

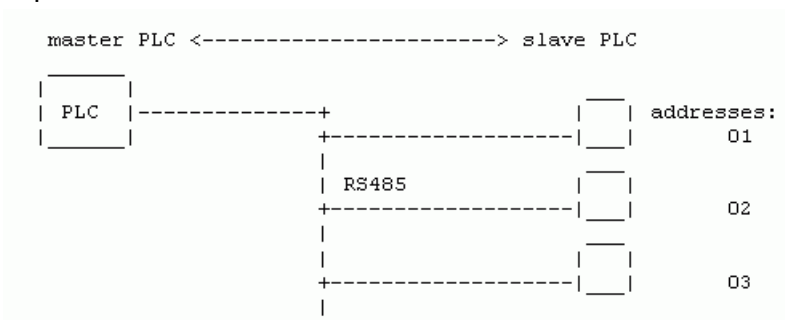
# Protokol MODBUS pro MORSE

## Popis protokolu

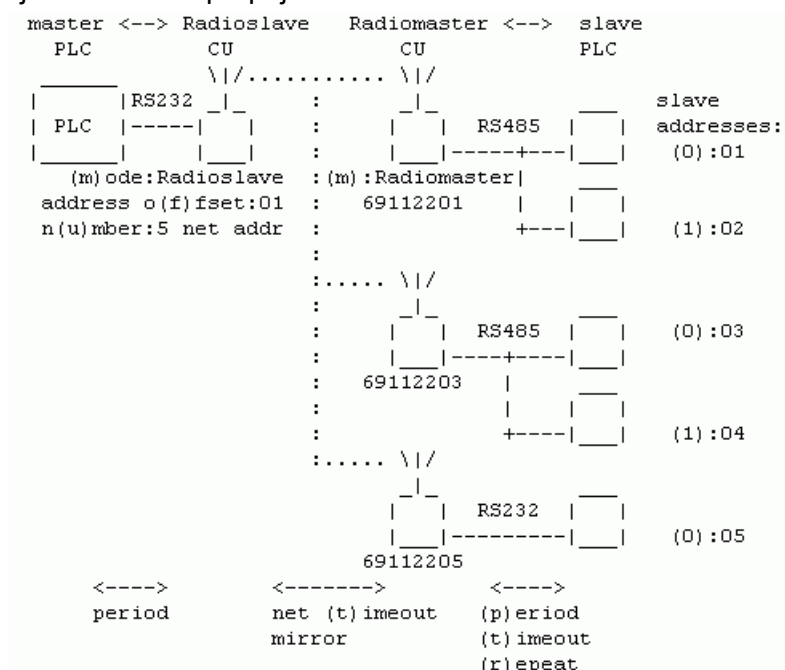
verze 10.0.9.0  
6. listopadu 2013

### 1. Úvod

Protokol MODBUS ve standardní podobě obsahuje jednoho Mastera a skupinu Slave spojených sítí RS485. Master cyklicky obvolává jednotlivé Slave a čte z nich data. Do toho Master podle potřeby vkládá povely pro Slave. Každý povel od Mastera je povinně potvrzen nebo obsahuje odpověď s daty odpovídajícími funkci rámce. Master nemá svoji vlastní adresu. Slave může mít adresu v intervalu 1 – 247, adresa 0 je užitá pro funkci modbus broadcast.



Na dalším schématu je síť Modbus propojená rádiovou sítí MORSE.



Slave PLC jsou připojeny jednotlivě nebo po skupinách k MORSE CU (communication unit, modem, rádio), které místně zastupují funkci Master PLC.

Sběrnice Modbusu je přerušena vloženou rádiovou sítí, která zprostředkovává spojení ve třech dále popsaných režimech. Radioslave (RS) a Radiomaster (RM) jsou CU s protokolem Modbus.

Radioslave má adresu Modbus shodnou s dolním byte svojí MORSE adresy. Dolní byte adresy CU Radiomaster je shodný s jednou z adres připojených slave PLC, pro směrování ostatních PLC se použije funkce „multiaddressing“ v menu (N)odes (e)dit. Znaky v závorkách jako (p)eriod se označují parametry protokolu, uveden je také příklad adres.

Protokol MODBUS pro MORSE může pracovat ve třech režimech

- transparent
- cache
- packet

Všechny režimy se chovají z hlediska PLC Master a Slave stejně, tedy Master posílá dotazy ve formátu Modbus na Slave a dostává odpovědi. Podobně Slave dostává dotazy a posílá odpovědi. Rozdíl je v přenosu této komunikace sítí MORSE. Režim Transparent do sítě přenáší celou komunikaci, režimy Cache a Packet podstatně redukuje nadbytečnou zátěž sítě.

### Transparentní režim

Všechny pakety, které přijdou z připojeného Master PLC do CU Radioslave jsou ihned vysílány sítí MORSE k příslušné vzdálené CU Radiomaster a předány do Slave PLC. Paket musí obsahovat v prvním byte adresu Slave, ve druhém číslo funkce Modbus, pak data a nakonec kontrolní součet. Paket projde protokolem i sítí MORSE beze změny. Zpráva od Slave PLC je akceptována pouze jako odpověď na dotaz a je odeslána na adresu tazatele. Režim je vhodný jen pro malé sítě s delším intervalem dotazů Master - Slave.

### Cache režim

CU Radiomaster dotazuje připojené PLC Slave v krátkém intervalu (p)eriod a získaná data ukládá do své paměti cache. Teprve když dojde ke změně dat v této paměti, je odeslán paket sítí MORSE do CU Radioslave. Ta udržuje ve své paměti data od všech PLC Slave připojených přes MORSE síť. Na dotaz, který je prováděn s krátkou periodou, pak předá data do PLC Master. Přenos povelů od Mastera do Slave, který je méně častý, probíhá v transparentním režimu.

Režim cache přenáší sítí MORSE pouze změny dat (+ refresh v delším časovém intervalu), proto je vhodný pro větší sítě. Slave může vysílat pouze jako odpověď na přijatý povel, přímá vzájemná komunikace Slave - Slave není možná.

Master v režimu Cache obslouží max. 50 Slave (fw 740) od fw 749 zvládne MR400 250 Slave, MR25 pouze 50 Slave.

### Packet režim

V paketovém režimu je zachována periodická komunikace master <—> slave na drátových linkách RS485 nebo RS232, to je Master PLC <—> Radioslave, Radiomaster <—> Slave PLC. Při této komunikaci je přenášen pouze krátký descriptor a teprve při nové informaci se přenáší celý datový buffer. Na

základě informací z datového bufferu pak CU vygeneruje paket MORSE, který je odeslán sítí MORSE k cílové CU.

Takto se stírá rozdíl master - slave. PLC Slave může odeslat zprávu bez výzvy a to i pro jiného PLC Slave.

Režimy Transparent a Cache nebo také Transparent a Packet mohou pracovat současně. Režim Transparent bývá v těchto případech využíván pro servisní zásahy do PLC.

## Všechny režimy

vyžadují, aby Master dovedl počkat na odezvu povelu od Slave delší čas než při komunikaci po prostém sériovém kanálu. Odezva na SCC je v desítkách msec, odezva na RFC může při nepříznivých podmínkách dosahovat i několika sekund.

## 2. Formát dat

Přehled funkcí Modbusu pro čtení a zápis z různých částí paměti PLC. Podrobnější popis v článku „Formát rámce MODBUS pro MORSE.“

function/8 (hex)	jednotka number/16	PLC
čtení	<--	
zápis	-->	
02	<-- bits	Bin IN  <- fyzický vstup  <-  <-
01	<-- bits	
05	--> lbit	Bin OUT  -> fyzický výstup  ->
0F	--> bits	
04	<-- words	Analog IN  <-
06	--> lword	
03	<-- words	Holding
10	--> words	Registers

Obr. 1: Funkce MODBUSu

Přehled formátů funkcí Modbus (č. funkce, směr přenosu informace, název funkce, velikost jednotky num je 1 nebo 16 bit):

Master-Slave	DOTAZ od Mastera				ODPOVĚĎ od Slave			
<-->								
01 <-- B_out		01						
02 <-- B_inp		01						
adr/8  fce/8	start/16	num/16	crc/16	adr/8	fce/8	cnt/8	data/8*cnt	crc/16
03 <-- H_Reg		16						
04 <-- Inp_R		16						
adr/8  fce/8	start/16	num/16	crc/16	adr/8	fce/8	cnt/8	data/8*cnt	crc/16

```
05 --> B_out
|adr/8| fce/8| start/16| 0xFF00| crc/16| =set 1 bit ON
|adr/8| fce/8| start/16| 0xFF00| crc/16|
|adr/8| fce/8| start/16| 0x0000| crc/16| =set 1 bit OFF
|adr/8| fce/8| start/16| 0x0000| crc/16|

06 --> H_Reg
|adr/8| fce/8| start/16| data/16| crc/16| =write 1 word
|adr/8| fce/8| start/16| data/16|crc/16|

0F --> B_out          01
|adr/8| fce/8| start/16| num/16| cnt/8| data/8*cnt| crc/16|
|adr/8| fce/8| start/16| num/16| cnt/8| data/8*cnt| crc/16|

10 --> H_Reg          16
|adr/8| fce/8| start/16| num/16| cnt/8| data/16*num|crc/16|
|adr/8| fce/8| start/16| num/16| cnt/8| data/16*num|crc/16|

odpověď na chybný povel          Err
|adr/8| 0x80+fce /8| excode/8| crc/16|
```

**adr**        adresa automatu na sběrnici Modbus

**fce**        funkce, kterou automat vykoná po přijetí rámce

**start**      počáteční adresa dat (výstupu), která budou zpracována

**num**        počet wordů (f 03,04,10,17) nebo bitů (f 01,02,0F) pro čtení nebo zápis

**cnt**        počet byte nutných pro přenos požadovaných dat

**data**       stavy čtených nebo zapisovaných registrů

**crc**        zabezpečovací slovo

**excode**    číslo výjimky, specifikuje chybu

1. chybné číslo funkce
2. chybná adresa dat
3. chybný obsah dat
4. neobsazeno
5. potvrzené přijetí povelu, jehož provedení je pomalé
6. odmítnutí, Slave je zaměstnán výkonem pomalého povelu

Příklad komunikace:

```
15:28:06.780 tx      8 | S00
0403 1000 0001 809F
15:28:06.784 rx;i    7 | S00
0403 0200 0074 44
```

04 dotazovaná adresa  
 03 čtení z Holding registru  
 1000 od adresy 1000  
 0001 číst 1 word  
 809F crc  
 04 odpovídající adresa  
 03 čtení z Holding registru  
 02 přečteny 2 byte  
 0000 obsah čtených byte  
 7444 crc

### 3. Implementace v systému MORSE

Režim modemu se nastavuje (zde pro SCC2) v menu SPe2t:

```

MODBUS parameters:
PLC Master - CU RADIOSLAVE ... CU RADIOMASTER - Slave PLC
(m)ode:RADIOSLAVE (wired to master)
(a)utomaster:OFF
(c)ache:ON (p)acket:OFF (t)rans:ON

(M)aster (S)lave
(A)utomaster
(C)ache
(P)acket
(T)rans

(s)ervices De(f)aults menu
(O)ld menu (sw ver =< 5.74)
(q)uit
>>
    
```

- (m)ode (m)ode:RADIOSLAVE (wired to master) - pozice modemu v síti
- (a)uto (a)utomaster:OFF - Radioslave může mít zapnutou funkci automaster. Při přerušení dotazů od mastera na RS485 pak přebírá funkci master a zajišťuje komunikaci s ostatními účastníky okruhu RS485.
- (c)ach (c)ache:ON - volba režimů
- (p)ack (p)acket:OFF - volba režimů
- (t)rans (t)rans:ON - volba režimů
- (M)ast toto a další podmenu obsahují parametry pro zvolené režimy

### 3.1. Modem jako RADIOSLAVE

Radioslave je přes SCC připojen k PLC Master a pohledu Mastera zastupuje všechny PLC Slave v síti. Pomocí parametrů `o(f)fset` a `n(u)mber` jsou definovány pro RS adresy všech PLC Slave. Podle režimu definovaného v menu `SPe2t` pak RS komunikuje s modemy RM, které jsou umístěny u jednotlivých PLC Slave.

```
slave parameters:
address o(f)fset:1 n(u)mber:5 net addresses
address type (o)ut: MORSE
address type (i)n: MORSE
(r)repeat discard:5 (deprecated)
d(e)vice type:PLC
Sep (a)ddress:5
(q)uit
>>
```

- `o(f)f`     `address o(f)fset:1` – adresy PLC Slave tvoří souvislou řadu, zde je uvedena nejnižší z nich
- `n(u)m`    `n(u)mber:5` - počet obsluhovaných PLC Slave (max. 50 pro fw do 740, fw 749 a vyšší zvládne s MR400 až 250 Slave, pro MR25 je limit 50 Slave)
- `(o)ut`    `address type (o)ut: MORSE/MODBUS` - v **RS** pouze pro Paketový režim - pro pakety odcházející do sítě se odvozuje adresa cílového PLC Slave buď z jeho adresy MORSE nebo z jeho adresy MODBUS obsažené v datech.
- `(i)n`     `address type (i)n: MORSE` - v **RS** pouze pro Paketový režim - pro pakety přicházející ze sítě se odvozuje adresa zdrojového PLC Slave buď z jeho adresy MORSE nebo z adresy MODBUS obsažené v datech
- `(r)ep`    `(r)repeat discard:5 (deprecated)` - poznámkou deprecated jsou označeny zrušené nebo nedoporučené parametry
- `d(e)v`    `d(e)vice type:PLC` - typ připojených PLC Slave:
- PLC – připojeno obecné PLC nebo PC s MODBUS protokolem
  - SEP - připojeno zařízení SEP ve starém formátu (ne MTF)
  - PLC+MTD - připojena zařízení s MODBUS protokolem a také SEP nebo ADIO moduly s MTF formátem
- `(a)dd`    `Sep (a)ddress:5` – pokud je zapnut režim PLC+MTD, pak se zde definuje rozsah adres pro MODBUS PLC a pro MTF zařízení (adresy nižší než `Sep Address` jsou vždy MODBUS PLC, adresy shodné a vyšší než `Sep address` jsou vyhrazeny pro zařízení MTF - ADIO, SEP)

### 3.2. Modem jako RADIOMASTER

Radiomaster vystupuje v síti MORSE pod adresou, jejíž poslední byte je shodný s jednou z `Modbus slave addr:`, například 69112203. Zprávy pro další z nich přijímá pomocí funkce Multiaddressing (v menu **Ne**). Adresa příslušného Radioslave je uvedena v položce `(d)estination:`.

Komunikace na lince RS485 (nebo na RS232 pro jediného Slave) probíhá s periodou (p)eriod: (zde 200 ms), na odpověď se čeká max. po dobu (t)imeout:, počet opakování je nastaven parametrem (r)epeat.

```

master parameters:
(d)estination:691122FFh destination
d(e)vice type (deprecated):PLC
Modbus slave addr: (0):3 (1):4 (2):5 (3):0
Modbus slave addr: o(f)fset:1 n(u)mber:0
address type (o)ut: MORSE
address type (i)n: MORSE
(a)ddress mask:FFh (deprecated)
(p)eriod:20 period i(n) : *10ms
(t)imeout:10*100 ms
(r)epeat:2
DPM(B) bcast compat:OFF
(q)uit
>>

```

- (d)est (d)estination:691122FFh - adresa Radioslave v MORSE síti, využívá režim Cache pro odesílání zpráv RM -> RS, dále pro chybová hlášení
- (0) Modbus slave addr: (0):5 (1):0 (2):0 (3):0 - seznam stanic Slave zahrnutých do obvolávacího cyklu, adresy je třeba obsazovat od parametru (0), např.:(0),(1),(2); od **sw 749** se Modbus slave adresy zadávají v **dekadickém** formátu. Je-li počet slave vyšší, lze alternativně využít parametry o(f)fset a n(u)mber.
- o(f)f Modbus slave addr: o(f)fset:1 - definování počáteční adresy pro delší interval PLC adres, od **sw 749**
- n(u)m n(u)mber:0 - počet PLC, interval začíná od offsetu, od **sw 749**
- (o)ut address type (o)ut: MORSE/MODBUS - pro pakety odcházející do sítě se odvozuje adresa zdrojového PLC Slave buď z jeho adresy MORSE nebo z jeho adresy MODBUS obsažené v datech.  
  
Volba MORSE se používá pro jedno PLC s adresou shodnou s posledním byte nódu. Volba MODBUS se používá při více PLC na sběrnici nebo při neshodě adresy PLC a nódu.
- (i)n address type (i)n: MORSE/MODBUS - pro pakety přicházející ze sítě se odvozuje adresa cílového PLC Slave buď z jeho adresy MORSE nebo z adresy MODBUS obsažené v datech
- (p)er (p)eriod:20 - perioda pro obvolávání stanic Slave na RS485 nebo RS232, doba mezi přijetím odpovědi a vysláním nového dotazu. Rozměr jednotky času je určen následujícím parametrem. Pro režim Cache a Packet.
- i(n) period i(n) : \*10ms / sec - jednotka času pro periodu je 10ms nebo 1sec. Zde je perioda 20\*10ms = 200ms.
- (t)im (t)imeout:10\*100 ms - max. doba čekání na odpověď na SCC. Po dobu čekání je SCC neaktivní, tedy ani nepředává případné další příchozí pakety.
- (r)ep (r)epeat:2 - max. počet opakování na SCC

(B) DPM(B) bcast compat:OFF - speciální parametr pro DPMB

### 3.3. Transparentní režim

V transparentním režimu jsou sítě přenášena všechna data z Mastera do Slave. Používá se pro přenos výkonných povelů od Mastera v režimu Cache. Pro obousměrný přenos je transparentní režim vhodný pouze pro velmi malé sítě s pomalým cyklem obvolávání „timeout“. Pro zamezení přenosu rušivých paketů používáme v RM kontroly viz níže.

Radiomaster po odeslání paketu do Slave očekává max. po dobu **SPe2tMt** (= timeout) odpověď od Slave, kterou pak pošle sítě MORSE do Radioslave.

RM odpovídá na MORSE adresu zdroje. Tím lze mít v síti více transparentních RS.

```
transparent parameters:
(A)rt table No:0
# ART dest:      gw:
#   mmnnffff    hhhhllll
#   mtf No Fce   high low addr (use help in default menu)
# BEWARE! IF YOU CHANGE CONTENT OF THE TABLE,
# YOU SHOULD RESTART (INIT) THIS PROTOCOL!
check (f)unction:ON
check a(d)dress:OFF
check (C)RC:OFF (deprecated)
check (n)et No:OFF
allow (r)ead req:OFF
(D)etect transp/cache<->packet by :CRC
Net(B)ase:0000 Net(M)ask:0000
(c)ommand cache:OFF (t)im::0s
(q)uit
>>
```

- (A)rt (A)rt table No:0 - tabulka Art se běžně nepoužívá.  
Pouze v případě komunikace ve formátu MTF slouží k převodu funkcí MTF na funkce Modbus.  
Přesnější popis v odstavci Cache režim.
- (f)un check (f)unction: - tato a další kontroly slouží k vyloučení cizích paketů, které se mohou objevit při transparentním přenosu
- ON - funkce musí být jednou z řady 0x01, 2, 3, 4, 5, 6, F, 10, 17, 1E platí pro RM i RS
  - OFF - číslo funkce není kontrolováno
- a(d)d check a(d)dress: - kontrola adresy Slave PLC
- ON - adresa musí být jednou z adres v menu **SPe2tM0**, 1, 2, 3, tedy jednou z adres připojených Slave PLC, platí pro RM
  - OFF - adresa není kontrolována
- (n)et check (n)et No: - kontrola číslování paketů



- ON - kontrola čísel morse paketů, paket odpovědi je označen shodným číslem jako dotaz na úrovni MORSE, musí být zapnuto v RM i RS
  - OFF - kontrola číslování je vypnuta
- (r)ead allow (r)ead req: - vkládání transparentních povelů v cache režimu
- ON - dovoluje Modbus centru posílat povel read do sítě k PLC i když pro ně není definován prostor v paměti cache. Tyto povel jsou pak odeslány do RM v transparentním režimu. Definuje se pouze pro RS při použití CACHE mode, od **sw 749**
  - OFF - v CACHE mode se povel read mimo definovanou cache zahazují. Platí pro RS, od **sw 749**
- (D)et (D)etect transp/cache<->packet by : - pokud je zapnut současně mód paketový a některý další, je nutno rozlišit, jak má být zpracován příchozí paket. Toto nastavení je společné pro všechny tři režimy a lze jej provést z menu SPe2tT (T)rans nebo (C)ache nebo (P)acket. Možnosti:
- (c) CRC - pokud vypočtené CRC souhlasí, je paket považován za Cache nebo Transparentní, pokud CRC nesouhlasí je považován za Paketový
  - (n) NetBase and NetMask - adresa src je porovnána s parametrem Net(B)ase v rozsahu Net(M)ask. Pokud je shodná, je paket zpracován v Transparentním nebo Cache režimu. Není-li shodná, je paket zpracován v režimu Paketovém.
- (B)ase Net(B)ase:00FF - nastavení Base pro rozlišení mezi Transparent/Cache a Paket režimem, pracuje se jen se spodní polovinou MORSE adresy
- (M)ask Net(M)ask:FFFF - nastavení Mask pro rozlišení mezi Transparent/Cache a Paket režimem
- (c)om (c)ommand cache: - PLC Master posílá dotazy Modbus do RS. Některá PLC očekávají odpověď po kratším čase, než je doba přenosu rádiovým kanálem z RS do RM a zpět. V tom případě PLC opakuje dotaz a tím nadměrně zaplňuje RF kanál. Proto použijeme (c)ommand cache, která pošle první dotaz a ostatní zahodí do doby než vyprší čas dle (t)im nebo než se na dotaz vrátí odpověď. Nastavuje se v režimu **RS**
- ON - zapnuto
  - OFF - vypnuto, všechny pakety jsou ihned odeslány do RF kanálu
- (t)im (t)im:10s - timeout pro (c)ommand cache

### 3.4. Cache režim

Režim CACHE [keš, kešovací] se používá pro sběr dat z většího počtu PLC Slave. Doplnuje se Transparentním režimem pro přenos (méně častých) povelů ve směru Master → Slave.

V režimu cache jsou vytvořeny v PLC a v modemech shodné paměťové prostory - cache. Přenos dat Slave → RM probíhá na linkovém vedení s krátkou periodou  $SPe2tMp$  volenou v oblasti 100 až 200ms. Tím se udržuje v RM aktuální obraz stavu připojených Slave. Pokud v tomto obrazu nejsou změny, je odeslán síť MORSE do RS v intervalech  $SPe2tCt$ . Nastane-li v cache RM změna, je zpráva pro RS odeslána okamžitě. Takto se v cache RS udržují aktuální obrazy cache všech připojených Slave s mi-

nimálním zatížením rádiové sítě. PLC Master pak čte tuto cache v RS stejně, jako by četl stavy všech Slave přes síť Modbus.

Při sledování stavu cache paměti je přenášén po lince celý obsah cache. Obvolávání je řízeno Radiomasterem nebo PLC Masterem. Přenos informací probíhá jen směrem Slave → Master.

```
cache parameters:
(A)rt table No:1
# ART dest:      gw:
#   mmnnffff    hhhhllll
#   mtf No Fce   high low addr (use help in default menu)
# BEWARE! IF YOU CHANGE CONTENT OF THE TABLE,
# YOU SHOULD RESTART (INIT) THIS PROTOCOL!

(D)etect transp/cache packet by :CRC
Net(B)ase:0000  Net(M)ask:0000
net (t)imeout - mirror:30s
a(l)iasing:OFF
(g)lue to trans:off
(e)rr. report:SILENT  err. (a)dr:0h  err. (m)ask:0000h
(o)ld cache menu (since sw.630)
(q)uit
>>
```

- (A)rt (A)rt table No:1 - číslo tabulky Art, kde je definován prostor cache paměti, podrobněji viz níže. Vyplň nejdříve tabulku Art a teprve potom menu SPe.
- (D)et (D)etect transp/cache<->packet by : - pokud je zapnut současně mód paketový a některý další, je nutno rozlišit, jak má být zpracován příchozí paket. Toto nastavení je společné pro všechny tři režimy a lze jej provést z menu SPe2tT (T)rans nebo (C)ache nebo (P)acket. Možnosti:
- (c) CRC - pokud vypočtené CRC souhlasí, je paket považován za Cache nebo Transparentní, pokud CRC nesouhlasí je považován za Paketový
  - (n) NetBase and NetMask - adresa src je porovnána s parametrem Net(B)ase v rozsahu Net(M)ask. Pokud je shodná, je paket zpracován v Transparentním nebo Cache režimu. Není-li shodná, je paket zpracován v režimu Paketovém.
- (B)ase Net(B)ase:00FF - nastavení Base pro rozlišení mezi Transparent/Cache a Paket režimem, pracuje se jen se spodní polovinou MORSE adresy
- (M)ask Net(M)ask:FFFF - nastavení Mask pro rozlišení mezi Transparent/Cache a Paket režimem
- (t)im net (t)imeout - mirror:30s - s touto periodou je odesílán aktuální obsah cache z RM do RS, pokud v cache nenastaly změny
- a(l)i a(l)iasing:OFF - společná cache pro všechny funkce
- OFF - normální stav - pro každou funkci Modbus je definován samostatný prostor v cache paměti
  - ON - definovaná jen jedna cache paměť a zapisují se sem všechny funkce

- (g)lue (g)lue to trans:off
- off - normální stav
  - on - ke transparentní odpovědi z RM do RS je připojen v tomtéž paketu také obsah cache, tak se informace o provedení povelu dostane rychleji do RS
- (e)rr (e)rr. report:SILENT - chování při ztrátě komunikace na lince RM <-> PLC/SEP:
- NONE - **RM** - chybová zpráva není vyslána, pokračují hlášení v intervalu  $Spe2tCt$  se starými hodnotami
  - NONE - **RS** - Radioslave dále odpovídá na dotazy Master
  - SILENT - **RM** - při ztrátě komunikace na RS485 končí vysílání v intervalu  $Spe2tCt$  (v RM), RS zjistí chybu až po uplynutí času  $Spe2tCt$  (v RS)
  - SILENT - **RS** - Radioslave, který po dobu  $Spe2tCt$  nedostane zprávu od RM nebo dostane od RM chybové hlášení REPORT, zastaví odpovědi na dotazy z PLC Master.
  - REPORT - **RM** - při ztrátě komunikace na drátech se okamžitě generuje chybové hlášení, RS zjistí chybu ihned, funkční od verze 7.65
  - MASK - **RM** - při ztrátě komunikace na RS485 je vysílána k Masterovi dosavadní zpráva upravená tak, že na vybraný word (a) zprávy jsou operací OR přidány stanovené bity (m). Používá se pouze pro cache obsahující jediný blok dat (jeden řádek v Art). Příklad:

```
err. (a)dr:0h err. (m)ask:FFFFh
```

```
10:30:47.087 tx      8 | S03
0503 0010 0003 058A
10:30:47.148 rx;i   11 | S03
0503 06AA AABB BBCC CC12 33
10:30:49.149 tx      8 | S03      ...přerušeno spojení na RS485
0503 0010 0003 058A
10:30:52.151|          |691122FF 00000005|S03I  OUT  11||89 4usr 0
0503 06FF FFBB BBCC CC12 3A
```

Nultý word zprávy AAAA je operací OR změněn na FFFF.

- DATMOLUX - předdefinovaný formát pro DATMOLUX

- (a)dr err. (a)dr:0h - parametr pro režim MASK - adresa wordu od počátku bloku cash paměti
- (m)ask err. (m)ask:0000h - parametr pro režim MASK - word, který je přidán (OR) k vybranému wordu paměti cache

### Tabulka Art a CACHE

Paměťové bloky pro funkci cache definujeme shodně v RS a RM pomocí tabulky Art. Pro standardní komunikaci Modbusu definuje Art v každém svém řádku jednu cache paměť. Obsahuje pořadové číslo, funkci Modbus a rozsah vyhrazené paměti. Příklad:

```
ART No 1:
items: 3
```

```
default gw: 00000000 (0.0.0.0 )
dest:      gw:
00040002 00040000 (0.1.0.2   0.4.0.0   )
00050003 00020000 (0.2.0.3   0.2.0.0   ) ...délka 2 word
00060003 00140010 (0.3.0.3   0.20.0.16 ) ...délka 4 word
>>
```

### Formát zápisu dest a gw:

| rez/8 | No/8 | rez/8 | fce mb/8 | high addr/16 | low addr/16 |

- rez/8 - rezerva, 00
- No/8 - pořadové číslo, libovolné, slouží k rozlišení položek `dest` při shodné funkci modbus
- fce mb/8 - číslo funkce Modbus (01, 02, 03, 04). Funkce zapsaná s horním bitem 1, tedy 81, 82, 83, 84, vytvoří paměťový blok, který se nepřenáší ihned po změně obsahu. Je přenesen do RS teprve při změně jiného bloku nebo po čase `SPe2tCt`. Platí od verze 10.0.20.0.
- high addr/16 - adresa horního konce paměťové oblasti
- low addr/16 - adresa dolního konce paměťové oblasti

Například třetí řádek definuje cache paměť pro funkci 03 - čtení registrů, která obsahuje 4 wordy na adresách 0010, 0011, 0012, 0013.

Odpovědi na dotazy Modbusu jsou ukládány do jednotlivých cache pamětí podle čísla funkce Modbus. Pokud je více záznamů se stejným číslem funkce, pak jsou rozlišeny podle délky. Paměti pro funkce stejného čísla musí být definovány tak, aby se lišily délkou a byly v Art seřazeny od nejkratších nahoře po nejdelší dole. PLC Slave musí poskytovat data pro celé takto definované cache. Pokud jsou data kratší, pak komunikace neproběhne.

V Art je možno definovat max. 8 pamětí cache. Maximální objem všech definovaných cache je 1400 Byte u Radiomastera. To znamená že při refresh cache ze směru Radiomaster -> Radioslave může jít síť MORSE paket o maximální velikosti 1400 Byte uživatelských dat.

Pro Radioslave (v centru) je limitující paměť v modemu.

Alokovaná paměť v centru = (PočetPLC + PočetSEP + PočetADIO) × VelikostCache

- Pro MR25 je alokovaná paměť < 5000 Byte
- Pro MR400 je alokovaná paměť < 250 000 Byte

### ADIO, SEP a MTF v Modbusu

Master PLC může komunikovat se Slave ADIO nebo SEP, které pracují s formátem MTF.

Tato zařízení definujeme v RS v menu (S)lave parametry `SPe2tSe`, `SPe2tSa`. Tabulka Art pak provádí také převod mezi funkcemi MTF a Modbus. Kromě paměťových bloků CACHE pro čtení z modulů ADIO a SEP jsou navíc definovány bloky RULY pro zápis. Doporučená konfigurace Art s komentářem:

```
dest:      gw:                ...CACHE, MB <-- SEP
06010001 00080000 (6.1.0.1   0.8.0.0   ) ...read Dout   8 bit
01020002 00100008 (1.2.0.2   0.16.0.8  ) ...read Din    8 bit
```

07030004	000C000A	(7.3.0.4	0.12.0.10)	...read Aout	2 word
02040004	00090001	(2.4.0.4	0.9.0.1 )	...read Ain	8 word
				...RULY, MB -->	SEP
07070006	01020100	(7.6.0.6	1.2.1.0 )	...write Aout	2 word
06080005	00080000	(6.8.0.5	0.8.0.0 )	...write Dout	8 bit
0609000F	00080000	(6.9.0.15	0.8.0.0 )	...write Dout	8 bit

Formát zápisu dest a gw:

| mtf/8 | No/8 | rez/8 | fce mb/8 | high addr/16 | low addr/16 |

- mtf/8 - číslo funkce MTF, formát viz Protokol MTF pro MORSE<sup>1</sup>
- No/8 - pořadové číslo, libovolné, slouží k rozlišení položek `dest` při shodné funkci modbus
- fce mb/8 - číslo funkce Modbus pro CACHE (1, 2, 3, 4, varianta 81, 82, 83, 84 viz výše) nebo pro RULY (5, 6, F)
- high addr/16 - adresa horního konce paměťové oblasti
- low addr/16 - adresa dolního konce paměťové oblasti, adresa je v bitech nebo wordech podle typu funkce Modbus, viz kapitola Formát dat

Definovat lze nejvíce 8 CACHE a 4 RULY.

Paměti stejného čísla funkce Modbus (zde řádky No 3 a 4) jsou opět rozlišeny délkou a seřazeny od kratších k delším.

Uvedená tabulka je vhodná pro komunikaci s modulem ADIO i SEP. Master PLC musí vysílat dotazy odpovídající délkou připojenému zařízení, například pro Din ADIO dotaz na 2 bity.

**Tab. 1: Adresy použité v SEP**

Ob- last	Fce	Typ	SEP-Cache	Obsah
Dout	0x01	R	00-07 bit	Čtení binárních výstupů
Dout	0x05	W	00-07 bit	Zápis do bin. výstupů po 1 bitu
Dout	0x0F	W	00-07 bit	Zápis do binárních výstupů
Dinp	0x02	R	08-15 bit	Čtení z binárních vstupů
Ainp	0x04	R	0x001-0x008 word	Čtení z analogových vstupů
Aout	0x04	R	0x00A-0x00B word	Čtení z analogových výstupů
Aout	0x06	W	0x100-0x101 word	Zápis do analogových výstupů

Radiomaster vysílá pravidelná hlášení pro RS v intervalu Net timeout  $SPe2tCt$ , kromě toho vysílá také aktuální zprávy o změnách. Radioslave sleduje, jestli se každý RM ozval alespoň jednou za čas  $SPe2tCt$ .

Pokud ne, chová se dle nastavení error report.

Cache v RS jsou uspořádány podle adres Modbusu nebo podle MORSE adres. Pokud adresy nezačínají od jedné, lze nevyužitou oblast paměti pro Slave (0 až N-1) vynechat pomocí adres offsetu, para-

<sup>1</sup> <http://www.racom.eu/cz/support/prot/mtf/index.html>

metr `SPe2tSf`. Počet bloků cache pak lze přizpůsobit celkovému počtu Slave v síti parametrem `SPe2tSu`.

RS rozpoznává jednotlivá Slave PLC pro jejich zařazení do cache podle MORSE adres, ze kterých přišla zpráva. Pokud je potřebné rozlišovat PLC podle adres Modbus, je to možno nastavit typem adresy v parametru `SPe2tSo`, `SPe2tSi`.

### 3.5. Paketový režim

V paketovém režimu jsou v každém PLC i v modemech vytvořeny dva paměťové buffery pro přenos dat Slave → Radiomaster (Host to Net, H2N) a opačně (Net to Host, N2H). Délka bufferů je min. 250 byte (max. délka rámce Modbusu), max. 1600 byte (max. délka paketu MORSE).

Přenos dat v paketovém režimu může probíhat libovolným směrem, tedy Master ↔ RS, RM ↔ Slave, Slave ↔ Slave.

Radiomaster se periodicky ptá každého Slave na obsah prvního wordu bufferu H2N zvaného deskriptor. Pokud je nenulový, je z něj zjištěna délka pseudorámce připraveného v H2N a ten je v další komunikaci přenesen do RM. Pak je deskriptor smazán, což indikuje pro Slave možnost přenosu dalšího rámce. Podobně probíhá komunikace PLC Master - RS, kterou řídí Master.

Přenos z Radiomastera do Slave probíhá tak, že RM přečte deskriptor N2Hdesc v PLC Slave a je-li nulový, zapíše do N2H svůj pseudorámec. Slave po jeho zpracování zapíše do N2Hdesc nulový word na znamení, že buffer N2H je opět k dispozici.

```
packet parameters:
Modbus (a)ddress:5
(A)RT table No.:0 (deprecated)
(N)2H buffer:2000 (H)2N buffer:1000
Warning: Both addresses should be nonzero.
(s)imulator:OFF
(D)etect transp/cache<->packet by :CRC
Net(B)ase:0000 Net(M)ask:0000
(q)uit
>>
```

(a)ddr - Modbus (a)ddress:5 — Modbus adresa modemu na sběrnici 485

(N)2H - (N)2H buffer:2000 — adresa bufferu pro přenos „Net to Host“, to je z MORSE Net do Modbusu

(H)2N - (H)2N buffer:1000 — adresa bufferu „Host to Net“, to je z Modbusu do MORSE Net - adresy v paměti, na kterých začíná příslušný buffer pro ukládání dat posílaných Modbusem v paketovém režimu. Tyto adresy musí být zvoleny shodně u všech účastníků sítě Modbus.

Pojem *Net* zde představuje navazující síť MORSE počínaje nódem, *Host* je PLC Slave nebo PLC Master připojené přes SCC.

(s)im - (s)imulator:OFF — Pro testovací účely je možno použít MORSE CU jako simulátor nahrazující PLC Slave v paketovém režimu. V simulátoru je pak nutno zapnout tento parametr a současně přehodit obsah parametrů (N) a (H).

Pseudorámce H2Nfr a N2Hfr mají hlavičku délky 6 byte a data. Hlavička obsahuje potřebné údaje pro vytvoření MORSE paketu a jeho odeslání do Radioslave nebo jiného Radiomastera.

Struktura bufferů:

- H2N:

```
| H2Ndesc/16 | H2Nfr/modbusMRU |
```

- N2H:

```
| N2Hdesc/16 | N2Hfr/modbusMTU |
```

popis položek:

H2Ndesc „host to net descriptor“ obsahuje potřebné informace pro přesun paketu přes Modbus. Shodný formát má i N2Hdesc (net to host descriptor):

```
H2Ndesc: |ret/1|rep/1|No/2|res/1|rxsize/11|
```

```
N2Hdesc: |ret/1|rep/1|No/2|res/1|txsize/11|
```

- ret
- 0 - user pseudorámec
  - 1 - retranslační pseudorámec (vyhrazeno pro potřeby Racomu)

rep repeat bit

No číslo paketu

res rezerva, musí být nula

rxsize, velikost pseudorámce včetně adresy a typu v bajtech  
txsize

H2Nfr user pseudorámec

N2Hfr user pseudorámec

modbusMRU Maximum Receive Unit

modbusMTU Maximum Transmit Unit

Adresy jednotlivých bloků paměti (H2N, N2H), jsou v modemu volně konfigurovatelné podle potřeb připojeného zařízení. Pseudorámec obsahuje vlastní paket, určený pro transfer do/ze sítě. Uvnitř pseudorámce je ukryta hlavička obsahující síťové informace. Hlavička je v bufferu umístěna na následující pozici za descriptor. Struktura hlavičky a dat:

User pseudorámec:

T/8   D/1   R/4   N/3   A/32   data
-------------------------------------

T typ paketu

D bit DTE

- je-li 0, je vysílající DCE, A je adresa source
- je-li 1, je vysílající DTE, A je adresa destination

R rezervováno, musí být nula

N síťové číslo (přenáší se po síti)

A MORSE adresa v síti

data vlastní data pseudorámce

### Příklad:

Rámec paketového režimu Modbus přenášející data z RM do Slave:

```

                                AA AA      ...data
                                09 0169 1122 FFAA AA      ...user pseudorámec N2Hfr
                                00 0809 0169 1122 FFAA AA      ...N2H descriptor + N2Hfr
0510 2000 0005 0A00 0809 0169 1122 FFAA AAE5 E6 ...rámec Modbus, zápis
                                                pomocí funkce 0x10
```

Rámec přenášející data ze Slave do RM:

```

                                BB BB      ...data
                                09 8369 1122 FFBB BB      ...user pseudorámec H2Nfr
0503 0809 8369 1122 FFBB BB0F B4 ...rámec Modbus, čtení funkcí 0x03
```

Při čtení dat ze Slave do RM se nechte znovu deskriptor, protože ten je přenesen v předcházejícím kroku dialogu. Podrobnější příklady<sup>2</sup> jsou uvedeny v samostatném článku.

## Multiaddressing

Radiomaster, který obsluhuje několik Slave, používá Multiaddressing. Při zapnutí funkce Multiaddressing v menu Nodes jsou pakety, které byly směrovány routingem do linkového výstupu nódu, odeslány do výstupu user. Tím je dosaženo, že pakety ze sítě MORSE určené pro některého ze Slave připojených k RM, jsou Radiomasterem akceptovány a jako user pakety odcházejí do SCC s protokolem Modbus.

## 3.6. Automaster

```
Modbus automaster:
t(i)meout:0s
master mode after switching:
(c)ache:OFF (p)acket:OFF (t)rans:OFF
(q)uit
>>
```

t(i)meout:0s po této době klidu na RS485 převezme Radioslave ze zapnutým parametrem (a)utomaster úlohu Radiomastera a pokračuje v režimu určeném parametry (c)ache:ON/OFF (p)acket:ON/OFF (t)rans:ON/OFF. Po obnovení aktivity původního Radiomastera se vrátí do úlohy Slave.

---

<sup>2</sup> <http://www.racom.eu/cz/support/prot/mod-ex-1009/index.html>



### 3.7. Servisní menu

Synchronizace času v Modbusu a watchdog pro PLC Slave.

```
Modbus services:
(t)ime sync:OFF (m)ode:RECEIVER (p)eriod:0s
time (a)ddr:0000h time sync (b)it:0000h
(d)ebug addr:00000000h (deprecated)
radiomaster only:
(w)dog bit:0000h wd(o)g addr:0000h wdog p(e)riod:0s (F)unc16:OFF
(q)uit
>>
```

#### Parametry pro předávání času:

(t)ime	(t)ime sync: - zapnutí funkce přenosu časového údaje mezi Radiomasterem a Slave
(m)ode	(m)ode:RECEIVER - režim vysílání nebo příjem času <ul style="list-style-type: none"> <li>• SENDER - Radiomaster nebo Radioslave může být zvolen jako SENDER (vysílá čas)</li> <li>• RECEIVER - Radiomaster nebo Radioslave může být zvolen jako RECEIVER (akceptuje čas)</li> </ul>
(p)er	(p)eriod:0s - perioda předávání časového údaje se definuje pouze v Radiomasterovi
(a)ddr	time (a)ddr:0000h - adresa pro ukládání času, Master i Slave, nastavit podle adresy použité v PLC
(b)it	time sync (b)it:0000h - zákaznická funkce

Parametry pro **watchdog** se vkládají pouze do Radiomastera, poskytují pro PLC Slave možnost kontroly, zda trvá spojení s Radiomasterem.

(w)dog	(w)dog bit:0000h - periodicky zapisované slovo do Slave
wd(o)g	wd(o)g addr:0000h - adresa zápisu do Holding Registers ve Slave
p(e)r	wdog p(e)riod:0s - perioda zápisu
(F)un	(F)unc16:OFF - funkce Modbus použitá k zápisu do Slave <ul style="list-style-type: none"> <li>• ON - watch dog používá funkci 0x16</li> <li>• OFF - používá funkci 0x06</li> </ul>

#### Časová synchronizace

Protokol Modbus umožňuje předávat čas mezi MORSE CU a připojeným zařízením Modbus. Lze takto navázat na synchronizaci času v síti MORSE, viz příklad<sup>3</sup> v samostatném článku. Ve všech CU je třeba

<sup>3</sup> <http://www.racom.eu/cz/support/prot/mod-ex-1009/index.html>

zapnout synchronizaci SPe2tst a nastavit shodně adresu pro záznam času SPe2tsa. Jsou čtyři varianty konfigurace:

RS receiver	čas z PLC Master do RS, mód receiver, funkce 10, period 0
RM sender	čas z RM do PLC Slave, mód sender, funkce 10, period
RS sender	čas z RS do PLC Master, mód sender, funkce 03, period 0
RM receiver	čas z PLC Slave do RM, mód receiver, funkce 03, period

Parametr "period 0" znamená, že komunikace Modbus je řízena druhým účastníkem. Parametr "period" je nastaven podle potřeby, například 3600sec. V případě více PLC Slave připojených k RM probíhá synchronizace pouze s prvním z nich.

Příklad - RS ve funkci SENDER přijme dotaz na čas od Master PLC a odpovídá:

```
12:01:47.831 rxsim 8 | S02
0503 3000 0006 CB4C
12:01:47.832 tx 17 | S02
0503 0C47 3984 1B03 402F 010C 0D0A 6BA4 84
```

### Formát časového údaje

|gmtsec/32|R/1|ts/1|R/4|msec/10|sec/8|min/8|hour/8|day/8|month/8|year/8|

gmtsec aktuální čas, je použit GMT udávaný v sekundách od 1.1.1970 (Unix time)

R rezerva

ts timesavings, přepínač letní/zimní čas (1 - letní čas, 0 - zimní)

msec milisekundy v právě probíhající sekundě

Z výše uvedených položek jsou v CU generovány další, které obsahují lokální čas včetně korekce časové zóny. V povelu pro zápis času do CU mohou být následující položky libovolné, například nulové:

sec aktuální sekunda

min aktuální minuta

hour hodiny (0 - 23)

mday den v měsíci (1 - 31)

mon měsíc (0 - 11)

year rok (údaj je ve tvaru letopočet - 1900)

Složení uvedeného příkladu:

```
0503 0C - adresa Modbus 05, funkce 03, 12 byte
4739 841B - Unix time, sekundy od 1.1.1970
0340 - 0000bit zimní čas, 0x340 = 832ms
2F - 47 sec
01 - 01 min
```

0C	- 12 hod
0D	- 13 den
0A	- 10+1 = 11 měsíc
6B	- 107+1900 = 2007 rok
A4 84	- crc

12:01:47.832 - čas monitoringu odpovídá obsahu uvedeného rámce.

### Funkce watchdog

PLC Slave v Modbusu nemá možnost zjistit, jestli nebyla přerušena komunikace s Radiomasterem. Proto je zde možnost nastavit v RM funkci Watchdog, která zapisuje v pravidelných intervalech určené slovo na vybranou adresu do PLC Slave. Vše se nastavuje v menu `SPe2ts`. PLC pak může pravidelně číst a mazat tento záznam a udržovat tak informaci o existenci spojení.

### 3.8. Typ paketu

Krátký popis typů paketů na uživatelském rozhraní.

|U/1|B/1|H/1|subt/5|

- U link security bit - 1 označuje zabezpečený přenos
- B broadcast (multicast) bit - 1 označuje broadcastový paket
- H handicap/priority - 1 označuje nižší prioritu (handicap)
- subt subtype - nabývá těchto základních hodnot:

- `subt=0x09` - USER DATA - uživatelská data

Základní typ paketu pro přenos dat od zdroje (source) do cíle (destination). V kombinaci s nastaveným bitem U=1 vznikne nejčastější typ paketu 0x89, to je zabezpečený uživatelský paket.

- `subt=0x0A` - PROT DATA

Tento typ dat je určen pro řízení toku dat v uživatelském protokolu. Zpracování obou uvedených typů paketů v síti MORSE je stejné. Pakety jsou odesílány na adresu destination podle routingu a priorit nastavených na zúčastněných adresách. V případě ztráty paketu je chybové hlášení doručeno k původnímu odesílateli. Paket, který nese toto chybové hlášení, se však také může ztratit, tentokrát již bez další zprávy.

- `subt=0x0C` - PACK ERROR REPORT - paket s chybovou zprávou

Zpráva o chybách v síti MORSE. První word je Error Number (číslo chyby), další část zprávy obsahuje podrobnější informace o chybě v síti. Generování těchto zpráv je možno zapnout nebo vypnout pro celou síť.

Dále jsou uvedena některá čísla chyb:

- 1 PACKET\_NOT\_CONFIRMED - paket není potvrzen
- 2 STORE\_TIMEOUT - vyčerpán store timeout

- 3 NO\_CHANNEL\_ASSIGNED - není přiřazen kanál
  - 4 ACCESS\_TIMEOUT\_ERROR - vyčerpán access timeout
  - 6 WRONG\_PACKET\_FORMAT - špatný formát paketu
  - 7 DEST\_PROT\_MISSING - chybí protokol na adrese destination
  - 8 WRONG\_PATH - špatná cesta
  - 9 WIRE\_LINK\_FAIL - chyba na drátové lince
- sub<sub>t</sub>=0x10 – SERVICE REQUEST – servisní požadavek  
Požadavek o službu MORSE.
  - sub<sub>t</sub>=0x12 – SERVICE REPORT – servisní zpráva  
Zpráva služby MORSE.

### 3.9. Příklady

Příklady pro transparentní, paketový a cache režim jsou uvedeny v samostatném článku MODBUS příklady<sup>4</sup>. Další příklady paketového režimu jsou obsaženy také ve starším popisu MODBUS 574<sup>5</sup>.

## 4. Historie

- Tento popis platí pro verzi sw 10.0.9.0 z 9.10.2007.
- Verze sw 657 (4.3.2004) až 678 používají také parametry (deprecated).
- Cache menu pro verze do sw 630 je obsaženo v „SPe0tCo“.
- Menu pro verze do sw 574 je v „SPe0tO“.
- Popis pro sw 574 (20.5.2002) s podrobnějším výkladem a s příklady paketového režimu je v článku „MODBUS 574“.

---

<sup>4</sup> <http://www.racom.eu/cz/support/prot/mod-ex-1009/index.html>

<sup>5</sup> [http://www.racom.eu/cz/support/protocols\\_docum/bc260\\_\\_modbus574.html](http://www.racom.eu/cz/support/protocols_docum/bc260__modbus574.html)