Restricting Communications Access

Control of the Unit through the communications interface can be restricted in two ways:

- Restricting Access with Protect Settings
  The protect mode's security setting can be used to write-protect the set values. The write-protected set values can be read through the communications interface, but not changed.
- Restricting Access with the Remote/Local Processing Setting
  The remote/local processing setting determines whether set values can be overwritten by key operations or through the communications interface. Change the mode setting as necessary to enable settings to be changed locally or remotely. The remote/local processing setting can be changed through the communications interface or by key operations (in the option menu).

1, 2, 3...

Restrictions in remote processing

In remote processing, settings cannot be changed with key operations. Only the remote/local switch (operating command) is valid.

If you attempt to change a displayed setting in remote processing with the keys, a message will appear indicating that the Unit is in remote processing and the display will revert to the previous set value display.

All settings which aren't write-protected can be changed through the communications interface when the Unit is in settings mode. Only set values can be changed while the Unit is in RUN mode. Changes to settings are reflected in the display immediately.

Restrictions in local processing

In local processing, settings cannot be changed through the communications interface (data-write commands).

If you attempt to change a setting in local processing with a data-write command, a mode error response will be returned and the setting will not be overwritten. There are no restrictions on the data-read commands.