SERIAL TRANSMISSION PROTOCOL FOR X-NOVA ELECTRONIC LOCK

Rev.	Date	Description
0	21/01/2016	First emission
1	25/01/2016	Completion of some information.
2	05/02/2016	At pt. 4 “COMMAND TICKET REQUEST TO WORK” added more details on the validity of the command time
3	10/05/2016	At pt. 8 “TRANSMISSION” added that the bolt latch must be outside to allow authentication At pt. 9 “REMARK ON THE COMMUNICATION” added more details on query of the lock status after the maneuver.
4	12/10/2016	Added new command to read the internal information of the lock (pt 8 “INTERNAL VOLTAGE”)., so the following points 8-12 in rev. 3 became 9-13 in rev. 4. Introduced the final board with the connections described in pt 13.
5	10/03/2017	At pt.8 “INTERNAL INFORMATION” Correct indication bytes PL0, PL1 reading of the internal voltage: PL0 = m.s.b ; PL1 = l.s.b.
6	20/04/2017	Update of layout and graphics.

GENERAL INSTRUCTIONS

Mottura Serrature di Sicurezza S.p.A. thanks you for choosing this product and reminds you as follows:
- Read the instructions very carefully before installing the device or doing any maintenance work on the product.
- All assembly and connection procedures must be done according to the Rules of Good Practice as well as in conformity to current law.
- DO NOT install the product in explosive environments or atmospheres or in the presence of flammable fumes/gases.
- DO NOT install the product on doors with risk of contact with water or atmospheric agents unless adequately protected.
- Always switch off the power supply and disconnect all live parts before doing any installation or maintenance work on the product. Take all possible precautions to eliminate the risk of electrical shock when doing the installation or maintenance procedures described in this manual.
- In case of problems contact authorized dealers only.

When installing the lock, first connect all of the selected peripherals and then the power supply.
If you have to disconnect the wires, always disconnect the power supplies first.
The warranty does not cover damage due to negligence, carelessness or use in any manner not described in these instructions.
Mottura Serrature di Sicurezza S.p.A. may change the characteristics of the products described in this document and of the document itself at any time and without notice.

PROTOCOL:
The communication protocol will be set as follows:
Baud rate = 19200
Data bits = 8
Stop Bits = 1

The client device is MASTER
The lock is SLAVE

After sending a command , wait for the answer for at least 1000 ms (receive timeout).

The framework of the transmission is as follows:

```
-----------------------------------------------------------------------------------------
| MRK1 | MRK2    | COM | NBY |....|....|....|....|....|....|....|....|CHKS|
-----------------------------------------------------------------------------------------
```

MRK1 = Marker 1 start of transmission (0xAA)
MRK2 = Marker 2 start of transmission (0x55)
COM = Command
NBY = Number of bytes transmitted in the payload (8 in this case, max 16)
.... = Bytes of payload
CHKS = Checksum (one byte)

The checksum is the XOR of all the previous bytes from the first in order of transmission.

Values of "COM" (command):

1. **0x01 = STATUS REQUEST LOCK**
   To require the state to the lock: status byte (ST)

MASTER question						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	01	02	00	00	FC

SLAVE answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	01	02	00	**ST**	

Description byte ST (state):
bit<0> = state door (0 = open ; 1 = close)
bit<1> = state bolt latch (0 = outside ; 1 = inside)
bit<2> = state latches (0 = not outside ; 1 = outside)
bit<3> = battery status (0 = charged ; 1 = low)
bit<4> = status lock (0 = all is OK ; 1 = error)
bit<5> = 0
bit<6> = 0
bit<7> = 0 RESERVED , DO NOT USE.

2. **0x02 ENCRYPTION KEY REQUEST (FOR AUTHENTICATION)**
   The master sends this command to know the encryption key (16 bytes) of the lock, the lock will respond only if latches and door are open (safe condition). The lock randomly generates a new encryption key "KEY" replacing the previous one, then encrypts it with a fixed encryption key (hexadecimal values listed below) and sends it in response to the MASTER that must store it permanently.

PL0 = KEY0 ^ 0x56
PL1 = KEY1 ^ 0x1E
PL2 = KEY2 ^ 0x14
PL3 = KEY3 ^ 0x53
PL4 = KEY4 ^ 0x50
PL5 = KEY5 ^ 0x70
PL6 = KEY6 ^ 0x88
PL7 = KEY7 ^ 0xE3
PL8 = KEY8 ^ 0xB6
PL9 = KEY9 ^ 0x20
PL10 = KEY10 ^ 0xFA
PL11 = KEY11 ^ 0x45
PL12 = KEY12 ^ 0xBC
PL13 = KEY13 ^ 0x89
PL14 = KEY14 ^ 0x24
PL15 = KEY15 ^ 0xED

MASTER question						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	02	02	00	00	FF

SLAVE positive answer												
MRK1	MRK2	COM	NBY	....	....	....	....	....	....	....	....	....
AA	55	02	10	PL0	PL1	PL2	PL3	PL4	PL5	PL6	PL7	PL8

SLAVE positive answer (continuation)							
....	....	....	....	....	....	....	CHKS
PL9	PL10	PL11	PL12	PL13	PL14	PL15	

SLAVE negative answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	02	02	00	FF	00

The lock responds positively if it is in a position to accept authentication.
The lock responds negatively if it is NOT in the condition of authentication.

3. **0x03 SEND THE IDENTITY OF MASTER (FOR AUTHENTICATION)**
   The master must have or generate a unique number of 8 bytes that will be the identity “ID” for recognition, store it permanently and send it to lock, which will only respond if latches and door are open (safe condition).
   This command must be sent immediately after sending the command 0x02, encrypted with the key "KEY" as follows:

PL0 = ID0 ^ KEY0
PL1 = ID1 ^ KEY1
PL2 = ID2 ^ KEY2
PL3 = ID3 ^ KEY3
PL4 = ID4 ^ KEY4
PL5 = ID5 ^ KEY5
PL6 = ID6 ^ KEY6
PL7 = ID7 ^ KEY7
PL8 = random ^ KEY8
PL9 = random ^ KEY9

PL10 = random ^ KEY10
PL11 = random ^ KEY11
PL12 = random ^ KEY12
PL13 = random ^ KEY13
PL14 = random ^ KEY14
PL15 = random ^ KEY15

MASTER question												
MRK1	MRK2	COM	NBY	....	....	....	....	....	....	....	....	....
AA	55	03	10	PL0	PL1	PL2	PL3	PL4	PL5	PL6	PL7	PL8

MASTER question (continuation)							
....	....	....	....	....	....	....	CHKS
PL9	PL10	PL11	PL12	PL13	PL14	PL15	

SLAVE positive answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	03	02	00	00	FE

SLAVE negative answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	03	02	00	FF	01

The lock responds positively if it is in a position to accept authentication.
The lock responds negatively if it is NOT in the condition of authentication.

4. **0x04 TICKET REQUEST TO WORK**
   Before sending a command of work you have to ask for a "TK" ticket (4-bytes) to the lock which randomly generates and sends it encrypted as described below.
   This ticket must be used immediately (**we suggest < 1 sec. , max 5 sec. if the lock is maintained wake**) in the next command WORK (0x05).

PL0 = TK0 ^ KEY0
PL1 = TK1 ^ KEY1
PL2 = TK2 ^ KEY2
PL3 = TK3 ^ KEY3
PL4 = random ^ KEY4
PL5 = random ^ KEY5
PL6 = random ^ KEY6
PL7 = random ^ KEY7
PL8 = random ^ KEY8
PL9 = random ^ KEY9
PL10 = random ^ KEY10
PL11 = random ^ KEY11
PL12 = random ^ KEY12
PL13 = random ^ KEY13
PL14 = random ^ KEY14
PL15 = random ^ KEY15

MASTER question						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	04	02	00	00	F9

SLAVE positive answer												
MRK1	MRK2	COM	NBY	....	....	....	....	....	....	....	....	....
AA	55	04	10	PL0	PL1	PL2	PL3	PL4	PL5	PL6	PL7	PL8

SLAVE positive answer (continuation)							
....	....	....	....	....	....	....	CHKS
PL9	PL10	PL11	PL12	PL13	PL14	PL15	

SLAVE negative answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	04	02	00	FF	06

The lock responds positively if it has been authenticated.
The lock responds negatively if it is NOT authenticated.

5. **0x05 WORK OPERATION**
   This command must be sent immediately after TICKET REQUEST TO WORK (0x04) which uses the "TK" value (only valid for this operation).
   It is used to request an opening, a closing or an opening followed by an automatic closure. Command must be structured and encrypted as follows:

PL0 = TK0 ^ ID0 ^ KEY0
PL1 = TK1 ^ ID1 ^ KEY1
PL2 = TK2 ^ ID2 ^ KEY2
PL3 = TK3 ^ ID3 ^ KEY3
PL4 = TK0 ^ ID4 ^ KEY4
PL5 = TK1 ^ ID5 ^ KEY5
PL6 = TK2 ^ ID6 ^ KEY6
PL7 = TK3 ^ ID7 ^ KEY7
PL8 = TK0 ^ KEY8
PL9 = TK1 ^ KEY9
PL10 = TK2 ^ KEY10
PL11 = TK3 ^ KEY11
PL12 = TK0 ^ KEY12
PL13 = TK1 ^ KEY13
PL14 = TK2 ^ KEY14
PL15 = TK3 ^ CM ^ KEY15

The type of operation is achieved by placing the desired command in byte CM:
CM = 0 no operation
CM = 1 opening
CM = 2 closing
CM = 3 opening followed by an automatic closure

MASTER question												
MRK1	MRK2	COM	NBY	....	....	....	....	....	....	....	....	....
AA	55	05	10	PL0	PL1	PL2	PL3	PL4	PL5	PL6	PL7	PL8

MASTER question (continuation)							
....	....	....	....	....	....	....	CHKS
PL9	PL10	PL11	PL12	PL13	PL14	PL15	

SLAVE positive answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	05	02	00	00	F8

SLAVE negative answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	05	02	00	FF	07

The lock responds positively if all sent data are correct (ID e TK).
The lock responds negatively if the data do not match.

6. **0x06 OPEN FOR DEBUG (NOT IMPLEMENTED)**
   This command is implemented only on the prototype lock for debugging purpose.
   You get to open the lock without encrypted transmission.

MASTER domanda						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	06	02	00	00	FB

SLAVE positive answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	06	02	00	00	FB

7. **0x07 CLOSE FOR DEBUG (NOT IMPLEMENTED)**
   This command is implemented only on the prototype lock for debugging purpose.
   You get to close the lock without encrypted transmission.

MASTER domanda						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	07	02	00	00	FA

SLAVE positive answer						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	07	02	00	00	FA

8. **0x08 INTERNAL INFORMATION**
   This command requires the value of the voltage present inside the lock (in cents of a volt) and the number version of the firmware, is intended for debugging purposes.

MASTER question						
MRK1	MRK2	COM	NBY	....	....	CHKS
AA	55	08	02	00	00	F5

SLAVE positive answer												
MRK1	MRK2	COM	NBY	....	....	....	....	....	....	....	....	....
AA	55	08	10	PL0	PL1	PL2	PL3	PL4	PL5	PL6	PL7	PL8

SLAVE positive answer (continuation)							
....	....	....	....	....	....	....	CHKS
PL9	PL10	PL11	PL12	PL13	PL14	PL15	

PL0 = least significant byte of voltage
PL1 = most significant byte of voltage

Internal voltage = <PL1> ; <PL0> [cents of Volt]

Example:
PL1 = 0x03 ; PL0 = 0xC1
Internal voltage = 0x03C1 = 961 cents of Volt = 9,61 Volt

PL5 ÷ PL15 = firmware number in ASCII code (example: "EL20103F-01" where 20103 is the firmware number and 01 is the revision level)

PL5 = "E"
PL6 = "L"
PL7 = "2"
PL8 = "0"
PL9 = "1"
PL10 = "0"
PL11 = "3"
PL12 = "F"
PL13 = "-"
PL14 = "0"
PL15 = "1"

9. TRANSMISSIONS

The lock does not accept the work commands sent over the serial line if it has not been previously authenticated by the master.

AUTHENTICATION:
It takes place only if the lock is open (latches inside , bolt latch outside and door open).
The first command (COM = 0x02) that the MASTER sends needs to ask the lock to generate a new encryption key of 16-bytes, store it and use it to encrypt all commands that require it.
The second command (COM = 0x03) that the MASTER sends must contain an identification code number of 8-bytes (ID) that will be used for transmission. This ID must be encrypted with the key "KEY" received in the previous command, and sent to the lock. The lock stores ID permanently and use it to recognize work commands (0x05) by the MASTER.
If the above steps are successful, the two devices are authenticated to work together.
Authentication is required only the first time that you have to match the master device and the slave lock. If you make a new authentication the previous data will be overwritten.

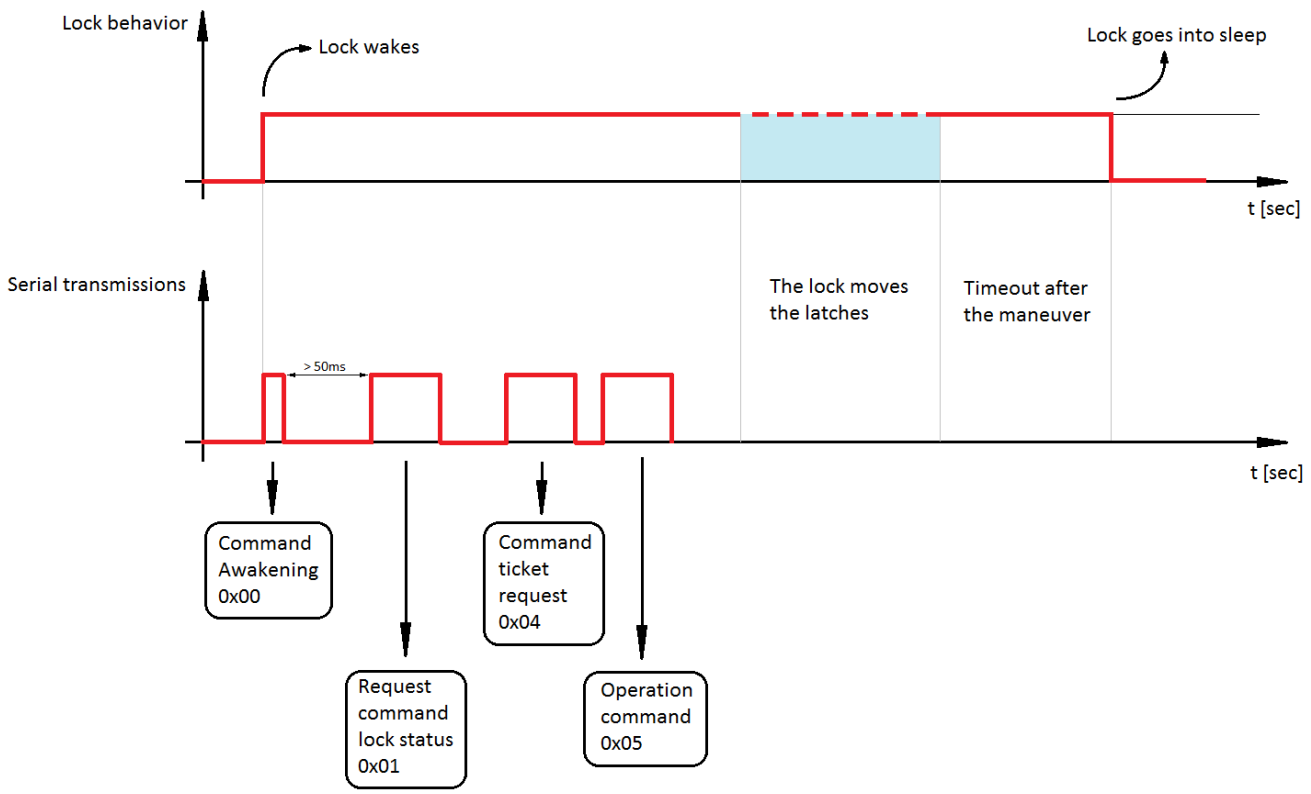
THE WORK OPERATION:
It is done by sending two commands in rapid sequence:

The first command (COM = 0x04) is used to request a ticket (TK) of 4-bytes to lock only valid for the next work command (0x05).
The lock sends the ticket by encrypting the entire payload with "KEY".
The second command (COM = 0x05) is used to send the identity of the master device (ID), the ticket for maneuver previously obtained (TK) and the desired command (CM) to the lock by encrypting the entire payload with "KEY".
If the lock finds the correct data, it performs the operation.
If the lock finds that the data is incorrect (for example an unauthenticated MASTER device tries to maneuver the lock), it does not perform the operation and after a number of attempts (5), it deletes the previous authentication.

10. REMARK ON THE COMMUNICATIONS

The lock is normally in sleep to consume less power, before sending any commands on the serial, awake the lock by sending a single byte at value of 0x00 and then wait 50 ms before sending other serial commands.
The lock after receiving a correct serial command, awakens and remains active for a few seconds (3 sec).
We suggest to ask the state to the lock before you decide which operation command send.
In the time that elapses between the execution of the maneuver and the entry into the sleep you can query periodically the lock to know the status after the maneuver.
WARNING: during the movement of the lock, serial communications are not active, therefore no response can be obtained.

Here's an example below:

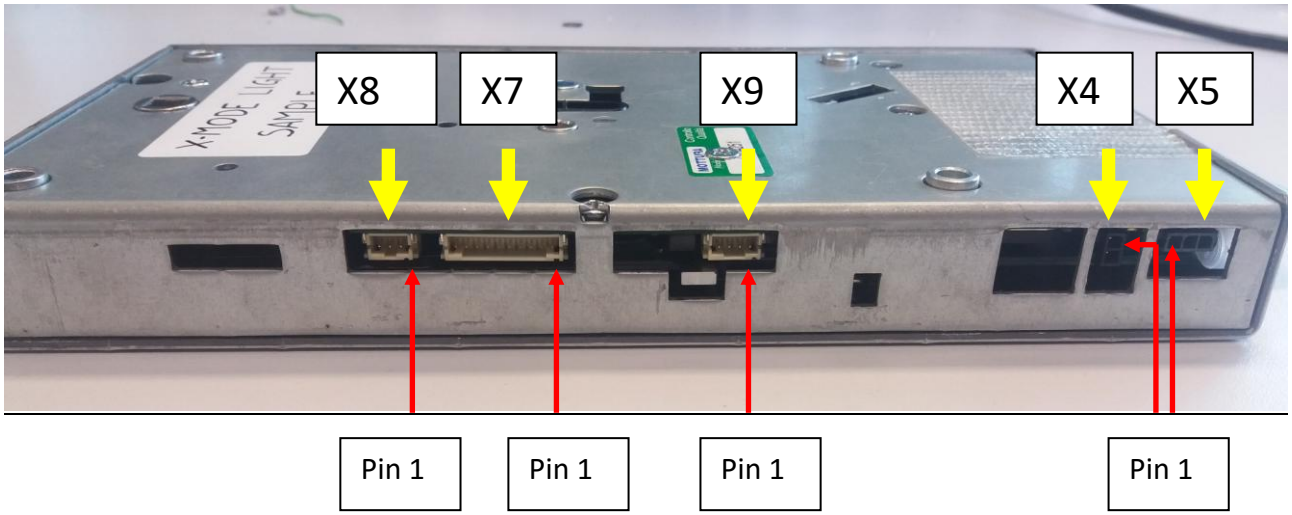


NOTE: The timing of these graphics are not real but only for example. The commands include the transmission and reception times.

11. **REMARK ON CURRENT CONSUMPTION BY SERIAL LINE RS232**
The lock during the sleep absorbs an average current <1 mA with serial port disconnected.
Connecting the serial port to the MASTER, lines RX and TX should draw less current as possible to extend the life of batteries.

12. **POWER SUPPLY LOCK**
Supply to the lock a mains voltage between 6.7 to 9.6 volts in direct current (Imax 2 A), or use 6 **alkaline battery 1,5 V(Zn/MnO2) type "D" (LR20).**
For mains voltage < 7.2 Vdc lock indicates that the battery is low.
For mains voltage < 6.6 Vdc the lock does not work.

13. **CONNECTIONS**



CONNECTOR	PIN	DESCRIPTION
X8	1	RX serial RS232 (reception of the slave)
	2	TX serial RS232 (transmission of the slave)
	3	GND
X9	1	VCC (3,2 V)
	2	RX (reception of the slave)
	3	TX (transmission of the slave)
	4	GND
X4	1	+12 Vdc (from the mains supply)
	2	GND
X5	1	n.c.
	2	+Vdc (from battery pack 9V)
	3	GND
All other pins are not relevant		

Mottura Serrature di Sicurezza S.p.A.
Strada Antica di Francia, 34 - 10057 Sant'Ambrogio (TO) - Italia
Tel. +39 011 9343111 - Fax +39 011 9312427
www.mottura.it