MTS-8

(Ver.141129)

GSM Transmitter (GPRS, SMS, CLIP)

With

Alarm Panel

Functionality

Main information

CE

MESSER – SPÓŁKA JAWNA

02-781 WARSZAWA, ul. ZAOLZIAŃSKA 9

tel: +4822 643 2023, fax: +4822 643 3130,

e-mail: marek@messer.com.pl, www.messer.com.pl

OPERATING MODES

MESSER MTS-8 GSM transmitters is a device intended to be used on the protected object and to report occurred alarm events to the Security Centre (**"SC"**)using the one of the following ways:

- **GPRS** digital data ("Send Event@GPRS"),
- **SMS** text message ("Send Event@SMS1"),
- **CLIP** message ("Send Event@CLIP"),

It is also possible to send SMS message to the monitoring station only in case of missing GPRS service or corrupted receiving IP server (simultaneously programmed both options "Send Event@GPRS" and "Send Event@@SMS1").

Independently of the communication with the server of the Security Centre, the transmitter may send chosen information (alarms) to the owner of the protected object (SMS2) containing clear description of the situation.

Also in case if the CLIP messaging, the transmitter May send a text message to the object's owner (simultaneously programmed both options "Send Event@CLIP" and "Send Event@@SMS1").

It is not recommended to use mixed mode CLIP+GPRS, however it is also possible to program and realize.

The transmitters are working in mode TCP/IP "client" Chile the receiving system is a TCP/IP "server". Because of this it is required to have constant IP address at the receiver side (Security Centre).

❑ REPORTING METHODS

When the transmitter is operating in GPRS mode, after sending anything to the receive Server waits programmable idle time (”TCP closing”) and then closes the connection with the remote server (a session with GPRS is still established). It is to reduce the load of the routers, server and operating system with the not needed volume of simultaneously opened connections.

Closing the TCP/IP session begins the counting of the next timer called ”Modem RST” (modem restart). When this timer is finished the device performs full modem restart including GPRS session (warn for costs). But any successful transmission is canceling this timer and the moment of restart is delayed. This procedure is to keep control on the properly working (connected) device but also to keep the costs under programmable control. To avoid unnecessary restarts the ”GPRS test interval” has to be set shorter than ”Modem RST” value.

If the transmitter cannot establish the connection with the main server address (”Server IP1”) to send there a message, then tries to do it to the backup server address (”Server IP2”). If it is still impossible, the transmitter sends a message over SMS form (only if an option ”Send message @GPRS is set on). If the Security Centre doesn’t have backup server IP then both addresses must be programmed the same. IP addresses maybe programmed as digits (like 19x.155.12.1:7551) or like the DNS names (like www.messer.com.pl:7551) as well.

Transmitter sends the periodic SMS tests within programmable time intervals (”SMS1 test interval”). But if the transmitter is working In GPRS mode then SMS tests are sent only in when GPRS session is not possible to establish.

In the CLIP mode (”Sent Event@CLIP”), the transmitter is calling to ”SMS1 phone number”, if nobody pick it up the transmitter tries to ”SMS2 phone number” – if still unsuccessful the SMS1 message is sent (but only if option ”Send Event@SMS1” is set on). SMS protocol ”2” is a clear form readable for every phone user. Protocols ”0” and ”1” are encrypted form destined for automated software.

❑ RECEIVE METHODS

There is a few methods how to receive the messages from the MESSER MTS-8 transmitters. But in every cases the main part of the receive system is some software with functionality of the TCP/IP Server and constant IP address must be provided.

- the simplest method is to use automated software equipped with the driver compatible with our transmitters. The driver is listening at proper IP address and “sending” received messages directly into the database of the software.

- the clients who don’t have that software may use our special driver-decoder which simulates popular phone monitoring receivers. The messages received over IP are delivered to the automated software through RS232 using popular protocols "Surgard MLR2" or "RC4000". In practice, the drivers for these protocols are available in every automated software for Monitoring systems. This is the most universal solution.

- the customers having Messer RMV-2003/1 Radio station (receiver) can use it also as buffer/decoder of the encrypted GSM messages from our transmitters. However the software Messer Server (program) listening at IP address and converting it to RS232 to deliver it to the station input is necessary. In this case the messages are in form 4+2 and CID protocol cannot be used. Decoded messages are sent to the automated software on the same RS232 connection the same and together with received radio messages.

❑ HARDWARE FEATURES

MTS-8 transmitter is equipped with 8 alarm inputs and three programmable, remotely controlled outputs. Additional (ninth) input, named IN0, is destined for future solutions (not in use on the moment).

Alarm inputs have many operating options: NO/NC, immediate (24h), delayed (entry/exit), follower (corridor), stay (nightly), allowed or not to bypass, and on/off (destined to Arm/Disarm the built-in alarm system). This internal alarm panel is divided into two independent partitions armed together or separately. Each alarm input may be assigned to only one selected partition or to the both of them. Also the entry/exit times are programmable. Partitions are controlled (armed) with freely pointed on/off zones.

The device holds three programmable outputs open-collector type. An output OUT1 is specially designed to load the alarm siren with maximal current 500mA, the current of the rest two outputs is 200mA each. Each output have its own programmable timer which allow to reach the following functions: output active on time (timer value 1-254sec), till disarm the system (value 0sec), so long as event lasts (value 255sec). The outputs may be also remotely controlled by the user's commands delivered as the text messages (SMS2).

ALARM PANEL CONTROLLED WITH LCD KEYPADS

Transmitter is also equipped with simple alarm panel. It may be controlled (armed/disarmed) using selected alarm input or LCD keypads KBD-816LCD. Keypads may be also used to program almost all parameters of the device. To connect the keypad, the transmitter must be equipped with special local interface (IFC-01GP/BUS). Up to seven users is possible to create in the system and up to four keypads can be connected. Each user has his own programmable password code (Main User code is 11111111). All the keypads are supervised and equipped with sabotage tampers against taking them off the wall or cut the communication wires. Proper alarm message is sent in case of any sabotage fact.

CONTACT ID RECEIVER

The transmitter can also receive "ContactID" or "Ademco DTMF 4+2" messages from external alarm panel connected over its phone line output. Received message is buffered and transferred to the remote monitoring centre using GPRS or SMS transmission. To activate the function of the phone decoder, it is necessary to check an option General/System Devices/DTMF module (or IFC module depending of the software version) in the settings parameters.

To connect the phone line the transmitter must be equipped with local interface named IFC-01GP/BUS/DTMF. This interface is universal – allows to connect or the phone line of the alarm panel, or the LCD keypads. Selection of the function is realized by the setting of the jumper on the interface. Jumper ON is to get function of the keypads interface (onboard LED is blinking slowly). Jumper set OFF is giving function of the phone input interface (onboard LED is blinking fast).
It is not possible to have both functions simultaneously.

❑ REMOTE MANAGEMENT

Some functions of the transmitter may be remotely managed by the the commands of the Security Centre Server (using TCP/IP or SMS1), or by text messages from the end-user (SMS2). Every commands are protected with programmable passwords against the possible sabotage acts.

SERVER COMMANDS over TCP/IP

(the command must contain the ”Server Password”)

- **Data/Time setting**

Transmitter sends to the Server periodical requests for the data/time update (with programmable intervals ”Data/time update”):

[xxxx123402ACxxxxxxxxxxxxxxxx*3725]$0D

Server command to set time/data in the transmitter is:

***1234*87654321*00*20141115235555*$0A**

```
*           - separator
1234        - object number
02AC        - date/time requesting event
87654321    - server password in-transmitter (”Server Password”)
00          - internal command number of time/date update
20141115    - new data 2014.11.15
235555      - new time 23:55:55
$0A and $0D - termination (hex format)
```

As the feedback the transmitter sends the periodic test signal.

- **Getting information about inputs status**

(From the hardware version v.141129)

At any time, the Server may send the request for the status using command:

***1234*87654321*08*$0A**

As the feedback the transmitter is sending the signal with message code **02A9.**

Status of the inputs is send together with every signals. See description in the section containing communication string details.

- **Remote control of the PGM outputs (“SMS ALARMS” over TCP/IP)**

(From the hardware version v.141129)

In the system there is possible to initiate three “SMS Alarm” messages. It is possible using tex messages or commands over TCP/IP. Each alarm may have assigned required outputs and is case of the alarm – proper outputs are activated with their programmable timers. Text control messages are descriibed in the further part, here are the commands of server (by TCP/IP):

```
*1234*87654321*0A*$0A          = SMS ALARM 1      ;feedback code: 0432
*1234*87654321*0B*$0A          = SMS ALARM 2      ;feedback code: 0433
*1234*87654321*0C*$0A          = SMS ALARM 3      ;feedback code: 0434
*1234*87654321*0D*$0A          = SMS RESTORE 1*   ;feedback code: 0435
*1234*87654321*0E*$0A          = SMS RESTORE 2*   ;feedback code: 0436
*1234*87654321*0F*$0A          = SMS RESTORE 3*   ;feedback code: 0437
```

*RESTORE SIGNAL may cancel ONLY an alarm activated by previous SMS ALARM with timer set to 255sec.

SERVER COMMANDS over SMS1 Phone

These commands must contain the ”Server Password” and must be incoming from the SMS1 phone number.

#1234#87654321#3E# = Device restart *****
#1234#87654321#3F# = GSM modem restart
#1234#87654321#20#5555# = New object ID *****
#1234#87654321#21#192.168.100.100:1201# = New Server IP1 address
#1234#87654321#22#192.168.100.200:1201# = New Server IP2 address
#1234#87654321#23#+48605000000# = New Phone SMS1******
#1234#87654321#24#+48605000000# = New Phone SMS2******

*** From the hardware version v.140919**
****From the hardware version v.150303**

1234 - object number
87654321 - server password in-transmitter (”Server Password”)
3F,20,21,22… - internal command number
5555 - new object ID
+48605000000 - new phone number
the rest - new IP address of the server number of the TCP/IP port

USER’S COMMANDS over SMS2 Phone

These commands must contain the ”Main User password” and must be incoming from the SMS2 phone number.

1234 - object number
11111111 - Main User (1) default password

- **Changing the User’s passwords**

#1234#11111111#01#11111111# = New password of the User 1 11...
#1234#11111111#02#22222222# = New password of the User 2 22...
#1234#11111111#03#33333333# = New password of the User 3 33...
#1234#11111111#04#44444444# = New password of the User 4 44...
#1234#11111111#05#55555555# = New password of the User 5 55...
#1234#11111111#06#66666666# = New password of the User 6 66...
#1234#11111111#07#77777777# = New password of the User 7 77...

- **Arming/Disarming an Alarm the System**

#1234#11111111#1A# = PART A Armed
#1234#11111111#1B# = PART B Armed
#1234#11111111#1C# = PART A Armed in STAY
#1234#11111111#1D# = PART B Armed in STAY
#1234#11111111#1E# = PART A DisArmed
#1234#11111111#1F# = PART B DisArmed

- **Miscellaneous**

#1234#11111111#10# = SYSTEM STATUS(SMS2)

- **Remote control of the PGM Outputs (“SMS ALARMS” over text message)**

In the system there are available three “SMS Alarm” messages. Each alarm maybe assigned to required outputs and is case of the alarm – proper outputs are activated with their programmable timers.

```
#1234#11111111#0A#            = SMS ALARM 1
#1234#11111111#0B#            = SMS ALARM 2
#1234#11111111#0C#            = SMS ALARM 3
#1234#11111111#0D#            = SMS RESTORE 1*
#1234#11111111#0E#            = SMS RESTORE 2*
#1234#11111111#0F#            = SMS RESTORE 3*
```

*RESTORE SIGNAL may cancel ONLY an alarm activated by previous SMS ALARM with timer set to 255sec.

❑ TCP/IP COMMUNICATION with the RECEIVE SERVER

MTS-8 transmitter may communicate with receiving Server using one of two available TCP/IP protocols (”GPRS Format”).

Protocol 0: Short ”M3000-GSM” encrypted protocol is destined to be received by Messer’s software converting the strings received by TCP/IP into RS232 communication with Messer’s Monitoring Station unit. The Station decode it and send to the operation software in open and clearly readable form using one of few popular 4+2 protocols.

Protocol 1: It is the text protocol named ”MESSER-GSM 1.151” described below. Every Monitoring Software manufacturer may write proper TCP/IP driver-server and serve it directly without any additional hardware units or other decoders.

- **Introduction**

The transmitter is a TCP/IP protocol client, the receiving driver is a TCP/IP protocol server – opening the port and listening to this.

In some cases the driver sends the control commands to the transmitters or answers to their questions. These signals must contain the server password compatible with the one existing in settings of the remote device. We can suppose that every transmitters in the network of the operator (monitoring centre) use the same password – so the password in driver may be set as one common for everybody.

Driver services:
- Basic signals (internal messages of the transmitter)
- Extended signals (i.ex. containing phone protocols like Contact ID, Ademco 4+2, GPS locations or any other)
- date/time updates
- control commands (to change some settings or get some status of the device)

- **Basic signals:**

Sample string:
[00111001501020121231135045 24*4025]$0D

Description:
[AB CD EEEE **xxxx** yyyyMMdd hhmmss FF * **vvvv**] $0D

[	- start of the string
A	- system arming status – see description below
B	- power (battery and AC) status – see description below
CD	- group of devices (ID)
EEEE	- object number (any ASCII)
xxxx	- an event (any ASCII), **ATTENTION!**.
yyyyMMdd	- data (year, month, day)
hhmmss	- time (hour, min, sec)
FF	- signal level (CSQ, any ASCII)
*	- separator
vvvv	- inputs status or extended data, **ATTENTION!**.
]	- ending
$0D	- hex value

ATTENTION!

Section **xxxx** – this is an event code (see the table in the end of manual) which informs what kind of the event has occurred.

Section **vvvv** – normally it carries information about the inputs status described below. But in some cases there is placed other information and its type is determined by the message in **xxxx** section. I.e. xxxx = 02AD means that it is forwarded phone protocol message in **vvvv** section. The section **vvvv**, doesn't have constant length and content – it can be differ in according to the type of the message. See below "Extended signals" description.

THE INPUTS STATUS:

The inputs status is shown in the end of every messages (after star character), it is in hex form (sample below is *0040):

[xxxx123402AA20141115235555***0040**]$0D

Interpretation:

```
INPUT#      8765 4321
VALUE       8421 8421
```

First byte (00 in 0040) is not used. Second byte (40 in 0040) consist status:

IN1 0001
IN2 0002
IN3 0004
IN4 0008
IN5 0010
IN6 0020
IN7 0040
IN8 0080

Sample:

IN1 and IN6: 0021,
IN1 and IN2 and IN8: 0083.
Etc, etc.

SYSTEM ARMING AND POWER STATUS:

```
AB = [S S S S R R 1 1]
      | | | |     | |
 STAY_B | B |     | BATT
   STAY_A   A     ACC
```

Samples:

```
ACC=OK/BATT=OK    -> xx00h
ACC=OK/BATT=ERR   -> xx01h
ACC=ERR/BATT=OK   -> xx02h
ACC=ERR/BATT=ERR  -> xx03h

B=OFF/A=ON        -> 01xxh
B=ON/A=OFF        -> 02xxh
B=ON/A=ON         -> 03xxh
STAY_A=ON/B=ON    -> 12xxh
```

- **Extended signals (data)**

One of the possible extender signals are phone protocols received from the external alarm panels connected to the transmitter by the telephone output (an event code **xxxx = 02AD**). Actually these are three popular phone monitoring protocols: ContactID (CID), Ademco DTMF 4+2 (ADE) and PagerDSC (DSC).

Sample:
ADE: [00111001**02AD**2012123113504524*1155027A15]$0D
CID: [00111001**02AD**2012123113504524*21550181171020018]$0D
DSC: [00111001**02AD**2012123113504524*31550A1#]$0D

Decription:
ADE: [ab CD 1001 **02AD** 20121231 135045 24 * T ACCT MT XY S] $0D
CID: [ab CD 1001 **02AD** 20121231 135045 24 * T ACCT MT Q XYZ GG CCC S] $0D
DSC: [ab CD 1001 **02AD** 20121231 135045 24 * T ACCT XY#] $0D

T - type of the phone protocol (1=ADE, 2=CID, 3=PagerDSC, 4…)
ACCT - received object number
MT - DTMF phone mark (CID=18/98, ADE=17/27)
Q - CID event qualifier (1,3,6)
XYZ - CID event code
XY - ADE event code
GG - CID object partition
CCC - zone or user
S - CID or ADE checksum
- constant mark In PagerDSC protocol
$0D - hex

❑ SMS COMMUNICATION to the SERVER at the Security Centre (SMS1)

The transmitter has two SMS protocols dedicated for communications with the Server located at the Security Centre (”SMS1 Format”) and third used when the system is not using SMS-server and we have requirement to send some messages for second User additionally.

Protocol #0: Short Message mode, only two digits of the report code and object identification by the incoming sms phone number in header.

Protocol #1: Communication string ”MESSER-GSM 1.151” identical like over TCP/IP (except removed $0D at the end).

Protocol #2: The same strings like used for SMS2 (see below).

❑ SMS Notifications to the User (SMS2)

In case of different system events (i.e. alarms, arming/disarming, technical problems etc.), the transmitter can send SMS notifications to the User using SMS2 phone number. It is possible to choose which events will be reported.

SMS1 phone number may be used as the phone for the notifications of the another User. To obtain it, the “SMS1 format“ must be set to value “2“. In this case the possibility to send alarm messages to the SMS monitoring server (at Security Centre) is lost.

Sample SMS’es:

Zone 5 Alarm

ALARM	**–**	type of event
Z05@A	**–**	zone number and its partition
(A)/(_)	**–**	system arming status (Part A armed, B disarmed)
Basement	**-**	description of the zone (editable)

Partition A Arming

SYSTEM	**–**	type of event
PGM A+	**–**	partition A arming using PGM zone
(A)/(_)	**–**	system arming status (Part A armed, B disarmed)
Mr Burgess	**-**	name of the User

❑ LED INDICATORS

Left LED
off = Low BATT and Missing 230V
blinking fast = Low BATT and 230V OK
blinking slow = BATT OK and Missing 230V
on = BATT OK and 230V OK

Central LED
off = initialization after restart
blinking fast = CARD OK
blinking slow = APN logging OK (GPRS exists)
on = TCP/IP server connected

Right LED
normally is OFF, blinking single when any event appears and blinking together with others when PIN code error.

Red LED
shows the strength of the GSM signal level blinking from 1-8 times (as higher as more). Signal level is tested in every few minutes. Press TEST switch to speed it up and get actualized information.

❑ CONFIGURATION SOFTWARE

- **Communication parameters**

/ **IP1 Server**; main server address and port, IP number or DNS name,
/ **IP2 Server**; back-up server address and port, must be the same as main if back-up is not used,
/ **Server password**; use the same in all transmitters connected to the server,
/ **CARD PIN**; anything or nothing for PIN-less card,
/ **Tel.1(SMS1->Station)**; phone nr of the server SMS-Receiver, number must be written in international form +48xxxxxxxxx (i.e. to Poland),
/ **Tel.2(SMS2->User.)**; phone nr for User notifications and control sms-es,
/ **Tel.3 (DTMF)**; phone for messages incoming from external alarm panel,
/ **GPRS format;** 0 = M3000 protocol, 1 = ”MESSER-GSM 1.151” protocol,
/ **SMS1 format;** 0 = Two digits codes, 1 = ”MESSER-GSM 1.151 protocol”,
/ **SMS2 format;** for future solution,
/ **ID Station;** set 0 when used M3000 receiver decoder, not used in other cases.

- **System timers**

/ **TCP closing**; session termination delay, recommended 20s at least,*
/ **GPRS test interval**; periodic tests to TCP/IP server and CSQ (signal level) checking interval,*
/ **SMS1 test interval**; used in case of missing GPRS connection,*
/ **CLOCK Update intrl**; interval of update it with server (recommended 24h),*
/ **Entry delay**; delays for entry zones of alarm panel,
/ **Exit delay**; delays for exit zones of alarm panel,,
/ **Modem RST (restart)**; delay of modem restart (and GPRS session re-login) in case of TCP/IP session failure, MUST be set longer than GPRS test interval!!! Modem is restarted without delay if "Modem RST" timer is set 0sec.

**Set value 0sec to disable the timer function.

- **Output timers**

System has 8 outputs with individually programmable timers. Value of timer determines both time and type of operating as well:

- 0sec: means "to disarm",
- 1-254sec: means "on this time" and "to disarm",
- 255sec means: "until an event is continued",

Activating may be executed by every system events assigned to an output. It can be i.e. alarms, arms/disarms, power statuses (230V or BATT), sms commands (see "User commands by SMS2 phone") etc.

- **System options**

/ **Test Auto reset**; each gprs transmission delay the next test signal,
/ **On/Off Siren Confirm**; Confirm; armin/disarming is confirmed with siren sound (OUT1),
/ **Send Event@;** choosing how to send the signals to receive server (GPRS, SMS, GPRS/SMS, CLIP),

- **Zone options**

/ NO;	select to set an input into Normally Opened mode,
/ 24h;	select if zone is not under arm/disarm control (generates an alarm even if system is not Armed),
/ Entry/Exit;	Zone delayed with timers declared in "System timers" part,
/ Follower;	corridor option, zone is not operating while entry/exit time, in other cases is regular alarm zone,
/ Stay;	zone is not active when system armed in Stay mode (night mode),
/ Bypass Enb;	select zones which can be bypassed by user,
/ Zone counter;	how many times the zone may activate an alarm, set 0 to disable the counter.
/ On/OFF Zone;	a zone for arming/disarming the System

❑ TECHNICAL SPECIFICATION

GSM Band	GSM900/850, DCS1800/1900
Sensitivity	-109dBm
Output Power GSM900/850	33dBm (+/-2,5), class 4
Output Power DCS1800/1900	30dBm (+/-2,5), class 1
Messaging type	GPRS (class 10), SMS, CLIP
Antenna	External, FME cable connector
Antenna Port discharge (air)	10kV
Antenna Port discharge (contact)	5kV
SIM Card interface	Standard-Mini, 1.8/3V
Alarm inputs (NO/NC)	8
Control outputs (PGM)	3
Power output (PWR)	1, Electronic fuse protected 500mA max.
Operating DC Voltage (battery)	9÷13.8VDC (nominal)
Operating AC Voltage	14.0Vac nominal
Standby DC Current	28mA max
Transmit Current	2.0A max peak
PWR Output Current	Electronic fuse protected 500mA max.
Operating temperature	5÷40°C
Storage temperature	-20÷80°C

- **EVENT CODES**

(two last digits only when using M3000 protocol)

```
;-----[Events to the SERVER]----|
TAMP1ALRM         :    0061     ; Tamper at keypad #1
TAMP2ALRM         :    0062     ; Tamper at keypad #2
TAMP3ALRM         :    0063     ; Tamper at keypad #3
TAMP4ALRM         :    0064     ; Tamper at keypad #4
230VFAIL          :    0068     ; Missing 230V
BATTFAIL          :    0069     ; Low Battery
FIREKey           :    006A     ; "Fire" keypad switch
EMERGENKey        :    006B     ; "Emergency" keypad switch
POLICEKey         :    006C     ; "Police" keypad switch
TAMP1REST         :    0070     ; Tamper at keypad #1 restore
TAMP2REST         :    0071     ; Tamper at keypad #2 restore
TAMP3REST         :    0072     ; Tamper at keypad #3 restore
TAMP4REST         :    0073     ; Tamper at keypad #4 restore
230VREST          :    0078     ; 230V return
BATTREST          :    0079     ; Battery return
;------------[01xx]-------------|
KEY01BUS          :    0180     ; BUS sabotage of keypad #1
KEY02BUS          :    0181     ; BUS sabotage of keypad #2
KEY03BUS          :    0182     ; BUS sabotage of keypad #3
KEY04BUS          :    0183     ; BUS sabotage of keypad #4
EXPBUS            :    0186     ; BUS sabotage of EXPander module
IFCBUS            :    0187     ; BUS sabotage of local IFC/DTMF module
KEY01BUSOK        :    0188     ; BUS sabotage of keypad #1 restore
KEY02BUSOK        :    0189     ; BUS sabotage of keypad #2 restore
KEY03BUSOK        :    018A     ; BUS sabotage of keypad #3 restore
KEY04BUSOK        :    018B     ; BUS sabotage of keypad #4 restore
EXPBUSOK          :    018E     ; BUS sabotage of EXP module restore
IFCBUSOK          :    018F     ; BUS sabotage of IFC/DTMF-module rest.
;------------[02xx]-------------|
SMSAlrm1          :    0290     ; Alarm SMS_1 from SMS2 phone
SMSAlrm2          :    0291     ; Alarm SMS_2 from SMS2 phone
SMSAlrm3          :    0292     ; Alarm SMS_3 from SMS2 phone
USER1KeySetup     :    0293     ; User programming mode entry
INSTAKeySetup     :    0294     ; Installer programming mode entry
NEWobjectNR       :    0295     ; Object ID changed by SMS (FWare: >140919)
NEWIP1sms         :    0296     ; IP1 changed by SMS
NEWIP2sms         :    0297     ; IP2 changed by SMS
SETsmsPassU1      :    0298     ; User1 password changed by SMS
SETsmsPassU2      :    0299     ; User2 password changed by SMS
SETsmsPassU3      :    029A     ; User3 password changed by SMS
SETsmsPassU4      :    029B     ; User4 password changed by SMS
SETsmsPassU5      :    029C     ; User5 password changed by SMS
SETsmsPassU6      :    029D     ; User6 password changed by SMS
SETsmsPassU7      :    029E     ; User7 password changed by SMS
RESTART           :    029F     ; Device restart
SMSRest1          :    02A0     ; Alarm SMS_1 from SMS2 phone restore
SMSRest2          :    02A1     ; Alarm SMS_2 from SMS2 phone restore
SMSRest3          :    02A2     ; Alarm SMS_3 from SMS2 phone restore
SYSsmsTEL1CNG     :    02A6     ; Phone #1 changed by SMS (FWare: >150303)
SYSsmsTEL2CNG     :    02A7     ; Phone #2 changed by SMS (FWare: >150303)
SYSsmsSTAT        :    02A8     ; System status sent by SMS
ZoneSTAT          :    02A9     ; Inputs status sent by server
TESTgprs          :    02AA     ; GPRS periodic test
TESTsms           :    02AB     ; SMS periodic test
TESTUpdClock      :    02AC     ; Data/Clock update request
DTMFDATA          :    02AD     ; DTMF (phone) event
ERRcmdFromSvr     :    02AE     ; Mistaken command from Server
SIMCOMRSTsms      :    02AF     ; Modem restart by SMS (FWare: >140919)
```

```
;------------[03xx]-----------------|
PARTAONSvr        :      03B0       ; Partition A armed by Server
PARTBONSvr        :      03B1       ; Partition B armed by Server
PARTAONsms        :      03B2       ; Partition A armed by SMS
PARTBONsms        :      03B3       ; Partition B armed by SMS
PARTAONz08        :      03B4       ; Partition A armed by PGM input
PARTBONZ08        :      03B5       ; Partition B armed by PGM input
PARTABONZ08       :      03B7       ; Partition A/B armed by PGM input
PARTAONStaySvr    :      03B8       ; Partition A armed in-STAY by Server
PARTBONStaSvr     :      03B9       ; Partition B armed in-STAY by Server
PARTAONStaSms     :      03BA       ; Partition A armed in-STAY by SMS
PARTBONStaySms    :      03BB       ; Partition B armed in-STAY by SMS
PARTAONStayZ08    :      03BC       ; Part. A armed in-STAY by PGM input
PARTBONStayZ08    :      03BD       ; Part. B armed in-STAY by PGM input
PARTAOFFsvr       :      03C0       ; Partition A disarmed by Server
PARTBOFFsvr       :      03C1       ; Partition B disarmed by Server
PARTAOFFsms       :      03C2       ; Partition A disarmed by SMS
PARTBOFFsms       :      03C3       ; Partition B disarmed by SMS
PARTAOFFz08       :      03C4       ; Partition A disarmed by PGM input
PARTBOFFz08       :      03C5       ; Partition B disarmed by PGM input
PARTABOFFz08      :      03C7       ; Partition A/B disarmed by PGM input

;------------[04xx]-----------------|
SMSAlrm1-server   :      0432       ; Alarm SMS_1 from server
SMSAlrm1-server   :      0433       ; Alarm SMS_2 from server
SMSAlrm1-server   :      0434       ; Alarm SMS_3 from server
SMSAlrm1-server   :      0435       ; Alarm SMS_1 from server restore
SMSAlrm1-server   :      0436       ; Alarm SMS_2 from server restore
SMSAlrm1-server   :      0437       ; Alarm SMS_2 from server restore
USR0OnSysA        :      04D0       ; Arming Part A without code
USR1OnSysA        :      04D1       ; User1 armed Partition A
USR2OnSysA        :      04D2       ; User2 armed Partition A
USR3OnSysA        :      04D3       ; User3 armed Partition A
USR4OnSysA        :      04D4       ; User4 armed Partition A
USR5OnSysA        :      04D5       ; User5 armed Partition A
USR6OnSysA        :      04D6       ; User6 armed Partition A
USR7OnSysA        :      04D7       ; User7 armed Partition A
USR0OnSysB        :      04D8       ; Arming Part B without code
USR1OnSysB        :      04D9       ; User1 armed Partition B
USR2OnSysB        :      04DA       ; User2 armed Partition B
USR3OnSysB        :      04DB       ; User3 armed Partition B
USR4OnSysB        :      04DC       ; User4 armed Partition B
USR5OnSysB        :      04DD       ; User5 armed Partition B
USR6OnSysB        :      04DE       ; User6 armed Partition B
USR7OnSysB        :      04DF       ; User7 armed Partition B
USR0StyOnSysA     :      04E0       ; Arming Part A/Stay without code
USR1StyOnSysA     :      04E1       ; User1 armed Partition A/STAY
USR2StyOnSysA     :      04E2       ; User2 armed Partition A/Stay
USR3StyOnSysA     :      04E3       ; User3 armed Partition A/Stay
USR4StyOnSysA     :      04E4       ; User4 armed Partition A/Stay
USR5StyOnSysA     :      04E5       ; User5 armed Partition A/Stay
USR6StyOnSysA     :      04E6       ; User6 armed Partition A/Stay
USR7StyOnSysA     :      04E7       ; User7 armed Partition A/Stay
USR0StyOnSysB     :      04E8       ; Arming Part B/Stay without code
USR1StyOnSysB     :      04E9       ; User1 armed Partition B/STAY
USR2StyOnSysB     :      04EA       ; User2 armed Partition B/STAY
USR3StyOnSysB     :      04EB       ; User3 armed Partition B/STAY
USR4StyOnSysB     :      04EC       ; User4 armed Partition B/STAY
USR5StyOnSysB     :      04ED       ; User5 armed Partition B/STAY
USR6StyOnSysB     :      04EE       ; User6 armed Partition B/STAY
USR7StyOnSysB     :      04EF       ; User7 armed Partition B/STAY
USR1OffSysA       :      04F1       ; User1 disarmed Partition A
USR2OffSysA       :      04F2       ; User2 disarmed Partition A
```

```
USR3OffSysA       :      04F3       ; User3 disarmed Partition A
USR4OffSysA       :      04F4       ; User4 disarmed Partition A
USR5OffSysA       :      04F5       ; User5 disarmed Partition A
USR6OffSysA       :      04F6       ; User6 disarmed Partition A
USR7OffSysA       :      04F7       ; User7 disarmed Partition A
USR1OffSysB       :      04F9       ; User1 disarmed Partition B
USR2OffSysB       :      04FA       ; User2 disarmed Partition B
USR3OffSysB       :      04FB       ; User3 disarmed Partition B
USR4OffSysB       :      04FC       ; User4 disarmed Partition B
USR5OffSysB       :      04FD       ; User5 disarmed Partition B
USR6OffSysB       :      04FE       ; User6 disarmed Partition B
USR7OffSysB       :      04FF       ; User7 disarmed Partition B

;------------[05xx]-----------------|
ALRMLine01AB      :      0500       ; Alarm from zone 1 in partition A/B
ALRMLine02AB      :      0501       ; Alarm from zone 2 in partition A/B
ALRMLine03AB      :      0502       ; Alarm from zone 3 in partition A/B
ALRMLine04AB      :      0503       ; Alarm from zone 4 in partition A/B
ALRMLine05AB      :      0504       ; Alarm from zone 5 in partition A/B
ALRMLine06AB      :      0505       ; Alarm from zone 6 in partition A/B
ALRMLine07AB      :      0506       ; Alarm from zone 7 in partition A/B
ALRMLine08AB      :      0507       ; Alarm from zone 8 in partition A/B
ALRMLine01A       :      0510       ; Alarm from zone 1 in partition A
ALRMLine02A       :      0511       ; Alarm from zone 2 in partition A
ALRMLine03A       :      0512       ; Alarm from zone 3 in partition A
ALRMLine04A       :      0513       ; Alarm from zone 4 in partition A
ALRMLine05A       :      0514       ; Alarm from zone 5 in partition A
ALRMLine06A       :      0515       ; Alarm from zone 6 in partition A
ALRMLine07A       :      0516       ; Alarm from zone 7 in partition A
ALRMLine08A       :      0517       ; Alarm from zone 8 in partition A
ALRMLine01B       :      0520       ; Alarm from zone 1 in partition B
ALRMLine02B       :      0521       ; Alarm from zone 2 in partition B
ALRMLine03B       :      0522       ; Alarm from zone 3 in partition B
ALRMLine04B       :      0523       ; Alarm from zone 4 in partition B
ALRMLine05B       :      0524       ; Alarm from zone 5 in partition B
ALRMLine06B       :      0525       ; Alarm from zone 6 in partition B
ALRMLine07B       :      0526       ; Alarm from zone 7 in partition B
ALRMLine08B       :      0527       ; Alarm from zone 8 in partition B
RESTLine01AB      :      0530       ; Restore zone 1 in partition A/B
RESTLine02AB      :      0531       ; Restore zone 2 in partition A/B
RESTLine03AB      :      0532       ; Restore zone 3 in partition A/B
RESTLine04AB      :      0533       ; Restore zone 4 in partition A/B
RESTLine05AB      :      0534       ; Restore zone 5 in partition A/B
RESTLine06AB      :      0535       ; Restore zone 6 in partition A/B
RESTLine07AB      :      0536       ; Restore zone 7 in partition A/B
RESTLine08AB      :      0537       ; Restore zone 8 in partition A/B
RESTLine01A       :      0540       ; Restore zone 1 in partition A
RESTLine02A       :      0541       ; Restore zone 2 in partition A
RESTLine03A       :      0542       ; Restore zone 3 in partition A
RESTLine04A       :      0543       ; Restore zone 4 in partition A
RESTLine05A       :      0544       ; Restore zone 5 in partition A
RESTLine06A       :      0545       ; Restore zone 6 in partition A
RESTLine07A       :      0546       ; Restore zone 7 in partition A
RESTLine08A       :      0547       ; Restore zone 8 in partition A
RESTLine01B       :      0550       ; Restore zone 1 in partition B
RESTLine02B       :      0551       ; Restore zone 2 in partition B
RESTLine03B       :      0552       ; Restore zone 3 in partition B
RESTLine04B       :      0553       ; Restore zone 4 in partition B
RESTLine05B       :      0554       ; Restore zone 5 in partition B
RESTLine06B       :      0555       ; Restore zone 6 in partition B
RESTLine07B       :      0556       ; Restore zone 7 in partition B
RESTLine08B       :      0557       ; Restore zone 8 in partition B
;-----------------------------------|
```