

# Protocolo MARA

Versión 1.4 (?)

Tramas Ethernet

# Conceptos básicos del sistema

- ▶ Protocolo binario maestro/esclavo.
- ▶ Comunicación cliente/servidor.
- ▶ Comunicación por *polling*
- ▶ Modo RS485 multi-punto y modo punto a punto (PtP) sobre TCP.
- ▶ Mara/RS485 entre concentrador y red de placas de campo.
- ▶ Mara/TCP entre concentrador y centro de control (SCADA/HMI).

## Esquema

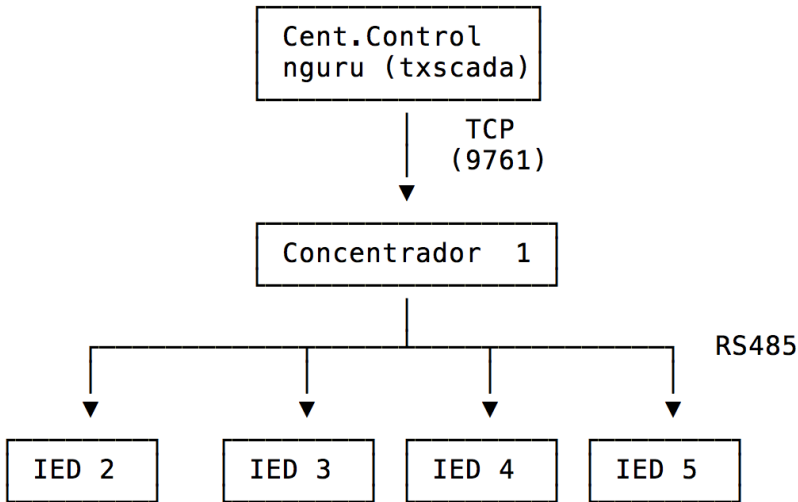


Figure 1: Jeraquía de comunicaciones

# Mara encapsulado en TCP

- ▶ Desde el punto de vista de sockets:
- ▶ El maestro es el cliente (connect)
- ▶ El esclavo es el servidor (accept).
- ▶ El servidor (a.k.a. **concentrador**) escucha conexión en puerto 9761. Responde comandos Mara que envía el cliente. *Atiende un solo cliente.*
- ▶ El servidor tiene *aguas abajo* una red de IEDs:
- ▶ Los IEDs se comunican en Mara con el concentrador en modo multi-punto (no PtP) mediante RS485.
- ▶ Los IEDs realizan la función de adquisición de estados y eventos.
- ▶ El concentrador guarda una tabla global de estados de todos los IEDs (el concentrador también es un IED) y una pila de eventos.
- ▶ El cliente es un software SCADA/HMI bautizado nguru ya que es el depredador patagónico natural de la Mara.

## Estructura básica

Ejemplo paquete de comando 0x10, con destino 01 y origen 40.

	SOF	QTY	DST	SRC	SEC	COM	BCCH	BCCL
Valor	FE	08	01	40	80	10	80	A7
Byte	0	1	2	3	4	5	6	7

- ▶ *SOF* Start of Frame. Indica que comienza una trama.
- ▶ *QTY* Cantidad total de bytes de la trama (hasta 0x8-0xFF)
- ▶ *DST* Destino 1-64 (fijo en 1 para concentrador).
- ▶ *SRC* Origen 1-64 (fijo en 1 para concentrador).
- ▶ *SEC* Número de secuencia empieza en 0x20 y termina en 0x7F.
- ▶ *COM* Comando
- ▶ *BCCH* y *BCCL* parte alta y baja de checksum

# Notas sobre los campos

- ▶ Cuando la comunicación es TCP, el destino siempre es 1 para los comandos. No se tiene en cuenta la dirección destino de las respuestas.
- ▶ El campo *SEQ* es incrementado por el cliente TCP (centro de control). Esto permite al concentrador descartar buffer de retransmisión.

# Comandos de Mara

- ▶ Puesta en Hora
- ▶ COM=0x12 y SEC=0xBB
- ▶ No tiene respuesta
- ▶ Pedido de estados y eventos
- ▶ COM=0x10
- ▶ La respuesta responde 4 arreglos
  - ▶ Estados
  - ▶ SV (varsys)
  - ▶ DI
  - ▶ AI
  - ▶ Eventos
  - ▶ Digitales
  - ▶ Analógicos

# Estructura de estados

- ▶ Los estados están compuestos por

Longitud + 1	dato	dato	dato	dato
can_sv (0x05)	byte 0	byte 1	byte 2	byte 3
can_di (0x05)	byte 0	byte 1	byte 2	byte 3
can_ai (0x05)	byte 0	byte 1	byte 2	byte 3

- ▶ can\_sv, can\_di, can\_ai son fijos y su valor es siempre impar ya que indica el corrimiento para llegar al siguiente can\_\* (+1) y la cantidad de siempre son words de 2 bytes.
- ▶ En el caso de no usarse alguno de los arreglos el valor sería 1 y y para un solo valor 3, para 2 words 5, etc.



- ▶ Las SV están orientadas a bytes, siempre en cantidades pares. Se utilizan para diagnóstico interno (corrimiento de relojes, cantidad de resets).
- ▶ Las DI se descomponen en words de 2 bytes, componiendo el estado de un puerto de 16 bits. Cada DI corresponde a un IED.

```

<tr><td>#</td><td colspan="2">IED 1</td><td colspan="2">IED
<tr>
    <td>0x05
    </td>
    <td>0xAA</td><td>0xBB</td>
    <td>0xCC</td><td>0xDD</td>

</tr>

```

# Pruebas con Arquicom.exe

- Para utilizar un servidor de debug, podemos usar netcat.

```
nc -l 9761 | xdd -u
```

```
Default
~ » nc -l 9761 | xdd -u
00000000: FE08 0440 FA10 03A7 FE08 0540 FB10 01A7 ...@.....@....
00000010: FE08 0240 FC10 03A7 FE08 0340 FD10 01A7 ...@.....@....
00000020: FE08 0440 FE10 FFA7 FE08 0540 FF10 FDA7 ...@.....@....
00000030: FE08 0240 0010 FFA7 FE08 0340 0110 FDA7 ...@.....@....
00000040: FE08 0440 0210 FBA7 FE08 0540 0310 F9A7 ...@.....@....
00000050: FE08 0240 0410 FBA7 FE08 0340 0510 F9A7 ...@.....@....
00000060: FE08 0440 0610 F7A7 FE08 0540 0710 F5A7 ...@.....@....
00000070: FE08 0240 0810 F7A7 FE08 0340 0910 F5A7 ...@.....@....
00000080: FE08 0440 0A10 F3A7 FE08 0540 0B10 F1A7 ...@.....@....
00000090: FE08 0240 0C10 F3A7 FE08 0340 0D10 F1A7 ...@.....@....
000000a0: FE08 0440 0E10 EFA7 FE08 0540 0F10 EDA7 ...@.....@....
000000b0: FE08 0240 1010 EFA7 FE08 0340 1110 EDA7 ...@.....@....
000000c0: FE08 0440 1210 EBA7 FE08 0540 1310 E9A7 ...@.....@....
000000d0: FE08 0240 1410 EBA7 FE08 0340 1510 E9A7 ...@.....@....
000000e0: FE08 0440 1610 E7A7 FE08 0540 1710 E5A7 ...@.....@....
000000f0: FE08 0240 1810 E7A7 FE08 0340 1910 E5A7 ...@.....@....
```

- En Linux y OSX es necesario tener instalado wine.

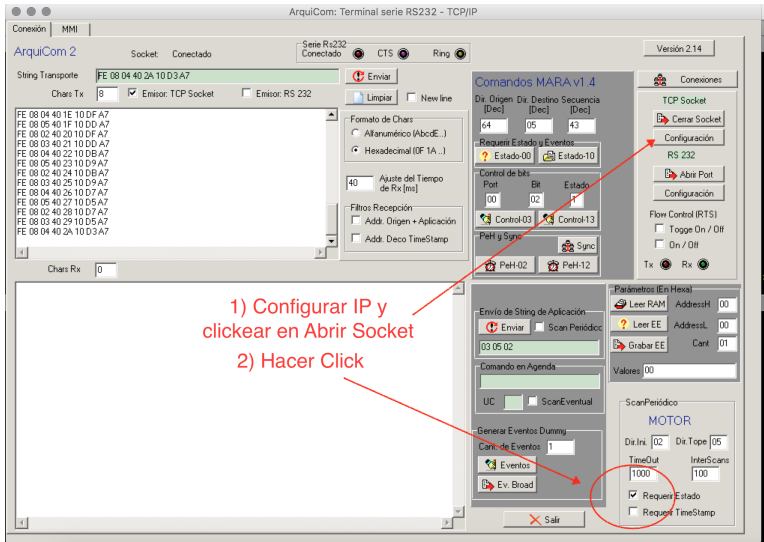


Figure 3: Arquicom