INSTITUTO ARGENTINO
DEL PETROLEO Y DEL GAS

PRÁCTICA RECOMENDADA

PR IAPG-SC-41-2025-00

PROTOCOLOS DE SEGURIDAD UTILIZADO POR CADA COMPUTADOR DE FLUJO

La presente PR fue aprobada en la reunión de Comisión Directiva el 21 de marzo de 2024

1 NOTAS ESPECIALES

• Por tratarse de una Práctica Recomendada (PR) las acciones, modalidades operativas y técnicas en ellas incluidas, carecen de contenido normativo, legal o interpretativo, y no resultan obligatorias ni exigibles por terceros bajo ninguna condición.
• No podrán ser invocadas para definir responsabilidades, deberes, ni conductas obligatorias para ninguno de los sujetos que las utilice, ya que sólo integran un conjunto de consejos para el mejoramiento de las operaciones comprendidas.
• La adopción de una PR no libera a quien la utilice del cumplimiento de las disposiciones legales nacionales, provinciales y municipales, como así tampoco de respetar los derechos de patentes y /o propiedad industrial o intelectual que correspondieren.
• El IAPG no asume, con la emisión de esta PR, la responsabilidad propia de las Compañías, sus Contratistas y Subcontratistas, de capacitar, equipar o entrenar apropiadamente a sus empleados. Así mismo el IAPG no releva ni asume responsabilidad alguna en lo que respecta al cumplimiento de las Normas en materia de salud, seguridad y protección ambiental.
• Toda cita legal o interpretación normativa contenida en el texto de esta PR no tiene otro valor que el de un indicador para la conducta propia e interna de quienes voluntariamente la adopten o utilicen, bajo su exclusiva responsabilidad.
• La presente PR fue aprobada en la reunión de Comisión Directiva, celebrada en Sede Central, el 21 de marzo de 2024.

2 PROPÓSITO

El propósito de este documento es informar las distintas opciones de los protocolos de seguridad utilizado por cada computador de flujo.

3 COMPUTADOR DE FLUJO

3.1 Alcance

Describe las recomendaciones de seguridad de los puertos de comunicación de los distintos computadores de flujo utilizado actualmente en las unidades de medición de líquido de transferencia de custodia.

3.2 Definiciones

RS232 EIA standard –Conector DB9: utilizado para distancias cortas, conexión punto a punto.
RS485 EIA standard for two-wire differential bidirectional –Conexión de 2 hilos o 4 hilos: utilizado para distancias largas, ya sea punto a punto o conexiones multipunto.
Ethermet TCP/IP: utilizados para comunicarse a través de una red de área local (LAN) o una red de área amplia (WAN).

4 COMPUTADOR DE FLUJO FLOW – X

A continuación, se detallan los niveles de seguridad que ofrece el computador de flujo a nivel hardware y software. Se trata de la seguridad que ofrece el equipo a nivel usuario ya sea a través del computador o a través del software.

4.1 Seguridad y protección de datos nivel Hardware.

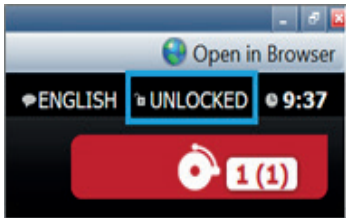
4.1.1 Switch de bloqueo

Cada módulo tiene un switch mecánico que asegura que no será posible modificar el software metrológico a través de la interfaz de usuario (pantalla táctil) o las interfaces de comunicación (serial o ethernet)

- Si el switch está activado, no será posible sobrescribir la aplicación, el firmware y el software en el computador. Sin embargo, será posible la lectura de datos del computador.
- Si el switch está activado, no será posible cambiar la configuración o controlar comandos con nivel de seguridad 1000 o mayor.
- Si el switch está activado, solo comandos con nivel de seguridad menor a 1000 pueden ser modificados, luego de que un usuario autorizado se haya registrado. Todos los comandos de configuración que son legalmente relevantes tienen un nivel de seguridad 1000 o superior.

Funciones normales de operación como selección de display, reconocimientos de alarmas e impresión de reportes no son inhabilitadas por el switch.

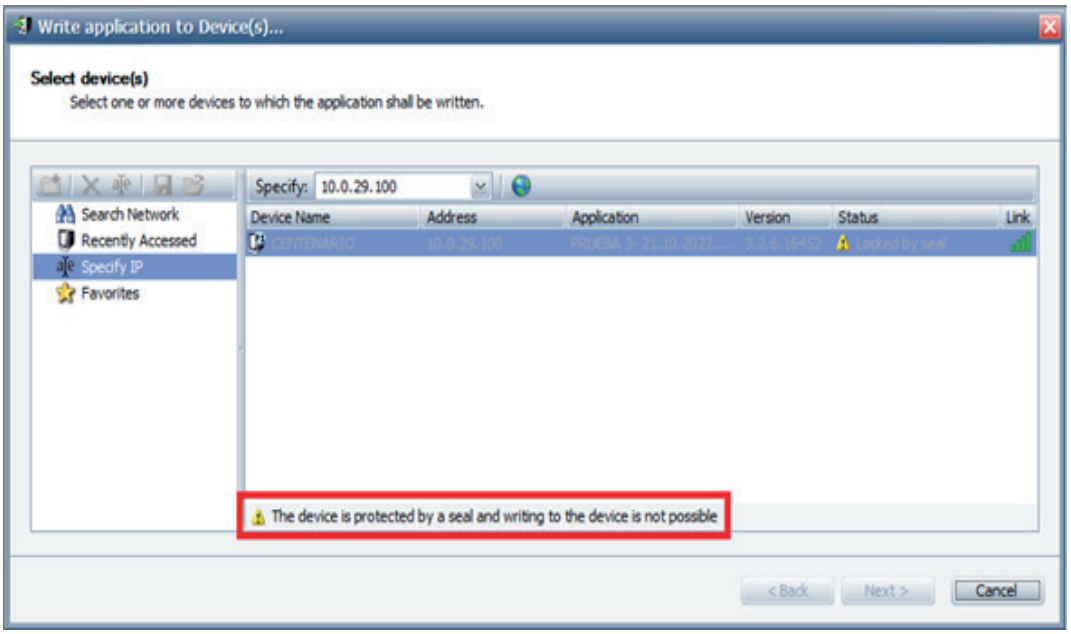
Cuando esta desactivado el switch se visualiza en pantalla un icono de candado abierto con la leyenda desbloqueado (unlocked).



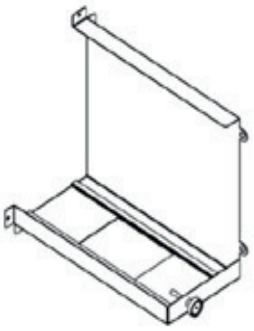
Activando el switch se visualiza el icono del candado cerrado con la leyenda bloqueado (locked). En la imagen de abajo se muestra cómo actúa la seguridad del switch. Luego de registrarnos con un usuario de nivel 2000 o superior, al querer cargar una configuración en el computador se puede leer en pantalla “el dispositivo está protegido con un sello y escribir en el dispositivo no es posible” (*the device is protected by a seal and writing to the device is not posible*)

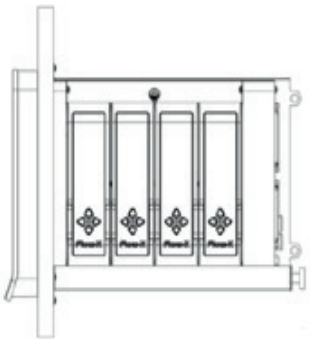
4.1.2 Sello metrológico

El computador tiene un freno que puede ser cerrado y precintado. Cuando el freno está cerrado no se puede acceder físicamente al switch de bloqueo.
Se recomienda por seguridad activar el switch de bloqueo antes de que el freno sea cerrado y precintado. De esta forma no será posible desmontar un módulo sin antes abrir el soporte y romper el precinto.



Para todas las carcasas existe la opción de dejar que una entidad oficial selle el computador con un precinto, a fin de evitar el acceso al switch de bloqueo. Para el Flow-X/P se utiliza una barra para sellar con un precinto todos los módulos instalados.





4.2 Protección de datos nivel software

Para esta práctica recomendada se usó el software base “Spirit Flow X-press (basic mode)” versión 3.2.6. Se recomienda mantener siempre actualizado el software con la última versión para evitar problemas de compatibilidad con otros archivos de configuración.
A demás, se recomienda usar la versión profesional del software “Spirit Flow X-press (professional mode)” para tener acceso a configuraciones más avanzadas del computador. Para habilitar esta versión es necesaria la licencia profesional otorgada por el fabricante.

4.2.1 Usuario, contraseñas y niveles de seguridad

El computador de flujo puede restringir y/o permitir el acceso a diferentes parámetros de configuración, según el usuario que lo esté operando.
El computador permite crear diferentes usuarios, algunos con acceso parcial y otros con acceso total a la configuración del computador.
Los siguientes usuarios y contraseñas vienen por default y son usadas para las aplicaciones estándar en líquidos o gas.

User name	Password	PIN code	Security level
operator	operator	000123	500
tech	tech	898989	750
engineer	engineer	101010	1000
administrator	admin	123321	2000

- Nombre de usuario (User name) y contraseña (password) se usan para acceder desde la pantalla táctil.
- PIN code y nivel de seguridad (security level) se usa para acceder desde el display del modulo

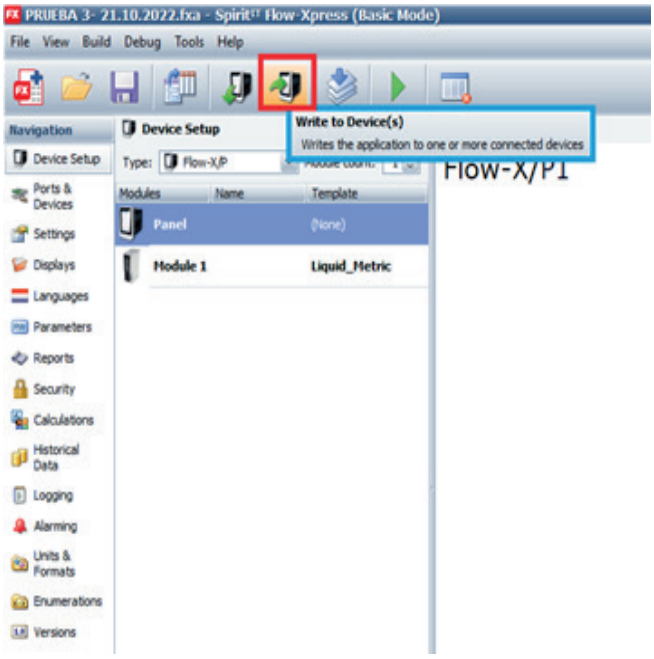
Se recomienda cambiar los nombres de usuarios y contraseñas desde el software o directamente desde la pantalla táctil.
Cada usuario tiene un nivel de seguridad especifico el cual determina que puede y que no puede hacer el usuario con el computador. Por otro lado, cada parámetro también tiene asignado un nivel de seguridad. Los niveles de seguridad por default de estos parámetros son:

Parámetro	Nivel de seguridad
Reconocimiento de alarmas (Acknowledge alarms)	500
Suprimir alarmas (Suppress alarms)	1000
Bloqueo de sello de parámetros (Parameter seal lock)	750
Escribir aplicación (Write application)	2000
Leer aplicación (Read application)	n/a
Modificar credenciales de usuario (Modify user credentials)	2000
Cambio de configuración (Change settings)	2000
Guardar/imprimir reportes (Print/save repots)	500
Cambio de hora (Change time)	600
Leer credenciales de usuario (Read user credentials)	1000

Solo usuarios con al menos el nivel requerido están habilitados para cambiar los parámetros. Usuarios con un nivel por debajo no podrán ejecutar estos parámetros.
Los niveles de seguridad de los parámetros se pueden modificar como:

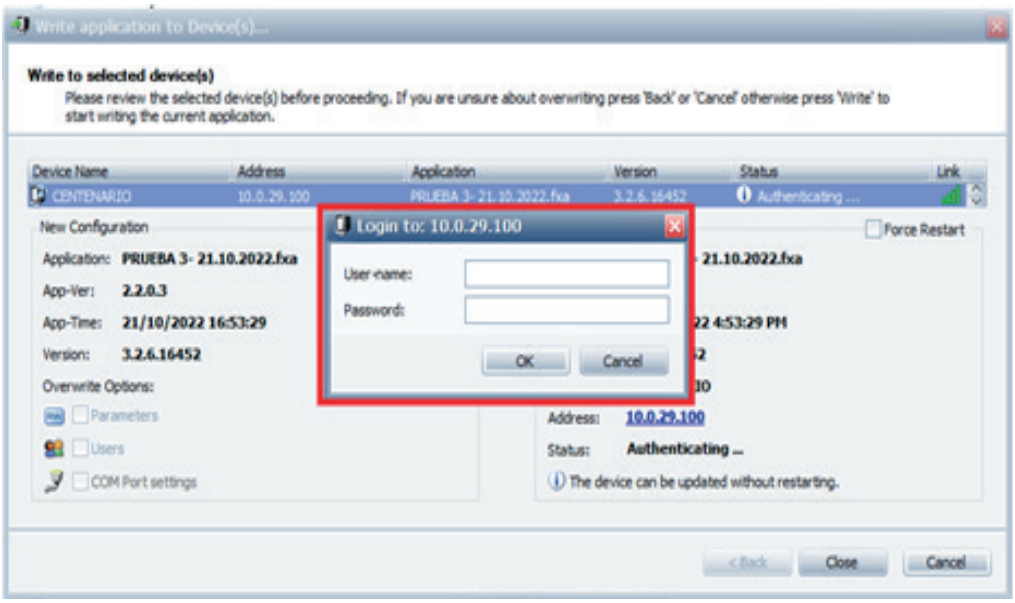
- n/a (no aplica).
- Con numeración desde 1 hasta 100000.

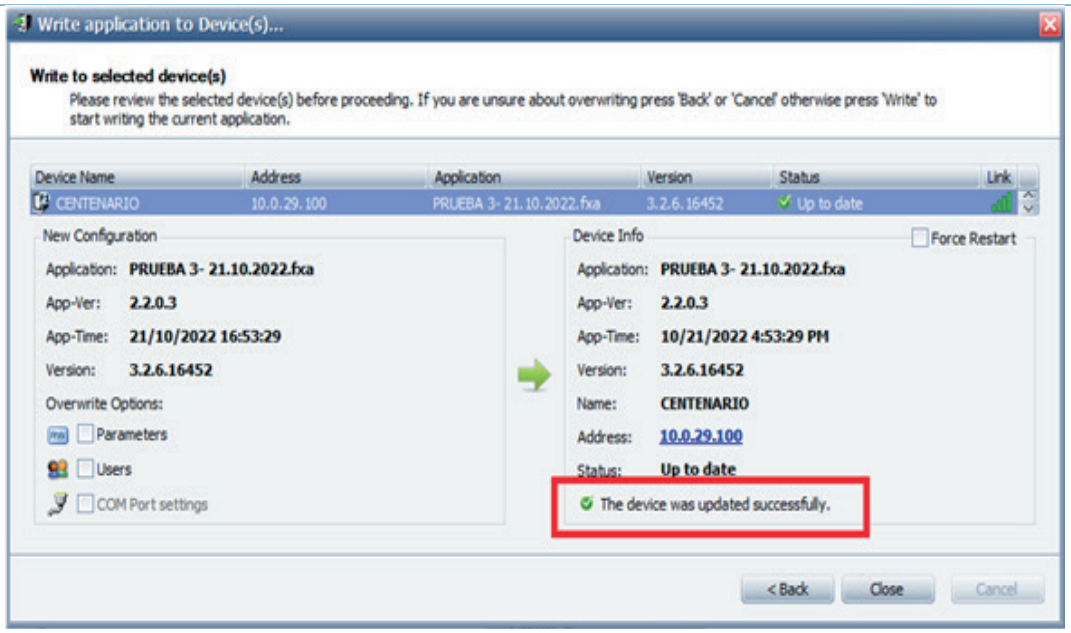
A modo de ejemplo, se procede a cargar una configuración en el computador (write application), parámetro que tiene un nivel de seguridad por default de 2000.



En este punto se deberá establecer la conexión con el computador escribiendo la dirección IP del mismo.

Si accedemos con el usuario “administrator” (contraseña “admin”) que tiene nivel de seguridad 2000 estaremos habilitados para escribir la configuración en el computador. Durante la carga de la configuración el computador se reiniciará y al finalizar aparecerá la leyenda “el dispositivo fue actualizado exitosamente” (*the device was uppdate succesfully*)





En cambio, si realizamos la misma operación, pero ahora con el usuario “operator”, de nivel de seguridad 500, el software entra en un bucle en donde nos vuelve a aparecer la pantalla de registro de usuario, ya que interpreta que el nivel de seguridad no es suficiente para realizar esta operación

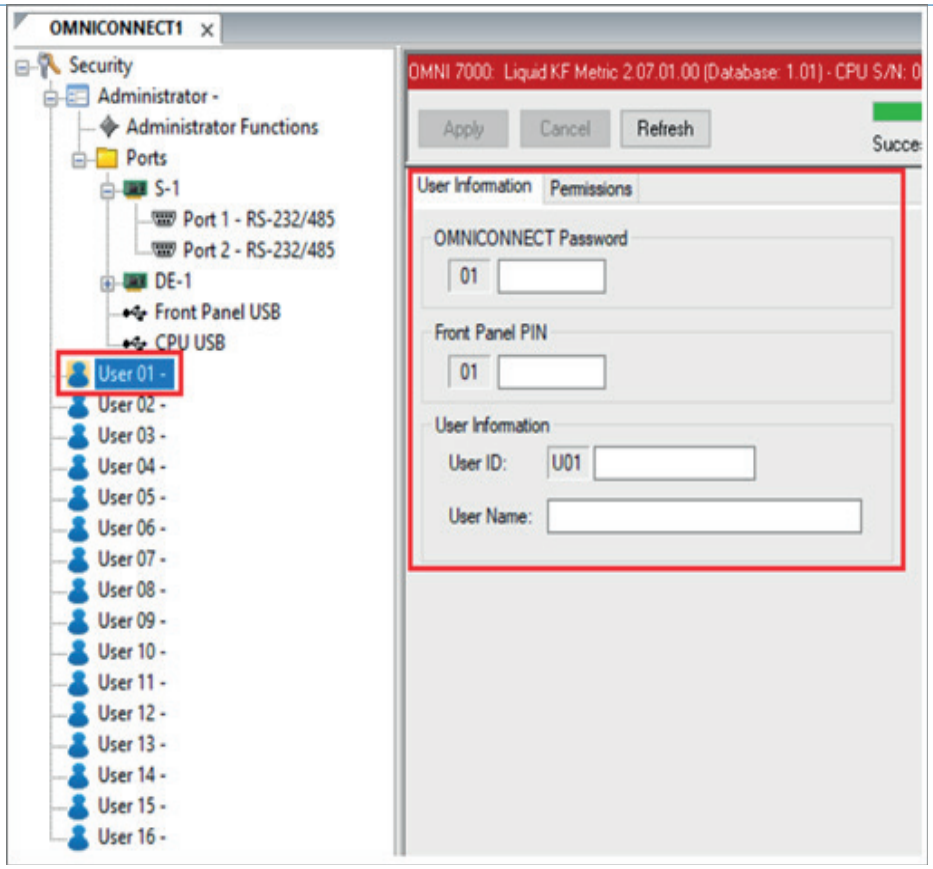
5 COMPUTADOR DE FLUJO OMNI 7000

A continuación, se detallan los niveles de seguridad que ofrece el computador de flujo a nivel hardware y software. Se trata de la seguridad que ofrece el equipo a nivel usuario ya sea a través del computador o a través del software

5.1 Seguridad y protección de datos nivel Hardware

5.1.1 Usuario

Como se puede observar, se pueden dar de alta hasta 16 usuarios para utilizar el Panel Frontal y el OmniConnect. Para este boletín, se utilizará como ejemplo el User 01 ya que lo mismo puede replicarse con el resto de los 16 usuarios.
Una vez seleccionado el User 01, en el centro de la pantalla se muestra la configuración de las credenciales:



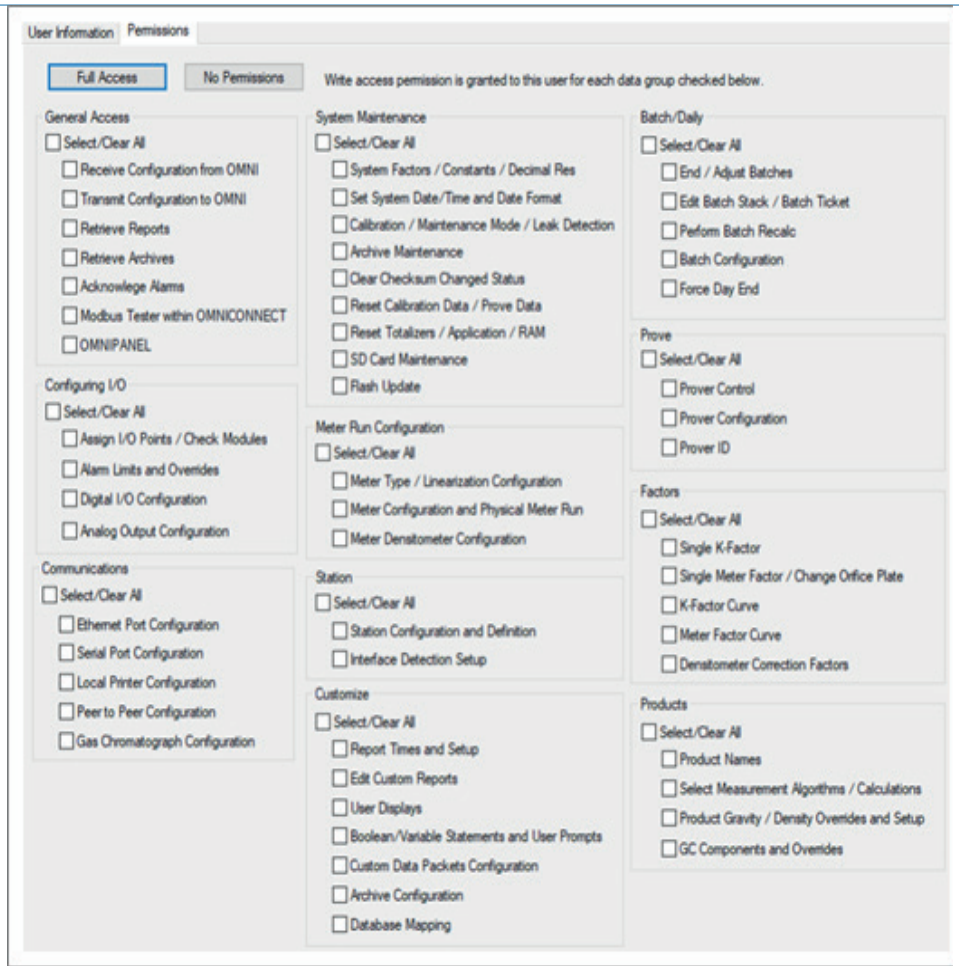
Los Passwords para el inicio de sesión tanto en el OmniConnect como para el panel frontal pueden tener hasta 6 caracteres. En el caso del Omniconnect, los 6 caracteres pueden ser alfanuméricos mayúsculas/minúsculas. En cambio, para el panel frontal, los caracteres deben ser numéricos.

Nota: Para ambos casos, se puede utilizar el mismo Password mientras sean numéricos.
El campo User Information permite cargar el ID de usuario que aparecerá registrado en los Audit Trail que almacenan todos los cambios generados en el computador.

- El User ID puede ser hasta 12 caracteres alfanuméricos.
- El User Name puede ser hasta 32 caracteres alfanuméricos.

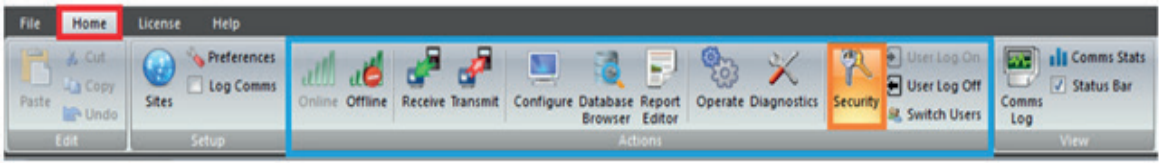
5.1.2 Permisos (Permissions)

Como se puede observar, se pueden configurar los mismos permisos detallados anteriormente en la seguridad de puertos de comunicación.

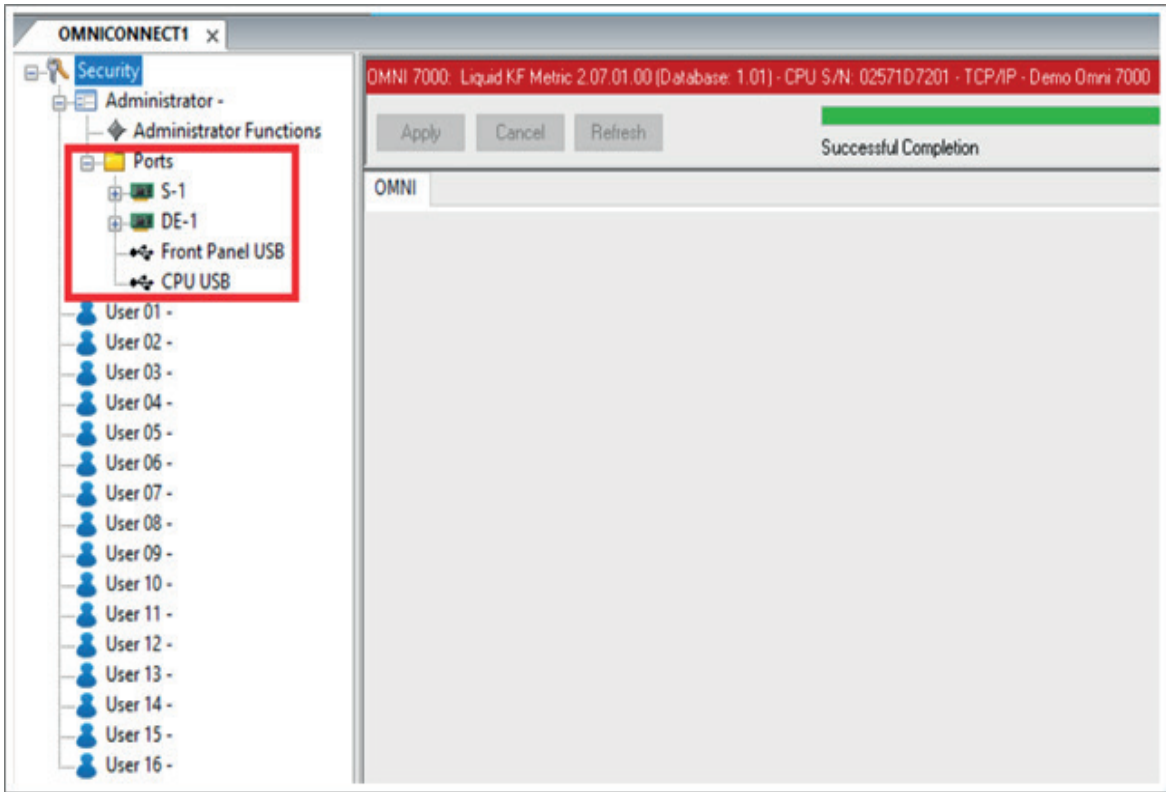


5.1.3 Seguridad de puertos

Para acceder a la configuración de la seguridad de puertos, deberá seleccionar en la barra Actions (Celeste), el icono Security (Naranja), dentro de la pestaña Home (Rojo)



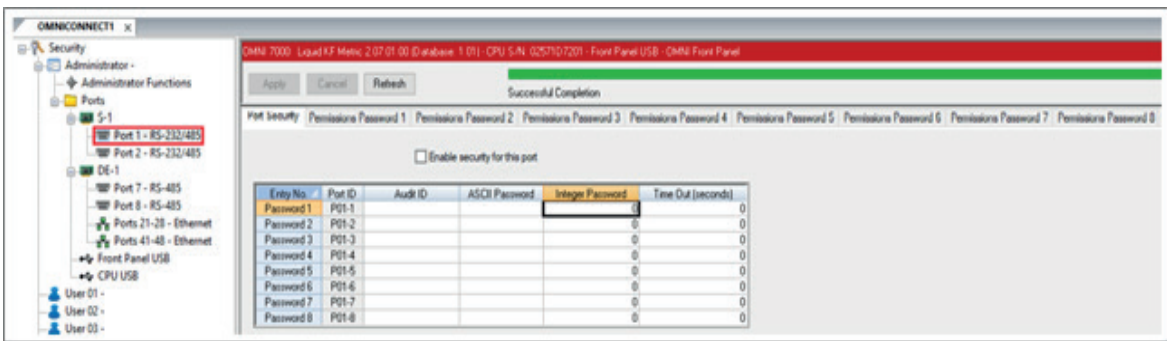
En la parte izquierda de la pantalla, aparecerá el árbol de navegación Security. Ir hacia la opción Ports (indicado en Rojo):



La cantidad de puertos a configurar está relacionada a la cantidad de módulos de comunicación de su computador.

El utilizado para este PR tiene:
• 1 módulo S: 2 puertos RS232/485.
• 1 módulo DE: 2 puertos RS232/485 y 2 puertos Ethernet.
• 1 puerto USB en el panel frontal.
• 1 puerto USB en la CPU.

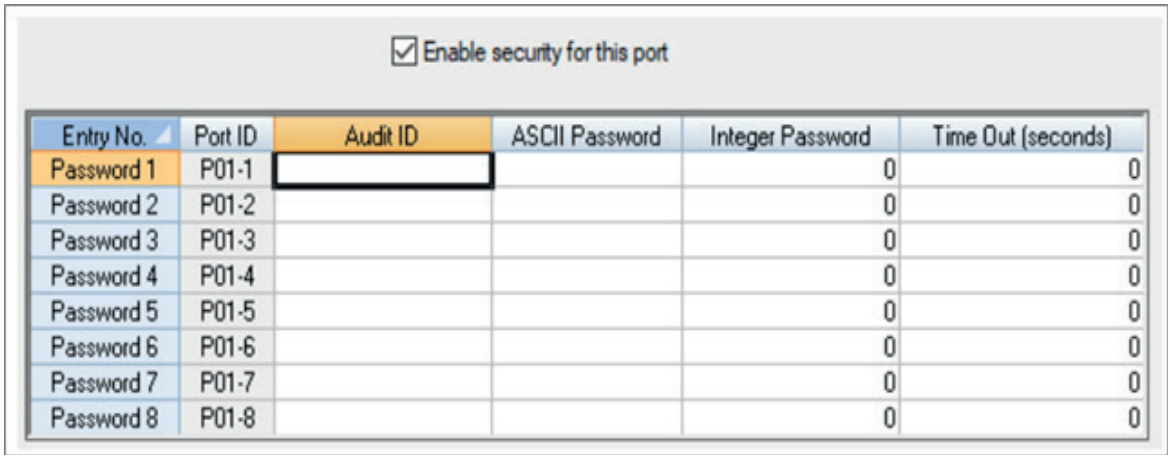
Para configuración de la seguridad, se utilizará como referencia el Port 1 – RS232/485 ya que el resto de los puertos se configura de la misma manera, salvo que cambia el ID del puerto (Port ID).



Para dar de alta la seguridad del puerto, se deberá seleccionar la casilla: *Enable security for this port.*

5.1.4 Alta de Usuario y credenciales

En la siguiente imagen, se podrá observar que se pueden dar de alta 8 usuarios diferentes para un mismo puerto:



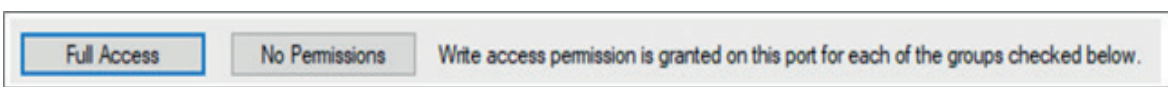
Entry No.	Port ID	Audit ID	ASCII Password	Integer Password	Time Out (seconds)
Password 1	P01-1			0	0
Password 2	P01-2			0	0
Password 3	P01-3			0	0
Password 4	P01-4			0	0
Password 5	P01-5			0	0
Password 6	P01-6			0	0
Password 7	P01-7			0	0
Password 8	P01-8			0	0

La información dentro de este cuadro corresponde a:

• Port ID: Identificación del puerto: P01 corresponde al puerto 1, -1 al -8 corresponde al usuario 1 al 8.
• Audit ID: Campo alfanumérico de 10 caracteres para darle un nombre al usuario, que servirá para identificarlo en los reportes de auditoría.
• ASCII Password: Password del usuario en código ASCII de 8 caracteres.
• Integer Password: Password del usuario en número entero de 9 dígitos.
• Time Out (seconds): es el tiempo que tiene el usuario para seguir con su sesión iniciada sin realizar ningún movimiento en el puerto. Pasado ese tiempo, el computador desconectará al usuario. Una vez definido los ID del puerto, su contraseña y su time out correspondiente, se necesitará configurarle los permisos correspondientes.

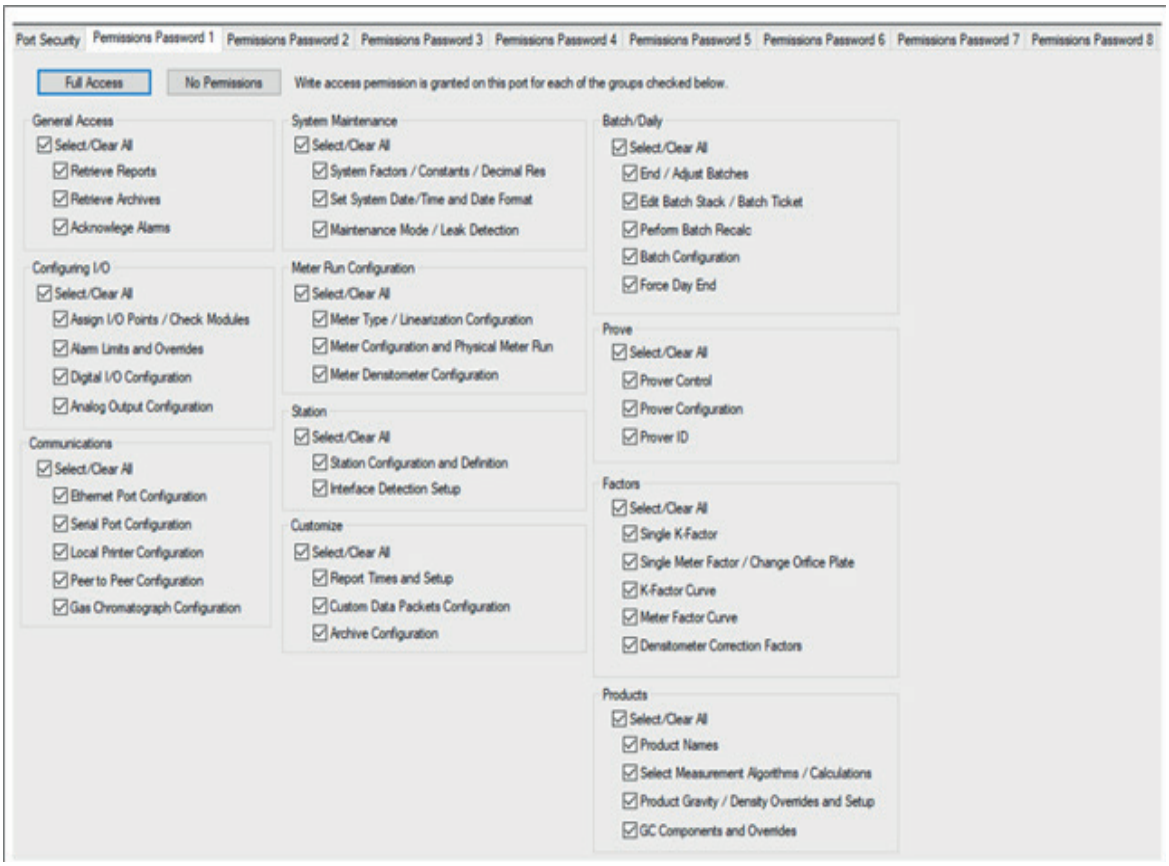
5.1.4 Permisos de Accesos

Para cara usuario se puede definir los permisos para interactuar con el computador. En el caso que el usuario deba tener acceso total al computador, se podrán seleccionar todas las opciones haciendo clic en el botón Full Access. Si en cambio el usuario puede tener solo determinados permisos, puede hacer click en No Permissions e ir seleccionando uno a uno aquellos permisos individuales que tiene ese puerto.



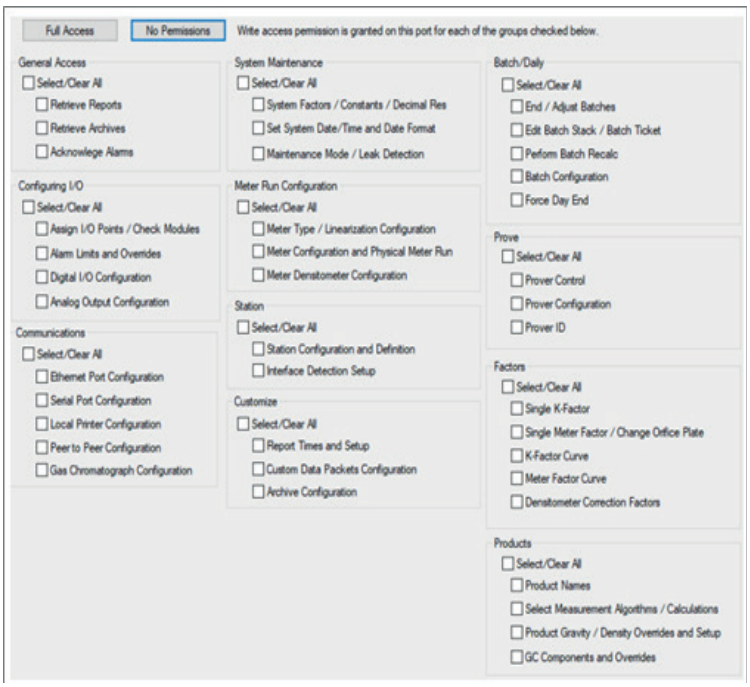
5.1.5 Acceso total (Full Access)

Como se puede observar, presionando el botón de Full Access, se activan todos los permisos habilitados para el usuario del correspondiente puerto:



5.1.6 No Permissions

Presionando el botón de No Permissions, se desactivan todos los permisos para poder ser activados uno a uno según el nivel de acceso del usuario de dicho puerto:



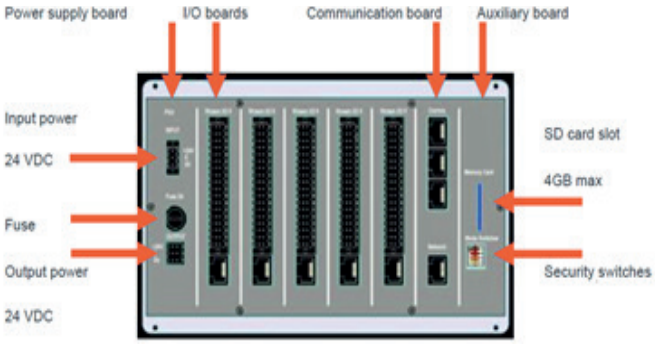
6 COMPUTADOR DE FLUJO SUMMIT 8800

6.1 Seguridad y protección de Datos nivel Hardware

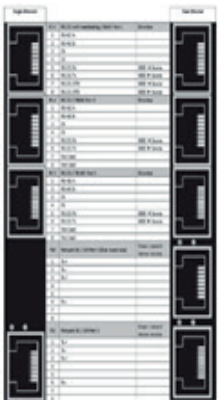
6.1.1 Puerto de programación en Panel Frontal

El puerto de programación ubicado en el panel frontal es un puerto USB tipo B versión estándar. Se utiliza para la descargar configuraciones, ingresar archivos o datos y subir resultados, tablas e informes de datos. Se lo debe utilizar siempre junto con el Software Summit 8800 para Windows.

6.1.2 Hardware



6.1.3 Módulos de Comunicación

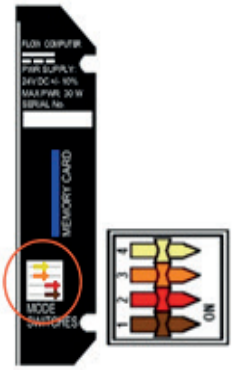


Tarjeta Single Ethernet:
- 3 Puertos serie RS232/RS485.
- 1 Puerto ETHERNET.

Tarjeta Dual Ethernet:
- 3 Puertos serie RS232/RS485.
- 2 Puertos ETHERNET.

6.1.4 Switches de modo de control del panel trasero

En el panel trasero hay 4 Switches de Modo o Función. Estos controles determinan el modo de operación básica del SUMMIT 8800.



PUENTE Nº	ON [CONECTADO]	OFF [DESCONECTADO]
1	Modalidad "Run Mode"	Modalidad "Boot Mode"
2	Sin Función	
3	Seguridad 2 Conectado	Seguridad 2 Desconectado
4	Seguridad 3 Conectado	Seguridad 3 Desconectado

	Switch			
Function	1	2	3	4
Open	On	Off	Off	Off
Partial Secured	On	Off	Off	On
Full Secured	On	Off	On	On
Run	On	Off	X	X
Boot	Off	Off	Off	Off

Para la operación Normal se debe ajustar la unidad en modo “Run Mode”. El modo “Boot Mode” sólo debe utilizarse para la descarga de Versiones Nuevas de Software en conjunción con el software operativo provisto para Windows.

• Si ambos Switches 3 y 4 se configuran en “Off” se abre “OPEN”, el modo de seguridad de la máquina.
• Si ambos Switches de Seguridad 3 y 4 se configuran en “On” el modo de seguridad de la máquina es total “FULL”.
• Si el modo de uno solo de los dos Switches, 3 o 4 en forma indistinta, se configura en “On” el modo de Seguridad de la máquina es parcial “PARTIAL”.

6.1.5 Configuración de Seguridad

Abierto	Se pueden realizar cambios, incluida la descarga de una nueva aplicación.
Parcial	La aplicación existente se puede cargar, cambiar y descargar de nuevo
Full	La conexión es posible y las aplicaciones se pueden cargar, pero no se pueden descargar

6.1.3.1 Full Acceso -Full Access

En Full Access se puede realizar las siguientes tareas
• Programar el computador de flujo.
• Calibrar entradas y salidas.
• Cambiar parámetros.

Sin Acceso
• No se puede programar el computador de caudal.
• No se puede calibrar entradas y salidas.
• No se pueden cambiar los parámetros.

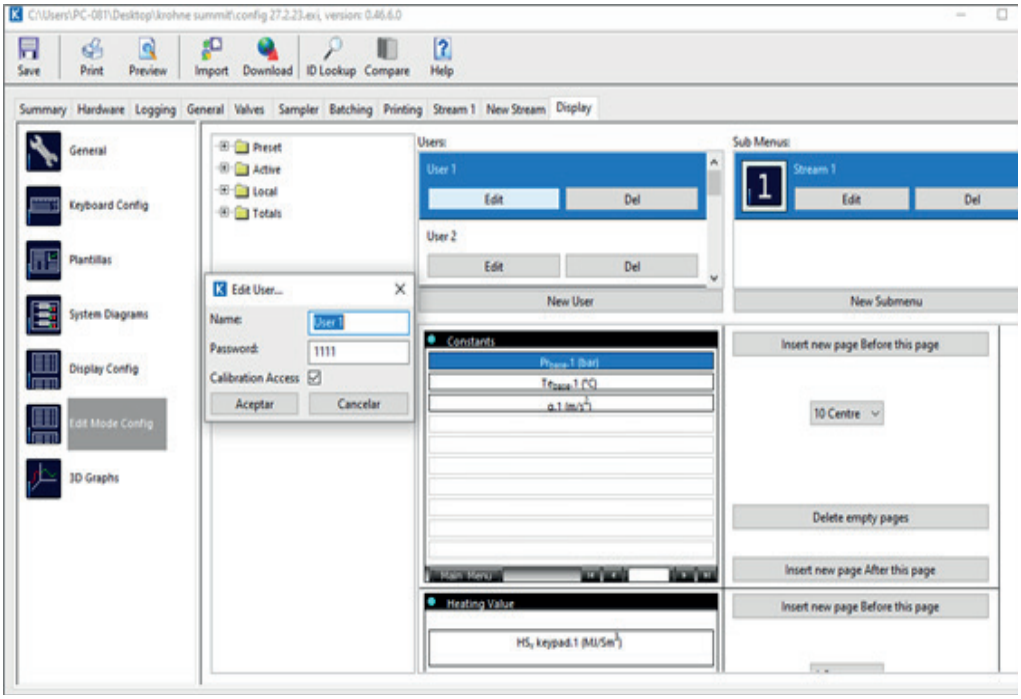
6.1.3.2 Modo Parcial - Partial Mode

• Acceso limitado
• Inicio sesión en el modo de edición. Sólo el Usuario 1 Disponible.
• Los elementos que no se pueden cambiar están deshabilitadas.
• La configuración se hará con el configurador.

6.2 Seguridad nivel software

Para la seguridad del computador se pueden configurar distintos usuarios con diferentes accesos cada uno de ellos.

Se accede desde display/edit mode config y se le puede configurar el nombre del usuario, una contraseña, acceso a la calibración, el menú del display así como también las constantes para los cálculos:

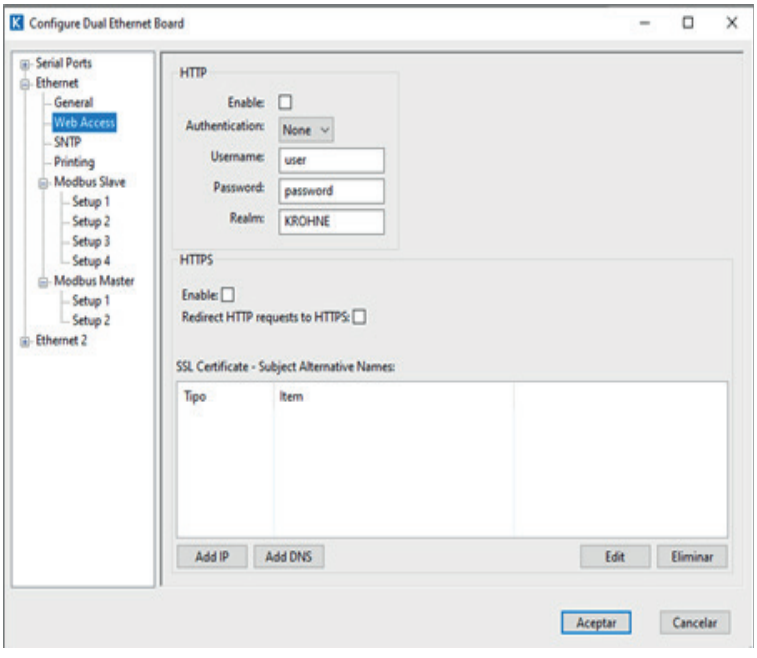


Por default los usuarios definidos son 3

User 1	Password 1111
User 2	Password 2222
User 3	Password 3333

6.2.1 Acceso web

Summit tiene un servidor web incorporado que proporciona acceso de solo lectura a todas las pantallas y permite la descarga de informes de ID de datos activos y de registros de alarma y auditoría.
Se puede acceder al sitio web ingresando su dirección IP en el navegador cuando el acceso web está activado. El acceso web se activa/desactiva desde hardware/configuración del puerto/ ethernet/web Access.



La IP por defecto es 192.168.0.100. Si se utiliza una Ethernet dual, incluso las pantallas se pueden ver (solo lectura) a través del sitio web.

6.3 Protocolos comunicación

DSfG protoco	Digitale Schnittstelle für Gasmessgeräte, un protocolo para la comunicación entre dispositivos y hosts en el mercado alemán
Modbus Slave	Se utiliza para permitir que los dispositivos remotos lean los datos de resultados de la Unidad, ya sea a través del puerto serie o del puerto Ethernet. Hay varias versiones disponibles, incluidas Modbus RTU y ASCII y Modbus sobre TCP/IP. Este Modbus
CTE Protoco	Comunicazione a trame estese, un protocolo para la comunicación de acogida en el mercado italiano
SOAP protoco	Protocolo simple de acceso a objetos, un protocolo estándar basado en XML para la comunicación de host a través de Ethernet utilizando el protocolo HTTP.
HTTP web access	El Protocolo de transferencia de hipertexto es el protocolo entre Summit y un navegador web. Esto permite el acceso a la web
HTML/ HTML5 language	El lenguaje de marcado de hipertexto es utilizado por Summit en su sitio web. HLML5 se utiliza en el sitio web para presentar dinámicamente las pantallas Summit.
SNTP protocol	El protocolo de tiempo de red simple se utiliza para sincronizar la hora con los servidores de tiempo
FTP protocol	Protocolo de transferencia de archivos para enviar informes a impresoras o servidores de archivos
SMTP protocol	Protocolo de transferencia de correo simple, para enviar informes por correo electrónico

6.3.1 Los protocolos básicos utilizado por el computador son tres capas de hardware

RS232	Utilizado para distancias cortas, conexiones punto a punto
RS485	Utilizado para largas distancias, ya sea punto a punto o conexiones multipunto
Ethernet	Ethernet es la forma preferida de comunicarse a través de una red de área local (LAN)

6.3.2 Códigos de colores de los registros

En la lista de registros cada uno de ellos tiene asignado un color, amarillo o rojo. Estos representan

🔴	Punto Rojo	Los datos son de lectura/escritura y se pueden cambiar a través de Modbus.
🟡	Punto Amarillo	Los datos son de solo lectura y no se pueden cambiar a través de Modbus

Los registros de lectura/escritura puede ser posible cambiarlos a través de la pantalla. El 90% de los datos serán de solo lectura, pero elementos como composiciones de gas, hora/fecha, Meter Factor se escriben comúnmente sobre Modbus.

NOTA: Aunque la ID puede ser de lectura/escritura, la configuración de seguridad determina si la ID realmente puede ser escrito.

6.3.3 Tipo de registros

- Preset data: Los datos típicos serían valores del teclado, límites operativos, selección de ecuaciones, datos de calibración para turbinas y densitómetros y placas de orificios.

Estos datos estarían presentes en un informe de configuración y le permiten ver para qué está configurado el computador de caudal.

Se utiliza para la validación y formará la suma de verificación de datos (visible en la página de información del sistema).

Por ejemplo, si una suma de verificación de datos cambia, la configuración del computador ha cambiado y calcula resultados diferentes a lo esperado.

Por lo general, se configura y se deja solo, solo se actualiza después de la validación, por ejemplo, cada 6 meses / 1 año.

- Active data: Estos valores cubren las entradas al computador de flujo. Por ejemplo, desde el cromatógrafo, transmisores de presión y temperatura, medidores, etc.

También Valores calculados en el computador de flujo. P.ej. Caudales, Z, Promedios, Densidad, etc.

- Local data: Datos que un operador puede cambiar localmente para realizar tareas de mantenimiento. Por ejemplo, apagar transmisores individualmente sin generar alarmas. Configurar el modo de mantenimiento o modo de prover.

- Totals: totales para los streams y estación. El contenido de estos archivos es almacenado en una memoria RAM no volátil y se protegen con la batería.

- Custom: Variables definidas por el usuario. Permite que los cálculos, realizados en un script LUA (lenguaje de programación usado por el computador), se utilicen en una configuración.

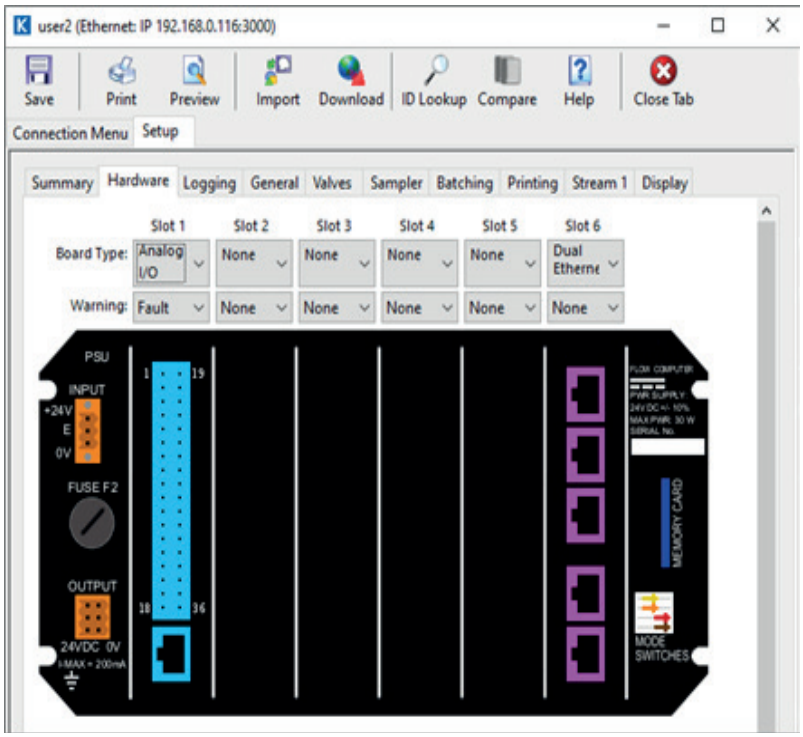
6.3.4 Índice de los registros (ID index)

Estos son los números que aparecen al final del ID de los registros. El índice 1 corresponde al registro más reciente, mientras que el 2 es un registro más viejo. Por ejemplo Pr.used.1 y Pr.used.2

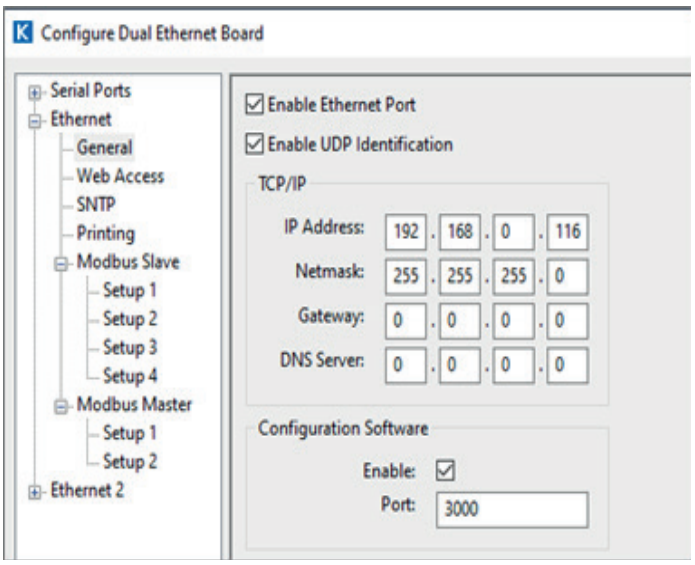
Para cambiar el índice se hace doble click sobre el registro de la lista.

6.4 Modbus slave

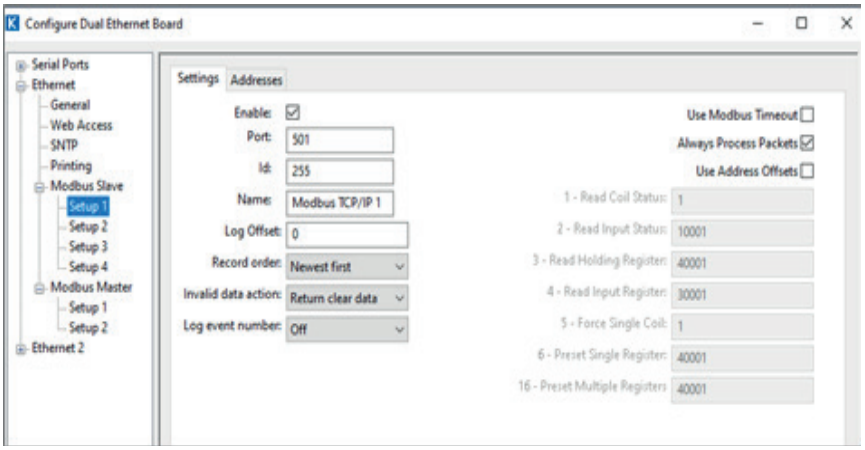
Se configura al computador como un esclavo modbus para luego encuestar los registros con el software modbus pool. Primero se configura el puerto con protocolo TCP/IP y se cargan los registros



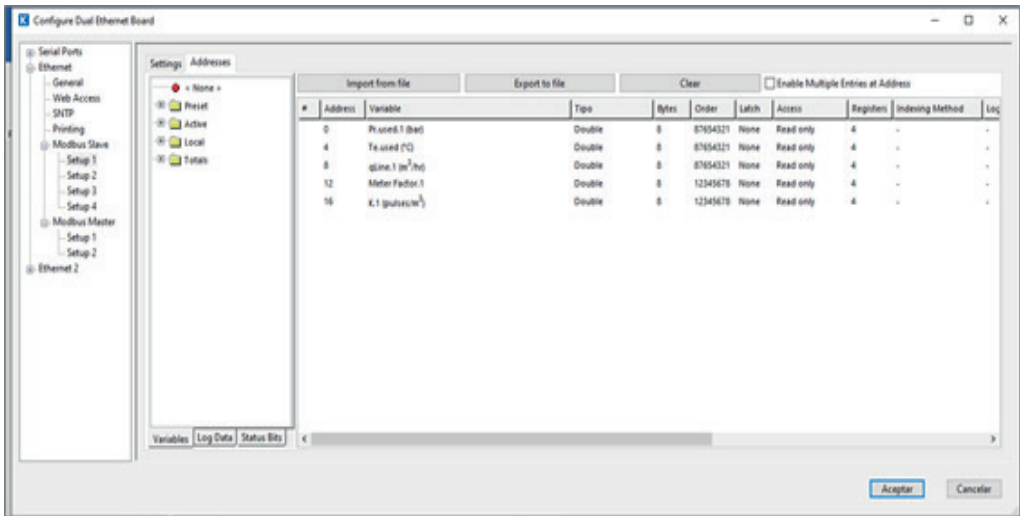
Entramos a la configuración general del puerto en ethernet/general. Allí habilitamos el puerto y le damos una IP:



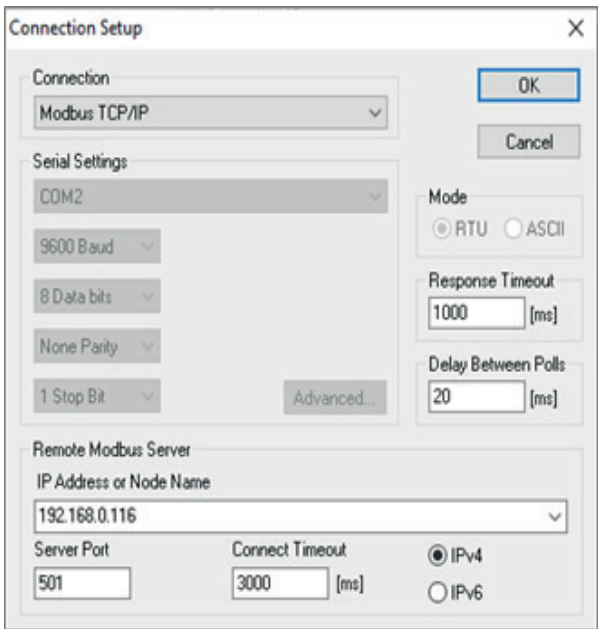
En modbus slave/setup 1 habilitamos el modbus esclavo y anotamos los valores de port e ID. nos servirán para establecer la comunicación con el maestro (modbus pool).



Se cargan los registros que queremos encuestar en la pestaña addresses. En este caso seleccionamos la presión y temperatura de línea, el caudal y meter factor:

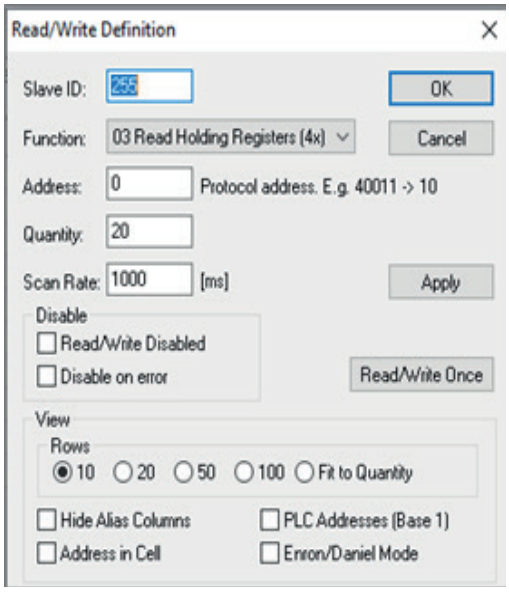


En el maestro modbus pool configuramos la conexión como modbus TCP/IP, con la IP y el server port tal cual configuramos el puerto:



Addresses empiezan en 0. Esto depende de como se enumera los registros en la lista de registros.

quantity, depende de la cantidad de registros que queremos traer. Es registers del mapa modbus multiplicado por la cantidad de registros, en este caso 4 x 5 = 20.



7 COMPUTADOR DE FLUJO ROC

A continuación, se detallan los niveles de seguridad que ofrece el computador de flujo a nivel hardware y software. Se trata de la seguridad que ofrece el equipo a nivel usuario ya sea a través del computador o a través del software

7.1 Seguridad y protección de datos nivel Hardware.

7.1.1 Usuario

El computador de flujo ROC, si bien puede conectarse un display con teclado opcional externo, requiere de un software ROCLINK800 para su configuración.

Es posible controlar la seguridad del computador de dos maneras:

-Seguridad ROCLINK 800: – Habilita quién puede acceder (iniciar sesión) con el software ROCLINK 800 y el nivel de acceso asignado a un usuario.

-Seguridad del dispositivo: permite quién tiene acceso a los puertos de comunicación ROC y la pantalla LCD.

-Seguridad ROCLINK800

si es la primera vez que accede, escriba el “User ID:” LOI. El password por omisión es 1000. Cuando incorpore un password y escribe por ejemplo 0009, la ROC lo tomara como 9. El password siempre son 4 dígitos numéricos desde 0000 hasta 9999.

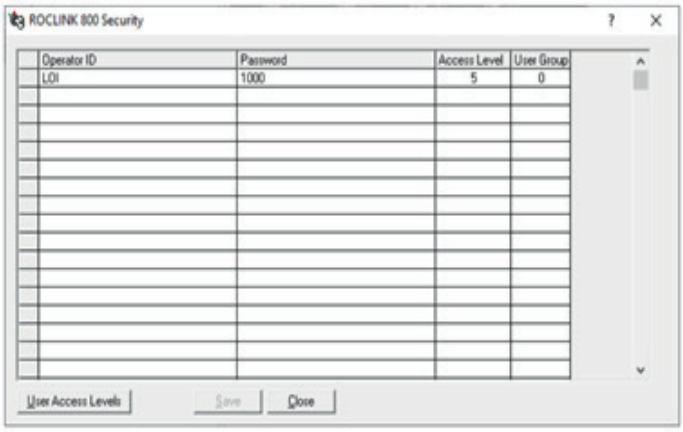
Se puede tener más de un usuario con el mismo password.

A través de este software, se pueden configurar hasta 64 usuarios de tres caracteres cada uno y cuatro dígitos numéricos en el modo normal (desde 0000 hasta 9999).

Si activa la opción de Seguridad Mejorada deberá escribir los usuarios con entre 3 y 30 caracteres alfanuméricos y sus contraseñas entre 8 y 32 caracteres alfanuméricos. (ROC > Seguridad)

Para ello, siga los siguientes pasos:

1 Seleccione Utilidades > Seguridad ROCLINK 800.
2. Ingrese una ID de operador.
Ingrese tres caracteres alfanuméricos para la identificación del operador.
Por lo general, estas son las iniciales de la persona que opera el dispositivo.



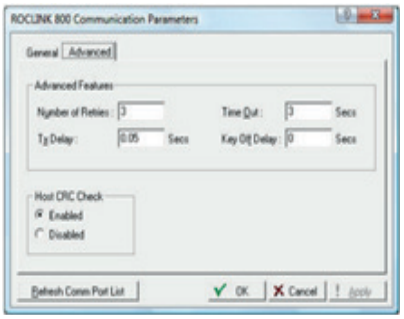
3. Entre el password.

4. Entre el nivel de acceso deseado.

Introduzca el nivel de acceso deseado para el usuario. 0 es el nivel más bajo (menos inclusivo) que permite el acceso al menor número de pantallas.

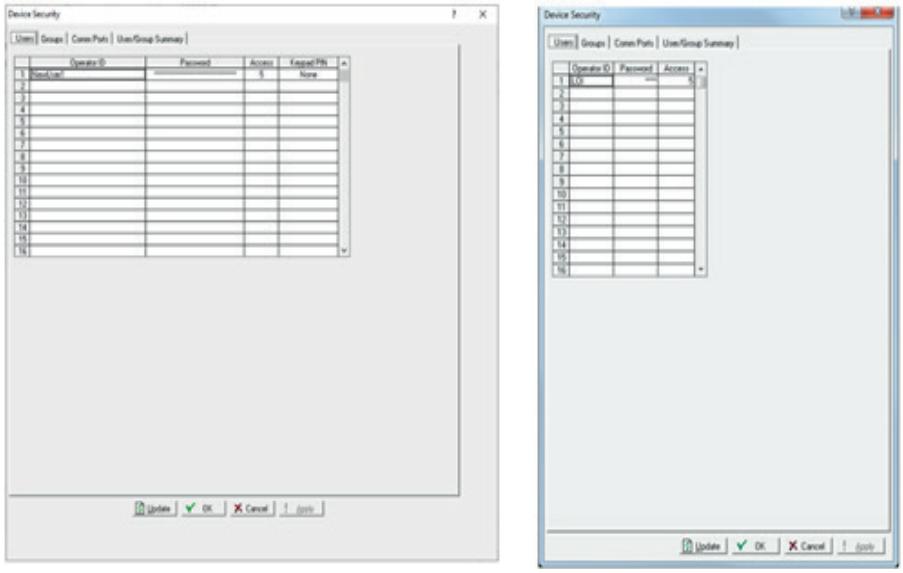
SI NO SE AGREGA EL USUARIO EN ROC > Security EL MISMO NO PODRÁ ACCEDER AL DISPOSITIVO. Esto sucede debido a que la ventana Utilities > ROCLINK 800 Security da acceso únicamente al software, y la ventana ROC > Security da el acceso al dispositivo.

5 es el nivel de acceso más alto (más inclusivo) y permite acceso a todas las pantallas. Cada nivel de acceso permite el acceso a pantallas en ese nivel y cualquiera heredado de niveles de acceso inferiores. Por ejemplo, un ID de operador con nivel de acceso 3 puede acceder a pantallas con niveles 0,1, 2 y 3.



7.1.2 Seguridad del dispositivo

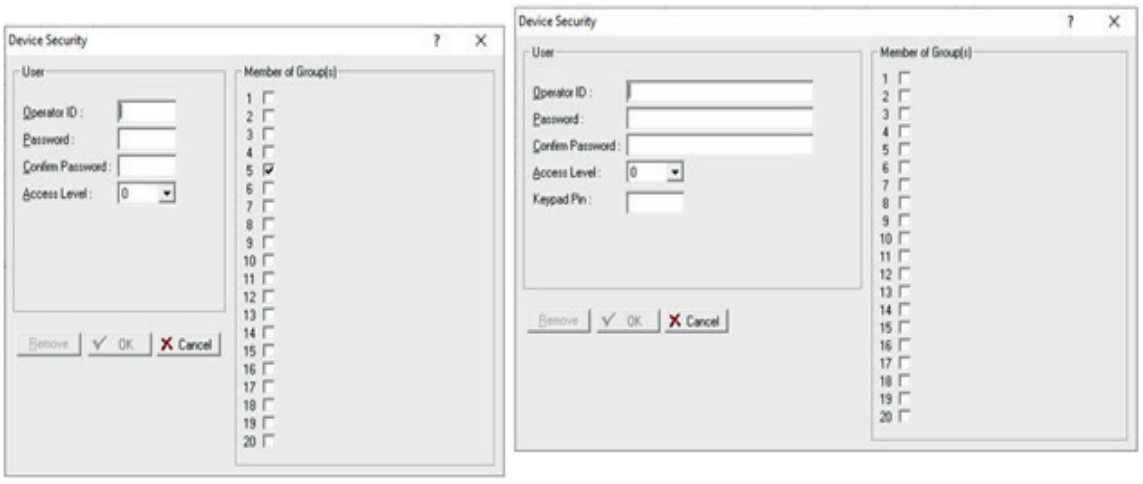
Use la pantalla de Seguridad del dispositivo para controlar quién tiene acceso a Puertos Comm en un dispositivo específico. Cuando habilita esta función, debe iniciar sesión en ROCLINK 800 para usar el puerto de comunicaciones. Puede habilitar esta función en cada puerto de comunicaciones por separado. Para acceder a la pantalla Seguridad del dispositivo, seleccione ROC > Security. Le aparecerá la pantalla Seguridad del dispositivo.



SI NO SE AGREGA EL USUARIO EN ROC > Security EL MISMO NO PODRÁ ACCEDER AL DISPOSITIVO. Esto sucede debido a que la ventana Utilities > ROCLINK 800 Security da acceso únicamente al software, y la ventana ROC > Security da el acceso al dispositivo.

7.1.3 Agregado y eliminación de usuarios

Esta sección detalla cómo agregar y eliminar usuarios en Device Security. Agregar un usuario ID de operador:
1. Seleccione ROC > Seguridad.
2. Haga clic en una celda vacía de la tabla. Se visualizará el cuadro de diálogo Seguridad del dispositivo.



3. Complete el cuadro.
4. Seleccione OK, donde aparecerá un cartel mostrando el usuario agregado
Para eliminar un usuario simplemente seleccione el ID del mismo y haga clic en Remove. Luego en Yes. Aparecerá un cartel indicando el usuario eliminado.

7.1.4 Tabla de Grupos

En caso que tenga un teclado con display instalado, puede establecer hasta 20 únicos grupos de usuarios.Para crear un grupo:
1. Seleccione ROC > Security.
2. Seleccione la pestaña Grups. Aparecerá la pantalla Grupos.
3. Ingrese el nombre del grupo en cuestión (como operadores, técnicos o supervisores).
4. Haga clic en Apply para guardar los cambios

7.1.5 Tabla de Grupos

Cuando ingrese a la pestaña Comm Ports, aparecerá:

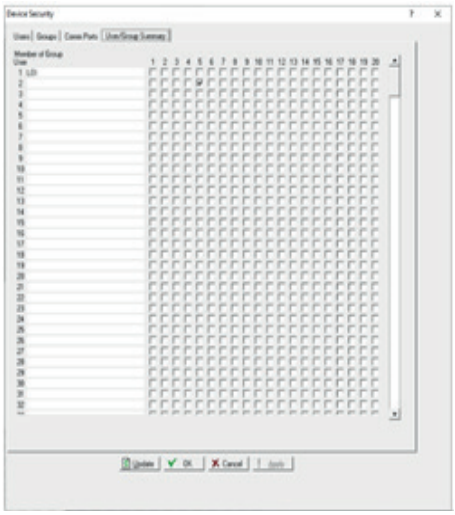
Seleccione las siguientes opciones de seguridad, para cada puerto COM:
-Disabled: Todas las solicitudes de inicio de sesión, son aceptadas.

-User ID Enabled: Las solicitudes de inicio de sesión se aceptan si la identificación del operador y la contraseña son válidos. Al iniciar sesión con éxito, el acceso completo es permitido.

-User Acces User Enabled: Las solicitudes de inicio de sesión se aceptan si el ID y la contraseña del operador son válidos. Al iniciar sesión correctamente, el usuario está restringido por el nivel de acceso.

7.1.8 Ficha Resumen de usuario/grupo

La pestaña Device Security > User/Grup Summary muestra una tabla que resume las asociaciones definidas entre usuarios y grupos. Refleja los usuarios que definió en la pestaña Usuarios y los grupos definida en la pestaña Grupos.
También puede usar esta tabla para modificar esas asociaciones. Haga clic en un cuadro para agregar (o eliminar) una ID de usuario de un grupo. Haga clic en Apply para guardar cualquier cambios.



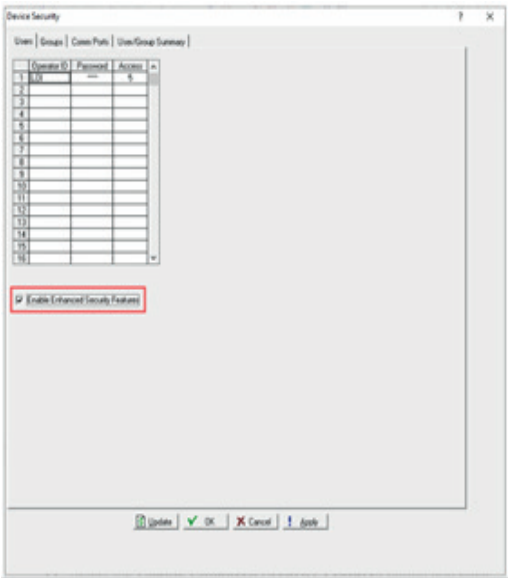
7.1.9 Seguridad Mejorada

Para poder trabajar en este apartado usted debe ejecutar ROCLINK 800 como administrador en Windows.

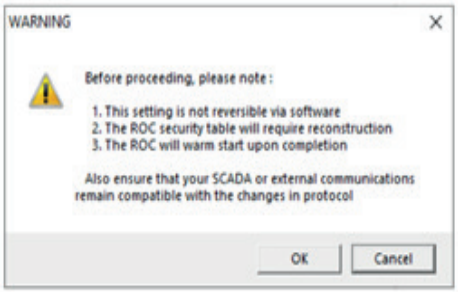
Debe iniciar sesión en ROCLINK 800 con un nivel de administrador IDENTIFICACIÓN.

Una vez que opte por el formato complejo de nombres de usuario/contraseñas, no puedrá volver al formato de seguridad anterior.

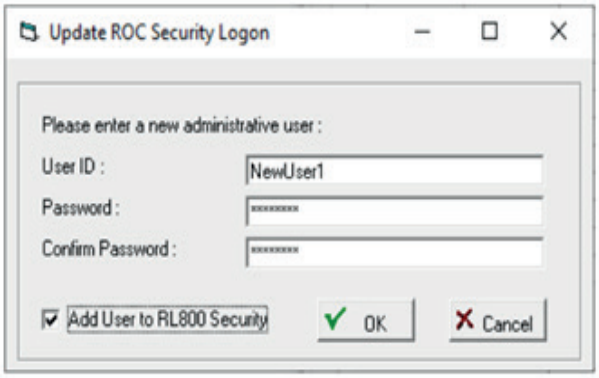
1.Seleccione Utilities > ROCLINK 800 Security
Se muestra la siguiente pantalla:



Seleccione la opción “Enable Enhanced Security Features” (Habilitar funciones de seguridad mejoradas) y haga clic en Aplicar. Aparecerá un cuadro de diálogo de advertencia:

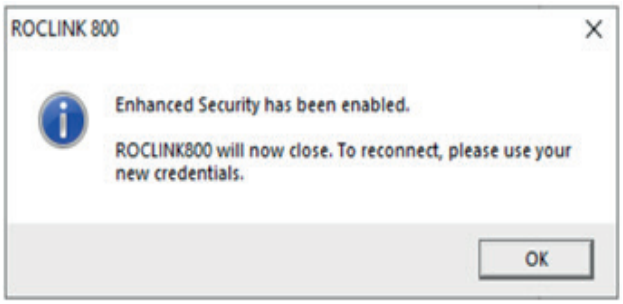


Haga clic en OK para optar por la nueva mejora de seguridad. Aparecerá el cuadro de diálogo Actualización de Inicio de sesión de seguridad de ROC:



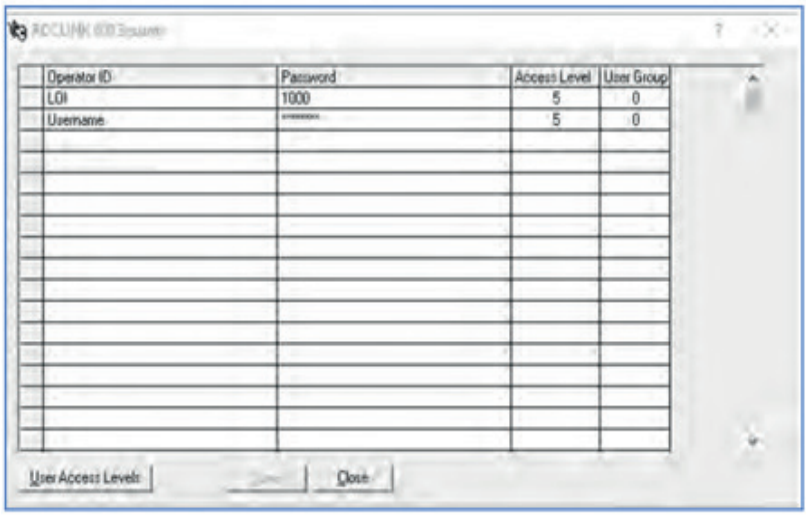
Defina una nueva identificación de usuario y contraseña para el administrador. Seleccione Agregar usuario a la seguridad de RL800, opción para agregar automáticamente este ID de usuario administrativo a la tabla de seguridad.

Haga clic en OK cuando el ROCLINK acepte el nuevo usuario y contraseña, y aparecerá el siguiente mensaje:



Después de obtener el nuevo ID:
1. Inicie sesión en ROCLINK con el nuevo ID de operador administrador y contraseña.

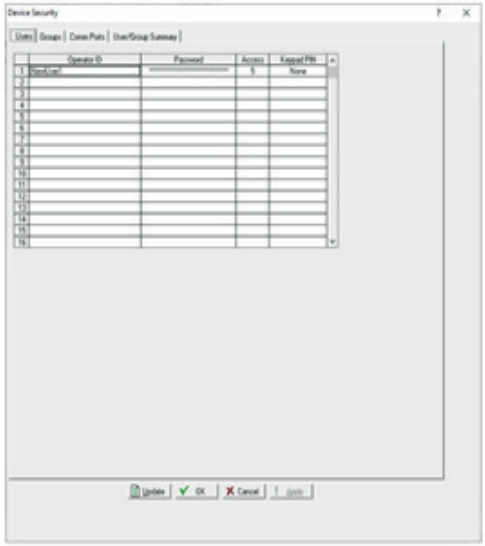
Acceda a la pantalla de seguridad de ROCLINK 800 (Utilities > ROCLINK 800 Security).



Una vez que implemente la nueva seguridad mejorada, deberá modificar la tabla de seguridad del dispositivo para cada dispositivo.

Una vez que configure un dispositivo para usar el ID más largo (ID/contraseñas), no podrá iniciar sesión en ese dispositivo usando usuarios antiguos.

Inicie sesión en un dispositivo y acceda a su tabla de seguridad (ROC > Security):



Defina nuevos ID de operadores (de al menos 3 y no más de 30 caracteres alfanuméricos/especiales) y contraseñas (de al menos 8 y no más de 32 caracteres alfanuméricos/especiales).

7.1.10 Puertos de comunicación

Para cumplir con la directiva de seguridad, debe habilitar la seguridad por ID de usuario o nivel de acceso de usuario, para cada puerto de comunicación.

7.1.11 Puerto Ethernet

Para el caso del puerto ethernet, no existe seguridad en este computador. Segun el fabricante se puede asegurar ese puerto adquiriendo aparte, un firewall / gateway.

8 COMPUTADOR DE FLUJO OMNI 6000/3000

A continuación, se detallan los niveles de seguridad que ofrece el computador de flujo a nivel hardware y software. Se trata de la seguridad que ofrece el equipo a nivel usuario ya sea a través del computador o a través del software

8.1 Seguridad y protección de datos nivel Hardware

8.1.1 Switch de bloqueo

El modulo principal (el que contiene el display) tiene un switch mecánico que asegura que no será posible modificar el software metrológico a través de la interfaz de usuario (pantalla y teclado). Si el switch está en “Lock” (hacia abajo):

- No será posible cambiar configuraciones y parámetros desde el panel frontal.
- Solo será posible la configuración y activación de comandos operativos.
- Se podrán leer datos desde el display del computador y a través de la comunicación.
- Se podrá alterar las configuraciones desde los puertos serie siempre y cuando la configuración “Lockout SW Active?” este en “N” (desactivada) para el puerto del cual se quiera acceder. (ver 4.3.1)
- Se mostrará la siguiente alarma en pantalla al intentar cambiar un parámetro fuera de las acciones de operación desde el teclado.

8.1.2 Sello metrológico

El computador de flujo tiene un gabinete que, al cerrarse, impide el acceso al switch de bloqueo. Para poder acceder al switch, se debe levantar suavemente el display y tirar de este, deslizándose por dentro del gabinete.

Para evitar que se pueda modificar el estado del switch el gabinete tiene dos orificios ubicados en la parte superior trasera del mismo por los cuales se puede pasar un precinto y evitar el acceso tanto al rack como al switch sin antes romper el precinto. De esta forma las autoridades que comprueben el estado del equipo podrán asegurarse de que no a sido modificado. Para el caso de los computadores con montaje de display y rack separado, se deberá precintar la puerta del tablero de modo de no tener acceso al switch posterior del display.

8.2 Protección de datos nivel software

Para esta práctica recomendada se usó el software "Omnicom" versión 1.6. Se recomienda mantener siempre actualizado el software con la última versión para evitar problemas de compatibilidad con otros archivos de configuración. La licencia del mismo se debe adquirir a través del fabricante.

8.2.1 Usuario, contraseñas y niveles de seguridad

El computador de flujo puede restringir y/o permitir el acceso a diferentes parámetros de configuración, según el usuario que lo esté operando.
El único usuario que viene por omisión es el privilegiado, el cual concede acceso a todos los parámetros y configuraciones. Cuya contraseña de fabrica es OMNI.

Los demás usuarios se deben configurar, Permitiendo accesos limitados. Tales se describen a continuación:

Level 1: Da permisos para un acceso de nivel técnico, dando acceso a la mayoría de parámetros dentro del computador a excepción de las entradas y salidas asignadas automáticamente para el sensor presión diferencial, el de temperatura y el de presión. Tampoco podrá modificar variables programables o booleanas declarables. Este nivel SI podrá cambiar la contraseña de Level 1 (así misma).

Level 1A: Da acceso para cambiar los "Meter Factor" y los "K Factor". Así como los factores de corrección de los densímetros.

Level 2: Permite acceder a los parámetros para operador. Entre los cuales se incluye la configuración manual del override de los transductores, y de la gravedad del producto. Así como las operaciones para el prover y batching.

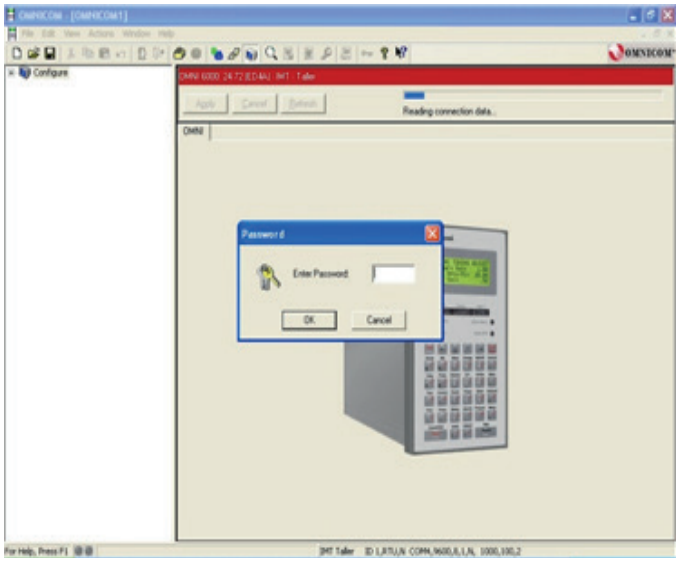
Se recomienda cambiar la contraseña del usuario privilegiado si se tiene la de fábrica, y asignar las contraseñas necesarias de manera que tengan solo los permisos necesarios quienes operen con el computador. De esta manera, cuidando la integridad de las configuraciones del computador.

8.2.2 Configuración de usuarios

Para configurar los usuarios presionar Prog, Setup, Enter. Desde este menú principal acceda a "Misc Configuration" apretando Enter y luego a "Password Maintenance" apretando Enter nuevamente y tendrá como primera opción la contraseña del usuario privilegiado seguida por las otras 3 contraseñas opcionales.

8.3.1 Contraseñas y bloqueos para puertos Serie

Desde el mismo menú que las demás contraseñas (4.2.2), se puede asignar una clave a los puertos serie de manera individual. Si uno intenta conectarse a través de un puerto con contraseña esta se pedirá para poder conectarse con el computador.



También es posible inhabilitar la descarga de configuraciones al computador por medio de los puertos serie de forma individual con el parámetro “Lockout SW Active?” del menú de las contraseñas (4.2.2). Esta configuración permite que el switch de bloqueo físico, deshabilite la escritura del puerto de comunicaciones correspondiente (es individual para cada puerto).

Asimismo, se puede deshabilitar todas las descargas de configuración al computador por medio de la opción “Disable download” que se encuentra en el mismo menú. (ver Cuadro 1)

Esta opción solo aparecerá si El LED “Program” está en color rojo, para esto se debe ingresar la contraseña privilegiada en el mismo menú o bien otro parámetro.

Para un mejor entendimiento se muestra el siguiente cuadro:

"*Disable Download*"	Switch de Bloqueo Físico	Parámetro "*Lockout SW Active?*"	El puerto Puede escribir?
Y	N/A	N/A	NO
N	**Lock**	Y	NO
N	**Lock**	N	SÍ
N	**Enabled**	N/A	SÍ

N/A: No afecta

8.3.2 Contraseñas y bloqueos para puertos Serie

Los puertos ethernet disponen de un sistema de filtros para evitar que computadoras no autorizadas puedan acceder al equipo. Estas configuraciones se realizan por el software omnicom y solo serán configurables si la placa ethernet correspondiente está instalada y es reconocida por el equipo.

Para acceder a estas configuraciones debe dirigirse a la carpeta Ports en el arbol de la izquierda y seleccionar el puerto que quiera configurar, luego hacer clic en Security

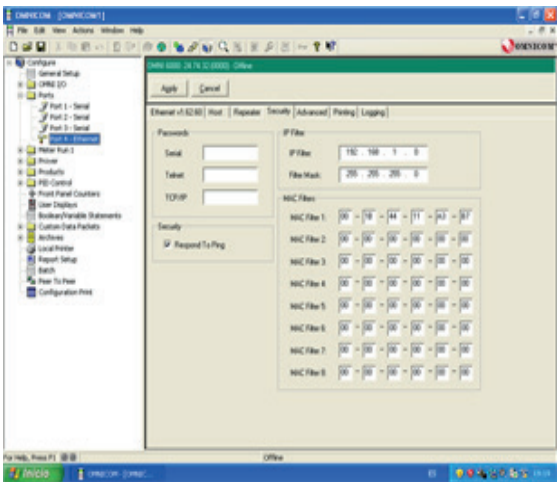
Cada puerto ethernet puede tener un filtro de dirección IP, de mascara, y de dirección MAC.

El filtro de dirección IP puede limitar el acceso a una única dirección ó a un rango de direcciones IP, estando desactivado cuando la dirección sea 0.0.0.0.

Para dar acceso a una sola IP se debe colocar la misma en el campo de IP y escribir 255.255.255.255 en el campo del filtro de la máscara, indicando que todos los números de la IP del dispositivo que se conecte deben ser iguales a los del filtro de IP.

Si se quiere colocar un rango de direcciones IP, debe ingresar una de las IP que se encuentre dentro del rango en el filtro IP y en el filtro de máscara debe escribir que números se verificarán.
El filtro de direcciones MAC permite habilitar la conexión a tan solo un selecto grupo de dispositivos. Ingrese la dirección MAC de los mismos en los filtros para habilitarlos o deje los campos en 00-00-00-00-00-00 para deshabilitarlos.

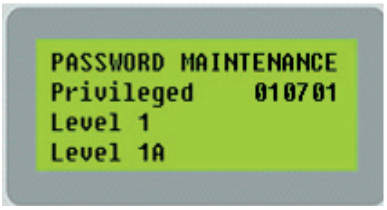
Ejemplo de rango de direcciones IP con filtro de MAC para un único dispositivo:

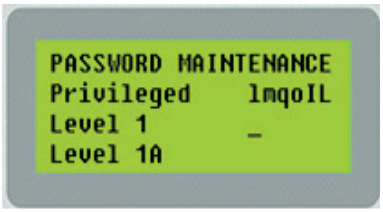


También es posible configurar una contraseña tanto para el puerto RS-232/RS-485 y la conexión por Telnet, como para el puerto Ethernet desde el mismo menú. Si se quiere desactivar la conexión por Telnet se debe cambiar el puerto a 0 en la pestaña de Ethernet (la primera).

8.4 Recuperar contraseña de usuario privilegiado

En el caso de que pierda la contraseña del usuario privilegiado deberá dirigirse al menú “Password Maint” (4.2.2). Allí deberá ingresar “010701” En “Privileged”, cuando presione Enter el número será reemplazado por un código. Estas deben ser entregadas a OMNI donde se le dará una contraseña válida.





9 COMPUTADOR DE FLUJO FMC²

A continuación, se detallan los niveles de seguridad que ofrece el computador de flujo a nivel hardware y software. Se trata de la seguridad que ofrece el equipo a nivel usuario ya sea a través del computador o a través del software.

9.2 Seguridad y protección de datos nivel Software.

9.2.1 Usuarios

El computador tiene un sistema de usuarios por niveles. Estos van desde el nivel 2 hasta el 9 los siguientes usuarios por defecto son:

Administrator (2): Con un nivel de acceso de 2, su función es administrar los distintos usuarios y menús, de forma que asigna la contraseña y el nivel a cada uno. Además, es capaz de crear y configurar menús, así como modificar los niveles necesarios para acceder a estos. No puede usarse para operar.

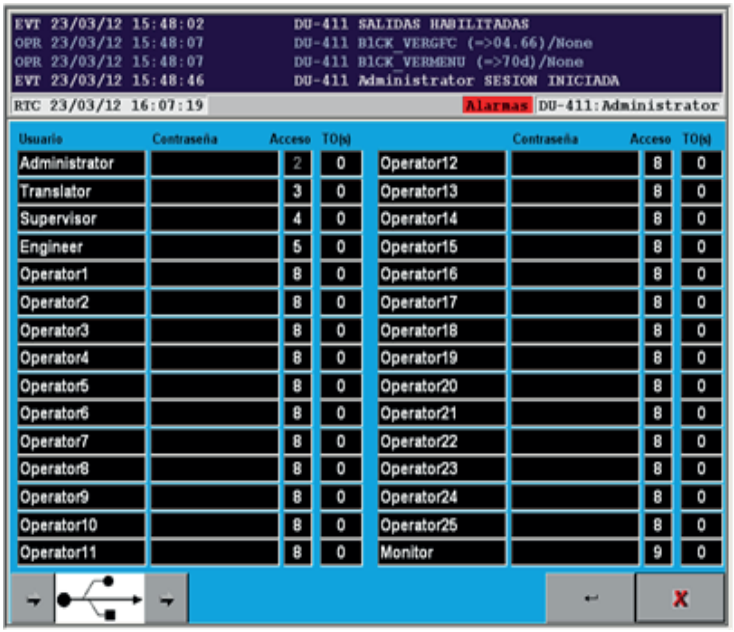
Translator (3): Con un nivel de acceso de 3 es capaz de modificar el idioma que en el que se presta la información de los menús. No puede usarse para operar.

Supervisor (4): Con un nivel de acceso de 4, es el nivel más alto de operación. Teniendo acceso por completo a todas las funciones relacionadas como backups y configuraciones.

Engineer (5): Con un nivel de acceso de 5, tiene acceso a todas las funciones de operación.Operator (8): Con niveles de acceso de 8, solo tiene acceso a funciones de operación como proving y batching.

Monitor (9): Con un nivel de acceso de 9 y solo es capaz de desplazarse por los menús sin la capacidad de alterar nada.

Estos usuarios son configurables desde el menú “User” estando logueado como administrador. Una vez en este se podrán ver todos los usuarios, sus contraseñas y sus niveles de acceso, pudiendo ser todo configurado aquí mismo. Tanto para el nombre de los usuarios como para sus contraseñas se pueden utilizar símbolos. Para los nombres del usuario se recomienda utilizar hasta 10 caracteres,

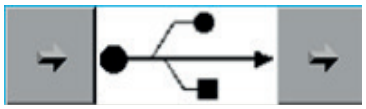


mientras que para las contraseñas simplemente se tiene un máximo de 79 caracteres. Tener en cuenta que si se deja la contraseña en blanco el usuario podrá ser ingresado solo con el nombre, por lo tanto se debe tener en cuenta que si no se va a utilizar un usuario se le debe asignar una contraseña de igual manera, o dejarle un nivel de acceso de 9 para que sea incapaz de alterar parámetros u operar.

Para cambiar el nivel de cada parámetro se debe ingresar con un nivel de acceso de 2 (administrador). Cuando navegue por los menús aparecerán al costado derecho el nivel de acceso que se necesita para realizar cambios en el parámetro o realizar una acción, si se selecciona el nivel de uno de estos, dará la opción de cambiarlo

9.2.3 Guardar configuración de usuarios

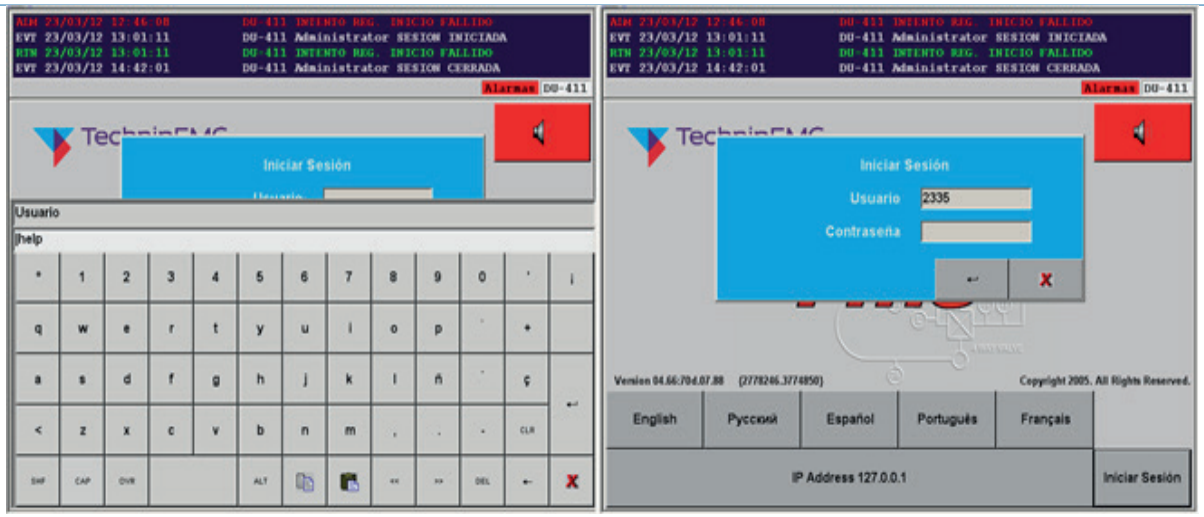
Para esto se necesitará conectar una memoria USB en el equipo (por la parte posterior del mismo). Una vez logueado como administrador, debe entrar en el menú de usuarios. En la esquina inferior izquierda aparecerá:



Con la flecha que apunta al símbolo USB se copiará la configuración de los usuarios a la memoria USB. Mientras que con la flecha que apunta desde el USB a la derecha copiará la configuración del USB al equipo. Esta acción NO se podrá realizar sin estar logueado con un usuario de nivel 2 (Administrador).

9.2.3 Recuperar contraseña de administrador

En el caso de que pierda la contraseña del administrador, se debe loguear con el nombre “help”. De esta manera el usuario se cambiará por un número.



Este número deberá ser entregado a FMC, quienes otorgarán una contraseña para el usuario numérico, esto hará que se loguee como administrador donde podrá cambiar la contraseña del mismo nuevamente.

11 COMPUTADOR DE FLUJO CONTROLWARE

A continuación, se detallan los niveles de seguridad que ofrece el computador de flujo a nivel hardware y software. Se trata de la seguridad que ofrece el equipo a nivel usuario ya sea a través del computador o a través del software.

11.1 Seguridad y protección de datos nivel Hardware

En la figura 1 se ve un croquis frontal de la RTU ControlWave indicando el modulo instalado en cada uno de los slots disponibles del chasis. En el slot 1 podemos apreciar que el equipo debe llevar el módulo PSSM (Power Supply/Sequencer Module) que cuenta con el switch RUN/REMOTE/LOCAL.

Ese interruptor (RUN/REMOTE/LOCAL) del módulo PSSM cuenta con una llave extraíble que permite al usuario configurar la unidad de la siguiente manera: Cuando se establece en 'RUN', este interruptor evita que el usuario realice cualquier operación de depuración/programación del ControlWave, como Iniciar/Detener, descarga de aplicación, etc.

El uso de la configuración 'LOCAL' o 'REMOTO' depende del tipo de conexión de red para la que se haya configurado el puerto de comunicación en cuestión (la selección del puerto puede ser IP, serie u OpenBSI).

Si un puerto de comunicación se ha configurado para comunicaciones IP o OpenBSI (BSAP), se considera un puerto remoto y el interruptor EJECUTAR/REMOTO/LOCAL debe establecerse en "REMOTO" para recibir una descarga de aplicación. Sin embargo, si el puerto de comunicación

en cuestión se ha configurado para comunicaciones en serie, se considera un puerto local y el interruptor EJECUTAR/REMOTO/LOCAL debe establecerse en 'LOCAL' para recibir una descarga. Nota: Cuando el interruptor RUN/REMOTE/LOCAL se ha establecido en la posición 'LOCAL', las comunicaciones a través de cualquier puerto de comunicación ControlWave son posibles, es decir, a través de un puerto de comunicación local o remoto. Sin embargo, cuando el interruptor RUN/REMOTE/LOCAL se ha establecido en la posición 'REMOTE', solo es posible la comunicación con un puerto de comunicación que se haya configurado como puerto de comunicación remoto. La llave extraíble utilizada para configurar el interruptor RUN/REMOTE/LOCAL se puede quitar o instalar mientras el interruptor RUN/REMOTE/LOCAL está en cualquier posición.

11.2 Seguridad Nivel Software

La RTU ControlWave puede admitir hasta 32 usuarios diferentes. Para agregar un usuario, se debe ingresar el nombre del usuario (hasta 16 caracteres) en el campo "Nombre de usuario" e ingresar una contraseña (hasta 16 caracteres) para el usuario en los campos "Contraseña" Y "Verificar" (La contraseña no aparecerá mientras la escribe). IMPORTANTE: Algunos programas de Open BSI como DataView, Downloader, etc. que se comunican con el controlador solo admiten nombres de usuario y contraseñas más cortos (10 caracteres o menos para el nombre de usuario, 6 caracteres o menos para la contraseña), por lo que es posible que convenga limitar la longitud de cada nombre de usuario y contraseña. Además, para comunicarse con esta unidad utilizando estos programas, los caracteres alfabéticos de la contraseña deben estar en MAYÚSCULAS.

A continuación, debe seleccionar los privilegios para este usuario haciendo clic en "Custon"(Personalizar) y luego seleccionar los privilegios individuales en el cuadro de lista "Privileges", para que se resalten. Alternativamente, puede elegir "Operator" (Operador), "Engineer" (Ingeniero) o "Administrator" (Administrador) para un usuario en particular, lo que resaltará automáticamente los privilegios asociados con esas categorías de usuarios.
Cuando se hayan seleccionado todos los privilegios deseados, haga clic en el botón [ADD] (Agregar) y el usuario se agregará al sistema.

NOTA: Cada controlador de la serie ControlWave tiene un usuario especial llamado RDB_Max. Esta cuenta de usuario define los privilegios máximos permitidos para los mensajes del protocolo RDB que ingresan a la unidad de la serie ControlWave. (RDB es utilizado por programas como DataView, Data Collector, etc.) No puede eliminar el usuario RDB_Max ni cambiarle el nombre, pero puede cambiar sus privilegios.