

Propuesta temas CNO:
Sistemas de Control y Protección
Red Inteligente



Comisión de Regulación
de Energía y Gas



Contrato 2019-034
Consultoría Código de Redes

ÍNDICE

ÍNDICE	2
1 SISTEMAS DE CONTROL Y PROTECCIÓN.....	3
1.1 NORMAS.....	3
1.2 REQUERIMIENTOS	4
1.3 ARQUITECTURA.....	4
1.4 <i>COMMON INFORMATION MODEL</i> – CIM.....	5
1.5 CIBERSEGURIDAD.....	5
1.6 REPOSITÓRIO DE CASOS DE USO COMÚN.....	6
1.7 INTEROPERABILIDAD	7
1.8 PROTOCOLOS	8
1.9 SISTEMA DE CONTROL	8
1.10 SISTEMA DE PROTECCIÓN	9
1.10.1 PROTECCIÓN DE LÍNEA	9
1.10.2 PROTECCIÓN DE BARRAS	11
1.10.3 PROTECCIONES DE INTERRUPTOR	11
1.10.4 PROTECCIÓN TRANSFORMADORES Y REACTORES	12
1.10.5 UNIDAD DE MEDICIÓN DE FASOR	13
1.11 ACCIONES DE LAS PROTECCIONES EN EL STN	13
1.11.1 DESCONEXIÓN DE ELEMENTOS EN FALLA	13
1.11.2 TIEMPOS DE ACTUACIÓN PROTECCIÓN PRINCIPAL	14
1.11.3 ACTUACIÓN PROTECCIÓN DE RESPALDO	15
1.11.4 RECIERRE LÍNEAS DE TRANSMISIÓN	15
1.11.5 VERIFICACIÓN DE SINCRONISMO	15
1.11.6 TELEPROTECCIÓN	16
1.12 SISTEMA DE TELECOMUNICACIONES	16
2 REDES INTELIGENTES	18

1 SISTEMAS DE CONTROL Y PROTECCIÓN

1.1 Normas

Los Sistemas de Control y Protección y sus componentes deberán cumplir con lo estipulado en las siguientes normas:

- a) NERC CIP – *Cyber Security*.
- b) ISO/IEC 15408 - *Information technology -- Security techniques -- Evaluation criteria for IT security*.
- c) ISO/IEC 18045 - *Information technology -- Security techniques -- Methodology for IT security evaluation*.
- d) ISO/IEC 19790 - *Information technology -- Security techniques -- Security requirements for cryptographic modules*.
- e) IEC 60255 - *Measuring relays and protection equipment*.
- f) IEC 60834 - *Teleprotection equipment of power systems - Performance and testing*.
- g) IEC 60870 - *Telecontrol equipment and systems*.
- h) IEC 61000 - *Electromagnetic compatibility (EMC)*.
- i) IEC 61508 - *Functional safety of electrical/electronic/programmable electronic safety-related systems*.
- j) IEC 61850 - *Communication networks and systems for power utility automation*.
- k) IEC 61970 - *Energy management system application program interface (EMS-API)*.
- l) IEC 62264 - *Enterprise-control system integration*.
- m) IEC 62325 - *Framework for energy market communications*.
- n) IEC 62351 - *Power systems management and associated information exchange - Data and communications security*.
- o) IEC 62357 - *Power systems management and associated information exchange*.
- p) IEC 62443 - *Industrial communication networks - Network and system security*.
- q) IEC 62488 - *Power line communication systems for power utility applications*.
- r) IEC 62559 - *Use case methodology*.
- s) IEC TR 63069 - *Industrial-process measurement, control and automation - Framework for functional safety and security*.

1.2 Requerimientos

Los sistemas de control y protección deberán cumplir lo estipulado en:

- a) Numeral ¡Error! No se encuentra el origen de la referencia.- ¡Error! No se encuentra el origen de la referencia..
- b) Numeral ¡Error! No se encuentra el origen de la referencia.- ¡Error! No se encuentra el origen de la referencia..
- c) Numeral ¡Error! No se encuentra el origen de la referencia.- ¡Error! No se encuentra el origen de la referencia..
- d) Numeral ¡Error! No se encuentra el origen de la referencia.- ¡Error! No se encuentra el origen de la referencia..
- e) Numeral ¡Error! No se encuentra el origen de la referencia.- ¡Error! No se encuentra el origen de la referencia..
- f) Numeral ¡Error! No se encuentra el origen de la referencia.- ¡Error! No se encuentra el origen de la referencia..

1.3 Arquitectura

Los sistemas de control y protección y su integración al centro de control deberán tener la arquitectura que se estipula en la publicación IEC TR 62357-1:2016 - *Power systems management and associated information exchange - Part 1: Reference architecture*.

En la Figura 4-1 – Estructura lógica de un sistema automatizado para subestaciones, se presenta la ejecución en una subestación.

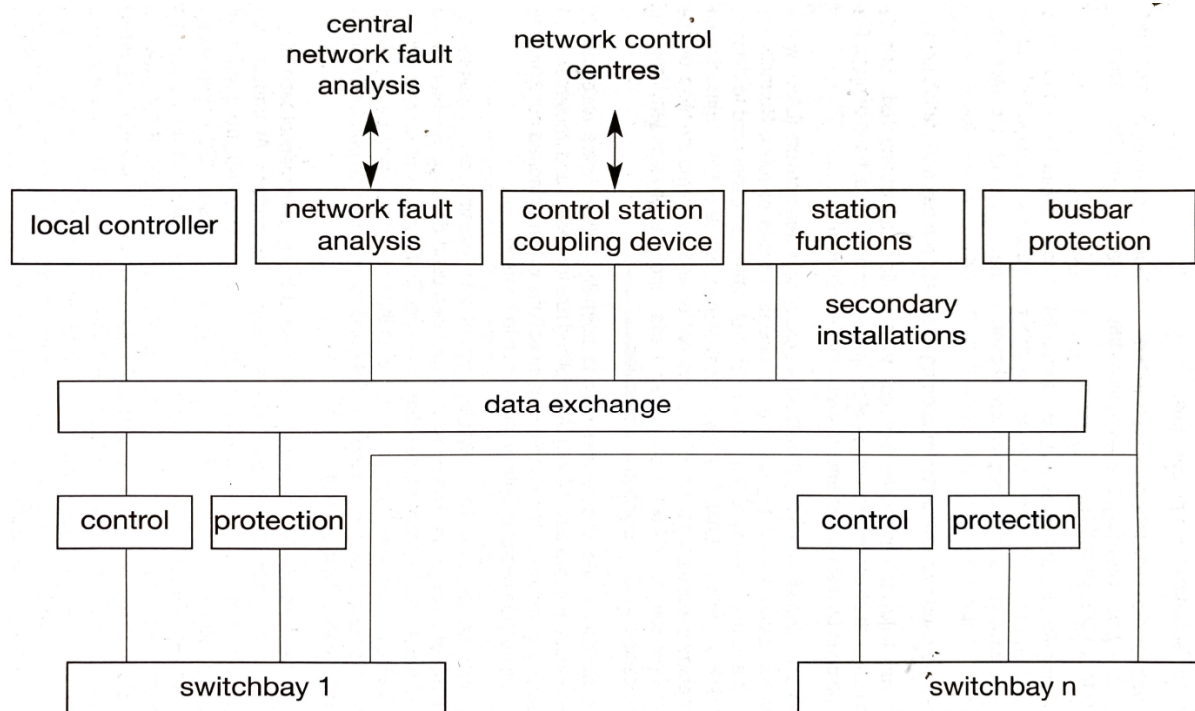


FIGURA 1-1 – ESTRUCTURA LÓGICA DE UN SISTEMA AUTOMATIZADO PARA SUBESTACIONES

1.4 Common Information Model – CIM

El modelo de información común (*Common Information Model – CIM*) para los sistemas de transmisión deberá realizarse de acuerdo con lo estipulado en la norma IEC 61970:2018 SER - *Energy management system application program interface (EMS-API)* – (todas las partes).

Se podrá tomar como base el CIM del mercado europeo de acuerdo con los delineamientos del reporte técnico IEC TR 62325-103:2017 - *Framework for energy market communications - Part 103: Review of information exchanges within the deregulated European style retail energy market from a CIM perspective*.

1.5 Ciberseguridad

Se deberán implementar las medidas de ciberseguridad que estipula el *North American Electric Reliability Corporation – Critical Infrastructure Protection* (NERC CIP), así:

- a) CIP-002 - *Critical Cyber-Asset Identification*. La identificación de los activos críticos fue realizada por el Comité Nacional de Operación y se deberá utilizar dicha identificación.

-
- b) CIP-003 - *Security Management Controls*.
 - c) CIP-004 - *Personnel and Training*.
 - d) CIP-005 - *Electronic Security Perimeter*.
 - e) CIP-006 - *Physical Security of Critical Cyber-Assets*. Los componentes de los sistemas de control y protección deberán cumplir esta norma.
 - f) CIP-007 - *Systems Security and Management*.
 - g) CIP-008 - *Incident Reporting and Response Planning*.
 - h) CIP-009 - *Recovery Plans for Critical Cyber-Assets*.

Se deberán seguir las guías del Reporte Técnico IEC TR 63069:2019 - *Industrial-process measurement, control and automation - Framework for functional safety and security*, para la adecuada aplicación de la norma IEC 61508 - *Functional safety of electrical/electronic/programmable electronic safety-related systems* (todas las partes) y de la norma IEC 62443 - *Security for industrial automation and control systems* (todas las partes).

La seguridad de la información para las operaciones de control del sistema de energía debe seguir lo estipulado en la norma IEC 62351:2018 SER - *Power systems management and associated information exchange - Data and communications security* – (todas las partes).

1.6 Repositório de casos de uso común

Con el fin de tener uniformidad en la información y facilitar las actividades de incorporación de nuevos componentes o la modernización de los existentes, el Centro Nacional de Despacho – CND – administrará el repositorio de casos de uso común y para tal fin, se deberá tener en cuenta la siguiente guía:

- a) El reporte técnico IEC TR 62559-1:2019 - *Use case methodology - Part 1: Concept and processes in standardization* deberá ser utilizado como la base para un repositorio de casos de uso común, utilizado para recopilar casos en una plataforma colaborativa común. El repositorio se utiliza para organizar y armonizar los casos de uso con el fin de proporcionar casos de uso genérico ampliamente aceptados como base para el trabajo de normalización ulterior.
 - b) La cláusula 13 del reporte técnico IEC TR 62357-2:2019 - *Power systems management and associated information exchange - Part 2: Use Cases and role model*, servirá de modelo de caso de uso para el STN.
-

1.7 Interoperabilidad

La interoperabilidad deberá soportarse en la norma IEC 61850:2019 SER - *Communication networks and systems for power utility automation* – (todas las partes). Las comunicaciones en la subestación deberán cumplir lo estipulado en las siguientes normas:

- a) IEC 61850-2 - *Communication networks and systems in substations – Part 2: Glossary.*
- b) IEC 61850-3 - *Communication networks and systems in substations – Part 3: General requirements.*
- c) IEC 61850-4 - *Communication networks and systems for power utility automation – Part 4: System and project management.*
- d) IEC 61850-5 - *Communication networks and systems in substations – Part 5: Communication requirements for functions and device models.*
- e) IEC 61850-6 - *Communication networks and systems for power utility automation – Part 6: Configuration description language for communication in electrical substations related to IEDs.*

En la Figura 4-2 – Automatización Inteligente de Subestaciones, se presenta un ejemplo de cómo puede materializarse la interoperabilidad.

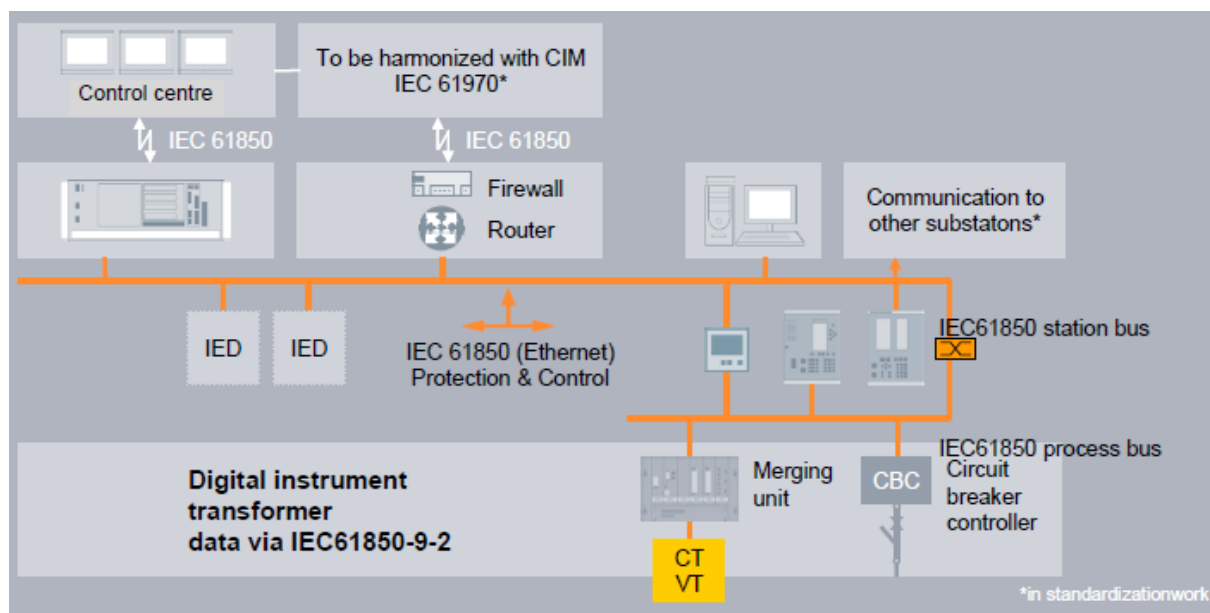


FIGURA 1-2 – AUTOMATIZACIÓN INTELIGENTE DE SUBESTACIONES

1.8 Protocolos

Se deberán utilizar los siguientes protocolos de comunicación:

- a) Las comunicaciones entre el Nivel 0 y el Nivel 1 deberá realizarse mediante un *Process-Bus*: IEC 62271-3:2015 - *High-voltage switchgear and controlgear - Part 3: Digital interfaces based on IEC 61850*, para interruptores y seccionadores e IEC 61850-9-2:2011 - *Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3*, para los transformadores de corriente y tensión.
- b) Las comunicaciones entre el Nivel 1 y el Nivel 2 deberá realizarse mediante un *Station-Bus*: IEC 60870-5-103:1997 - *Telecontrol equipment and systems - Part 5-103: Transmission protocols - Companion standard for the informative interface of protection equipment*.
- c) Entre Nivel 2 y Nivel 3 (estas publicaciones son de gran relevancia para la Red Inteligente - *Smart Grid*):
 - IEC 60870-5-101:2015 - *Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks*.
 - IEC 60870-5-104:2016 - *Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles*.

1.9 Sistema de Control

El Sistema de Control de la subestación deberá tener en cuenta los siguientes delineamientos:

- a) La marcación de los eventos debe realizarse de acuerdo a la norma IEC/IEEE 61850-9-3:2016 - *Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation*, la cual especifica un perfil de protocolo de tiempo de precisión (*Precision Time Protocol* - PTP) que deberá permitir el cumplimiento de las clases de sincronización más altas tanto de IEC 61850-5 e IEC 61869-9 como para IEC 61869-9:2016 - *Instrument transformers - Part 9: Digital interface for instrument transformers*.

- b) El diseño deberá tener en cuenta lo estipulado en la cláusula 9.1, *Monitoring and Control Systems*, de la norma IEC 61936-1:2010 - *Power installations exceeding 1 kV a.c. - Part 1: Common rules*.
- c) La norma IEC 61850 - *Communication networks and systems for power utility automation*, estipula una red de área local (Local Area Network - LAN), donde todos los dispositivos conectados tienen los mismos derechos o roles de comunicación.
- d) Las conexiones físicas deberán ser mediante fibra óptica y esta red debe ser duplicada.
- e) Los IEDs de control podrán ser incorporados en los IEDs de protección, siempre y cuando no perjudique el desempeño del sistema y tanto la protección principal 1 como la protección principal 2 incorporen las funciones de control.

1.10 Sistema de Protección

Los componentes del Sistema de Protección deberán cumplir las estipulaciones de la norma IEC 60255-1:2009 - *Measuring relays and protection equipment - Part 1: Common requirements*.

1.10.1 Protección de línea

Las líneas de transmisión del STN deben protegerse como se detalla a continuación:

- a) **Protección de línea 1.** Deberá ser de distancia con tres zonas hacia adelante y con un tiempo de actuación máximo en zona 1 de 40 ms al 80% de su ajuste. Deberá poseer esquemas de teleprotección configurable de acuerdo con las necesidades del sistema, al igual que funciones de cierre en falla, lógica de terminal débil, eco, bloqueo por oscilación de potencia, bloqueo por pérdida de tensión y deberá ser inmune a la inversión de tensión por efectos de la compensación serie. Deberá tener disparo selectivo por fases para fallas monofásicas y disparo trifásico para fallas bifásicas y trifásicas, Esta protección deberá cumplir lo estipulado en la norma IEC 60255-121:2014 - *Measuring relays and protection equipment - Part 121: Functional requirements for distance protection*.
- b) **Protección de línea 2.** Deberá ser de comparación direccional y con un tiempo de actuación máximo de 40 ms. Deberá tener inmunidad a la inversión de tensión por efectos de la compensación serie, compensación de la corriente capacitiva en líneas largas, compensación del retardo del canal de comunicaciones y poseer la lógica de cierre en falla. Deberá tener disparo selectivo por fases para fallas monofásicas y

disparo trifásico para fallas bifásicas y trifásicas. Esta protección deberá cumplir lo estipulado en la norma IEC 60255-12:1980 - *Electrical relays - Part 12: Directional relays and power relays with two input energizing quantities*.

c) **Protección por sobrecorriente direccional a tierra.** Esta protección deberá operar en un esquema de comparación direccional. Puede ser implementada como un relé independiente o como una función de la Protección de Línea 1 o de la Protección de Línea 2. Esta protección deberá cumplir lo estipulado en la norma IEC 60255-151:2009 - *Measuring relays and protection equipment - Part 151: Functional requirements for over/under current protection*.

d) **Protección por sobretensión.** Esta protección deberá operar cuando se exceda el umbral de tensión seleccionado en tiempo definido. Puede ser implementada como un relé independiente o como una función de la Protección de Línea 1 o de la Protección de Línea 2. Esta protección deberá cumplir lo estipulado en la norma IEC 60255-127:2010 - *Measuring relays and protection equipment - Part 127: Functional requirements for over/under voltage protection*.

e) **Localizador de fallas.** El localizador de fallas deberá tener una precisión del 5% y puede ser implementado como un relé independiente o como una función de la Protección de Línea 1 o de la Protección de Línea 2. La información deberá ser transmitida al CSM, CND o CRD, según sea el caso.

f) **Registrador de fallas.** El registrador de fallas deberá tener una frecuencia de muestreo mínima de 600 Hz, para que permita analizar armónicos hasta de orden 5, puede ser implementado como un relé independiente o como una función de la Protección de Línea 1 o de la Protección de Línea 2. El formato de datos deberá cumplir con lo estipulado en la norma IEC 60255-24:2013 - *Measuring relays and protection equipment - Part 24: Common format for transient data exchange (COMTRADE) for power systems*. La información deberá ser transmitida al concentrador que designe el Transportador y el CSM, CND o CRD, según sea el caso.

g) **Disparo directo transferido.** El disparo directo transferido se dará cuando los reactores de línea no posean interruptor y tienen una falla, por sobretensión y dependiendo de la configuración de la subestación, por falla interruptor y falla en barras. Esta última, si el exceso de reactivos demanda la desconexión de las líneas que queden en vacío.

- h) Teleprotección.** Los equipos de teleprotección deberán tener al menos cuatro señales (una comparación direccional, dos disparos permisivos y un disparo directo transferido) y cumplir las estipulaciones de la norma IEC 60834 - *Teleprotection equipment of power systems - Performance and testing*.

1.10.2 Protección de barras

Las barras deberán tener una protección diferencial de barras del tipo distribuido, inmune a las diferencias de las características de los transformadores de corriente.

1.10.3 Protecciones de interruptor

Los interruptores deberán tener las siguientes protecciones:

- a) Protección de falla interruptor.** Ante la falla de un interruptor a la apertura por un disparo proveniente de una protección, deberá enviar comando de disparo a los interruptores adyacentes. Puede ser implementada como un relé independiente o como una función de la Protección Diferencia de Barras, de la Protección de Línea 1 o de la Protección de Línea 2. Esta protección deberá cumplir lo estipulado en la norma IEC 60255-151:2009 - *Measuring relays and protection equipment - Part 151: Functional requirements for over/under current protection*.
- b) Supervisión circuitos de disparo.** Deberá dar alarma cuando se interrumpa el circuito de disparo para todos y cada uno de los circuitos de disparo de las dos bobinas de disparo del interruptor.
- c) Verificación de sincronismo.** Para cierres manuales y ante disparos trifásicos, se deberá verificar el sincronismo de los dos circuitos a conectar y cuando se cumplan los criterios de diferencia de tensión y ángulo, se podrá dar el cierre manual o el recierre trifásico, según sea el caso. Puede ser implementada como un relé independiente o como una función de la Protección de Línea 1 o de la Protección de Línea 2.
- d) Recierre.** Deberá dar recierre monopolar para fallas monofásicas y recierre tripolares para fallas bi o trifásicas, este último con verificación de sincronismo. Puede ser implementada como un relé independiente o como una función del relé de verificación de sincronismo, de la Protección de Línea 1 o de la Protección de Línea 2.
- e) Relé de disparo con bloqueo.** Deberá dar disparo sobre ambas bobinas de disparo de los tres polos.

1.10.4 Protección transformadores y reactores

Los transformadores y reactores deberán tener las siguientes protecciones:

- a) **Protecciones mecánicas y térmicas propias.** Las protecciones que se estipulan en el literal **¡Error! No se encuentra el origen de la referencia.** del numeral **¡Error! No se encuentra el origen de la referencia. - ¡Error! No se encuentra el origen de la referencia.**, deberán dar disparo, alarma o información de la magnitud, dependiendo de las necesidades. Las protecciones térmicas deberán cumplir con lo estipulado en la norma IEC 60255-149:2013 - *Measuring relays and protection equipment - Part 149: Functional requirements for thermal electrical relays*. La información de la temperatura del medio ambiente, la temperatura del transformador y la sobrecarga admisible (potencia y duración), deberá ser enviada al CSM, CND o CRD, según las necesidades.
 - b) **Protección Principal.** Deberá ser diferencial, corregir la diferencia horaria entre los diferentes devanados y ser inmune a las diferencias en las magnitudes de corriente ocasionadas por la derivación en que esté operando el transformador. Esta protección deberá cumplir lo estipulado en la norma IEC 60255-13:1980 - *Electrical relays - Part 13: Biased (percentage) differential relays*.
 - c) **Protección de Respaldo.** Deberá ser de sobrecorriente de tiempo definido. Esta protección deberá cumplir lo estipulado en la norma IEC 60255-151:2009 - *Measuring relays and protection equipment - Part 151: Functional requirements for over/under current protection*.
 - d) **Registrador de fallas.** El registrador de fallas deberá tener una frecuencia de muestreo mínima de 600 Hz, para que permita analizar armónicos hasta de orden 5, puede ser implementado como un relé independiente o como una función de la Protección Principal o de la Protección de Respaldo. El formato de datos deberá cumplir con lo estipulado en la norma IEC 60255-24:2013 - *Measuring relays and protection equipment - Part 24: Common format for transient data exchange (COMTRADE) for power systems*.
 - e) **Relé de disparo con bloqueo.** Deberá dar disparo sobre ambas bobinas de disparo de los tres polos.
-

1.10.5 Unidad de Medición de Fasor

Todas las bahías de línea y de transformador deberán poseer una Unidad de Medición de Fasor (PMU) que cumpla con lo estipulado en la norma IEC/IEEE 60255-118-1:2018 - *Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems – Measurements*. Puede ser implementada como un relé independiente o como una función de la protección de línea, para el caso de líneas de transmisión, o como una función de la protección diferencial del transformador, para el caso de bahías de transformador.

Las inestabilidades que preceden a un apagón en grandes redes eléctricas son detectadas por una PMU, las cuales requieren un sincronismo de tiempo absoluto superior a 4 μ s entre las PMI situadas en extremos remotos.

Por la anterior razón, las PMU requieren de una sincronización exigente y esta se debe realizar de acuerdo con la norma IEC/IEEE 61850-9-3:2016 - *Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation*.

La información de la PMU deberá ser transmitida al concentrador que designe el Transportador y el CND.

1.11 Acciones de las protecciones en el STN

1.11.1 Desconexión de elementos en falla

Los elementos en falla deberán ser desconectados por su sistema de protección e interruptores asociados, como se detalla a continuación:

- a) Líneas de transmisión. Deberán ser desconectadas de la falla por medio de disparos monopoles para fallas monofásicas o disparos tripolares para fallas bi o trifásicas. Deberán estar equipadas con teleprotecciones para garantizar que el extremo remoto desconecte en el menor tiempo posible, ya sea en esquema de comparación direccional o con disparos permisivos.
- b) Reactores de línea. Los disparos que se produzcan tanto por las protecciones eléctricas como por las protecciones mecánicas deben ser dados por medio de un relé de disparo con bloqueo, para garantizar que no se produzcan cierres no deseados sobre el reactor en falla. Si el reactor no tiene interruptor, se deberá dar

disparo en el interruptor de la línea y enviar un comando de disparo directo transferido al interruptor del otro extremo de la línea.

- c) Transformadores de potencia. Los disparos que se produzcan tanto por las protecciones eléctricas como por las protecciones mecánicas deben ser dados por medio de un relé de disparo con bloqueo, para garantizar que no se produzcan cierres no deseados sobre el transformador en falla. Los disparos se deberán dar sobre todos los interruptores conectados al transformador, independientemente del nivel de tensión.
- d) Barras. La protección diferencial de barras, ante una falla en la barra, deberá dar disparos a todos los interruptores conectados a la barra por medio de un relé de disparo con bloqueo, para garantizar que no se produzcan cierres no deseados sobre la barra en falla. Si la subestación tiene esquemas de barras, dependiendo de los estudios eléctricos, en caso de que el sistema no sea capaz de absorber los reactivos de las líneas desconectadas en un solo extremo, se deberá enviar un comando de disparo directo transferido a los interruptores del otro extremo de las líneas a los que el estudio de coordinación de protecciones lo disponga.
- e) Interruptores Automáticos. Los interruptores deberán estar equipados con protecciones de falla interruptor para que, en el evento de falla de este, se dé disparo a los interruptores adyacentes de forma tal que la falla quede despejada satisfactoriamente. Si hay un interruptor localizado remotamente en otra subestación y este debe abrir para despejar la falla, deberá enviarse un comando de disparo directo transferido al interruptor remoto. Los disparos deberán efectuarse por medio de un relé de disparo con bloqueo, para garantizar que no se produzcan cierres no deseados sobre la falla. Para esquemas de subestación en interruptor y medio, la protección de falla interruptor deberá poseer tres etapas si solo hay transformadores de corriente en un solo lado del interruptor para las acciones por falla en la zona muerta, y dos etapas si el interruptor tiene transformadores de corriente de ambos lados.

1.11.2 Tiempos de actuación protección principal

El despeje de la falla, incluyendo el tiempo de la actuación de la protección principal y tiempo de apertura del interruptor, no deberá superar los siguientes tiempos:

- a) Para 550 kV: 80 ms
-

b) Para 220 kV: 100 ms

c) Para tensiones <220 kV: 120 ms

1.11.3 Actuación protección de respaldo

En el evento que la falla no sea despejada en los tiempos estipulados en el numeral 4.11.2 - Tiempos de actuación protección principal, la falla se deberá despejar por medio de las siguientes actuaciones:

- a) Si fue por falla de la protección principal, la protección de respaldo (zona 2 en las líneas de transmisión y sobrecorriente de tiempo definido en transformadores de potencia y reactores de línea) deberá enviar comando de disparo dentro de los 300 ms siguientes en que la falla en el sistema de potencia fue detectada por la protección de respaldo.
- b) Si falla el interruptor a la apertura, el disparo de respaldo deberá ser producido por la lógica de falla interruptor dentro de los 300 ms siguientes en que fue iniciada la lógica de falla interruptor. Se deberá confirmar el disparo en las dos bobinas de disparo del interruptor en falla y se deberá enviar disparo a los interruptores adyacentes y remotos que sean necesarios para despejar la falla.

1.11.4 Recierre líneas de transmisión

Las líneas de transmisión deberán recerrar de acuerdo con las siguientes directrices:

- a) Para disparos monopolares, deberá darse recierre monopolar. Si hay cierre en falla, deberá producirse un disparo tripolar definitivo dentro del tiempo de reclamo. El tiempo de recierre monopolar deberá ser de 500 ms para permitir la extinción del arco secundario y que el recierre sea exitoso.
- b) Para disparos tripolares, deberá darse recierre tripolar. El tiempo de recierre tripolar deberá ser de 300 ms y se deberá verificar el sincronismo en ambos lados del interruptor a cerrar. Si hay cierre en falla, deberá producirse un disparo tripolar definitivo dentro del tiempo de reclamo.

1.11.5 Verificación de sincronismo

Los interruptores de las líneas y transformadores deberán contar con verificación de sincronismo el cual permita el cierre del interruptor ante una de las siguientes circunstancias:

- a) Barra muerta – línea muerta. Para cierres manuales, útil durante la recuperación de un evento mayor en el sistema de transmisión.
- b) Barra viva – línea muerta. Para cierres manuales y recierres tripolares.
- c) Barra muerta – línea viva. Para cierres manuales y recierres tripolares en esquema de interruptores.
- d) Barra viva – línea viva en sincronismo. Para cierre manuales y recierres tripolares.

1.11.6 Teleprotección

Cada línea de transmisión deberá contar con sistema de teleprotección con cuatro señales:

i) una señal de comparación direccional, ii) dos señales de disparo permisivo, y, iii) un comando de disparo directo trasferido.

1.12 Sistema de Telecomunicaciones

El Sistema de Telecomunicaciones deberá ser diseñado e implementado cumpliendo la norma NERC CIP – *Cyber Security*. Cabe destacar que, desde el punto de vista de la subestación, este es la puerta de acceso tanto a las informaciones deseadas como a las no deseadas.

Los enlaces que se requieren entre la subestación y el Centro de Supervisión y Maniobras – CSM- del Transportador, el Centro Nacional de Despacho – CND – de XM o el Centro Regional de Despacho – CRD – del Operador de Red – OR -, según sea el caso, son:

- a) Voz operativa de responsabilidad del Transportador. Puede utilizar como medio telefonía IP, red privada, red pública, red satelital o telefonía celular.
- b) Voz operativa de responsabilidad del CND o del CSM. Puede utilizar como medio telefonía IP, red privada, red pública, red satelital o telefonía celular, pero el medio deberá ser diferente al del Transportador.
- c) Cada línea de transmisión deberá contar con un sistema de teleprotección con cuatro señales: i) una señal de comparación direccional, ii) dos señales de disparo permisivo, y, iii) un comando de disparo directo trasferido.
- d) Correo electrónico. Cada subestación deberá poseer un buzón de correo electrónico donde en la dirección se pueda identificar inequívocamente el nombre del operador y el nombre de la subestación.
- e) Un canal de datos con protocolo IEC 60870-5-101/104 para el enlace entre el Nivel 2 de la subestación y el Nivel 3 del CSM o CND, a cargo del Transportador.

- f) Un canal de datos con protocolo IEC 60870-5-101/104 para el enlace entre el Nivel 2 de la subestación y el Nivel 3 del CSM o CND, a cargo del CSM o del CND.
- g) Un canal de datos para la estación de ingeniería remota.
- h) Un canal de datos para la información comercial que se estipula en el Código de Medida.

2 REDES INTELIGENTES

La evolución de los sistemas de potencia y los retos que deben afrontar para integrar óptimamente los nuevos desarrollos, demandan el trabajo colaborativo entre los diferentes actores del mercado: gobierno, entidades de normalización, proveedores, empresas de energía y usuarios.

Los retos que se tienen que afrontar son variados y dispares e incluyen:

- Incremento de la carga en el sistema de potencia
- Incremento de la distancia entre generación y carga
- Fluctuación de las energías renovables no convencionales
- Nuevas cargas (vehículos híbridos y eléctricos)
- Mayor uso de los recursos energéticos distribuidos
- Presión de costos
- Desverticalización de los agentes del mercado
- Aumento de las operaciones energéticas
- Consumo transparente y precios para el consumidor
- Importante injerencia de los reguladores

Los anterior, demanda mayor observabilidad y controlabilidad de la red eléctrica y sus componentes. Esto exigirá un mayor nivel de sintaxis y semántica, de interoperabilidad de los diversos componentes, de soluciones y sistemas, que en conjunto apalancan un sistema de energía. Adicionalmente, deben tenerse en cuenta requisitos tales como la seguridad de la inversión a largo plazo y el ambiente legal.

La Red Inteligente (SG- Smart Grid) es la respuesta para hacer frente a estos retos y adicionalmente, proporciona una visión para el futuro sistema de energía en el largo plazo.

La Red Inteligente involucra toda la cadena energía, desde la conversión hasta el consumidor. El flujo de energía cambia de ser unidireccional (desde la generación a través de las redes de transmisión y distribución a los consumidores) a un flujo bidireccional. Adicionalmente, la forma en que se opera un sistema de potencia cambia de un enfoque jerárquico de arriba hacia abajo a un control distribuido.

La interoperabilidad y la seguridad de la Red Inteligente demandan basar todos los desarrollos e inversiones en un marco sólido de normas, el cual es el núcleo de los nuevos

desarrollos La IEC, como única organización internacional de normalización en el campo electrotécnico, está idealmente posicionada para contribuir al desarrollo de la Red Inteligente y sus efectos beneficiosos para la sociedad en su conjunto.

El alcance que cubre la Red Inteligente es el siguiente:

- HVDC y FACTS
- Prevención de apagones/EMS
- Gestión avanzada de distribución
- Automatización de distribución
- Automatización de subestaciones inteligentes
- Recursos energéticos distribuidos
- Infraestructura de medidores avanzados
- Respuesta a la demanda y gestión de carga
- Hogar inteligente y automatización de edificios
- Almacenamiento de energía eléctrica
- Electromovilidad
- Monitorización de condiciones

El desarrollo de la Red Inteligente deberá darse en forma gradual, para lo cual todas las iniciativas que surjan para modificar, actualizar o mejorar la normatividad para el Sector Eléctrico, se deberán efectuar con miras a incorporar los principios que rigen una Red Inteligente y de esta forma, facilitar el paso a constituir una Red Inteligente con todas las bondades que esta brinda.

Para el desarrollo de la Red Inteligente y sus diferentes componentes y sistemas, se adoptan las recomendaciones que da el IEC TC57.