

LPI No. BID V-607-LPI-O-BID-L1223-RSND-CNELCORP-
ST-OB-001

CORP CONSTRUCCIÓN DE LA S/E LA AVANZADA DE
138/69 kV – GD

BOLETÍN N° 7
ENMIENDAS AL DDL

19 DE ENERO DE 2023

ENMIENDA Nro.1:

TEXTO ORIGINAL:

“Servicios auxiliares de 125 VDC

Se refiere a dos cargadores de baterías y un banco de baterías de 125 Vdc. La integración de señales de alarma y medidas de este sistema SAS se realizará mediante señales eléctricas, es decir, contactos libres de voltaje para las señales de alarma y transductores que tomen las medidas de V de barra, V de baterías, I de carga e I de baterías y los convierta en señales de 4-20 mA.”

TEXTO MODIFICADO:

“Servicios auxiliares de 125 VDC

El sistema de servicios auxiliares de 125 VDC dispone de transductores que tomen las medidas de V de barra, V de baterías, I de carga e I de baterías y los convierta en señales de 4-20 mA, las cuales deben ser integradas al controlador de este sistema, de igual forma deberá integrar señales de alarma mediante contactos libres de voltaje.

Adicionalmente, todas las señales supervisión, alarmas, mediciones y comandos de los cargadores de baterías deben ser transmitidos al sistema de control distribuido de la subestación. Esto se lo puede realizar ya sea por medio de contactos secos, miliamperios y/o protocolos de comunicaciones, como Modbus TCP/IP.”

ENMIENDA Nro. 2

TEXTO ORIGINAL

2.9.3. Comando local nivel 2 (Subestación)

El comando local en nivel 2 debe realizarse mediante una de las dos interfaces IHM locales, que deben permitir la operación de la subestación en todas sus funcionalidades. Para esto, se debe utilizar los enclavamientos programados en los BCUs de cada posición, que son los que finalmente evalúan si el comando se puede ejecutar o no.

Todas las funciones de comando de nivel 2 deben ser controladas por una de las dos unidades (seleccionables) centrales de adquisición y control (ver sección 2.14.1).

En este nivel se debe incluir un firewall para tecnologías de operación con la finalidad de proteger de posibles ataques internos y externos, así como facilitar la configuración segura de equipos de protección, control y medición de la subestación.

2.10. Comando remoto

TEXTO MODIFICADO

2.9.3. Comando local nivel 2 (Subestación)

El comando local en nivel 2 debe realizarse mediante una de las dos interfaces IHM locales, que deben permitir la operación de la subestación en todas sus funcionalidades. Para esto, se debe utilizar los enclavamientos programados en los BCUs de cada posición, que son los que finalmente evalúan si el comando se puede ejecutar o no.

Todas las funciones de comando de nivel 2 deben ser controladas por una de las dos unidades (seleccionables) centrales de adquisición y control (ver sección 2.14.1).

En este nivel se debe incluir un firewall para tecnologías de operación con la finalidad de proteger de posibles ataques internos y externos, así como facilitar la configuración segura de equipos de protección, control y medición de la subestación, *y se ubicará al interior de la sala de control principal de la subestación.*

ESPECIFICACIONES TÉCNICAS FIREWALL INDUSTRIAL

Características Generales

- Diseño industrial robusto
- Creado para entornos hostiles y rango de temperatura: -40° a 70°C
- Endurecido para inmunidad a vibraciones, golpes, sobretensiones y ruido eléctrico.

Diseñado para soportar ambientes de subestaciones y centrales IEEE1613.

Año de fabricación: 2022 en adelante, no debe tener una fecha publicada para “End of Sale” y “End of Support”

Interfaces de red (Cobre): ≥ 2 de 1Gbps

Interfaces de red (Fibra óptica): ≥ 2 SFP (Fibra o tipo “combo”):

1 transceivers SFP 1000BASE-LX, 1310nm, 10km, LC, monomodo.

1 transceivers SFP 1000BASE-SX, 850nm, 550M, LC, multimodo.

Conectividad a Red: Las interfaces de red de cobre y/o fibra deberán conectarse a los switches de la red SAS y a los equipos de comunicación hacia el exterior, desde donde se podrá acceder de forma remota.

Puertos de consola: ≥ 1 , USB y/o RJ45 y/o DB9

Fuentes de poder: 2 fuentes redundantes 1+1 de 125VDC.

Protección: IP20 o mayor

Administración centralizada, incluye software.

Suscripciones de seguridad: ≥ 3 años (para IPS, Application Control)

Interfaz de gestión: Gestión local del dispositivo y remota para visibilidad y gestión centralizada

Control de acceso: Full Stateful Inspection (Operaciones de firewall en capa 2, capa 3)

Auditoría y control: Radius, SNMPv3, syslog, NTP

Networking, soporte de al menos:

- NAT
- VLANS – IEEE 802.1Q
- QoS

- Enrutamiento estático y dinámico
- SNMPv3

VPNs

- Control de acceso remoto con o sin agente
- Site to Site VPN IPSEC - IPSEC - AES
- Acceso remoto VPN para al menos 20 usuarios.

Sistema de Detección y Prevención de Intrusiones (IPS), debe permitir:

- Reglas enfocadas a la detección de amenazas en equipos industriales y redes.
- Identificación de abusos de protocolo o cuando el tráfico no cumple con los estándares del protocolo.
- Protecciones para contra exploits de vulnerabilidades específicas de ICS y CVEs, tomando en consideración las fuentes de inteligencia externas (firmas, actualizaciones y bases de datos).

Control de aplicaciones

- Identificar y control de aplicaciones industriales.
- Visibilidad de protocolos ICS/OT y Control

Protocolos y estándares OT: Debe soportar al menos los siguientes:

- Modbus
- DNP3
- BACNet
- Ethernet/IP
- GOOSE
- IEC-61850
- IEC-60870-5-104
- MMS
- OPC-UA
- CIP
- S7

Estándares para emisiones/inmunidad electromagnética

- FCC
- CE

Estándares industriales

- IEC 61850-3 Electric Substations Communications Networking
- IEEE 1613 Electric Power Stations Communications Networking

Cables de poder incluidos

Garantía técnica de fábrica: Mínimo 3 años

Soporte de fábrica: Mínimo 3 años

ENMIENDA No.3

MODIFÍCASE, los Documentos de la Licitación (DDL), Parte I. Sección IV. Formularios de Licitación, Lista de Cantidades – 3.3 TABLA DE DATOS GARANTIZADO SUMINISTRO DE EQUIPOS DE SISTEMA SUPERVISIÓN, CONTROL, PROTECCIÓN Y MEDICIÓN, COMUNICACIONES, Y AUXILIARES DE SUBESTACIÓN, Tabla 3.3.3: Sistema de supervisión, control, protección, medición.

TEXTO ORIGINAL:

Tabla 3.3.3 SISTEMA DE SUPERVISION, CONTROL, PROTECCION, MEDICION

ITEM	CARACTERISTICAS	UNIDAD	ESPECIFICACIÓN REQUERIDA	ESPECIFICACION OFERTADA
1	Funcionalidad del Sistema			
1.1	Tiempo real (1)	%	>= 99.95	
2	Monitoreo (1)	%	>= 99.98	
3	Capacidad del Sistema			
3.1	Numero de IEDS que el sistema puede incluir	c/u	>= 20	
4	Redundancia			
4.1	Computadores de adquisicion	c/u	2	
4.2	Operar conjuntamente en HOT STAND BY		SI	
4.3	Cambio automatico sin interrupcion cuando falle una de las dos unidades		SI	
5	IHM	c/u	2	
6	Velocidad de comunicación interna del SAS (2)			
	Tiempo de adquisicion/Integridad de los datos/Metodo de intercambio de:			
6.1	Alarmas	s	1s/Media/Espontaneo	
6.2	Comandos	s	1s/Alta/Espontaneo	
6.3	Datos de estado de proceso	s	medidas/Media/Espontaneo	
6.4	Consulta de eventos con estampa de tiempo	s	10s/Baja/A pedido	
6.5	Datos de interbloqueo entre IDE's	s	5ms/Alta/Espontaneo	
6.6	Datos de interbloqueo, informacion de estado de otros automatismos	s	100ms/Alta/A pedido	
6.7	Disparo por proteccion	s	3ms/Alta/Espontaneo por falla en el sistema de potencia o en el equipo primario	
7	Protocolos de comunicación (3):			
7.1	Interna del SAS		IEC 61850	
7.2	Con los Centros de Control (CNEL y Cenace)		IEC 60870-5-101/104,DNP 3.0	
7.3	Con IEDS de otro Fabricante		IEC 60870-5-103 para comunicaciones con IEDS de proteccion de otro Fabricante que no tenga interfase IEC 61850	
7.4	Con Perifericos (transformadores, servicios auxiliares , grupo diesel, etc.)		Modbus RTU o DNP (3)	
8	Numero de muestras por ciclo en los IEDS de proteccion	c/u	20 (IEC 61850)	
9	Disponibilidad del sistema (1)		99.95	
9.1	IEDS	%	>99.98% (1)	
9.2	Comunicación entre IEDS	%	>99.97% (1)	
9.3	Comunicación entre Nivel 1 y Nivel 2	%	>99.97%	
9.4	Comunicación entre Nivel 1 y Nivel 2(el nivel 3 considerado mediante un simulador de protocolo)	%	>99.98% con manejo en tiempo real	
9.5	Disponibilidad Total tomando en cuenta fallas menores	%	> 99.97%	

TEXTO MODIFICADO:

Tabla 3.3.3: Sistema de supervisión, control, protección, medición

ITEM	CARACTERÍSTICAS	UNIDAD	ESPECIFICACIÓN REQUERIDA	ESPECIFICACION OFERTADA
1	Funcionalidad del Sistema			
1,1	Tiempo real (1)	%	>= 99.95	
2	Monitoreo (1)	%	>= 99.98	
3	Capacidad del Sistema			
3,1	Numero de IEDS que el sistema puede incluir	c/u	>= 20	
4	Redundancia			
4,1	Computadores de adquisición	c/u	2	
4,2	Operar conjuntamente en HOT_STAND BY		SI	
4,3	Cambio automático sin interrupción cuando falle una de las dos unidades		SI	
5	IHM	c/u	2	
6	Velocidad de comunicación interna del SAS (2)			
	Tiempo de adquisición/Integridad del los datos/Método de intercambio de:			
6,1	Alarmas	s	1s/Media/Espontaneo	
6,2	Comandos	s	1s/Alta/Espontaneo	
6,3	Datos de estado de proceso	s	medidas/Media/Espontaneo	
6,4	Consulta de eventos con estampa de tiempo	s	10s/Baja/A pedido	
6,5	Datos de interbloqueo entre IDE's	s	5ms/Alta/Espontaneo	
6,6	Datos de interbloqueo, información de estado de otros automatismos	s	100ms/Alta/A pedido	
6,7	Disparo por protección	s	3ms/Alta/Espontaneo por falla en el sistema de potencia o en el equipo primario	
7	Protocolos de comunicación (3):			
7,1	Interna del SAS		IEC 61850	
7,2	Con los Centros de Control (CNEL y Cenace)		IEC 60870-5-101/104,DNP 3.0	
7,3	Con IEDS de otro Fabricante		IEC 60870-5-103 para comunicaciones con IEDS de protección de otro Fabricante que no tenga interfase IEC 61850	
7,4	Con Periféricos (transformadores, servicios auxiliares , grupo diésel, etc.)		Modbus RTU o DNP (3)	
8	Numero de muestras por ciclo en los IEDS de protección	c/u	20 (IEC 61850)	
9	Disponibilidad del sistema (1)		99,95	
9,1	IEDS	%	>99.98% (1)	
9,2	Comunicación entre IEDS	%	>99.97% (1)	
9,3	Comunicación entre Nivel 1 y Nivel 2	%	>99.97%	
9,4	Comunicación entre Nivel 1 y Nivel 2(el nivel 3 considerado mediante un simulador de protocolo)	%	>99.98% con manejo en tiempo real	
9,5	Disponibilidad Total tomando en cuenta fallas menores	%	> 99.97%	

ITEM	CARACTERISTICAS	UNIDAD	ESPECIFICACIÓN REQUERIDA	ESPECIFICACION OFERTADA
10	Especificaciones de Firewall			
10,1	Características Generales			
	Diseño industrial robusto			
	Creado para entornos hostiles y rango de temperatura:		40° a 70°C	
	Endurecido para inmunidad a vibraciones, golpes, sobretensiones y ruido eléctrico			
10.2	Diseñado para soportar:		Ambientes de subestaciones y centrales IEEE1613	
10.3	Año de fabricación:		2022 en adelante, no debe tener una fecha publicada para "End of Sale" y "End of Support"	
10,4	Interfaces de red (Cobre):		>= 2 de 1Gbps	
10,5	Interfaces de red (Fibra óptica):		>= 2 SFP (Fibra o tipo "combo")	
10.6	1 transceivers :		SFP 1000BASE-LX, 1310nm, 10km, LC, monomodo.	
10.7	1 transceivers :		SFP 1000BASE-SX, 850nm, 550M, LC, multimodo.	
10.8	Conectividad a Red:		Las interfaces de red de cobre y/o fibra deberán conectarse a los switches de la red SAS y a los equipos de comunicación hacia el exterior, desde donde se podrá acceder de forma remota.	
10,9	Puertos de consola:		>= 1, USB y/o RJ45 y/o DB9	
10,1	Fuentes de poder:		2 fuentes redundantes 1+1 de 125VDC	
10,11	Protección:		IP20 o mayor	
10,12	Suscripciones de seguridad:		>= 3 años (para IPS, Application Control)	
10,13	Interfaz de gestión:		Gestión local del dispositivo y remota para visibilidad y gestión centralizada	
10,14	Control de acceso:		Full Stateful Inspection (Operaciones de firewall en capa 2, capa 3)	
10,15	Auditoría y control:		Radius, SNMPv3, syslog, NTP	
10,16	Networking, soporte de al menos:		NAT	
			VLANS – IEEE 802.1Q	
			QoS	
			Enrutamiento estático y dinámico	
			SNMPv3	
10,17	VPNs		Control de acceso remoto con o sin agente	
			Site to Site VPN IPSEC - IPSEC - AES	
			Acceso remoto VPN para al menos 20 usuarios.	
10,18	Sistema de Detección y Prevención de Intrusiones (IPS), debe permitir:		Reglas enfocadas a la detección de amenazas en equipos industriales y redes.	
			Identificación de abusos de protocolo o cuando el tráfico no cumple con los estándares del protocolo.	
			Protecciones para contra exploits de vulnerabilidades específicas de ICS y CVEs, tomando en consideración las fuentes de inteligencia externas (firmas, actualizaciones y bases de datos).	
10,19	Control de aplicaciones		Identificar y control de aplicaciones industriales.	
			Visibilidad de protocolos ICS/OT y Control	
10.20	Protocolos y estándares OT: Debe soportar al menos los siguientes:		Modbus	
			DNP3	
			BACNet	

			Ethernet/IP	
			GOOSE	
			IEC-61850	
			IEC-60870-5-104	
			MMS	
			OPC-UA	
			CIP	
			S7	
10,21	Estándares para emisiones/inmunidad electromagnética		FCC	
			CE	
10,22	Estándares industriales		IEC 61850-3	
			IEEE 1613	
10,23	Cables de poder		incluidos	
10,24	Garantía técnica de fábrica:		Mínimo 3 años	
10,25	Soporte de fábrica:		Mínimo 3 años	

NOTAS ACLARATORIAS:

- (1) El oferente debe presentar cálculos de la confiabilidad ofertada, tanto para equipo individual como para sistema completo
- (2) El oferente debe presentar certificaciones de cumplimiento de estos tiempos o planes de pruebas para comprobación de tiempos ofertados
- (3) El oferente debe incluir en su oferta el valor de las licencias de los protocolos

Notas:

1. El OFERENTE debe llenar los datos en la columna ESPECIFICACIÓN OFERTADA y firmar cada una de las hojas.
2. En la columna ESPECIFICACION OFERTADA se deberá hacer referencia a catálogos, manuales u hojas de datos, se indicará la hoja, ítem y párrafo correspondiente. En caso de no indicar la referencia y no incluir la documentación respectiva, podría entenderse que no existe información técnica que avale lo especificado y será motivo de rechazo de la oferta.

Elaborado por la comisión evaluadora del proceso LPI No. BID V-607-LPI-O-BID-L1223RSND-CNELCORP-ST-OB-001.

INTEGRANTE 1

INTEGRANTE 2

INTEGRANTE 3