65 y para un nivel de confianza del 99%, F=2.33.

S=monto total de la inversión o la exposición total en riesgo.

σ= Desviación estándar de los rendimientos del activo.

t= horizonte de tiempo en que se desea calcular el VAR (holding period).

VaR para el sector energético

Para nuestro cálculo se tendría que para el sector energético, la caracterización del riesgo operativo asociado con eventos de apagón así como su cuantificación económica y efectos son un objeto de investigaciones con respecto a sus consecuencias sobre los clientes, las empresas y presupuesto del público.

Además Schreinner al analizar la aplicación VaR en sistema de distribución [26]. llegó a la conclusión de que la aplicación de metodología VaR en la evaluación de riesgos de los sistemas de energía se encuentra todavía en sus inicios porque es necesario comprender física, técnica y económicamente las competencias deben ser fusionados en modelos agregados. Se propuso un modelo de red simplificada con la definición del valor del portafolio. El trabajo de Alvehag al [27] había considerado un sistema de distribución de red más complejo con los clientes residenciales, agrícolas, industriales, comerciales y gubernamentales y propuso utilizar el VaR y el CVaR sobre el coste de sistema de interrupción como una medida de la fiabilidad del sistema.

Al Mei [28] desarrolló un modelo de apagón, basado en modelo de OPA con restricciones de estabilidad transitoria (OTS). Se describe el proceso en cascada de fracaso agregando al modelo La cascada no se describe el proceso de añadir a la criticidad auto organizada modelo, la dinámica del sistema eléctrico. VaR y CVaR conceptos cuantifican la demanda que no se suministra. Sin embargo, los aspectos financieros, tales como el costo por tipo de cliente, no se introducen.

El concepto de valor en riesgo también se aplica para hacer frente a otros tipos de problema de decisión como, por ejemplo, la estructuración de las carteras de los mercados eléctricos. El modelo de funcionamiento de mercados de la electricidad ha pasado progresivamente de una generación de mercado hacia un mercado mayorista eléctrico donde diferentes agentes pueden comercializar energía (generadores, transportadores, distribuidores con la competencia en el país y en el extranjero). Proveedores de energía, que puede comprar o vender electricidad en el mercado mayorista de energía o de otros agentes, debe incluir diferentes variables de riesgo para reducir la incertidumbre.

La propuesta utiliza el concepto de VaR y CVaR para evaluar el perfil costo de DNS para los eventos de las interrupciones en la red de transmisión (más de 110 KV), con el fin de cuantificar la exposición económica debido al riesgo de

interrupción del suministro eléctrico y así tomar decisiones de gestión. Utilizamos la información disponible sobre el histórico de DNS ocurrido desde 1996 a 2011 en el sistema eléctrico colombiano. El costo de la energía no suministrada se deduce de la UPME metodología [29]. Es una aproximación económica basada en las encuestas. Para el cliente residencial, se evaluó el bienestar. Para los clientes industriales y comerciales, la metodología propone un diferencial flujo de efectivo asociados con los ingresos o costos causados por la pérdida de potencia de energía. Las encuestas de evaluación diferentes aspectos como las regiones, nivel económico, tamaños industriales, pérdida de producción en cada cliente.

Definimos una relación general para cuantificar el VaR del costo mensual de la demanda no suministrado con el sistema de energía eléctrica. Esta es una función del número de eventos, la energía no suministrada, la duración de las fallas, el comienzo hora de los fallos, la demanda de energía y el coste de la energía nivel de pérdida. Se utilizó funciones de distribución de probabilidad empírica y estable para adaptarse a la distribución de frecuencia de las interrupciones. Acerca de la gravedad (DNS) y la duración de las interrupciones, encontramos el comportamiento de la ley de poder, que ya había sido identificado [30]. Por otra parte, el análisis estadístico muestra evidencia de comportamiento escalonado con diferentes agregaciones de tiempo.

VALORACIÓN DE VAR DE DEMANDA NO SUMINISTRADA EN SISTEMAS DE ENERGÍA ELÉCTRICA

El sector financiero cuantifica la pérdida potencial del portafolio o el riesgo de mercado utilizando el índice de VaR, propuesto inicialmente por JP Morgan Bank [27]. VaR es el índice de riesgo más comúnmente se hable en el sector financiero. Las valoraciones de pérdida de la economía se basan en el portafolio continúan vuelve R y el modelo de VaR en general está indicado después de [31]:

$$VAR = -w_0 * \left(R^* - \mu \right) \quad (1)$$

Donde:

- W0= initial value of portfolio,
- R^* = critical Return given a confidence level,
- μ = expected Return.

- W0= valor inicial del portafolio,
- R^* = retorno crítico con un nivel de confianza
- μ =rendimiento esperado

VaR resume la pérdida máxima esperada en un Horizonte de tiempo con un nivel de confianza dado. En la forma más general , puede ser derivado de la función de distribución de probabilidad del portafolio en el futuro valor de f(x). En un determinado nivel de confianza c y nivel de significación a = 1 - c, se puede encontrar la peor realización Posible o pérdidas (VaR) de manera que la probabilidad de que se supere este valor es c:

$$VAR_C = \left\{ x / P(x > VAR) \leq 1 - c \right\} = \left\{ x / \ f(x) \geq c \right\} \quad (2)$$

O

$$c = \int_{-\infty}^{VaR} f(x) dx \quad (3)$$

Dependiendo de la función de distribución de probabilidad de los rendimientos R, la relación (32) puede tomar diferentes formas. Por ejemplo, si R tiene una distribución normal:

$$VaR = W_0 q_c \sigma_p \sqrt{t} \quad (4)$$

Con

- qc, el valor de la distribución normal estándar, dependiendo del nivel de confianza (con un nivel de confianza del 95% qc=1.64)
- $\sqrt{t}$, la raíz cuadrada del tiempo, que describe la cartera de volatilidad para los diferentes períodos de tiempo (propiedad de escala de tiempo),
- σ_p, la desviación estándar de la cartera, que se define por

  $\sigma_p = \sqrt{[w_i]^T * [\Omega] * [w_i]}$
- Wi, La desviación estándar de la cartera.
- Ω, la rentabilidad, matriz de varianza - covarianza del portafolio.

El valor condicional en Riesgo (CVaR) es bien conocido como medida de riesgo más consistente. Se define como la pérdida esperada, si las pérdidas son mayores de VaR y se denomina déficit esperado Déficit o pérdida de la cola que esperaba. VaR y CVaR dependen de la función de distribución de probabilidad de los factores de riesgo. Si L es una pérdida en exceso de valor en riesgo (evento en la cola de la pérdida distribución), el condicional Value-at-Risk nos dice cuánto podríamos esperar perder. Este concepto se parece a la gravedad.

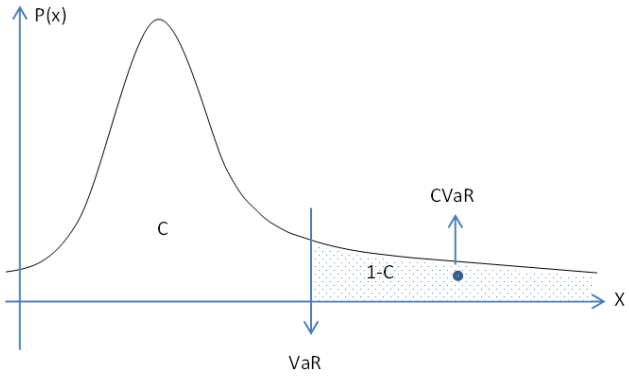


Figura 12. VaR y CVaR diagrama

Centro aplicado a la cola de la función de distribución de probabilidad de las pérdidas:

$$CVaR = E\left[L / L > VaR\right] \quad (5)$$

En forma general, CVaR se define como:

$$CVaR = (1-c)^{-1} \int_{VaR}^{\infty} x * f(x) * dx \quad (6)$$

Se dice CVaR es la pérdida media ponderada por probabilidad ahí VaR, es relativamente fácil de calcular si cortamos la cola de la distribución de la pérdida agregada por encima del valor en riesgo (X> VaR) en N rebanadas y luego calcular la pérdida media ponderada por probabilidad. La figura 12 representa este concepto VaR y CVaR se pueden aplicar para medir el Riesgo operativa.

Estamos preocupados por la cuantificación las perdidas por posibles fallos en un sistema de energía con el propósito de cobertura . La pérdida potencial es, en general, el producto de la probabilidad de que se produzca un fallo (frecuencia) y de su costo asociado (severidad). Debido a que dos o más Procesos estocástico representan el fenómeno, no es generalmente fácil de obtener la función de distribución de la pérdida agregada (LDA) y la necesidad de utilizar métodos

numéricos. El método utilizado con frecuencia es Simulación Monte-Carlo [32], [33], [34], [35]. Tenemos LDA en una forma simple:

$$LDA = \sum_{i=1}^{N} X_i \quad (7)$$

Donde N representa el número de eventos de falla (frecuencia de eventos), Xi es la pérdida económica de cada evento (severidad del evento). Las pérdidas totales son el resultado de dos fuentes de aleatoriedad, la frecuencia y la gravedad. Ambos son al azar variables con procesos estocásticos asociados y anteriormente identificado. Dependiendo del contexto, los factores de riesgo adicionales deben ser identificados e integrados a la relación (7).

De acuerdo al artículo lo que se realizo fue el tratamiento estadístico de una serie de tiempo en la cual se caracterizarían las fallas ocurridas de acuerdo al nivel de riesgo de estas. Para esto se clasificaron los tipos de fallas ocurridos por horas, días y meses con el fin de determinar las frecuencias de estas y así proceder a obtener una información más específica para analizar a qué tipo de distribución se ajustaban mejor los datos y así crear un modelo para la cuantificación de la demanda no suministrada y llevarla a un costo, con el objeto de determinar las pérdidas de los eventos de acuerdo al su duración para las empresa de generación, distribución y transmisión de energía eléctrica.

2.6 METODO PARAMETRICO DENOMINADO SIMULACION MONTECARLO

Este método fue propuesto por Boyle[2] y consiste en la generación de números aleatorios (random) para calcular el valor del portafolio generando escenarios. Un nuevo número aleatorio sirve para generar un nuevo valor del portafolio con igual probabilidad de ocurrencia que los demás y determinar la pérdida o

ganancia en el mismo. Este proceso se repite un gramo número de veces (10000 escenarios) y los resultados se ordenan de tal forma que pueda determinar un nivel de confianza especifico.

Las mayores ventajas de utilizar este método es la posibilidad de evaluar instrumentos no lineales, como las opciones. Este efecto no se puede obtener en las dos metodologías descritas anteriormente. [42]

Luego del reconocimiento de los elementos para determinar las fallas y los métodos para cuantificar el valor al riesgo de estas, en las líneas de transmisión eléctricas en Colombia, se puede apreciar que existen diversas formas de analizar los datos para obtener un resultado, en cuanto a mediciones y ajustes del valor al riesgo. Sin embargo en el siguiente capítulo, veremos que la cuantificación de los riesgos y la detección de las fallas en los sistemas de transmisión, se pueden estudiar y analizar desde diferentes métodos y con diversos modelos que nos mostraran resultados en casos de forma parcial y en otros de forma partículas, con una tendencia a dar análisis mas cualitativos que cuantitativos.

Por tal motivo se revisa el estado del arte con respecto a las tendencias actuales de los modelos y las simulaciones para la detección de fallas en las líneas de transmisión de energía.

CAPITULO III

ANTECEDENTES

3.1 REVISIÓN DEL ESTADO DEL ARTE

En esta secciòn se presentan los diversos avances en el estudio y las investigaciones de las fallas presentadas en las lineas de transmisiòn de energia electrica, como tal estan enfocadas a mostrar que factores tecnologicos presentan fallas, como se evidencian y con que metodologias se abordan para identificarlas y tomar acciones en un momento determinado. En los siguientes articulos se evidencia la importancia de la detecciòn de estas fallas en el momento oportuno y el valor que puede llegar a representar para el mercado electrico ya que estos deben suplir una demanda que es variable. Por tal motivo el identificar y cuantificar las fallas tecnologicas por medio de las distintas tecnicas, metodologias y modelos expresados por los investigadores es de suma importancia para el avance en la predicciòn de problemas en los sistemas de transmisiòn y para la disponibilidad y confiabilidad de los mercados energeticos.

Todos los problemas detectados en las diversas variables tecnologicas se reunen en gran medida en los sistemas de comunicaciones que se utilizan en los sistemas de transmisión, asi como en los sistemas ESCADA, por tal razón se enfocará los nuevos desarrolos y avances en los estudios en estos 2 factores tecnologicos.

A continuacion se presentan los estudios que han arrojados resultados confiables y puntos de vista diferentes por medio de aplicaciòn de nuevas metodologias que orientan las investigaciones a la identificación y clasificaciòn de los fallos.

Se debe tener en cuenta que el fin de cada uno de estos avances y descubrimiento de nuevos modelos tienen como objeto tener la informaciòn para luego realizar tratamiento de estos datos y mostrar el VaR de estos factores tecnologicos en los sistemas de transmisiòn de energia electrica en el mercado colombiano.

3.2 INTERNACIONALES

3.2.1 Study of Online Fault Diagnosis for Distributed Substation Based on Petri Nets [43]

Esta investigaciòn hace referencia a las principales fallas y a la configuraciòn de las protecciones de las subestaciones de distribuciòn. Un nuevo modelo de diagnostico de fallas basado en redes de petri es propuesto en este articulo. En el modelo de diagnostico de redes de petri todas las clases de fallas tienen un token especifico que hacen fàcil y clara la localizaciòn de la falla y el entendimiento de la secuencia de los eventos de falla, el diagnosticoes implementado para resolver algunas ecuaciones matriciales que tienen una velocidad computacional rapida y un resultado definido. El enfoque es particularmente adecuado para el diagnostico en fallas de lineas de subestaciones.

Hay enormes cantidades de dispositivos en una subestaciòn larga esto es impractico para determinar las matrices de falla como un todo dentro del sistema.

Los componentes en las subestaciones son clasificados en varios grupos, acordando sus funciones y tipos, entoces diferentes modos son construidos por cada grupo. Este es un modelo general que no es obligstorio por la topologia y las configuraciones de protecciòn del relevo de la subestaciòn. En una subestaciòn hay bus de variables, transformadores y lineas de transmisiòn, esto requiere ser cnfigurado para protecciones de diferentes corrientes sobre los transformadores con capacidad por encima de 6300 KVA, si la diferencia de las protecciones es restringida, esta puede abrir el circuito del breaker en ls 2 lados del transformador . estas caracteristicas son indeseables para la protecciòn de sobrecorriente, que puede abrir solo un lado del circuito del breaker . Casi siempre, solo pocos metodos pueden construir un modelo general para diagnosticar las fallas de las protecciones diferenciales de corrientes.

Considerando el clima hay diferentes protecciones o no, el componente de los modelos de diagnostico pueden ser divididos en dos tipos. Uno es el componente

del modelo de falla sin diferencial de protecciòn, incluyendo lineas ordinarias, obstrucciones de bus sin diferencial de protecciòn y transformadores con capacidades de pequeña longitud con 6300 KVA sobre los cuales usualmente el diferencial de protecciòn no es requerido. El otro es un componente del modelo de diagnostico de falla con diferencial de protecciòn

3.2.2 SCADA System Cyber Security – A Comparison of Estándar [44]

Los sistemas SCADA son vitales para la operaciòn y control de infraestructuras criticas tales como los sistemas de transmisiòn electrica, existen un numero de guias y estandares que tienen que ser desarrollados para soportar las utilidades de los sistemas de pode r electricos en sus esfuerzos de cyber seguridad. El metodo usado es basado en una comparaciòn de l uso de resultados claves verificables en el estandar, luego se agrupan dentro de diferentes categorias. La ocurrencia de los resultados claves es conatada y comparada con hechos.

Los estandares de las especificaciones de SCADA son mas focalizadas en tecnicas de medidas de conteos, tal como corta fuegos y detecciòn de intrusos, donde ISO/IEC 17799 esta mas focalizada sobre las medidas de conteo organizacionales.

Metodo de comparasiòn de tres fases, primero, el estadar para comparar donde seleccionamos basados en un conjunto de criterios. Segundo. Hay estandares donde estudiando en profundidad para extraer informaciòn sobre recomendaciones de seguridad y descripciòn de ataques en ellos. La extracciòn de la informaciòn de alli en adelante agrupada y cada grupo es asociado con un numero de palabras claves y frases que representan el contenido.Finalmente, las palabras claves y frases tienen que ser usadas para cuantificar el focus de estanar en diferentes recomendaciones de seguridad y amenazas.

Selecciòn de Estandar

Existe un largo nùmero de estandares y recomendaciones que es de relevancia para aquello concerniente acerca de la seguridad SCADA. Estos estudios empiezan con una comprensiòn de la busqueda para producir documentos para cuerpos de estandarizaciòn y agencias gubernamentales. En estas busquedas los siguientes criterios son usados para determinar si un estandar puede ser incluido o no.

1. El estandar es viable en ingles.
2. E estandar es publicado por un cuerpo de estandarizacion o una agencia del gobierno
3. El estandar puede enfocarse en sistemas de seguridad SCADA
4. El estandar /guia puede focalizarse en sistemas SCADA como un todo, esto no puede focalizarse en subsistemas o componentes tales como dispositivos electronicos inteligentes.

La racionalidad para el segundo criterio es para incluir todos aquellos estandares que son producidos por autoridades en el campo. Por lo tanto hacer que sea ampliamente reconocido.El tercer criterio sirve para eliminar aquellos estandares que no representan el requerimiento y priorizaciòn que son directamente aplicables para sistemas SCADA.

Agrupaciòn de recomendaciones y amenazas

Despues de identificar los documentos relevantes, esos donde se estudio y se realizaròn las recomendaciones de seguridad como bien o como amenazas decribidas, donde extraemos de ellos. Esto entrega un numero sustancial de fases como “Implementaciòn de corta fuegos” para habilitar la comparaciòn, las recomendaciones y la extracciòn de ataques de los diferentes documentos donde se acuerdan agrupaciones para sus objetivos. Por instancia, relatamos recomendaciones para corta fuegos donde agrupamos en un grupo de recomendaciones y descripciòn de amenazas para varias especies de software

maligno son agrupados juntos. Estos son 26 grupos de recomendaciones de seguridad y 14 grupos de amenazas.

Cuantificando focalizaciòn de los estandares

Para comparar los 26 grupos de recomendaciones de seguridad y los 14 grupos de amenazas, un nùmero de palabras claves y frases claves son asociadas para cada grupo. Las palabras claves y las frases son identificadas por lectura de documentos usando desde el comienzo. La extracciòn de las frases como un punto de inicio.

Las palabras claves son identificadas el numero de ocurrencias de cada palabra clave y frases en cada uno de los documentos incluidos en el conteo. El numero de ocurrencia para un grupo puede ser calculado como la suma de estas palabras claves. El nùmero de ocurrencias de las frases y palabras claves son contadas en ISO/IEC 17799 y agregadas usando el mismo procedimiento.

Para habilitar la comparaciòn entre ISO/IEC 17799 y el estandar SCADA y las lineas guias el resultado es normalizado con el nùmero total de palabras claves ocurridas en el testo comparado. Los valores de normalizaciòn verdaderos representam la parte de los requerimientos totales que son asociados con cada grupo. Estos valores de normalizaciòn son despues de estos referentes tomados como un foco. Esta comparaciòn es hecha para los 26 grupos de medidas de conteo.

3.2.3 Data Integrity Attacks and their Impacts on SCADA Control System [45]

La amenazas ciberneticas para infraestructuras criticas son un area de crecimiento concerniete. El ataque a la integridad de datos en los sistemas de poder atravez de redes de trabajo SCADA pueden tener efectos severos como es la perdidad operativa por la toma de malas desiciones, casi siempre por un ataque a la integridad para ser exitoso, los datos maliciosos pueden estar dentro de un rango

aceptable. Desde ahora, solo un ataque con inteligencia o un desconocimiento de la funcionalidad del sistema puede causar un ataque efectivo.

El impacto en el sistema fisico es estimado por magnitudes de generacion de carga desbalanceada y la desviaciòn de la frecuencia despues de un ataque exitoso en el control de generaciòn automatico (AGC).

Modelando un ataque sibernetico sobre un sistema de control

El modelo de ataque para un sistema de poder en una red de trabajo de energia. En un sistema de control el receptor del centro de control de datos es llevado desde el sensor hasta la toma de desiciones operacionales para un sistema fisico. Existen 2 tipos de señales que son criticas para una operaciòn estable. El sensado de señales desde el sensor hasta el sistema de control y la señal de control desde el modulo de control hasta el sistema fisico. La manipulaciòn ò perdidas de otros de esa señal puede resultar en una operaciòn inestable del sistema fisico. Un ataque sibernetico que resulte en la manipulaciòn de los datos es referido como un ataque integral y un ataque que resulta en perdidas prolongadas de control o sensado de la señal es referido como una ataque de negaciòn de servicio (DoS). El impacto del ataque, en muchos casos, es proporcional a la duraciòn del ataque.

Existen puntos de severos de vulnerabilidad en una red de trabajo donde un ataque u otros fallas de integridadd o DoS, pueden ser inyectados. La salida de las lineas y el cierre del sistema de control de revisiòn que existen entre el centro de contro y el sistema fisico. La señal de control y el sensado de la señal son transmitidos usando la red de trabajo SCADA.

Modelamiento de ataques a la integridad

Existen 2 formas definidas de ataque a la integridad. Un ataque minimo y un ataque màximo. $Y_i\ (t)$ puede ser la medida del sensor i a un tiempo t y $\left[yi^{min}(t), yi^{max}(t)\right]$, pueden ser el rango de posibles salidas desde el sensor. Un

ataque minimo es definido como un ataque integral donde la salida actual de . $Y_i\ (t)$, desde el sensor es modificada para ser $yi^{min}(t)$, similarmente, un ataque maximo es un ataque donde la salida actual de un sensor i a un tiempo t es modificada para ser $yi^{max}(t)$.

$$yi^{min}(t) = \begin{Bmatrix} Yi\ (t)\ para\ t\ \notin\ \tau a \\ Yi^{min}\ para\ t\ \in\ \tau a \end{Bmatrix}$$

$$yi^{max}(t) = \begin{Bmatrix} Yi\ (t)\ para\ t\ \notin\ \tau a \\ Yi^{max}\ para\ t\ \in\ \tau a \end{Bmatrix}$$

Donde $\tau a = [t_s, t_e]$, es la duraciòn del ataque, t_s y t_e son el tiempo de comienzo del ataque y el tiempo de final del ataque respectivamente.

El modelo del atque minimo y maximo puede ser extendido para la señan de control desde el centro de control como sigue: Si u_i(t), es la señal actual desde el centro de control y $\left[ui^{min}(t), ui^{max}(t)\right]$, es el rango de señales de control posibles , un ataque minimo puede ser cambiado u_i(t) para $ui^{min}(t)$, y un ataque maximo puede ser modificado $ui^{max}(t)$, los ataque minimo y maximo en señales de control pueden ser representados de la siguiente forma:

$$ui^{min}(t) = \begin{Bmatrix} Ui\ (t)\ para\ t\ \notin\ \tau a \\ Ui^{min}\ para\ t\ \in\ \tau a \end{Bmatrix}$$

$$yi^{max}(t) = \begin{Bmatrix} Ui\ (t)\ para\ t\ \notin\ \tau a \\ Ui^{max}\ para\ t\ \in\ \tau a \end{Bmatrix}$$

3.2.4 Propuesta de gestiòn de riesgos para scada en sistemas electricos [46]

En la actualidad los ataques cibernéticos son uno de los principales aspectos a considerar por parte de los entes gubernamentales y por las empresas prestadoras de servicios públicos, dado que dichas entidades son el blanco

preferido para desestabilizar el normal desempeño de las actividades de un sector determinado. En particular, la prestación del servicio eléctrico es fundamental para la operación de la mayor parte de las actividades diarias a nivel comercial, industrial y social de nuestro país.

Los centros de control eléctricos cuentan con el Sistema SCADA para tener información en tiempo real que facilite la supervisión, control y toma de decisiones necesarias para garantizar la seguridad y calidad en la prestación del servicio eléctrico.

SCADA y sus elementos principales

El SCADA consiste típicamente en una colección de equipos de cómputo conectados vía LAN donde cada máquina realiza una tarea especializada, como es la recolección de datos, la visualización y así sucesivamente. Para alcanzar un nivel aceptable de tolerancia de fallas con estos sistemas, es común tener computadores SCADA redundantes operando en paralelo en el centro de control. El SCADA de los sistemas eléctricos recibe toda la información de las subestaciones, se comprueba el funcionamiento del sistema eléctrico en su conjunto y se toman las decisiones para modificarlo o corregirlo si es del caso.

Los principales elementos que componen los Sistemas SCADA son:

Remote Terminal Units (RTU´s) o Estaciones remotas o Intelligent Electronics Device (IED’s)

La RTU es un pequeño y robusto computador que proporciona inteligencia en el campo para permitir quese comunique con los instrumentos. Es una unidad independiente (stand−alone) de adquisición y control de datos, cuya función es controlar el equipamiento del proceso en el sitio remoto, adquirir datos del mismo explorando las entradas de información de campo conectadas con ellos y transferirlos al sistema central SCADA [47].

Las RTU's tienen la capacidad de comunicarse por radio, microonda, satélite, fibra óptica, etc., y algunos estándares de comunicación han comenzado recientemente a emerge para RTU's, como son el DNP3 e IEC60870-5-104.

Las RTU´s han evolucionado a IED´s que corresponden a dispositivos electrónicos inteligentes capaces de supervisar y controlar procesos con funciones de Interfaz ser humano y máquina (HMI) y comunicación a sistemas superiores, es decir, sistemas SCADA sobre los estándares de comunicación mencionados.

Entre los elementos que las RTU’s/IED’s supervisan a nivel eléctrico son:

- Transformador de potencia

- Interruptor

- Seccionador

- Transformador de potencial

- Transformador de corriente

Master Terminal Unit (MTU) o HMI en Subestaciones y en Estación Principal

La parte más visible y "centro neurálgico" del sistema es llamado Master Terminal Unit (MTU) o Interfaz ser humano y máquina (HMI − Human Machine Interface), cuyas funciones principales son recolectar datos de las RTU’s o IED’s, salvar los datos en una base de datos, ponerlos a disposición de los operadores en forma de gráficos, analizar los datos recogidos para ver si han ocurrido condiciones anormales, alertar al personal de operaciones sobre las mismas, generar los informes requeridos y transferir los datos hacia y desde otros sistemas corporativos.

La MTU de SCADA se puede ejecutar en la mayoría de las plataformas y su tendencia es migrar hacia estándares abiertos como ODBC, INTEL PCs, sistemas estándares de gráficos y sistemas de computación corrientes.

La mayoría de los soluciones SCADA cuentan con HMI en las subestaciones (S/E) y HMI en el Centro de Control o Estación principal. Normalmente, los IED se comunican al HMI de S/E los que a su vez se comunican con el HMI principal.

Procesadores de Comunicaciones Front End La interfaz a la red de comunicaciones es una función asignada a un computador llamado Front End, el cual maneja toda la interconexión especializada a los canales de comunicaciones y realiza la conversión de protocolos de modo que el sistema principal pueda contar con datos en un formato estándar.

Debido a que los SCADA cubren áreas geográficas grandes, normalmente depende de una variedad de sistemas de comunicación: LAN normalmente confiables y de alta velocidad, y WAN menos confiables y de más baja velocidad; por lo que se han desarrollado técnicas para la transmisión confiable sobre diferentes medios. Los progresos recientes han considerado la aparición de un número apreciable de protocolos "abiertos".

Aplicaciones especiales

Casi todos los sistemas SCADA tienen software de aplicación especial, asociado generalmente al

monitoreo y al control.

PROTOCOLOS DE COMUNICACIÓN DEL SCADA

Los protocolos utilizados van de acuerdo con cada uno de los medios disponibles en la comunicación. Algunos de los más comunes son:

Protocolo IEC 61850

La norma IEC 61850 es un estándar internacional de comunicación para subestaciones automatizadas que se extiende a otros elementos del sistema eléctrico. El objetivo de la norma IEC 61850 es comunicar IEDs de diferentes fabricantes buscando interoperabilidad entre funciones y elementos, y la armonización de las propiedades generales de todo el sistema. Para lograrlo, la norma no solo define las comunicaciones, sino que también define un lenguaje de configuración

del sistema, condiciones ambientales y especificaciones de calidad de los equipos, y procedimientos para probar equipos. La norma IEC 61850 adopta como red de área local la red Ethernet y define diversos niveles lógicos y físicos en una subestación, como nivel estación, nivel campo y nivel proceso, no define ninguna topología en particular [48].

La posibilidad de implementar una instalación bajo IEC 61850, permite reducir el cableado entre los distintos aparatos de maniobra y protección, debido al remplazo de señales eléctricas por mensajes, que envían información digital o análoga.

Las tendencias en la automatización de las compañías eléctricas, especialmente de las subestaciones, convergen en una arquitectura de comunicaciones común con el objetivo de tener la interoperabilidad entre una variedad de IEDs encontrados en las subestaciones, que puede:

- Desarrollar un estándar internacional para las comunicaciones en el interior de una subestación automatizada.

- Conseguir interoperabilidad entre equipos de diferentes proveedores.

- Permitir la comunicación cerca de los equipos de potencia.

- Reducir el cableado convencional.

Protocolo Distributed Network Protocol - DNP3

La telemetría de radio es probablemente la tecnología base de SCADA. Una red de radio típica consiste en una conversación a través del repetidor situado en algún punto elevado y un número de RTU's que comparten la red. Todas las RTU's "hablan" sobre una frecuencia (F1) y escuchan en una segunda frecuencia (F2). El repetidor escucha en F1, y retransmite esto en F2, de modo que una RTU que transmite un mensaje en F1, lo tiene retransmitido en F2, tal que el resto de RTU's pueda oírlo. Los mensajes del Master viajan sobre un enlace de comunicación dedicado hacia el repetidor y son difundidos desde el repetidor en F2 a todas las RTU's. Si el protocolo de comunicaciones usado entre el Master y el repetidor es diferente al usado en la red de radio, entonces debe haber un "Gateway" en el sitio del repetidor [49].

DNP3 se ha utilizado con éxito sobre la red de radio, que encapsulado en TCP/IP, permite que una red de fines generales lleve los datos al Master. DNP3 es un protocolo SCADA moderno, en capas, abierto, inteligente, robusto y eficiente, que puede [47]:

- Solicitar y responder con múltiples tipos de dato en un solo mensaje.

- Segmentar mensajes en múltiples frames para asegurar excelente detección y recuperación de errores.

- Incluir en una respuesta, sólo datos cambiados.

- Asignar prioridad a los ítems de datos y solicitarlos periódicamente basado en su prioridad.

- Responder sin solicitud previa.

- Utilizar sincronización de tiempo con un formato estándar.

- Permitir múltiples operaciones punto a punto y al Master.

- Permitir objetos definibles por el usuario incluyendo

Protocolo IEC 60870-5-104

El protocolo IEC 60870-5-104 o IEC 104 es un estándar basado en el IEC 60870-5-101 o IEC 101. Utiliza la interfaz de red TCP/IP para disponer de conectividad a la red LAN y para conectarse a la WAN. La capa de aplicación IEC 104 se conserva igual a la de IEC 101 con algunos de los tipos de datos y los servicios utilizados.

Generalmente para los sistemas de energía, se utiliza el protocolo IEC 104 para el centro de control y el protocolo IEC 101 para la interacción con los IEDs.

La ventaja más grande del protocolo IEC 60870-5-104 es que habilita la comunicación a través de una red estándar y permite la transmisión de datos simultáneos entre varios dispositivos y servicios, debido a que el protocolo IEC 60870-5-104 define el uso de una red TCP como medio de comunicación [50].

Identificaciòn y valoraciòn de Activos de Informaciò en los sistemas SCADA

Los activos más importantes a tener en cuenta para el análisis de riesgos para un sistema SCADA son los siguientes: IED, HMI en S/E (HMI S/E), HMI en principal (HMI P/L), Front End (FE) y Protocolos (PT).

Los activos se valoran con base en los elementos principales para la seguridad de la información: Confidencialidad, Integridad, Disponibilidad, Trazabilidad y No repudio.

La valoración de los activos se puede realizar de acuerdo con la siguiente Tabla:

Tabla 5. Valoración de Activos

VALORACION DE ACTIVOS
CATASTROFICO
MAYOR
MODERADO
MENOR
INSIGNIFICANTE

Tabla 6. Resultado de valoración y su correspondiente justificación.

Activo	Confidencialidad		Integridad		Disponibilidad		Trazabilidad		No Repudio	
	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación
IED	Moderado	Información operativa convencional que no merece ser confidencial	Catastrófico	Por ser la unidad básica de recepción/envió de información, su integridad es de muy alta valoración.	Moderado	Indisponible la supervisión sobre el elemento o la función que realice el elemento indisponible	Catastrófica	Los cambios en IED realizados deben ser registrados para determinar los cambios a efectuar en HMI S/E y HMI Principal	Menor	Los cambios y quien los realiza en IED deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
HMI S/E	Moderado	Información operativa convencional que no merece ser confidencial	Moderado	Si su funcionamiento no es adecuado se realiza manejo del IED directamente	Mayor	La supervisión y control de la S/E se hace muy dispendiosa y la información no estaría disponible	Catastrófica	Los cambios en HMI S/E realizados deben ser registrados para determinar los cambios a efectuar en IED y HMI Principal	Menor	Los cambios y quien los realiza en HMI S/E deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
HMI Principal	Moderado	Información operativa convencional que no merece ser confidencial	Mayor	Si su funcionamiento no es adecuado se realiza manejo del HMI de todas las S/E o IED directamente	Catastrófica	La supervisión y control del Sistema eléctrico no podría realizarse.	Catastrófica	Los cambios en HMI principal realizados deben ser registrados para determinar los cambios a efectuar en IED y HMI de S/E	Menor	Los cambios y quien los realiza en HMI Principal deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
Front End	Moderado	Información operativa convencional que no merece ser confidencial	Mayor	Si su funcionamiento no es adecuado se realiza manejo del HMI de todas las S/E o IED directamente	Catastrófica	La supervisión y control del Sistema eléctrico no podría realizarse.	Catastrófica	Los cambios en Front End realizados deben ser registrados para determinar los cambios a efectuar en HMI Principal y HMI de S/E	Menor	Los cambios y quien los realiza en Front End deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
Protocolos	Insignificante	Protocolos utilizados son estándares	Menor	Los protocolos utilizados son confiables	Insignificante	No aplica el concepto de disponibilidad	Menor	No se ha visto la necesidad de verificar logs de estos protocolos	Insignificante	No aplica el concepto de no repudio

IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

Al igual que los activos, los riegos deben ser identificados y valorados con base en los elementos principales para la seguridad de la información: Confidencialidad, Integridad, Disponibilidad, Trazabilidad y No repudio.

En este paso se determinan los riesgos con base en las vulnerabilidades que se tienen y que son explotadas por las amenazas.

Tabla 7.Identificaciòn de la valoraciòn por simbolos y colores.

IA	INACEPTABLE
ID	INADMISIBLE
TO	TOLERABLE
AC	ACEPTABLE

Tabla 8. Valoraciòn del Riesgo – Perdida de Confiabilidad del Activo

VALORACION RIESGO - PERDIDA DE CONFIDENCIALIDAD DEL ACTIVO						
VULNERABILIDAD	AMENAZA	IED	HMI S/E	HMI P/L	FE	PT
Controles inadecuados de acceso físico/lógico	Abuso de Privilegios	IA		TO	TO	
	Acceso no autorizado	IA		IA	IA	
	Escaneos de red (I)	IA			IA	
	Análisis de trafico			IA		
Configuración incorrecta o Inadecuada	Abuso de privilegios	IA		TO	IA	
	Acceso no autorizado	IA	IA	IA	IA	
	Escaneos de red (I)	IA			ID	
	Análisis de trafico		IA	IA		
	Escapes de información			IA		
Poca conciencia sobre la seguridad de la información	Divulgación de información			IA		
	Ataque de ingeniería social			IA		
	Fuga/Robo de información			IA		
Inadecuado procedimiento de actualizaciones de seguridad y antivirus	Errores del administrador		IA	IA		
	Vulnerabilidad de programas		TO	IA		
	Difusión sw dañino		IA	IA		

Tabla 9: Valoraciòn del Riesgo – Perdida de Integridad del Activo

VALORACION RIESGO - PERDIDA DE **INTEGRIDAD** DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Controles inadecuados de acceso fisico/lógico	Abuso de Privilegios	IA	IA	IA		TO
	Acceso no autorizado	IA	ID	ID		IA
	Ataque dirigido	IA	ID	ID		
	Manipulación de la configuración		ID	ID	ID	TO
	Manipulación de programas		IA	IA		
Configuración incorrecta o inadecuada	Errores de administrador	IA	ID	ID		IA
	Abuso de privilegios	IA	IA	IA	IA	
	Acceso no autorizado	IA		IA		
	Difusión sw dañino		ID	ID		
	Fallas de software		ID	ID		IA
	Errores de los usuarios			IA		
	Fallas de hardware				ID	
	Ataque dirigido				ID	
	Vulnerabilidad de los programas					IA
Inadecuados esquemas de reposición de activos obsoletos	Acceso no autorizado		ID	ID	ID	
	Abuso de privilegios		IA	IA		
	Ataque dirigido		ID	ID	ID	ID
	Difusión sw dañino		ID	ID		
Insuficientes o inadecuados mantenimientos predictivos, preventivos y/o correctivos	Fallas de hardware				ID	
	Degradación de los soportes de almacenamiento				ID	

Tabla 10: Valoraciòn del Riesgo – Perdida de disponibilidad del Activo

VALORACION RIESGO - PERDIDA DE DISPONIBILIDAD DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Controles inadecuados de acceso fisico/lógico	Abuso de privilegios	IA	IA	IA		
	Acceso no autorizado	ID	ID	ID		
	Denegación de Servicios	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
Configuración incorrecta o inadecuada	Acceso no autorizado	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
	Caida del sistema por agotamiento de recursos		ID	IA	ID	
	Denegación de servicios	ID	ID	ID	ID	
Insuficiente protección contra virus y código malicioso	Fallas de sw		ID	ID		
	Vulnerabilidad de los programas		ID	ID		
	Denegación de servicios		ID	ID		
Punto único de fallo	Fallas de hardware				ID	
	Caidas del sistema por agotamiento de recursos				ID	
	Ataque dirigido				ID	
Insuficientes o inadecuados mantenimientos predictivos, preventivos y/o correctivos	Fallas de hardware				ID	
	Degradación de los soportes de almacenamiento				ID	
	Averia de origen fisico/lógico				ID	

Tabla 11. Valoraciòn del Riesgo – Perdida de Trazabilidad del Activo

VALORACION RIESGO - PERDIDA DE **TRAZABILIDAD** DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Escasos registros en logs o variables auditables	Fallas de hardware	IA				
	Errores de administrador	IA	IA	ID	IA	IA
	Acceso no autorizado	IA			IA	
	Ataque dirigido				IA	
	Abuso de privilegios				IA	
	Manipulación de la configuración		IA			IA
	Errores de configuración					IA
	Errores de monitorización					IA
	Destrucción de información		IA	ID		
Pocos mecanismos de control y Monitoreo	Errores de administrador	IA	IA	ID	IA	
	Errores de configuración	IA			IA	
	Ataque dirigido	IA	IA	ID		
	Errores de monitorización		ID	ID		

3.2.5 Sistema de respaldo nacional ante eventos de gran magnitud - SIRENA

Una aplicaciòn de Redes Inteligentes en el sistema de transmisiòn Nacional de Energia [51]

El proyecto SIRENA de XM, busca implementar un esquema de protecciòn de la integridad del sistema (ESPIS), de nueva generaciòn, que permita ejercer control y protecciòn del sistema para prevenir y mitigar la ocurrencia de eventos de gran magnitud en el sistema interconectado nacional.

¿Cómo se protege el sistema de potencia ante eventos?

Los operadores de los sistemas de potencia identifican restricciones para el transporte de energia en la red de transmisiòn utilizando unos criterios de seguridad y confiabilidad previamente definidos en la reglamentaciòn. El codigo de redes [52] es la base de estos criterios en colombia. La practica usual en la industria ha sido cubrirse ante eventos “creibles” con el fin de balancear la seguridad y la economia, aplicando criterios de estado estacionario y estabilidad

dinamica del sistema, de manera que este sea capaz de soportar contingencias preestablecidas sobre la red.

Por lo anterior, las contigencias de muy baja probabilidad de ocurrencia usualmente no son consideradas en los analisis y los sistemas no estan diseñadas para soportarlas. Sin embargo, en los casos en donde puede existir un gran impacto en los usuarios, es necesario identificar soluciones alternativas costo – efectivas.

El elemento subyacente a estas practicas es que no es posible alcanzar una operaciòn de un 100% confiable del sistema de potencia, debido a que:

El tamaño y la complejidad de los sistemas de potencia dificultad su control de parte de un operador humano.

Existen casi infinitas combinaciones de escenarios de operaciòn y contigencia, lo cual hace impractico el utilizar mecanismos de protecciòn previamente simulados

Aun el sistema mejor planeado ocurren eventos mas alla de lo creible y que llevan al sistema al limite de upervivencia , incluyendo errores humanos.

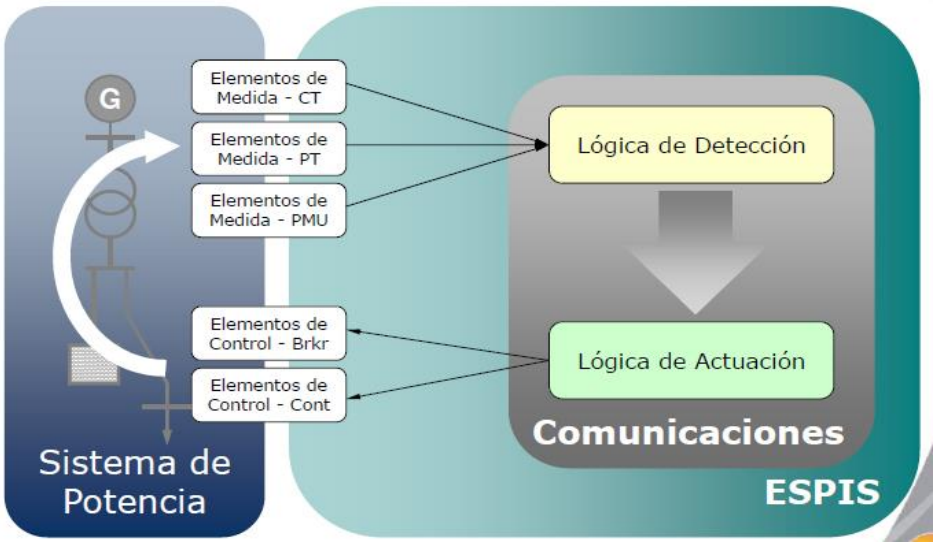
La soluciòn mas efectiva a la problemática descripta ha sido encontrda en la implementaciòn del Esquema de proteccion de la integridad de sistemas de potencia (ESPIS)

Esquema de Protecciòn de la Integridad del Sistema (ESPIS)

Los esquemas de proteccion de la integridad del sistema de potencia (ESPIS) son un conjunto de elementos de protecciòn y control que permiten detectar y controlar condiciones anormales de operaciòn en el sistema. Estos esquemas actuan sobre los equipos de la red con el fin de minimizar la extensiòn y duraciòn de los eventos, asi como colapsos parciales o totales de la demanda atendida. Aunque en la practica estan compuestos por elementos de protecciòn, se diferencias conceptualmente de la protecciòn de equipos, en su funciòn de

proteger el sistema (la continuidad de la atenciòn de la demanda) y no elementos de la red en particular.

Figura 13: Sistema ESPIS



Generalmente se implementan como protecciòn de ultima linea ante eventos de baja probabilidad de ocurrencia o ante condiciones de degradaciòn de la red (mantenimientos mayores, atentados, etc.) Estos son necessarios debido a que las protecciones “normales” no estan diseñadas para proteger el sistema, ni se pretende que lo hagan, y a que, y a que, adicionalmente, los humanos son lentos. Por lo tanto en muchos casos para protegerse ante eventos debe utilizarse una combinaciòn de hardware y software.[53]

Del estudio del estado del arte se puede ver que se estudian las fallas por medio de redes de petri, sistemas SCADA y otros software que miden de forma general las fallas que se presentan en las lineas de transmisiòn, sin embargo la mayor parte de los estudios encontrados estan enfocados en sistemas SCADA, los cuales veremos en el capitulo siguiente enfocandonos en especifico en las fallas de software e infraestructura que son de gran incidencia en el sistema de detecciòn de fallas de SCADA.

CAPITULO IV

4.1 CARACTERIZACIÒN DE LOS DATOS ESTADISTICOS DE LAS FALLAS EN LOS SISTEMAS ESCADA

En los sistemas SCADA se presentan diversos tipos de fallas que tienen como efecto la parálisis o la perdida de información, esto trae como consecuencia la desinformación de los controladores para la toma de decisiones, por tal motivo se estudiara las fallas más frecuentes y dentro de estas las más relevantes para los centros de operación que trabajan con sistemas SCADA.

Para esto trabajaremos con una base de datos suministrada por la compañía XM la cual consta de una serie de tiempo de 694 datos, los cuales clasificaremos y caracterizaremos para cuantificarlos y así poder emitir un concepto acerca de estos.

4.1.1 Fallas Operacionales

En primer lugar clasificamos las fallas en 2 grupos.

1. Fallas Operacionales

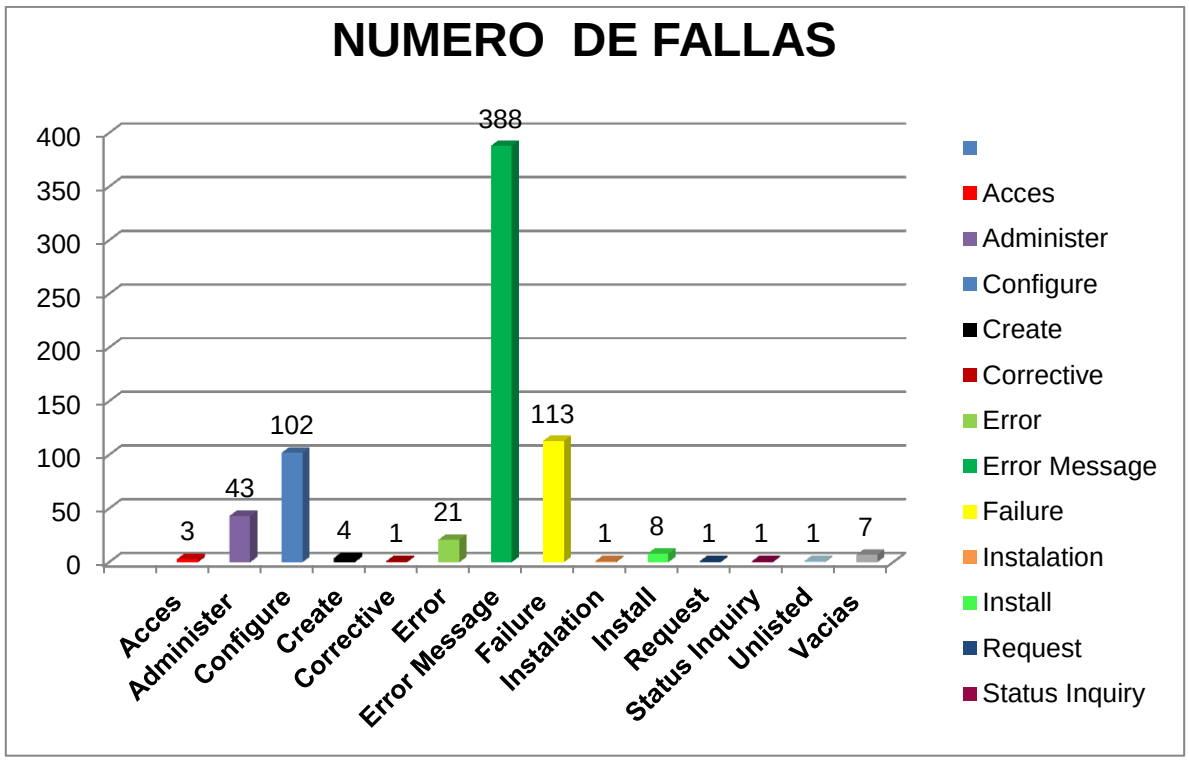
Las cuales tienen las siguientes fallas integradas en su lista del sistema SCADA

a. Corrective
b. Create
c. Error
d. Error Message
e. Acces
f. Administer
g. Configure
h. Failure
i. Instalation

j. Install
k. Request
l. Status Inquiry
m. Unlisted
n. Vacias

Estas son cuantificadas y graficadas con el fin de analizar cuál de las anteriores tiene mayor peso.

Gráfico 1: Número de fallas por errores operacionales



Como podemos observar en el grafico la mayor parte de la fallas está concentrada en 3 errores. Error Message (388), Failure (113) y configure (102), lo que indica que se debe estudiar la causa raíz de estas fallas y detectar el problema para minimizar el 86 % de las fallas operacionales.

4.1.2 Fallas de Producto

El segundo grupo de fallas en la serie de tiempo son las siguientes:

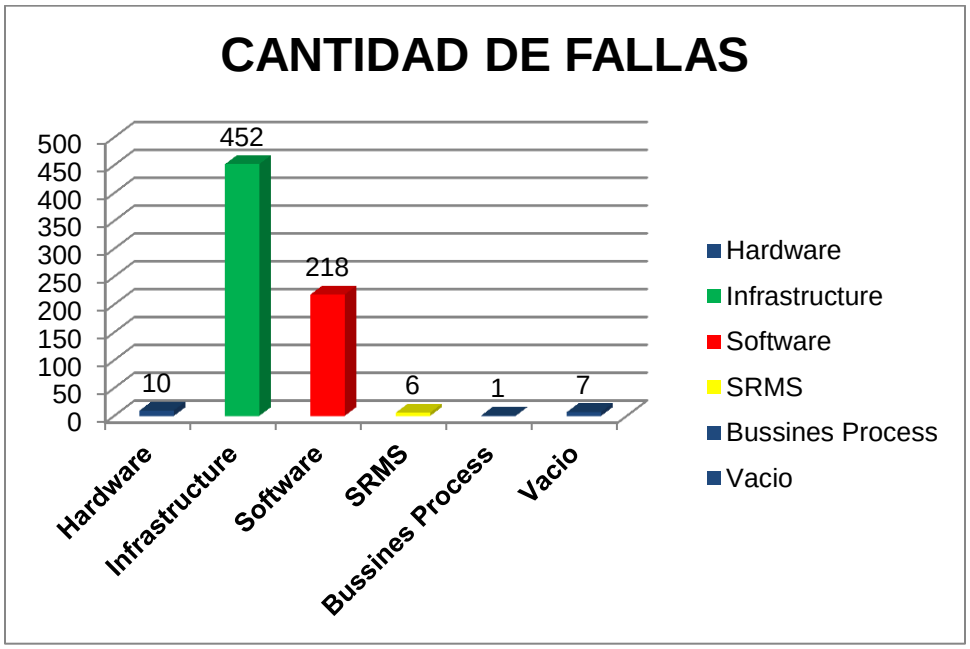
2. Fallas de producto

Estas son en las que nos enfocaremos para realizar nuestros análisis estadísticos y contienen el subgrupo integrado a las fallas del sistema SCADA

a. Hardware
b. Infraestructura
c. Software
d. SRMS
e. Bussines Process
f. Vacío

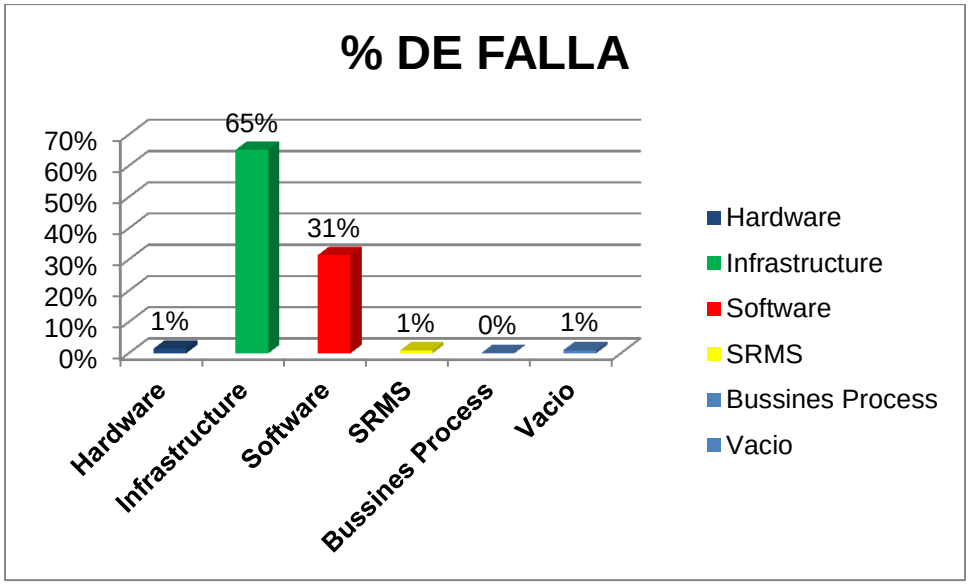
Estas son cuantificadas y graficadas con el fin de determinar cuáles son las que tienen mayor relevancia en el sistema SCADA:

Gráfico 2: Fallas por error en la falla de productos



Como podemos observar en la gráfica, las fallas que presentan con mayor frecuencia, son las de Infraestructura y las de software de las cuales se muestra el porcentaje en la siguiente gráfica

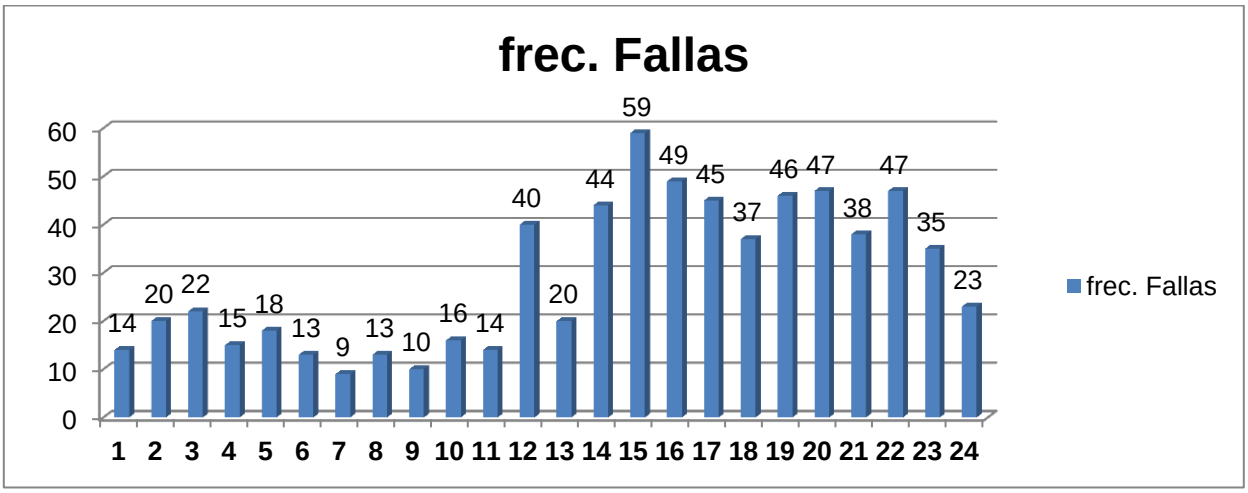
Grafico 3: Porcentaje de fallas



Estas representan el 96% de las fallas de producto, por tal motivo se estudiarán a continuación de forma detallada con el fin de saber de forma más detallada cual es la causa del problemas y en que periodos de tiempo es más frecuente.

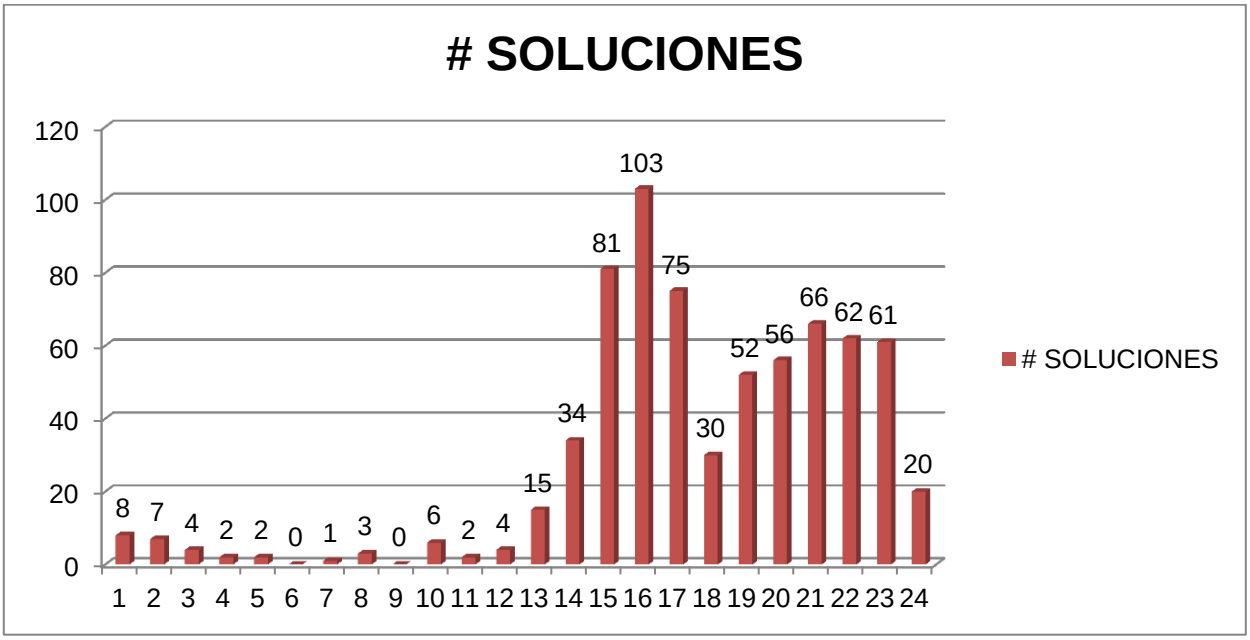
Lo primero que se realizo fue cuantificar las fallas totales para un periodo de 24 horas (1 día), con el objeto de ver el comportamiento de estas a determinadas horas.

Grafica 4: Frecuencia de fallas por hora



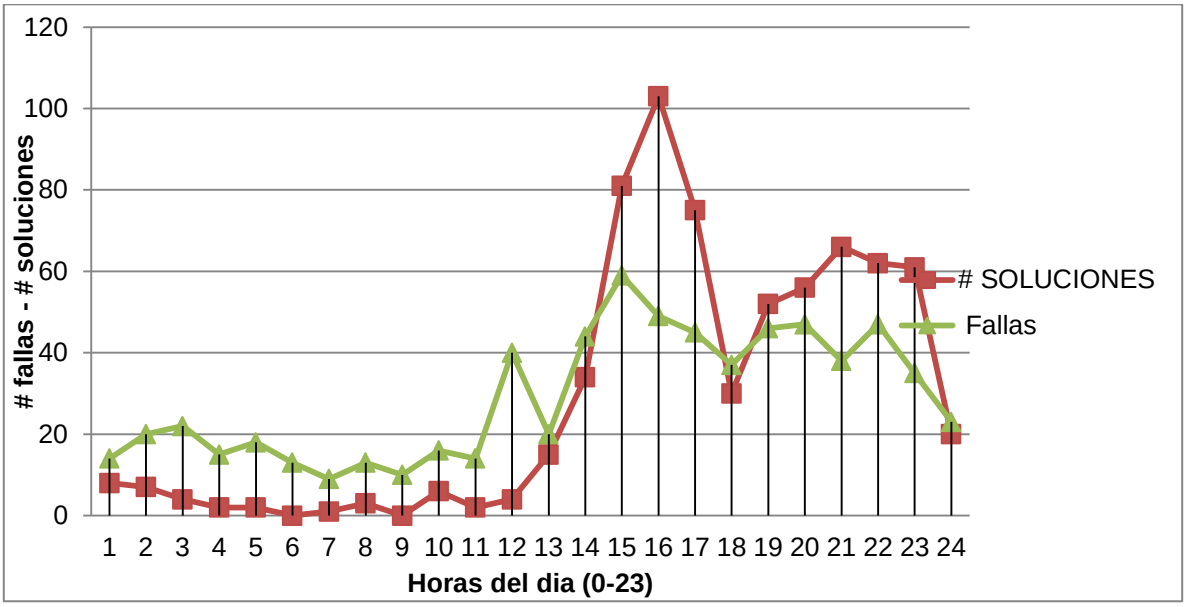
Analizando el gráfico se puede ver que las fallas más frecuentes se dan en las hora 12, 15, 19, 20 y 22, que es el tiempo en que existe mayor demanda de energía en las redes de transmisión, por lo tanto los fallos en estas horas pueden causar demanda no suministra generando pérdidas económicas a las compañías de transmisión de energía. Esto lo contrastamos con las soluciones presentadas en estas fallas de acuerdo al siguiente gráfico.

Grafico 5: Soluciones por Hora del día



Como se puede observar las horas en las que se dan las soluciones son muy diferentes a la hora en la que se presentan las fallas y se puede apreciar que la mayor parte de las soluciones son una hora o dos después de que estas se presentan, lo que es un lapso de tiempo muy largo si esto produce demanda no atendida.

Grafico 6: Fallas Vs Soluciones



Aquí se puede apreciar que las primeras 12 horas del día las soluciones se comportan inversamente proporcional a las fallas y las otras 12 horas se comporta directamente proporcional.

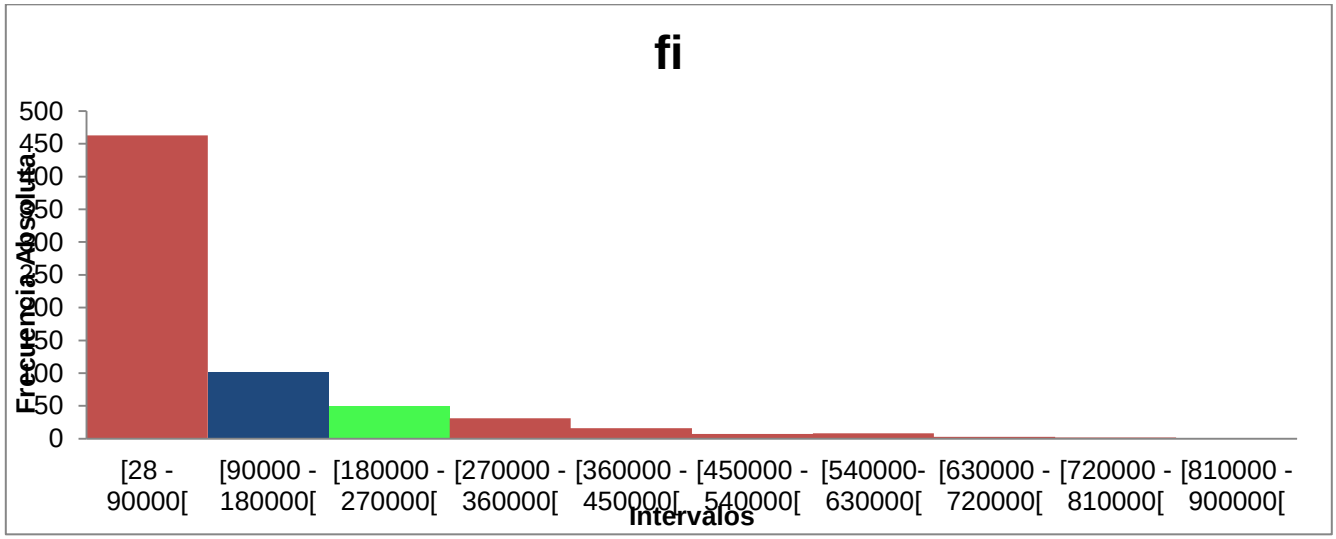
Ahora realizamos una distribución de frecuencia de los datos de tiempo de las fallas para ver en que rangos se ubican el mayor número de fallas, para esto se realiza la siguiente tabla en la cual tenemos 20 clases con el fin de obtener mayor información en cada intervalo de estos.

Tabla 12: Distribución de frecuencia de los tiempos de fallas.

Intervalos	Clases segundos	Clases Horas	fi	Fi	fr	Fr
[28 -90000[	90000	25	463	463	0,66714697	0,66714697
[90000 - 180000[	180000	50	102	565	0,14697406	0,81412104
[180000 - 270000[	270000	75	49	614	0,07060519	0,88472622
[270000 - 360000[	360000	100	31	645	0,04466859	0,92939481
[360000 - 450000[	450000	125	16	661	0,02305476	0,95244957
[450000 - 540000[	540000	150	7	668	0,01008646	0,96253602
[540000- 630000[	630000	175	8	676	0,01152738	0,9740634
[630000 - 720000[	720000	200	3	679	0,00432277	0,97838617
[720000 - 810000[	810000	225	2	681	0,00288184	0,98126801
[810000 - 900000[	900000	250	1	682	0,00144092	0,98270893
[900000 - 990000[	990000	275	3	685	0,00432277	0,9870317
[990000 - 1080000	1080000	300	2	687	0,00288184	0,98991354
[1080000 - 1170000[	1170000	325	1	688	0,00144092	0,99135447
[1170000 - 1260000[	1260000	350	1	689	0,00144092	0,99279539
[1260000 - 1350000[	1350000	375	0	689	0	0,99279539
[1350000 - 1440000[	1440000	400	2	691	0,00288184	0,99567723
[1440000 - 1530000[	1530000	425	0	691	0	0,99567723
[1530000 - 1620000[	1620000	450	1	692	0,00144092	0,99711816
[1620000 - 1710000[	1710000	475	1	693	0,00144092	0,99855908
[1710000 - 1820000]	1820000	505,5555556	1	694	0,00144092	1

Para visualizar de forma más clara la distribución de las frecuencia de los tiempo de fallas, se realizó el siguiente gráfico.

Grafico 7: Frecuencia Absoluta de los tiempos de fallas



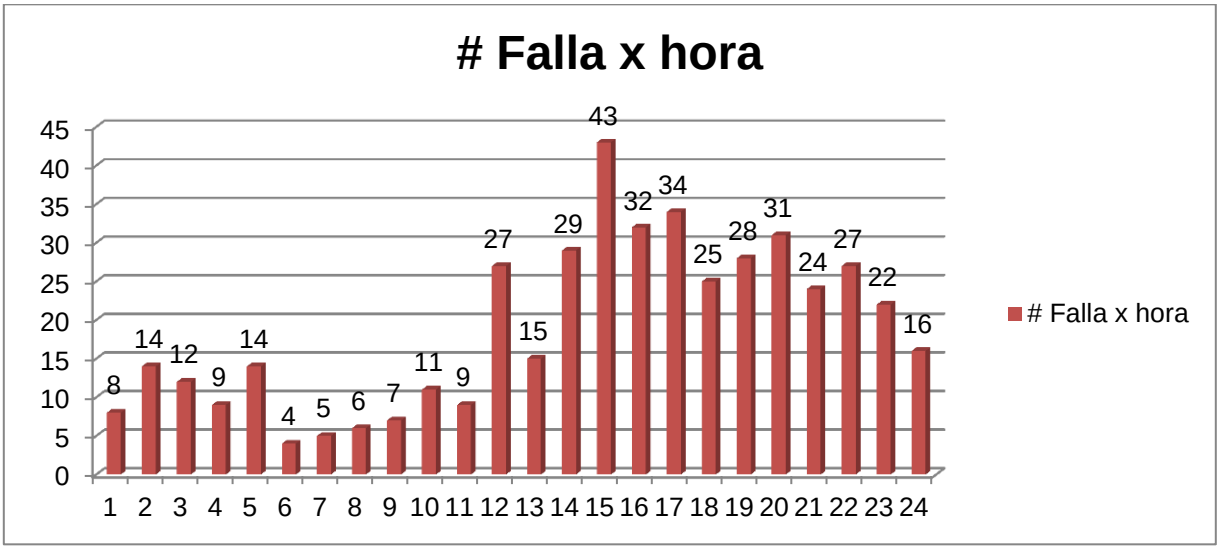
Se puede ver que la mayor parte de los tiempos de fallas se presenta en los primeros cuatro intervalos los cuales esta comprendidos entre los 28 y los 360000 segundos, lo que representan tiempos en los cuales se pueden presentar riesgos muy altos de corte temporal de la energía suministrada o un apagón total.

4.1.3 Fallas en Infraestructura y su cuantificación

Ya analizado de forma general las fallas de producto, se procede a analizar las fallas en la infraestructura, para esto realizamos una distribución de frecuencia de los eventos de fallas con respecto a la hora.

De esta obtenemos el siguiente gráfico:

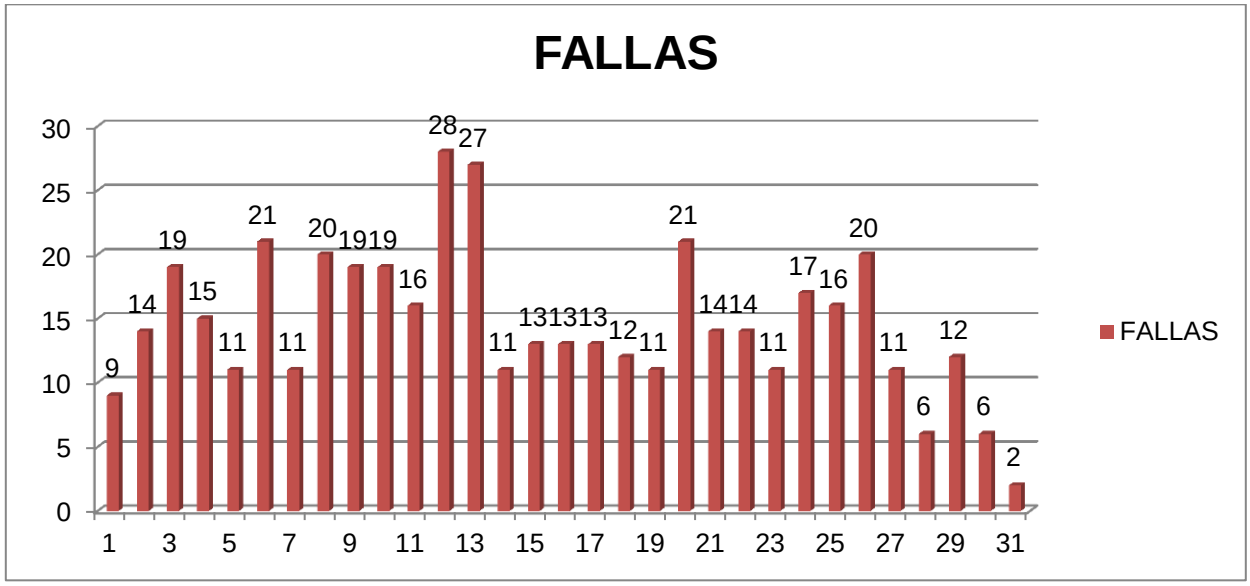
Grafico 8: Fallas de Infraestructura por hora del día



El número total de fallas en software es de 452, donde se observa que la gran mayoría de estas están concentradas en las horas 12, 15, 17 y 20, muy similares a las horas donde se presentan las fallas totales de producto.

Las fallas por Infraestructura representan el 65.1% de las fallas de producto; luego de analizar las horas de un día, se pasa analizar las fallas presentadas en los 31 días que componen un mes, con el fin de ver cuáles son los que muestran más frecuencias de falla.

Gráfico 9: Frecuencias de fallas por día del mes



Se observar que los día 3, 6, 12, 13, 20 y 26 es donde se presentan mayor número de fallas de Infraestructura siendo este un comportamiento irregular que no muestra un espacio consecuente entre los días con mayor frecuencia.

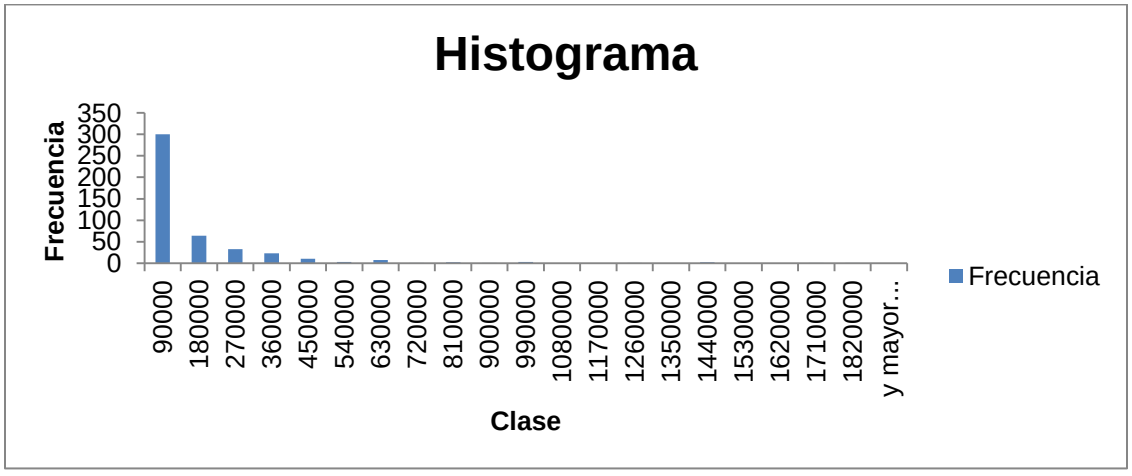
Se crea una tabla que contiene clase, probabilidad, frecuencia y hora de las fallas de Infraestructura y con esta se construye un histograma.

Tabla 13: Frecuencia de probabilidad

Clase	Probabilidad	Frecuencia	Horas
90000	0,663716814	300	25
180000	0,14159292	64	50
270000	0,07300885	33	75
360000	0,050884956	23	100
450000	0,022123894	10	125
540000	0,006637168	3	150
630000	0,015486726	7	175
720000	0,002212389	1	200
810000	0,004424779	2	225
900000	0,002212389	1	250
990000	0,006637168	3	275
1080000	0	0	300
1170000	0	0	325
1260000	0,002212389	1	350
1350000	0	0	375
1440000	0,004424779	2	400
1530000	0	0	425
1620000	0	0	450
1710000	0,002212389	1	475
1820000	0,002212389	1	505,5555556

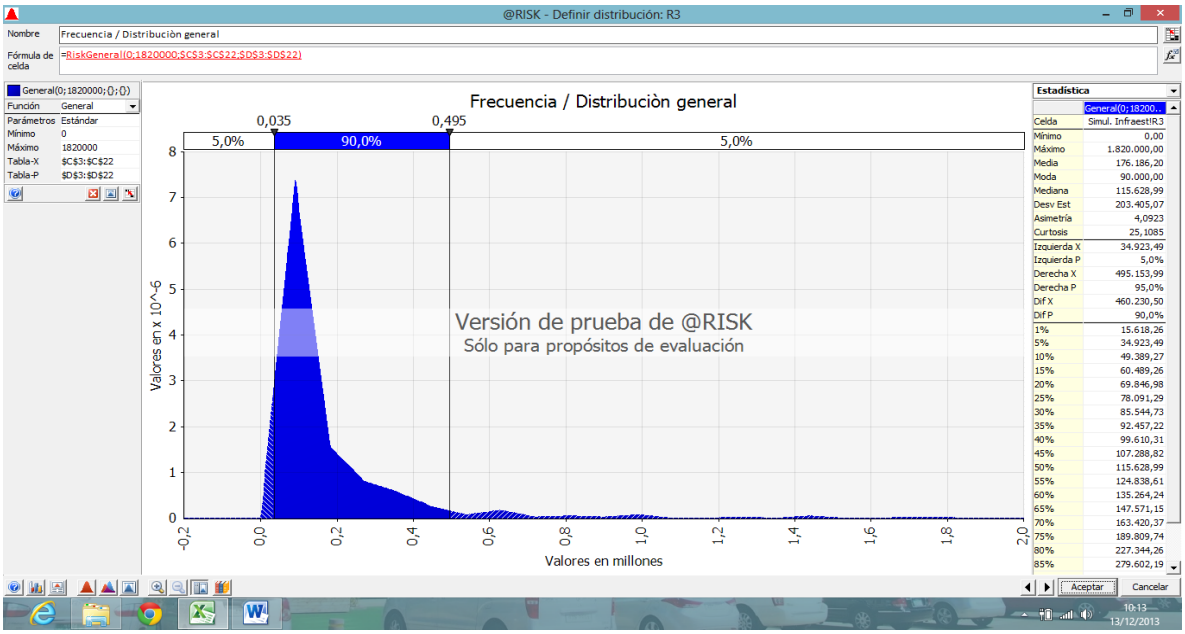
Con esta tabla se realiza el siguiente histograma:

Grafico 10: Histograma de distribución de frecuencia.



En el histograma se puede ver que el mayor número de fallas se presenta entre 90000 y 450000 segundos, siendo esto demasiado tiempo y representando un riesgo significativo para la ocurrencia de cortes o apagones.

Figura 14: Distribución general de fallas en infraestructura



Muestra una concentración de las fallas de infraestructura de un 90% y el resto de los valores por fuera de la franja es mínimo.

Ahora se calcula la probabilidad de una falla en una hora determinada, para esto debemos definir los Xi, los cuales son las 24 horas de 1 día y los Pi, que son la probabilidad de falla en cada hora.

Tabla 14: Probabilidad de fallas por hora del día

Hora (Xi)	Prob (Pi)
0	0,01769912
1	0,03097345
2	0,02654867
3	0,0199115
4	0,03097345
5	0,00884956
6	0,01106195
7	0,01327434
8	0,01548673
9	0,02433628
10	0,0199115
11	0,05973451
12	0,03318584
13	0,06415929
14	0,09513274
15	0,07079646
16	0,07522124
17	0,05530973
18	0,0619469
19	0,06858407
20	0,05309735
21	0,05973451
22	0,04867257
23	0,03539823

Al analizar los datos de la duración de las fallas de infraestructura por medio de @Risk, se observa que ninguna distribución estadística conocida se ajusta a tales datos, puesto que el valor p arrojado por el test estadístico chí-cuadrado es inferior al nivel de significancia alpha de 0.05. Adicionalmente las estadísticas de las diferentes distribuciones analizadas por @Risk difieren significativamente de los datos reales; por ejemplo, la mayoría de distribuciones arrojan valores negativos y las desviaciones estándar ajustadas difieren altamente de la real.

Dado que ninguna distribución conocida se ajusta a los datos, hemos decidido simular utilizando una distribución empírica construida a partir de los datos que se tienen (ver figura 15 y tabla 15).

Figura 15: Distribución empírica

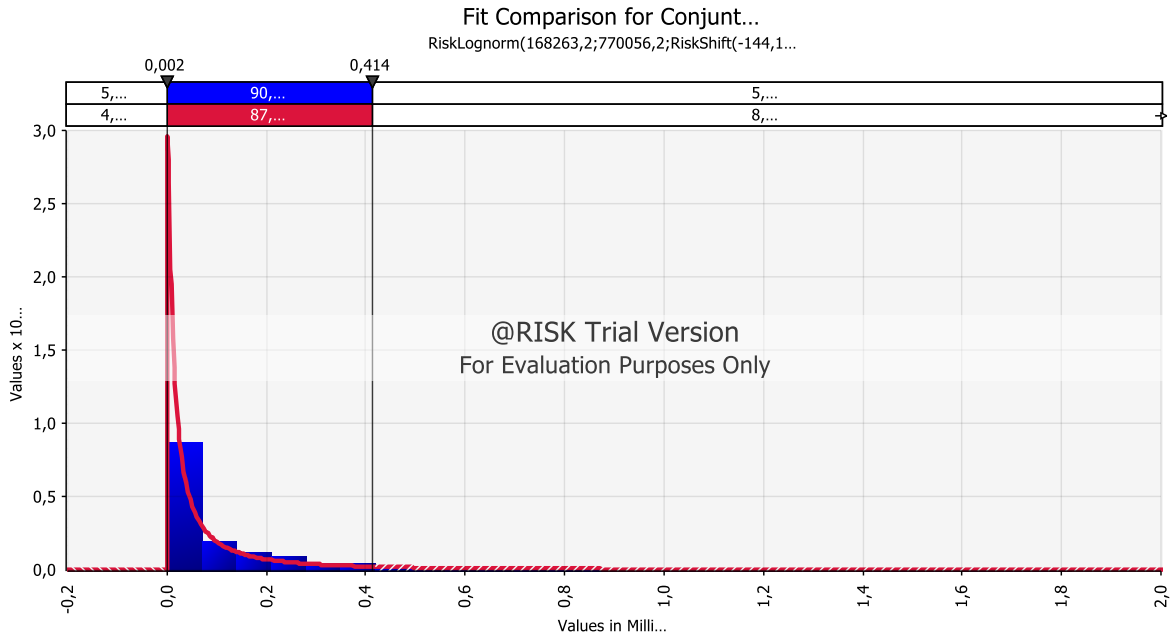
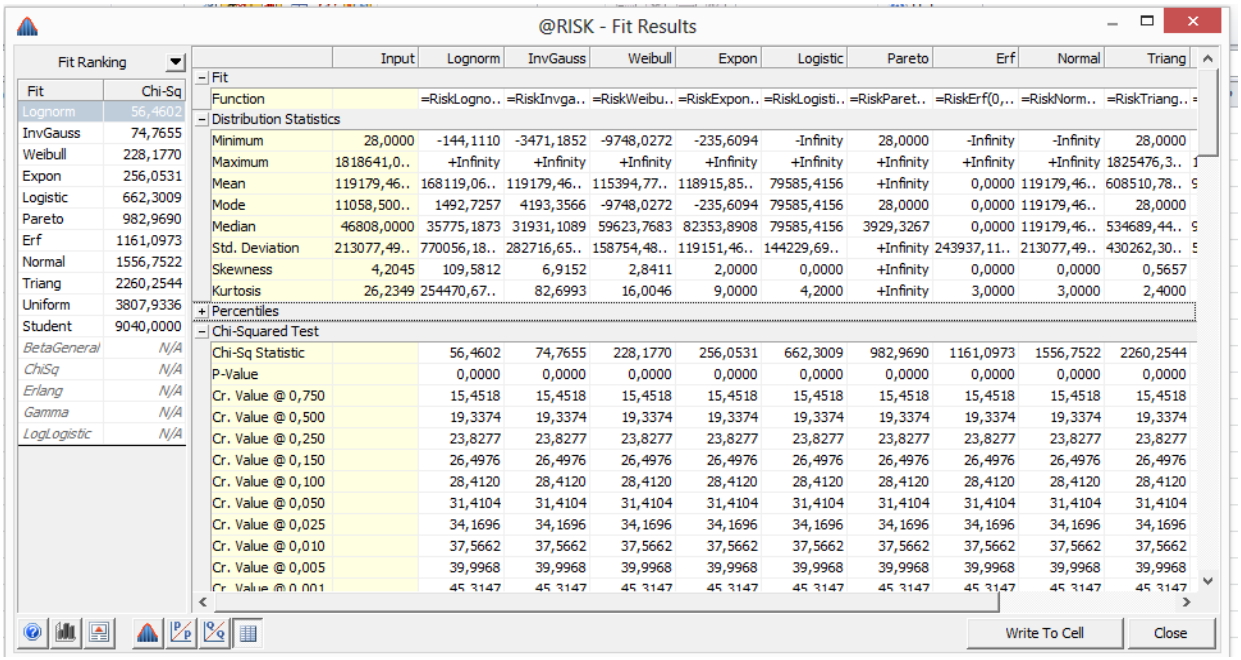


Tabla 15: Parámetros estadísticos de aceptación o rechazo



Teniendo este ajuste se procede a realizar la simulación en la cual hallamos la severidad (el tiempo que dura una falla en una posición n), ósea las pérdidas de distribución agregadas las cuales de forma matemática se calculan como $LDA = \sum_{t=1}^{N} Xt$, donde N es la frecuencia y X es el tiempo.
El LDA es el valor del VaR para un evento determinado, en este caso mostramos el valor para 2 eventos diferentes.

Para las fallas de infraestructura realizamos una simulación de 100 eventos los cuales nos van entregando en la casilla severidad el tiempo de duración de cada uno de estos en segundos y en la frecuencia el número de veces que este se presenta.

Tabla 16: Cuantificación del VaR por evento 1

Frecuencia	Evento	Severidad	Segundos	Total horas	Promedio horas
10	1	322248,7613	322248,761	89,5135448	8,95135448

Esto nos indica que la pérdida de tiempo en el día 1 sería de 8,9 horas, lo cual se concluye que este valor al riesgo sería demasiado alto teniendo en cuenta que un día tiene 24 horas.

Tabla 17: Cuantificación del Var por Evento 2

Frecuencia	Evento	Severidad	Segundos	Total horas	Promedio horas
26	23	425872,996	425872,996	118,298054	4,549925171

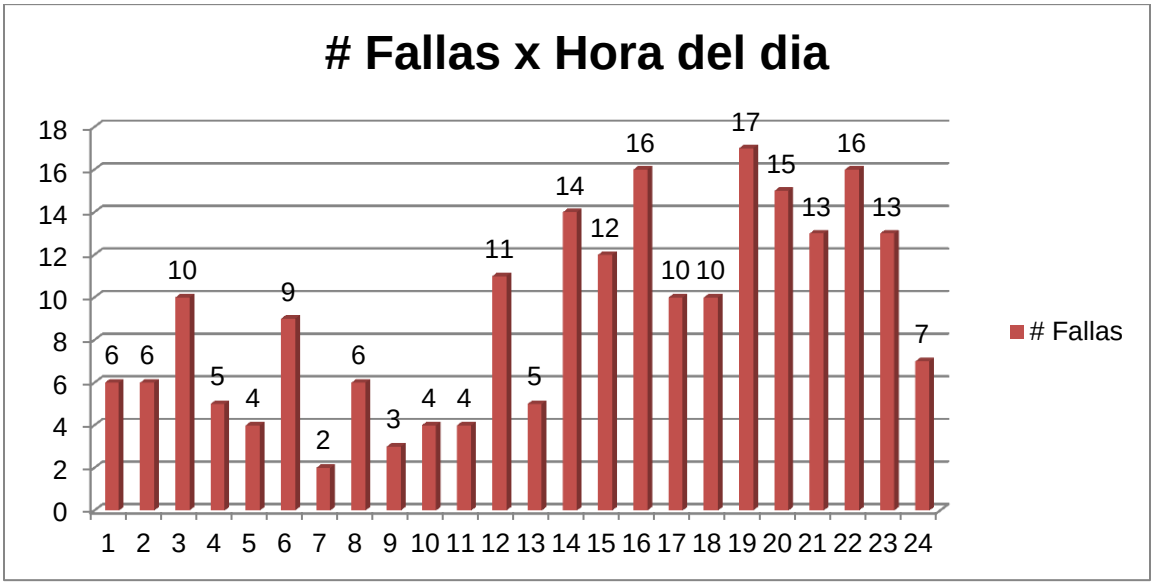
En este se puede apreciar que la pérdida de tiempo en el día 23, sería de 4,54 horas, lo cual indica que va disminuyendo con el paso de los días y por tanto las pérdidas son más pequeñas.

Con este tipo de simulaciones podemos ver el comportamiento en el largo plazo de una falla y cuantificar los tiempo para determinar o anticiparse a una solución.

4.1.4 Fallas en Software y su cuantificación

Ahora se realiza el análisis de las fallas de software, de las cuales se hace la caracterización de los datos y se obtienen 218 fallas en total, se separan los tiempos de duración de estas y se construye una tabla de distribución de frecuencia con el objeto de analizar donde se presentan la mayor parte de las fallas por hora, con esta se obtiene el siguiente gráfico.

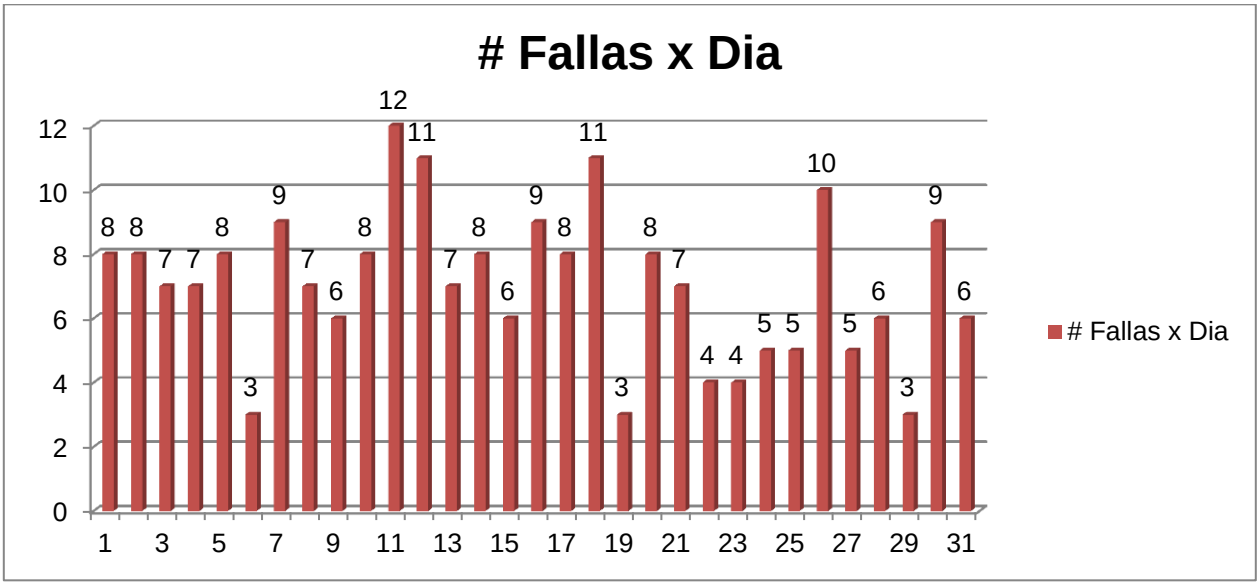
Grafico 11: Fallas de Software por hora del día.



En esta grafica se puede observar que el mayor número de fallas se presenta en las horas 12, 14, 16,19, 20 y 22, que son donde existe mayor demanda de suministro de energía, lo que indica que si el software llegará a producir por algún motivo un corte o un apagón, sería una gran pérdida de dinero para las empresas que la suministran.

Luego se analizan las fallas presentadas en un mes de 31 días, con el fin de obtener la frecuencia de estas por día. Se construye una tabla con los datos de días y fallas para obtener el siguiente gráfico:

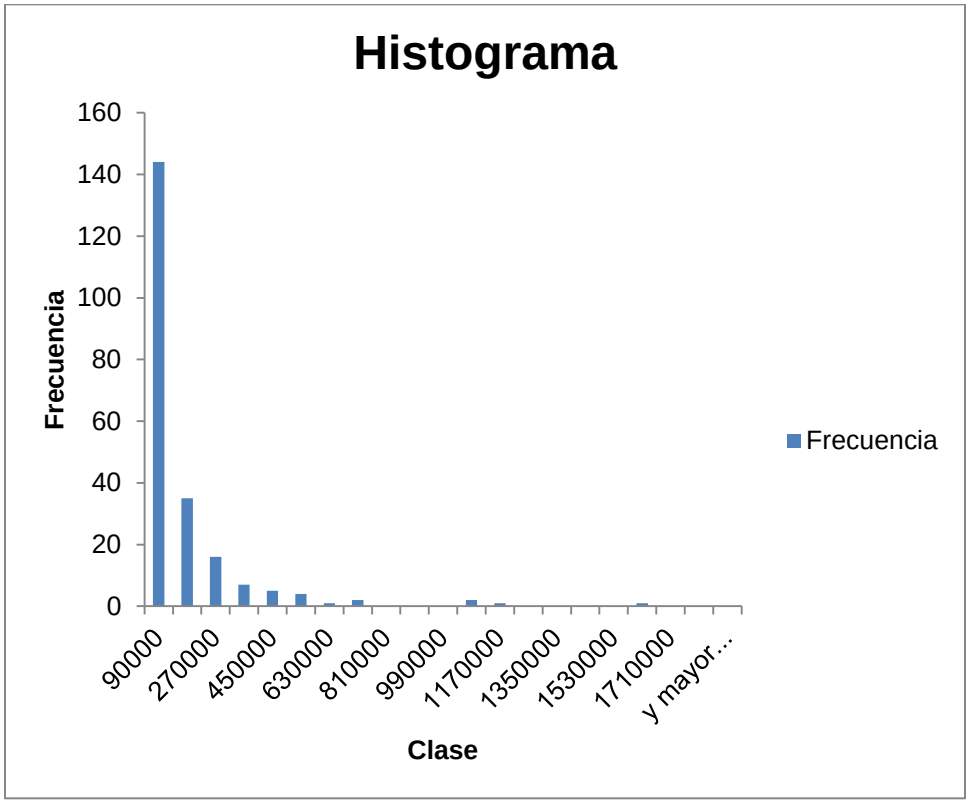
Grafico 12: Fallas de Software por día del mes



En la gráfica se aprecia que los días que presentan mayor número de fallas en el mes son los siguientes 7, 11, 16,18 y el 26, lo que muestra que el comportamiento de estas durante el mes es muy variable y no tiene un patrón establecido en el cual se pueda definir un ciclo de fallas. Sin embargo para estos dias se deben aplicar acciones preventivas con el fin de minimizar el riesgo y asi evitar que se presente una falla que saque al sistema de funcionamiento de forma parcial o total.

Se procede a construir una tabla con los datos de las fallas de software que contiene clase, probabilidad, frecuencia y hora, con esta construimos un histograma con el fin de analiza los fallas de acuerdo a los intervalos de tiempo en que se presentan.

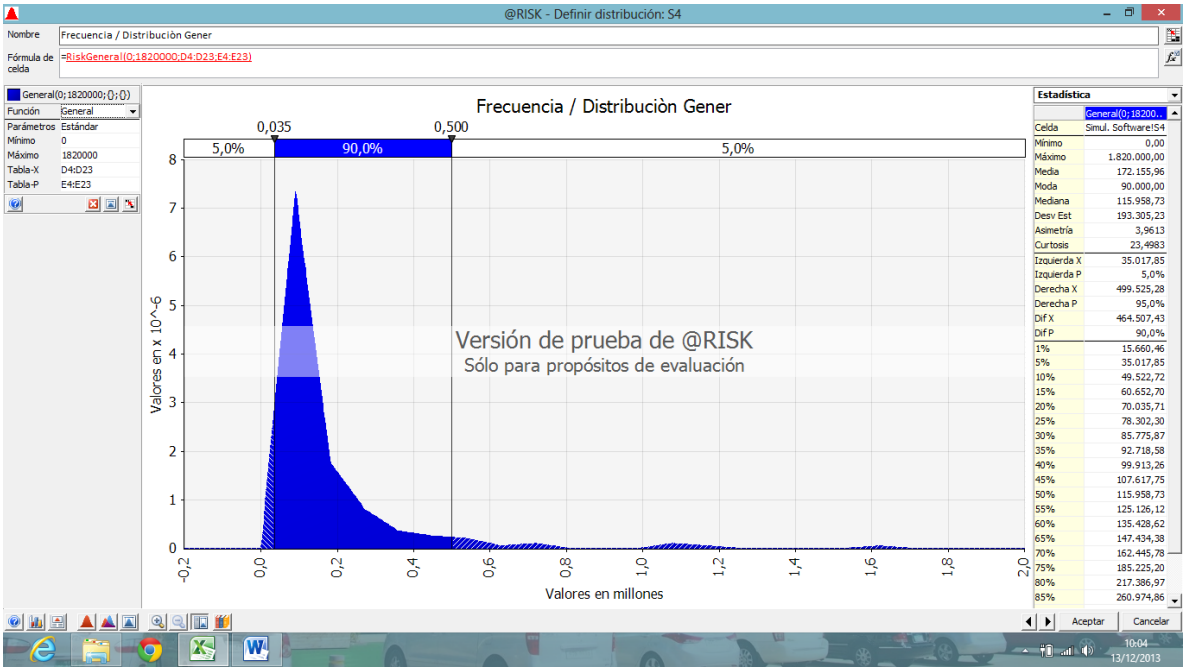
Grafico 13: Histograma de frecuencia de fallas Vs Clase



De nuevo esto nos muestra que la mayor parte de las fallas se concentran entre 90000 y 450000 segundos, el resto de estas no tiene tiempos de duración tan grandes los que es bueno, sin embargo el tener tantas fallas acumuladas en tiempos tan cortos puede producir un fallo y se debe evitar para no incurrir en un demanda no suministrada parcial o total.

Por medio de @Risk sacamos la distribución general de los datos la cual nos muestra la siguiente gráfica.

Figura 16: Distribución general de los datos de fallas en software



En esta podemos observar que la gran mayoría de las fallas están concentrados en los primeros intervalos (90%), luego de esta las que se presentan son mínimas.

Ahora se calcula la probabilidad de una falla en una hora determinada, para esto debemos definir los Xi, los cuales son las 24 horas de 1 día y los Pi, que son la probabilidad de falla en cada hora.

Tabla 18: Probabilidad de falla en cada hora

Hora (Xi)	Prob. (Pi)
0	0,02752294
1	0,02752294
2	0,04587156
3	0,02293578
4	0,01834862
5	0,0412844
6	0,00917431
7	0,02752294
8	0,01376147
9	0,01834862
10	0,01834862
11	0,05045872
12	0,02293578
13	0,06422018
14	0,05504587
15	0,0733945
16	0,04587156
17	0,04587156
18	0,07798165
19	0,06880734
20	0,05963303
21	0,0733945
22	0,05963303
23	0,03211009

Al analizar los datos de la duración de las fallas de software por medio de @Risk, se observa que la distribución estadística que más se ajusta a los datos es Pareto 2, puesto que el valor p arrojado por el test estadístico chí-cuadrado es 0,43 lo cual es mayor al nivel de significancia alpha de 0.05. Adicionalmente los parámetros como el minimo es igual, la media, la moda y la mediana no difieren mucho, pero la desviación estándar si tiene una variación significativa frente a la de entrada. (Ver figura 17 y tabla 18).

Figura 17: Distribución de Pareto 2

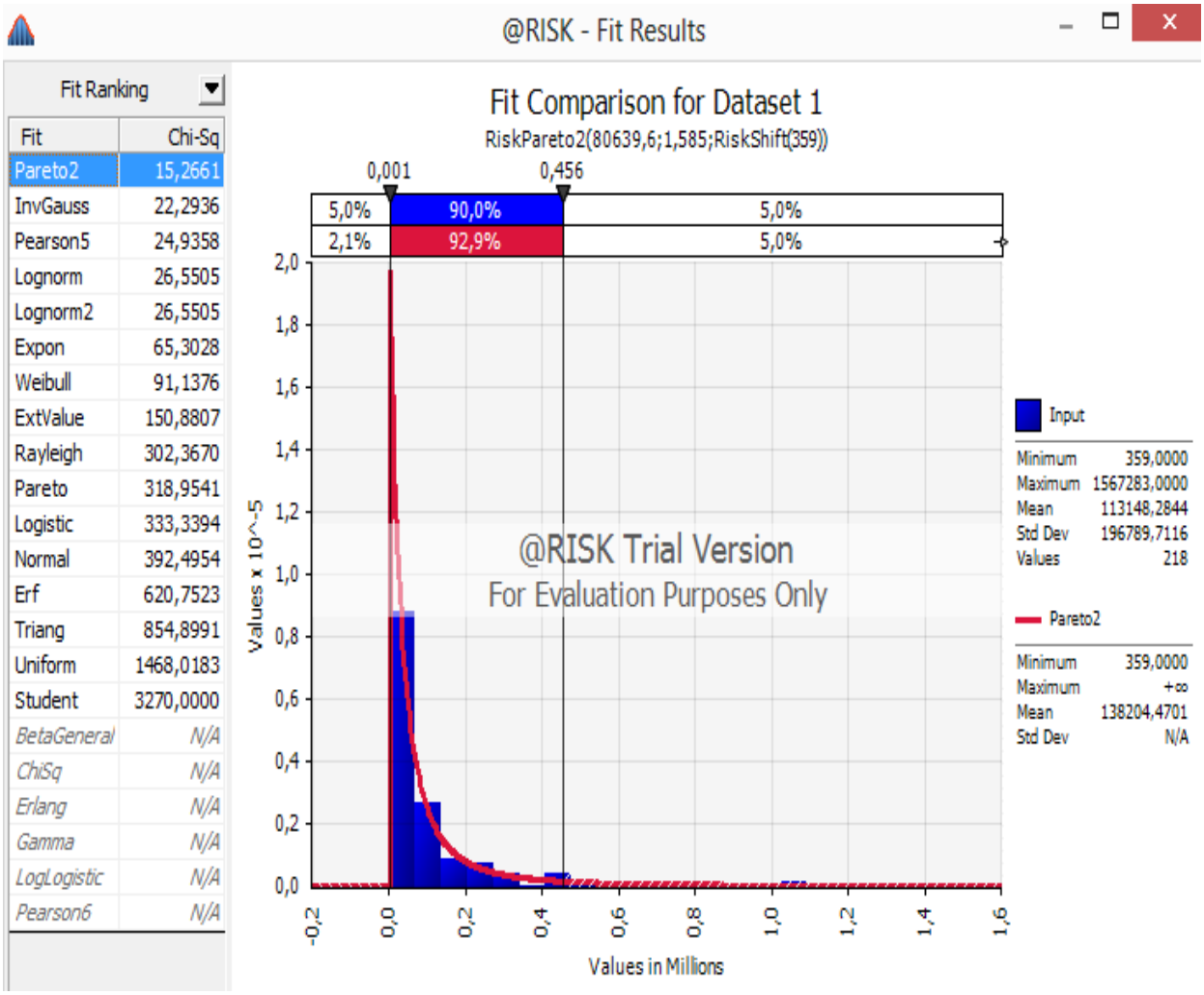
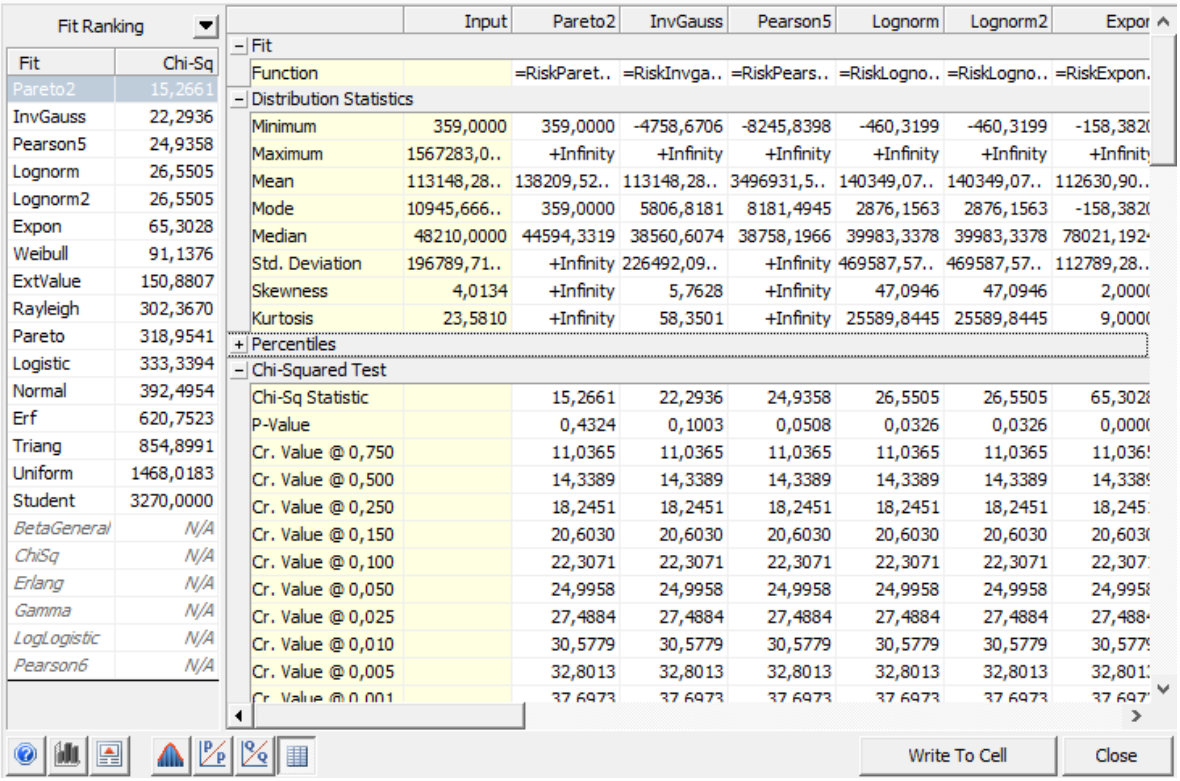


Tabla 19: Parámetros de aceptación o rechazo



Fit Ranking

Fit	Chi-Sq
Pareto2	15,2661
InvGauss	22,2936
Pearson5	24,9358
Lognorm	26,5505
Lognorm2	26,5505
Expon	65,3028
Weibull	91,1376
ExtValue	150,8807
Rayleigh	302,3670
Pareto	318,9541
Logistic	333,3394
Normal	392,4954
Erf	620,7523
Triang	854,8991
Uniform	1468,0183
Student	3270,0000
BetaGeneral	*N/A*
ChiSq	*N/A*
Erlang	*N/A*
Gamma	*N/A*
LogLogistic	*N/A*
Pearson6	*N/A*

	Input	Pareto2	InvGauss	Pearson5	Lognorm	Lognorm2	Expor
− Fit							
Function		=RiskParet..	=RiskInvga..	=RiskPears..	=RiskLogno..	=RiskLogno..	=RiskExpon.
− Distribution Statistics							
Minimum	359,0000	359,0000	-4758,6706	-8245,8398	-460,3199	-460,3199	-158,382(
Maximum	1567283,0..	+Infinity	+Infinity	+Infinity	+Infinity	+Infinity	+Infinit
Mean	113148,28..	138209,52..	113148,28..	3496931,5..	140349,07..	140349,07..	112630,90..
Mode	10945,666..	359,0000	5806,8181	8181,4945	2876,1563	2876,1563	-158,382(
Median	48210,0000	44594,3319	38560,6074	38758,1966	39983,3378	39983,3378	78021,192
Std. Deviation	196789,71..	+Infinity	226492,09..	+Infinity	469587,57..	469587,57..	112789,28..
Skewness	4,0134	+Infinity	5,7628	+Infinity	47,0946	47,0946	2,000(
Kurtosis	23,5810	+Infinity	58,3501	+Infinity	25589,8445	25589,8445	9,000(
+ Percentiles							
− Chi-Squared Test							
Chi-Sq Statistic		15,2661	22,2936	24,9358	26,5505	26,5505	65,302
P-Value		0,4324	0,1003	0,0508	0,0326	0,0326	0,000(
Cr. Value @ 0,750		11,0365	11,0365	11,0365	11,0365	11,0365	11,036
Cr. Value @ 0,500		14,3389	14,3389	14,3389	14,3389	14,3389	14,338
Cr. Value @ 0,250		18,2451	18,2451	18,2451	18,2451	18,2451	18,245
Cr. Value @ 0,150		20,6030	20,6030	20,6030	20,6030	20,6030	20,603(
Cr. Value @ 0,100		22,3071	22,3071	22,3071	22,3071	22,3071	22,307
Cr. Value @ 0,050		24,9958	24,9958	24,9958	24,9958	24,9958	24,995
Cr. Value @ 0,025		27,4884	27,4884	27,4884	27,4884	27,4884	27,488
Cr. Value @ 0,010		30,5779	30,5779	30,5779	30,5779	30,5779	30,577
Cr. Value @ 0,005		32,8013	32,8013	32,8013	32,8013	32,8013	32,801
Cr. Value @ 0,001		37,6973	37,6973	37,6973	37,6973	37,6973	37,697

Write To Cell | Close

Teniendo este ajuste se procede a realizar la simulación en la cual hallamos la severidad (el tiempo que dura una falla en una posición n), ósea las pérdidas de distribución agregadas, las cuales de forma matemática se calculan como $LDA = \sum_{t=1}^{N} Xt$, donde N es la frecuencia y X es el tiempo.

El VaR son las pérdidas de distribución agregadas LDA o también llamadas severidad

Para las fallas de software realizamos una simulación de 100 eventos los cuales nos van entregando en la casilla severidad lo que es el tiempo de duración de cada uno de estos en segundos y en la frecuencia el número de veces que este se presenta.

Tabla 20: Cuantificación de severidad 1

Frecuencia	Evento	Severidad	Segundos	Total H.	Promedio h.
4	1	88123,9457	88123,9457	24,4788738	6,11971845

Podemos observar que el VaR de acuerdo a la frecuencia sería de 6.11 horas perdidas, lo cual es un valor muy significativo para un día de 24 horas

Tabla 21: Cuantificación de severidad 2

Frecuencia	Evento	Severidad	Segundos	Total H.	Promedio h.
11	9	157263,073	157263,073	43,6841868	3,97128971

En el día 9 el VaR es de 3,9 horas, lo que indica que las pérdidas en este día se reducen y generan un riesgo menor.

Con este tipo de simulaciones podemos ver el comportamiento en el largo plazo de una falla y cuantificar el tiempo para determinar o anticiparse a una solución.

Al analizar las fallas de software y de Infraestructura se puede ver que tiene un comportamiento muy similar en la forma y los intervalos en los que se presentan, sin embargo son de mayor peso las fallas de infraestructura, siguiendo en su orden las de software, mostrando que está pueden ser causales de grandes riesgos para las empresas que suministran la energía.

CAPITULO V

CONCLUSIONES

La investigación presentada en esta tesis se orientó hacia la caracterización de los datos y el análisis del comportamiento de estos con el fin de cuantificar el tiempo de los eventos de falla específicamente los de software e infraestructura, esto con el objeto de minimizar los riesgos y reducir las pérdidas de dinero por fallos.

Como conclusiones generales del desarrollo de este trabajo se citan las siguientes:

- Las fallas presentadas en los sistemas SCADA han sido miradas de forma general por las empresas que suministran la energía y se han manejado de forma cualitativa lo que los ha llevado a ser imprecisos en la toma de decisiones por desconocimiento de las fallas particulares que integran el sistema.

- Los sistemas SCADA están integrados por dos componentes de falla los cuales son los de producto y los de operación, sin embargo los de producto tienen un peso mayor en la incidencia de las fallas en específico los de software e Infraestructura.

- Las fallas que se presentan en los sistemas SCADA en general se dan en tiempos de duración muy cortos, pero de gran incidencia y las soluciones se dan con una diferencia de tiempo considerable, lo cual podría afectar la demanda de energía.

- Gran cantidad de las fallas que se presentan en los sistemas SCADA no tienen una solución específica, ni un historia, lo que hace que cada que se

presente esta, los controladores del sistema no tengan la información para solucionar el problema de la forma correcta y en el menor tiempo posible.

- La cuantificación del tiempo de duración de una falla le permite a las empresas que la suministran, tomar acciones preventivas y construir planes de contingencia que le indique a los controladores del sistema, como proceder en una falla especifica

- Las fallas de Infraestructura son la de mayor predominancia en los sistemas SCADA, siendo las de software el 50% del total de las fallas de Infraestructura.

- Las fallas de infraestructura muestran un comportamiento de gran frecuencia en los primeros intervalos de de tiempo y se van haciendo casi imperceptibles en los tiempos de duración muy largos.

- Las fallas de Software concentran el 90% de estas en los intervalos de duración más pequeño, los grandes se vuelven casi imperceptibles.

- La frecuencia de ocurrencia de los eventos, tanto para fallas de software como para infraestructura, en periodos de tiempo tan cortos, representan un gran riesgo para las empresas que suministran energía, ya que las soluciones de estas, no son inmediatas y en caso de represamiento de fallas, el sistema podría colapsar.

- La cuantificación de las fallas por medio de simulaciones con gran número de iteraciones nos permite predecir el comportamiento de las fallas en el tiempo con el objeto de tomar acciones preventivas y darle al sistema el uso más eficiente posible para evitar incidentes parciales o totales.

REFERENCIAS BIBLIOGRÁFICAS

[1] Comité de Basilea II, Identificación de Riesgos Operativos. 2001

[2] Nanpeng Yu, “Financial Risk Management in Restructured, wholesale Power Markets: Concept and Tools” IEEE, 2010

[3] Alfonso de Lara Haro, “ Medición y control de riesgos financieros” Editorial Limusa S. A. Mexico 2008

[4] Jorion, Ph. (2003). Financial Risk Management Handbook. Wiley

[5] Humberto Llinás Solano, Carlos Rojas Álvarez, 2005, Estadística descriptiva y distribuciones de Probabilidad. Edit. Universidad del Norte

[6] CREG. Comisión de Regulación de Energía y Gas, SSPD. Superintendencia de Servicios Públicos

[7]Luis Corrales, Ph. (2007) Pag 1 -2. Interfaces de comunicación Industrial. Departamento de Automatización Industrial

[8] Luis Corrales, Ph. (2007) Pag 38 -39. Interfaces de comunicación Industrial. Departamento de Automatización Industrial.

[9] http://www.ehowenespanol.com/tipos-sistemas-scada-lista_87004/

[10] http://www.scadasystems.net/

[11] Gestion segura de redes SCADA Pag. 3, Cristina Alcaraz, Gerardo Fernandez, Rodrigo Romàn, Javier Lopez, Angel Balestegui. Universidad de Malaga.

[12] http://definicion.de/telecomunicacion/#ixzz2fIt8BWha

[13] https://sites.google.com/site/educaarh/mapa-conceptual

[14] Sistemas de Telecomunicaciones. Tema 1, Historia de las comunicaciones. Pag. 23, 24,25

[15] Mark Adamiak, W. Premerlani, and B. Kasztenny. “Synchrophasors: Definition, Measurement, and Application” GE Multilin Publications, pp 1-13, Mar. 2005. http://www.geindustrial.com

[16] J.M Selga R. Baumann , L Bjork, B Richarson. H Spelt “ Technical Brochure on communication concepts for control system” CYGRE CS35-WG13-TF13.03. Octubre de 1998

[17] J.M Selga R. Baumann , L Bjork, B Richarson. H Spelt “ Technical Brochure on communication concepts for control system” CYGRE CS35-WG13-TF13.03. Octubre de 1998

[18]Completar refencia de el tema de virus

[19] Hollman, E “Sistema experto en análisis de fallas en líneas eléctricas de transmisión” Centro de Ingeniería del Software e Ingeniería del Conocimiento (CAPIS), 2007

[20] www.pa.unionfenosa.com/images/estructura_red.jpg

[21]Líneas de Transmisión Eléctricas; IEEE UCSA, Pág. 2

[22] Funamashi, t.; Otoguro, H.; Mizuma, Y.; Dube, L.; Kizilicay, M.; Ametani, A. Influence of fault arc characteristics on the accuracy of digital fault locators. IEEE Trans. Power Delivery, vol. 2, Apr.2001, pp. 195–199.

[23] Lineamientos para fortalecer la expansión del sistema de transmisión nacional.Pag. 10 y 11. Ministerio de Minas y Energía – UPME. 2013

[24] Boletín estadístico de minas y energía 2007 – 2011 (Pag 152-153), XM año 2007. Unidad de planeación minero energética.

[25] Sanas Prácticas para la Gestión y supervisión del Riesgo Operativo – Comité de Basilea de Supervisión Bancaria – Publicación No. 96 Febrero de 2003

[26] S. Mei, F. He, X. Zhang, M. Cao, “Power Grid Complexity”, Tsinghua Press and Springer, 2011

[27] K. Alvehag, L. Söder, “Considering Extreme Outages in Cost-Benefit Analysis of Distribution Systems”, AUPEC’08 Autralasian Universities Power Engineering Conference, 2008

[28] S. Mei, F. He, X. Zhang, M. Cao, “Power Grid Complexity”, Tsinghua Press and Springer, 2011

[29] UPME, “Estudio de Costos de Racionamiento de Electricidad y Gas natural”, Documento No. C76-IN-F-010, Unidad de Planeamiento Minero Energética, Enero 2004

[30] I. Dobson, D.E. Newman, B.A. Carreras, V.E. Lynch, “An Initial complex systems analysis of the risk of blackouts in power transmission systems”, Power Systems and Communications infrastructures for the future, Beijing, 2002

[31] P. Jorion, “Value At Risk - The New Benchmark For Managing Financial Risk”, 3rd. Edition, Mcgraw-Hill, 2007

[32] V. Chavez Demoulin, P. Embrechts, J. Neslehová, ”Quantitative models for operational risk: Extremes, dependence and aggregation”, Journal of Baking & Finance, Vol. 30, N° 10, pp.2635–2658, 2006

[33] A. Chernobai, S.T. Rachev, “Applying robust methods to operational risk modeling”, The Journal of operational risk, Vol. 1, N°1, pp. 27-41, 2006

[34] M. Cruz, “Operational Risk Modeling and Analyst: Theory and Practice”, Incisive Media Investments Limited, Risk Book,2004

[35] D. Vose, “Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling”, John Wiley & Sons, 1996.

[36] UPME, “Metodología para la Actualización de la Curva de Costos Óptimos de Racionamiento de electricidad y Gas Natural”, Vol. 4, Cap. 3, Unidad de Planeamiento Minero Energetica, Enero 2004

[37] M. Sullivan, M. Mercurio, J. Schellenberg, M.A. Sullivan, “Estimated Value of service Reliability for electric utility customers in the united states”, LBNL Research Project Final Report, June 2009.

[38] J.C. Hull, “Options, Futures, and Other Derivatives”, Seventh Edition, McGraw Hill, 2008

[39] J. Pacheco, M. Rios, “Analisis de Vulnerabilidad del Sistema de Potencia Colombiano”, Tesis de Especializacion en Sistemas de Transmision y Distribucion Electrica, Universidad de los Andes, Colombia, Nov 2010

[40] G. Doorman, G. Kjolle, K. Uhlen, S.E. Huse, N. Flatabo, “Vulnerability of the Nordic Power Systems”, Main Report, SINTEF, Norway, 2004

[41] VaR Quantification for Demand Not Supplied in Electric Power Systems Santiago Medina H. * is with Mines School, National University of Colombia, (e-mail: smedina@unal.edu.co). Lilliam Urrego A., is with XM S.A. E.S.P, Colombia & National University of Colombia (e-mail: liurrego@xm.com.co). Heliodore Frederic, is with The Blackout Team, Alstom Grid, Paris, France (e-mail: frederic.heliodore@alstom.com). Ismail Boussaad, is with The Blackout Team Alstom Grid, Paris, France (e-mail: ismail.boussaad@alstom.com). Poullain Serge, is with The Blackout Team Alstom Grid, Paris, France (e-mail: serge.poullain@alstom.com) Courbon Eric, is with The Blackout Team Alstom Grid, Paris, France (e-mail: eric.courbon@alstom.com) Nakib Amir is with LISSI, University Paris Est, Créteil, France (e-mail: amir.nakib@u-pec.fr)

[42] Options Amontecarlo Approach. Phelim P. boyle. Journal of financial economics 4 (1997), pp.323-338

[43] (Mingrui Zhang, Member, IEEE, and Xin Jin, Hui Zhang, Student Member, IEEE)

[44] Teodor Sommestand, Gôran N. Ericsson, Senior Member, IEEE, Jakob Nordlander

[45] Siddharth Sridhar and G. Manimaran, Department of electrical and computer Engineering, Iowa State University, Ames, Iowa 50010.

[46] Maria J. Bernal Zuluaga, Central Hidroelectrica de Caldas S.A; Diego F. Mendoza, Universidad de San Buenaventura

[47] G. Clarke, D. Reynders & E. Wright. “Practical Moderm SCADA Protocols: DNP3, 60870.5 and Related Systems”. Great Britain, 2004.

[48] R. Vignoni, R. Pellizzoni & L. Funes. “Sistemas de automatización de subestaciones con IEDs IEC 61850: Comunicaciones, topologías”. Argentina, Mayo, 2009.

[49] D. G. Hernán. ”Implementación de Un sistema SCADA para la mezcla de dos sustancias en una industria química”. Online [En. 2012].

[50] Protocols IEC 60870-5-104. Online [Mar. 2012].

[51] Ramòn Leòn – Jorge Enrique Gomèz, Direcciòn de la planeaciòn de la operaciòn – CND, XM S.A. E:S.P Compañía de Expertos en Mercados

[52]CREG, Codigo de redes, Resoluciòn 025, 1995

[53]Begoviv, M. ; Madani, V.; Novosel, D. ; “System Integrity Protection Schemes (SIPS), “Bulk Power System Dynamics an d Control – VII. Revitalizing Operational Reliability, 2007 iREP Symposium, vol., no., pp.1-6, 19-24. Aug 2007