

SPYLOCK

USER GUIDE





Table of contents

1.	De	scrip	otion of the device	4
1	.1	SP	YLOCK views	5
2.	No	tice		7
3.	Ac	cess	ories	7
4.	De	vice	set up	8
5.	Те	chnie	cal specifications	8
6.	De	vice	functions	9
6	.1	Des	scription of the device functioning	9
7.	Sp	ylocl	< Management Software 1	1
7	.1	Pro	gramming Mode1	3
7	.2	Pas	ssword management1	5
	7.2	2.1	Security Password 1 and its functionality 1	5
	7.2	2.2	Reading of parameters1	6
	7.2	2.3	Date and time update with system data1	8
	7.2	2.4	Download of the stored log1	8
	7.2	2.5	How to change Password 12	0
	7.2	2.6	Security Password 2 and its functionality2	1
	7.2	2.7	Erasing memory 2	2
	7.2	2.8	How to enable firmware upgrade2	3
	7.2	2.9	How to change Password 22	3
8.	FΝ	/ Up	grade2	5
9.	На	rd R	eset2	9
10.	S	SPYL	OCK battery recharge2	9
11.	V	Varra	anty and liability conditions	1



Table of pictures

Figure 2 - SPYLOCK Top view 5 Figure 3 - SPYLOCK New OF COSE VIEW 5 Figure 4 - SPYLOCK New OF COSED CABLE 6 Figure 5 - SPYLOCK View OF COSED CABLE 6 Figure 6 - SPYLOCK View OF COSED CABLE 6 Figure 7 - SPYLOCK View OF COSED CABLE 6 Figure 10 - BATTERY LEVEL DISPLAYED 7 Figure 11 - LAST EVENT DISPLAYED 9 Figure 11 - LAST EVENT DISPLAYED 10 Figure 12 - DISPLAY SCROL 2 10 Figure 13 - DISPLAY SCROL 2 10 Figure 14 - DISPLAY SCROL 2 10 Figure 15 - DISPLAY SCROL 3 10 Figure 17 - DISPLAY SCROL 4 10 Figure 18 - Down To DETECT THE CONNECTED COM PORT IN A WINDOWS 7-8 BASED PC 14 Figure 21 - PASSWORD 1 EXAMPLE OF INSERTING 16 Figure 22 - READ OPERATION ADDUT COMPLETED 17 Figure 23 - DAT AND TIME CHARAGERES TETRIEVED 17 Figure 24 - SPYLOCK PARAMETERS RETRIEVED 17 Figure 25 - DEVENTS DOWNLOAD COMPLETED 17	FIGURE 1 - SPYLOCK OVERVIEW	4
FIGURE 3 - SPYLOCK SIDE VIEW 5 FIGURE 4 - SPYLOCK VIEW OF OPEN CABLE 6 FIGURE 5 - SPYLOCK VIEW OF CONSECTORS 6 FIGURE 7 - SPYLOCK VIEW OF CONSECTORS 6 FIGURE 7 - SPYLOCK VIEW OF CONSECTORS 7 FIGURE 7 - SPYLOCK VIEW OF CONSECTORS 7 FIGURE 9 - DISPLAY OF THE MESSAGE "DEVICE CLOSED" 8 FIGURE 10 - BATTERY LEVEL DISPLAYED 9 FIGURE 11 - LAST EVENT DISPLAY SCROLL 2 10 FIGURE 12 - DISPLAY SCROLL 2 10 FIGURE 13 - DISPLAY SCROLL 3 10 FIGURE 14 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 3 10 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 4 13 FIGURE 17 - PASSWORD 11:EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 22 - READ OPERATION COMPLETED 17 FIGURE 23 - DATE AND TIME CHANGE CONSERTING DIFFE	FIGURE 2 - SPYLOCK TOP VIEW	5
FIGURE 4 - SPYLOCK REAR VIEW 5 FIGURE 5 - SPYLOCK VIEW OF CODE CABLE 6 FIGURE 5 - SPYLOCK VIEW OF CONNECTORS 6 FIGURE 7 - SPYLOCK VIEW OF CONNECTORS 6 FIGURE 8 - DISPLAY OF THE MESSAGE "DEVICE CLOSED" 7 FIGURE 9 - DISPLAY OF THE MESSAGE "DEVICE CLOSED" 8 FIGURE 11 - LAST EVENT DISPLAYED 9 FIGURE 12 - DISPLAY SCROLL 1 10 FIGURE 13 - DISPLAY SCROLL 2 10 FIGURE 14 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DOSPLAY SCROLL 4 10 FIGURE 17 - DOS INFORMATION ABOUT COMPCT IN A WINDOWS XP BASED PC 14 FIGURE 21 - PASSWORD 1 20 FIGURE 23 - READIG INFORMEDES	FIGURE 3 - SPYLOCK SIDE VIEW	5
FIGURE 5 - SPYLOCK VIEW OF CLOSED CABLE 6 FIGURE 6 - SPYLOCK VIEW OF CLOSED CABLE 6 FIGURE 7 - SPYLOCK VIEW OF CONECTORS 6 FIGURE 8 - UNPACKING SPYLOCK 7 FIGURE 9 - DISPLAY SCHOLK 7 FIGURE 10 - BATTERY LEVEL DISPLAYED 9 FIGURE 11 - LAST EVENT DISPLAYED 10 FIGURE 12 - DISPLAY SCROLL 1 10 FIGURE 13 - DISPLAY SCROLL 3 10 FIGURE 14 - DISPLAY SCROLL 4 10 FIGURE 15 - DISPLAY SCROLL 3 10 FIGURE 16 - DISPLAY SCROLL 3 10 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 3 10 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 6 11 FIGURE 17 - DISPLAY SCROLL 7 13 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS 78 BASED PC 14 FIGURE 21 - PASSWORD 1 EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - EVENTS DOWNLOAD OPERED <td< td=""><td>FIGURE 4 - SPYLOCK REAR VIEW</td><td>5</td></td<>	FIGURE 4 - SPYLOCK REAR VIEW	5
FIGURE 6 - SPYLOCK VIEW OF CONNECTORS 6 FIGURE 7 - SPYLOCK VIEW OF CONNECTORS 6 FIGURE 8 - UNPACKING SPYLOCK 7 FIGURE 9 - DISPLAY OF THE MESSAGE "DEVICE CLOSED" 8 FIGURE 11 - LAST EVENT DISPLAYED 9 FIGURE 12 - DISPLAY SCROLL 1 10 FIGURE 13 - DISPLAY SCROLL 2 10 FIGURE 14 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 - DISPLAY SCROLL 4 10 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - SPYLOCK VARAMETERS RETRIEVED 17 FIGURE 25 - DATE AND TIME CHANGE SUNT THE "GETES YSTEM TIME" COMMAND 18 FIGURE 25 - DATE AND TIME CHANGE SUNT THE "GET SYSTEM TIME" COMMAND 18 FIGURE 25 - DATE AND TIME CHANGE SUNT THE SECURITY PASSWORD 1 20 FIGURE 26 - DEVENTS DOWNLOAD COMPLETED 17 <td< td=""><td>FIGURE 5 - SPYLOCK VIEW OF OPEN CABLE</td><td>6</td></td<>	FIGURE 5 - SPYLOCK VIEW OF OPEN CABLE	6
Figure 7 - SPYLOCK View or connectors. 6 Figure 8 - UnPacking SPYLOCK 7 Figure 10 - BATTERY LEVEL DISPLAYED 9 Figure 11 - LAST EVENT DISPLAYED 10 Figure 12 - DISPLAY SCROLL 2 10 Figure 14 - DISPLAY SCROLL 2 10 Figure 14 - DISPLAY SCROLL 3 10 Figure 15 - DISPLAY SCROLL 4 10 Figure 14 - DISPLAY SCROLL 4 10 Figure 15 - DISPLAY SCROLL 5 11 Figure 17 - DISPLAY SCROLL 6 11 Figure 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 Figure 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 Figure 20 - Log INFORMATION ABOUT COM PORT IN A WINDOWS 7-8 BASED PC 14 Figure 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 Figure 22 - READING IN PROGRESS 16 Figure 23 - READ OPERATION COMPLETED 17 Figure 24 - EVENTS DOWNLOAD COMPLETED 17 Figure 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND 18 Figure 26 - INSERTING THE NEW SECURITY PASSWORD 1 20 Figure 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 Figure 28 - LOG FILE: AN EXAMPLE	FIGURE 6 - SPYLOCK VIEW OF CLOSED CABLE	6
Figure 8 - UNPACKING SPYLOCK 7 Figure 10 - BATTERY LEVEL DISPLAYED 8 Figure 11 - LAST EVENT DISPLAYED 10 Figure 12 - DISPLAY SCOLL 1 10 Figure 13 - DISPLAY SCOLL 3 10 Figure 14 - DISPLAY SCOLL 3 10 Figure 15 - DISPLAY SCOLL 4 10 Figure 16 - SPYLOCK MANAGEMENT Sortware user INTERFACE 11 Figure 17 - DISPLAY SCOLL 4 10 Figure 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 Figure 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 Figure 21 - PASSWORD 1: EXAMPLE OF INSERTING 15 Figure 22 - READING IN PROGRESS 16 Figure 23 - BRAD OPERATION COMPLETED 17 Figure 24 - SPYLOCK ARAMETERS RETRIEVED 17 Figure 25 - DATE AND TIME CHANGED WATHE "GET SYSTEM TIME" COMMAND 18 Figure 26 - EVENTS DOWNLOAD COMPLETED 18 Figure 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 Figure 28 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 Figure 28 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 Figure 23 - SECURITY PASSWORD 2 21 Figure 24 - SPELOC N	FIGURE 7 - SPYLOCK VIEW OF CONNECTORS	6
FIGURE 9 - DISPLAY OF THE MESSAGE "DEVICE CLOSED". 8 FIGURE 10 - BATTERY LEVEL DISPLAYED 9 FIGURE 11 - LAST EVENT DISPLAYED 10 FIGURE 12 - DISPLAY SCROLL 1 10 FIGURE 13 - DISPLAY SCROLL 2 10 FIGURE 14 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - DISPLAY SCROLL 4 10 FIGURE 17 - DISPLAY SCROLL 5 11 FIGURE 17 - DISPLAY SCROLL 6 12 FIGURE 17 - DISPLAY SCROL 7 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 21 - PASSWORD 1 11 FIGURE 22 - READ OPERATION COMPLETED 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - SPYLOCK KRAMETER SETHEVED 17 FIGURE 25 - DATE AND TIME CHANGED VA THE "GET SYSTEM TIME" COMMAND 18 FIGURE 25 - DATE AND TIME CHANGED VA THE "GET SYSTEM TIME" COMMAND 18 <tr< td=""><td>FIGURE 8 - UNPACKING SPYLOCK</td><td>7</td></tr<>	FIGURE 8 - UNPACKING SPYLOCK	7
FIGURE 10 - BATTERY LEVEL DISPLAYED 9 FIGURE 11 - LAST EVENT DISPLAYED 10 FIGURE 12 - DISPLAY SCROLL 1 10 FIGURE 13 - DISPLAY SCROLL 2 10 FIGURE 15 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 - DISPLAY SCROLL 3 10 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED 17 FIGURE 25 - EVENTS DOWNLOAD COMPLETED 18 FIGURE 26 - EVENTS TOOLOG RETORING DIFFERINT DOWNLOAD FILES 19 FIGURE 27 - FILE EVENTS 'FOLDER STORING DIFFERINT DOWNLOAD FILES 19 FIGURE 28 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 31 - SECURITY PASSWORD 2 21 FIGURE 32 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 34 - ERASE MEMORY ENTRY SECURITY PASSWORD 1 20 FIGURE 35 - DEVICE IN	FIGURE 9 - DISPLAY OF THE MESSAGE "DEVICE CLOSED"	8
FIGURE 11 - LAST EVENT DISPLAYSCOLL 1 10 FIGURE 12 - DISPLAY SCROLL 1 10 FIGURE 13 - DISPLAY SCROLL 3 10 FIGURE 14 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 - DISPLAY SCROLT A 10 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS YP BASED PC 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING 16 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - SPYLOCK HARAMETERS RETRIEVED 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED 17 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 28 - LOG FILE: AN EXAMPLE 19 FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 31 - SECURITY PASSWORD 2 21 FIGURE 32 - INSERTING THE CURRENT SECURITY PASSWORD 2 21 FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION 22 FIGURE 34 - INSE	FIGURE 10 - BATTERY LEVEL DISPLAYED	9
FIGURE 12 DISPLAY SCROLL 1 10 FIGURE 13 DISPLAY SCROLL 2 10 FIGURE 14 10 FIGURE 15 DISPLAY SCROLL 4 10 FIGURE 16 SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 DISPLAY SCROLL 4 10 FIGURE 16 DISPLAY SCROLL 4 10 FIGURE 17 DISPLAY SCROLL 4 10 FIGURE 16 DISPLAY SCROLL 4 10 FIGURE 17 DISPLAY SHOWS THE DEVICE ENTERING PROGRAMMING MODE 13 FIGURE 20 LOG INFORMATION ABOUT COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 21 PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 22 READING IN PROGRESS 16 FIGURE 23 READ OPERATION COMPLETED 17 FIGURE 24 SPYLOCK PARAMETERS RETRIEVED 17 FIGURE 25 DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND 18 FIGURE 26 EVENTS DOWNLOAD COMPLETED 18 FIGURE 27 "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 28 INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 31 <td>FIGURE 11 - LAST EVENT DISPLAYED</td> <td>.10</td>	FIGURE 11 - LAST EVENT DISPLAYED	.10
FIGURE 13 - DISPLAY SCROLL 2 10 FIGURE 14 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 - DISPLAY SCROLL 4 11 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND 18 FIGURE 26 - LOG FILE: AN EXAMPLE 19 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD COMPLETED 19 FIGURE 26 - LOG FILE: AN EXAMPLE 19 FIGURE 27 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 30 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 31 - SECURITY PASSWORD 2 21 FIGURE 32 - INSERTING THE CURRENT SECURITY PASSWORD 2 21 FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION	FIGURE 12 - DISPLAY SCROLL 1	.10
FIGURE 14 - DISPLAY SCROLL 3 10 FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 15 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 - DISPLAY SHOWS THE DEVICE ENTERING PROGRAMMING MODE 13 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 23 - READING IN PROGRESS 16 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED 17 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 28 - LOG FILE: AN EXAMPLE 19 FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 30 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 32 - INSERTING SECURITY PASSWORD 2 21 FIGURE 34 - EASSE MEMORY: CONFIRM OPERATION 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE 23 FIGURE 36 - INSERTING THE NEW SECURITY PASSWORD 2 23 FIGURE 37 - DESVICE IN BOOT LOADER MODE AND READY TO UPGRADE 23 <	FIGURE 13 - DISPLAY SCROLL 2	.10
FIGURE 15 - DISPLAY SCROLL 4 10 FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 17 - DISPLAY SHOWS THE DEVICE ENTERING PROGRAMMING MODE 13 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED 18 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 31 - SECURITY PASSWORD 1 200 FIGURE 32 - INSERTING SECURITY PASSWORD 1 200 FIGURE 33 - SECURITY PASSWORD 1 21 FIGURE 34 - SEASE MEMORY PERFORMED 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE 23 FIGURE 34 - ERASE MEMORY PERFORMED 22 <t< td=""><td>FIGURE 14 - DISPLAY SCROLL 3</td><td>.10</td></t<>	FIGURE 14 - DISPLAY SCROLL 3	.10
FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE 11 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC. 14 FIGURE 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC. 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT IN A WINDOWS XP BASED PC. 14 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING. 16 FIGURE 22 - READING IN PROGRESS. 16 FIGURE 23 - READ OPERATION COMPLETED. 17 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED. 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND. 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED. 19 FIGURE 27 - FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES. 19 FIGURE 28 - LOG FILE: AN EXAMPLE. 19 FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1. 200 FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 2. 21 FIGURE 31 - SECURITY PASSWORD 2 21 FIGURE 32 - ERASE MEMORY: CONFIRM OPERATION. 22 FIGURE 34 - ERASE MEMORY: CONFIRM OPERATION. 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE. 23 FIGURE 36 - INSERTING THE NEW SECURITY PASSWORD 2. 23 FIGURE 37 - INSERTING THE NEW SECURITY PASSWO	FIGURE 15 - DISPLAY SCROLL 4	.10
FIGURE 17 - DISPLAY SHOWS THE DEVICE ENTERING PROGRAMMING MODE 13 FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED 17 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED 18 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 28 - LOG FILE: AN EXAMPLE 19 FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1 200 FIGURE 30 - INSERTING THE CURRENT SECURITY PASSWORD 1 200 FIGURE 31 - SECURITY PASSWORD 1 MODIFIED 21 FIGURE 34 - ERASE MEMORY CONFIRM OPERATION 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE 23 FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 2 23 FIGURE 37 - INSERTING THE CURRENT SECURITY PASSWORD 2 23 FIGURE 36 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE 23 FIGURE 37 - INSERTING THE EVENENCE 24	FIGURE 16 - SPYLOCK MANAGEMENT SOFTWARE USER INTERFACE	.11
FIGURE 18 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC. 14 FIGURE 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS 7-8 BASED PC. 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING. 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING. 16 FIGURE 22 - READ OPERATION COMPLETED. 16 FIGURE 23 - READ OPERATION COMPLETED. 17 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED. 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND. 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED. 18 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES. 19 FIGURE 28 - LOG FILE: AN EXAMPLE. 19 FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1. 20 FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 1 20 FIGURE 31 - EXCURTY PASSWORD 1 MODIFIED. 21 FIGURE 32 - INSERTING SECURITY PASSWORD 2 21 FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION. 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE. 23 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE. 23 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE. 23 FIGURE 36 - INSERTING THE NEW SECUR	FIGURE 17 - DISPLAY SHOWS THE DEVICE ENTERING PROGRAMMING MODE	.13
FIGURE 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS 7-8 BASED PC 14 FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING. 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING. 16 FIGURE 22 - READING IN PROGRESS. 16 FIGURE 23 - READ OPERATION COMPLETED. 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND. 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED. 18 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES. 19 FIGURE 29 - INSERTING THE NEW SECURITY PASSWORD 1 20 FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 1 20 FIGURE 30 - INSERTING SECURITY PASSWORD 1 20 FIGURE 31 - SECURITY PASSWORD 2 21 FIGURE 32 - INSERTING SECURITY PASSWORD 2 21 FIGURE 34 - ERASE MEMORY: CONFIRM OPERATION. 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE. 23 FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 2. 23 FIGURE 37 - NERTING THE NEW SECURITY PASSWORD 2. 24 FIGURE 36 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE. 23 FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 2. 24 FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2. 24<	FIGURE 18 – HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS XP BASED PC	.14
FIGURE 20 - LOG INFORMATION ABOUT COM PORT OPENING. 15 FIGURE 21 - PASSWORD 1: EXAMPLE OF INSERTING. 16 FIGURE 22 - READING IN PROGRESS 16 FIGURE 23 - READ OPERATION COMPLETED. 17 FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED. 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND. 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED. 18 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES 19 FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1 20 FIGURE 31 - SECURITY PASSWORD 1 20 FIGURE 32 - INSERTING SECURITY PASSWORD 1 20 FIGURE 34 - ERASE MEMORY CONFIRM OPERATION. 21 FIGURE 34 - ERASE MEMORY CONFIRM OPERATION. 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE 23 FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 2 23 FIGURE 37 - INSERTING THE CURRENT SECURITY PASSWORD 2 24 FIGURE 36 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE 23 FIGURE 37 - INSERTING THE CURRENT SECURITY PASSWORD 2 24 FIGURE 43 - ONLICING THE NEW SECURITY PASSWORD 2 24	FIGURE 19 - HOW TO DETECT THE CONNECTED COM PORT IN A WINDOWS 7-8 BASED PC	.14
FIGURE 21 – PASSWORD 1: EXAMPLE OF INSERTING16FIGURE 22 – READING IN PROGRESS16FIGURE 23 – READ OPERATION COMPLETED17FIGURE 24 – SPYLOCK PARAMETERS RETRIEVED17FIGURE 25 – DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND18FIGURE 26 – EVENTS DOWNLOAD COMPLETED18FIGURE 27 – "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES19FIGURE 28 – LOG FILE: AN EXAMPLE19FIGURE 29 – INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 30 – INSERTING THE NEW SECURITY PASSWORD 120FIGURE 31 – SECURITY PASSWORD 221FIGURE 32 – INSERTING SECURITY PASSWORD 221FIGURE 34 – ERASE MEMORY: CONFIRM OPERATION22FIGURE 35 – DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 – INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 – INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 36 – INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 – INSERTING THE CURRENT SECURITY PASSWORD 224FIGURE 38 – CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 – SECURITY PASSWORD 224FIGURE 40 – DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 – BOOTLOADER MODE AND READY FOR FW UPGRADE25FIGURE 42 – USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 – SELECTION OF FW UPGRADE FILE27FIGURE 44 – FW FLASHING OPERATION ACTIVATED28FIGURE 45 – FIRMWARE UPGRADE STARTED28FIGURE 45 – FIRMWARE UPGRADE STARTED28<	FIGURE 20 – LOG INFORMATION ABOUT COM PORT OPENING	.15
FIGURE 22 - READING IN PROGRESS16FIGURE 23 - READ OPERATION COMPLETED17FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED17FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND18FIGURE 26 - EVENTS DOWNLOAD COMPLETED18FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES19FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 30 - INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 31 - SECURITY PASSWORD 120FIGURE 33 - ENSERTING SECURITY PASSWORD 221FIGURE 33 - ENSERTING SECURITY PASSWORD 221FIGURE 34 - ERASE MEMORY ICONFIRM OPERATION22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 39 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 41 - BOOT LOADER MODE AND READY FOR FW UPGRADE24FIGURE 43 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 41 - BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOT LOADER HOST26FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - EVER HASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE COMPLETED<	FIGURE 21 – PASSWORD 1: EXAMPLE OF INSERTING	.16
FIGURE 23 - READ OPERATION COMPLETED.17FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED.17FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND18FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND18FIGURE 26 - EVENTS DOWNLOAD COMPLETED.18FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES19FIGURE 28 - LOG FILE: AN EXAMPLE.19FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1.20FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 1.20FIGURE 31 - SECURITY PASSWORD 1 MODIFIED.21FIGURE 32 - INSERTING SECURITY PASSWORD 2.21FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION.22FIGURE 34 - ERASE MEMORY PERFORMED.22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE.23FIGURE 36 - INSERTING THE NEW SECURITY PASSWORD 2.23FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 2.24FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2.24FIGURE 39 - SECURITY PASSWORD 2 MODIFIED.25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE.25FIGURE 41 - BOOTLOADER MODE AND READY FOR FW UPGRADE.25FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED.27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED.28FIGURE 44 - FW FLASHING OPERATION ACTIVATED.28FIGURE 45 - FIRMWARE UPGRADE COMPLETED.29FIGURE 45 - FIRMWARE UPGRADE COMPLETED.29FIGURE 45 - FIRMWARE UPGRA	FIGURE 22 – READING IN PROGRESS	.16
FIGURE 24 - SPYLOCK PARAMETERS RETRIEVED. 17 FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND. 18 FIGURE 26 - EVENTS DOWNLOAD COMPLETED. 18 FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES. 19 FIGURE 28 - LOG FILE: AN EXAMPLE. 19 FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 1. 20 FIGURE 30 - INSERTING THE CURRENT SECURITY PASSWORD 1. 20 FIGURE 31 - SECURITY PASSWORD 1 MODIFIED. 21 FIGURE 32 - INSERTING SECURITY PASSWORD 2. 21 FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION. 22 FIGURE 34 - ERASE MEMORY PERFORMED. 22 FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE. 23 FIGURE 36 - INSERTING THE NEW SECURITY PASSWORD 2. 23 FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 2. 24 FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2. 24 FIGURE 39 - SECURITY PASSWORD 2 MODIFIED. 25 FIGURE 39 - SECURITY PASSWORD 2 MODIFIED. 25 FIGURE 41 - BOOTLOADER MODE AND READY FOR FW UPGRADE 25 FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED 27 FIGURE 44 - FW FLASHING OPERATION ACTIVATED 28	FIGURE 23 – READ OPERATION COMPLETED	.17
FIGURE 25 - DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND18FIGURE 26 - EVENTS DOWNLOAD COMPLETED18FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES19FIGURE 28 - LOG FILE: AN EXAMPLE19FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 120FIGURE 31 - SECURITY PASSWORD 1 MODIFIED21FIGURE 32 - INSERTING SECURITY PASSWORD 221FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION22FIGURE 34 - ERASE MEMORY: CONFIRM OPERATION22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 225FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER HOST25FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 44 - FW CLASTING COMPLETED29FIGURE 44 - FUB CONNECTOR30FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION	FIGURE 24 – SPYLOCK PARAMETERS RETRIEVED	.17
FIGURE 26 - EVENTS DOWNLOAD COMPLETED18FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES19FIGURE 28 - LOG FILE: AN EXAMPLE19FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 120FIGURE 31 - SECURITY PASSWORD 1 MODIFIED21FIGURE 32 - INSERTING SECURITY PASSWORD 221FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION22FIGURE 34 - ERASE MEMORY PERFORMED22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 41 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED29FIGURE 46 - FIRMWARE UPGRADE STARTED20FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION RETIONELE30	FIGURE 25 – DATE AND TIME CHANGED VIA THE "GET SYSTEM TIME" COMMAND	.18
FIGURE 27 - "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES19FIGURE 28 - LOG FILE: AN EXAMPLE.19FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 120FIGURE 31 - SECURITY PASSWORD 1 MODIFIED21FIGURE 32 - INSERTING SECURITY PASSWORD 221FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION22FIGURE 34 - ERASE MEMORY PERFORMED22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER MODE AND READY FOR FW UPGRADE25FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE STARTED29FIGURE 47 - USB CONNECTION30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 26 – EVENTS DOWNLOAD COMPLETED	.18
FIGURE 28 - LOG FILE: AN EXAMPLE.19FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 120FIGURE 31 - SECURITY PASSWORD 1 MODIFIED21FIGURE 32 - INSERTING SECURITY PASSWORD 221FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION.22FIGURE 34 - ERASE MEMORY PERFORMED.22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER MODE AND READY FOR FW UPGRADE25FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 27 – "FILE EVENTS" FOLDER STORING DIFFERENT DOWNLOAD FILES	.19
FIGURE 29 - INSERTING THE CURRENT SECURITY PASSWORD 120FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 120FIGURE 31 - SECURITY PASSWORD 1 MODIFIED21FIGURE 32 - INSERTING SECURITY PASSWORD 221FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION22FIGURE 34 - ERASE MEMORY PERFORMED22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 39 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER HOST26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 45 - FIRMWARE UPGRADE STARTED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 28 – LOG FILE: AN EXAMPLE	.19
FIGURE 30 - INSERTING THE NEW SECURITY PASSWORD 120FIGURE 31 - SECURITY PASSWORD 1 MODIFIED21FIGURE 32 - INSERTING SECURITY PASSWORD 221FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION22FIGURE 34 - ERASE MEMORY PERFORMED22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER HOST26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 29 – INSERTING THE CURRENT SECURITY PASSWORD 1	.20
FIGURE 31 – SECURITY PASSWORD 1 MODIFIED21FIGURE 32 – INSERTING SECURITY PASSWORD 221FIGURE 33 – ERASE MEMORY: CONFIRM OPERATION22FIGURE 34 – ERASE MEMORY PERFORMED22FIGURE 35 – DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 – INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 – INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 – CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 – SECURITY PASSWORD 2 MODIFIED25FIGURE 40 – DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 – BOOTLOADER MODE AND READY FOR FW UPGRADE26FIGURE 42 – USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 – SELECTION OF FW UPGRADE FILE27FIGURE 44 – FW FLASHING OPERATION ACTIVATED28FIGURE 45 – FIRMWARE UPGRADE STARTED28FIGURE 47 – USB CONNECTOR20FIGURE 47 – USB CONNECTOR20FIGURE 48 – USB CONNECTOR30FIGURE 48 – USB CONNECTOR30FIGURE 49 – CHARGING OPERATION EVIDENCE30	FIGURE 30 – INSERTING THE NEW SECURITY PASSWORD 1	.20
FIGURE 32 - INSERTING SECURITY PASSWORD 221FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION.22FIGURE 34 - ERASE MEMORY PERFORMED.22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 2.23FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 2.24FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2.24FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE.25FIGURE 41 - BOOTLOADER HOST.26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CONNECTOR30FIGURE 48 - USB CONNECTON30FIGURE 48 - USB CONNECTON30FIGURE 49 - CHARGING OPERATION EVIDENCE.30	FIGURE 31 – SECURITY PASSWORD 1 MODIFIED	.21
FIGURE 33 - ERASE MEMORY: CONFIRM OPERATION.22FIGURE 34 - ERASE MEMORY PERFORMED.22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 2.23FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 2.24FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2.24FIGURE 39 - SECURITY PASSWORD 2 MODIFIED.25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE.25FIGURE 41 - BOOTLOADER MODE AND READY FOR FW UPGRADE.26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED.27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED.28FIGURE 45 - FIRMWARE UPGRADE STARTED.28FIGURE 46 - FIRMWARE UPGRADE COMPLETED.29FIGURE 47 - USB CONNECTOR.30FIGURE 48 - USB CABLE CONNECTION30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE.30	FIGURE 32 – INSERTING SECURITY PASSWORD 2	.21
FIGURE 34 - ERASE MEMORY PERFORMED.22FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 2.23FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 2.24FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2.24FIGURE 39 - SECURITY PASSWORD 2 MODIFIED.25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE.25FIGURE 41 - BOOTLOADER HOST.26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED.27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED.28FIGURE 45 - FIRMWARE UPGRADE STARTED.28FIGURE 46 - FIRMWARE UPGRADE COMPLETED.29FIGURE 47 - USB CONNECTOR.30FIGURE 48 - USB CONNECTOR.30FIGURE 49 - CHARGING OPERATION EVIDENCE.30	FIGURE 33 – ERASE MEMORY: CONFIRM OPERATION	.22
FIGURE 35 - DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE23FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 223FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER HOST26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 34 – ERASE MEMORY PERFORMED.	.22
FIGURE 36 - INSERTING THE CURRENT SECURITY PASSWORD 2.23FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 2.24FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2.24FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE.25FIGURE 41 - BOOTLOADER HOST.26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 35 – DEVICE IN BOOT LOADER MODE AND READY TO UPGRADE	.23
FIGURE 37 - INSERTING THE NEW SECURITY PASSWORD 224FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 224FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER HOST26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 36 – INSERTING THE CURRENT SECURITY PASSWORD 2	.23
FIGURE 38 - CONFIRMING THE NEW SECURITY PASSWORD 2.24FIGURE 39 - SECURITY PASSWORD 2 MODIFIED.25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE.25FIGURE 41 - BOOTLOADER HOST.26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED.27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED.29FIGURE 47 - USB CONNECTOR.30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE.30	FIGURE 37 – INSERTING THE NEW SECURITY PASSWORD 2	.24
FIGURE 39 - SECURITY PASSWORD 2 MODIFIED25FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE25FIGURE 41 - BOOTLOADER HOST26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 38 – CONFIRMING THE NEW SECURITY PASSWORD 2	.24
FIGURE 40 - DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE.25FIGURE 41 - BOOTLOADER HOST.26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 39 – SECURITY PASSWORD 2 MODIFIED	.25
FIGURE 41 - BOOTLOADER HOST.26FIGURE 42 - USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 - SELECTION OF FW UPGRADE FILE.27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 40 – DEVICE IN BOOT LOADER MODE AND READY FOR FW UPGRADE	.25
FIGURE 42 – USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED27FIGURE 43 – SELECTION OF FW UPGRADE FILE27FIGURE 44 – FW FLASHING OPERATION ACTIVATED28FIGURE 45 – FIRMWARE UPGRADE STARTED28FIGURE 46 – FIRMWARE UPGRADE COMPLETED29FIGURE 47 – USB CONNECTOR30FIGURE 48 – USB CABLE CONNECTION30FIGURE 49 – CHARGING OPERATION EVIDENCE30	FIGURE 41 – BOOTLOADER HOST	.26
FIGURE 43 - SELECTION OF FW UPGRADE FILE27FIGURE 44 - FW FLASHING OPERATION ACTIVATED28FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 42 – USB HUMAN INTERFACE DEVICE CLASS TO BE SELECTED	.27
FIGURE 44 – FW FLASHING OPERATION ACTIVATED28FIGURE 45 – FIRMWARE UPGRADE STARTED28FIGURE 46 – FIRMWARE UPGRADE COMPLETED29FIGURE 47 – USB CONNECTOR30FIGURE 48 – USB CABLE CONNECTION30FIGURE 49 – CHARGING OPERATION EVIDENCE30	FIGURE 43 – SELECTION OF FW UPGRADE FILE	.27
FIGURE 45 - FIRMWARE UPGRADE STARTED28FIGURE 46 - FIRMWARE UPGRADE COMPLETED29FIGURE 47 - USB CONNECTOR30FIGURE 48 - USB CABLE CONNECTION30FIGURE 49 - CHARGING OPERATION EVIDENCE30	FIGURE 44 – FW FLASHING OPERATION ACTIVATED	.28
FIGURE 46 – FIRMWARE UPGRADE COMPLETED 29 FIGURE 47 – USB CONNECTOR 30 FIGURE 48 – USB CABLE CONNECTION 30 FIGURE 49 – CHARGING OPERATION EVIDENCE 30	FIGURE 45 – FIRMWARE UPGRADE STARTED	.28
FIGURE 47 – USB CONNECTOR 30 FIGURE 48 – USB CABLE CONNECTION 30 FIGURE 49 – CHARGING OPERATION EVIDENCE 30	FIGURE 46 – FIRMWARE UPGRADE COMPLETED	.29
FIGURE 48 – USB CABLE CONNECTION	FIGURE 47 – USB CONNECTOR	.30
FIGURE 49 – CHARGING OPERATION EVIDENCE	FIGURE 48 – USB CABLE CONNECTION	.30
	FIGURE 49 – CHARGING OPERATION EVIDENCE	.30



1. Description of the device

SPYLOCK is an electronic reusable locking system of latest generation, designed for specific application in industry, transport and logistics and ideal solution to monitor moving of bags, cases, trolleys, etc. Easy to install and use it needs minimum maintenance and can work autonomously for very long time.

The following picture shows the main components of the device:



Figure 1 - SPYLOCK overview



1.1 SPYLOCK views



Figure 2 - SPYLOCK Top view



Figure 3 - SPYLOCK side view



Figure 4 - SPYLOCK rear view

Page 5 of 31

SPYLOCK User Guide_ EN v1.0





Figure 5 - SPYLOCK View of open cable



Figure 6 - SPYLOCK View of closed cable



Figure 7 - SPYLOCK View of connectors



2. Notice

- Keep carefully this User Guide for future use.
- Keep SPYLOCK far from children.
- Do not plunge the device into water or other liquids.
- When opening the package, check the device integrity and specifically check that SPYLOCK is not damaged because of improper transportation or handling.
- SPYLOCK is a maintenance-free device.
- SPYLOCK is power supplied by a rechargeable, Lithium long-life battery, which assures long operation time.
- SPYLOCK cannot be opened by the user, to access internal electronics.
- Opening the device can lead to damage of the same, to alter the characteristics of the product and void your warranty.

3. Accessories

When opening the package, check it include the following accessories:

- Pcs 1 SPYLOCK
- Pcs 1 USB memory stick with user guides, documentation, application software, drivers.
- Pcs 1 USB cable







4. Device set up

SPYLOCK installation is easy and fast. Quick user guide for device set up :

- Put SPYLOCK in place;
- Pass the SPYLOCK cable inside container handle holes and insert its tail into the SPYLOCK hole by keeping the locking button pushed;
- When the cable is in release the locking button to block the cable;
- Pull the cable up to check that it is properly closed. If the operation is done correctly, the device display shows the message "CLOS" to acknowledge the proper locking (see picture below).



Figure 9 - Display of the message "device closed"

• The device in in operation and ready to log events.

5. Technical specifications

Material	ABS
IP Protection	IP65
Operative Temperature	- 20°C / +55 °C
Storage Temperature	- 20°C / +55 °C
Size	131 x 67 x 35 mm
Wire standard lenght	110 mm
Wire diameter	2,5 mm
Wire material	Stainless steel
Weight	180 g
	Closing actuator coupling with spring
Mechanical closure	button
Display	Backlit White, 32 characters (2 x 16)
Communication interface	USB
Battery	Rechargeable 1100 mAh 3,7V
Memory storage	1000 data record
Password protection	Software
Tamper security	Sensor to detect case opening
Manufactured Code	UID CODE
Management Code	Software Code
RFID	HF NFC Tag



6. Device functions

The working principle of SPYLOCK is very simple: it acts as a logger of vents on the lock. It can register if and when one or more of the following events take place:

- Cable open OPEN
- Cable closed
 CLOS
- Cable cut
 CUT
- Tamper when case open TAOP
- Tamper when case closed TACL
- Low battery
 LOW
- General Error ERR

Moreover the device gives information about the battery level, at any switch on of the device:

- Valore 100 Battery fully charged;
- Valore 0 Battery fully discharged.

When the battery level is below level 36%, the display show the additional information of LOW BATTERY. In the LOW BATTERY mode the display backlight is deactivated.

When the battery level is below 20% SPYLOCK enters protection mode and automatically switches off. Battery recharge is necessary to switch it on again.

Typical battery life is of 700 cycles, where each cycle is composed by the three events opening/closure/push of the navigation button.

6.1 Description of the device functioning

SPYLOCK is an electronic device permanently idling in its stand-by status until one of the above mentioned events occur.

When one of those event occur SPYLOCK starts operating with the following operations:

- The display lights showing the detected event
- The event is stored into the device memory (type of event and time stamp)
- It is possible to display at any time SPYLOCK battery level by pressing for 1 sec. the navigation button. If the button is kept pushed the vent log is show step by step in a descending time mode.

The device is supplied by an USB rechargeable battery (see section 10 *SPYLOCK recharge*). When pushing the navigation button the display shows for 2 sec. the battery level:



Figure 10 - Battery level displayed

Immediately after the last stored event is displayed for 5 sec. and if no other event is activated, the display switches off automatically.





Figure 11 - Last event displayed

The message displays the following information:

- Serial identification number of the event (e.g. 0020)
- Event short description (e.g. CLOS = cable closed)
- Number associated to the vent and randomly generated by SPYLOCK (e.g. 701782)
- Event date (e.g. 16-07-15)
- Event time (e.g. 09:15)

If after displaying the last occurred even the navigation button is sequentially pushed, the display scrolls the SPYLOCK stored events by descending time of registration.



Figure 12 - Display scroll 1



Figure 14 - Display scroll 3



Figure 13 - Display scroll 2



Figure 15 - Display scroll 4



7. Spylock Management Software

"SPYLOCK MANAGEMENT Software" allows connecting PC to the device to modify its date and time, to modify the security passwords, to display and download events log, to erase memory, to display firmware version and eventually upgrade it.

When launching the program, the following main application window opens:



Figure 16 - SPYLOCK MANAGEMENT Software user interface



NOTE: "SPYLOCK MANAGEMENT Software" is an application software able to work under the environment of WINDOWS OS, 32 and 64 bit (Win XP, Win 7, Win Vista, Win8.1).

"CONNECTING" area:

COM PORT: shows the COM port number as assigned by Windows OS to which the SPYLOCK is to be connected (see also Section 7.1. – *Programming Mode*).

"PASSWORD" area: Manage passwords useful to set/manage SPYLOCK PASSWORD 1: security password PSW1: 000000 (n° 6 zeros). PASSWORD 2: security password PSW2: 000000 (n° 6 zeros). (see also Section 7.2 - Password Management)

"READ/PROGRAM" area: READ/PROGRAM DEVICE PARAMETERS "READ" button: when pushed it retrieves curr

"READ" button: when pushed it retrieves current SPYLOCK settings. "PROGRAM" button: used to program new settings into the SPYLOCK.

"SW RELEASE" area:

It displays the release number of the "SPYLOCK MANAGEMENT Software"

"DATA" area: Information about the SPYLOCK device

ID Product:	Numerical and univocal ID device code set by the manufacturer (6 digits)
ID:	Numerical ID device code set by the user (6 digits)
DATE:	Displays the date set on SPYLOCK
HOUR:	Displays the time set on SPYLOCK
NUMBER EVENTS:	Displays the number of events stored inside SPYLOCK memory
FW REVISION:	Displays SPYLOCK firmware version
GET SYSTEM TIME button:	Update date and time on SPYLOCK

NOTE: date and time are updated by using PC settings, so please check that PC date and time are correct.

"DEBUG BOX" area:

DEBUG

Displays operation currently performed by SPYLOCK (log of messages exchange between SPYLOCK and the management software).

"PASSWORD MANAGEMENT" area: MODIFICA PASSWORD

Allows setting or change of security passwords. (see also Section 7.2 - *Password Management*)

"BOOTLOADER" area: UPGRADE FW

"BOOT" button: SPYLOCK exits from operational mode and enters into UPGRADE Firmware mode. (see Section 8.0 - *FW Upgrade*) NOTE: it is strongly recommended that this operation is performed by a highly qualified technical staff or with the support of the device manufacturer.

TOOLBAR READ/WRITE PROGRESS



Toolbar that display the progress of current SPYLOCK activity.

"ERASE MEMORY" area:

ERASE MEMORY

"ERASE" button: permanently erases all the events stored in SPYLOCK.

"EVENTS" area: DOWNLOAD OF REGISTERED EVENTS

"DOWLOAD" button: enables the download of all teh registered events from the SPYLOCK to the PC. NOTA: downloaded data are permanently removed from the SPYLOCK.

EXIT button:

Exits the program.

7.1 Programming Mode

This is the procedure to enter device programming mode:

- 1 Launch "SPYLOCK Management Software"
- 2 Check that the device is with open cable NOTE: Only if the SPYLOCK cable is OPEN, the device can enter programming mode
- 3 Connect the USB cable between SPYLOCK and the PC (when the operation is properly done the SPYLOCK display shows the message "Programming").



Figure 17 - Display shows the device entering Programming Mode

4 Check at which COM port the device has connected. For PC Windows®: right click of the mouse on *This PC→Manage→ Device Manager* e aprire il menù *Ports (COM & LPT)* has shown in Figure 18 and Figure 19. The device port can be easily identified as "Cypress USB UART (COM X)" where X is the port number to be inserted into the Spylock Management Software window for connection.





Figure 18 – How to detect the connected COM port in a Windows XP based PC



Figure 19 - How to detect the connected COM port in a Windows 7-8 based PC

Insert the right COM Port number into the software user interface, push the "CONNECT" button; when the COM port communication is properly set the button status changes from "CONNECT" to "DISCONNECT". If the COM port number is higher than 9 it is possible to insert the COM port number manually: for instance if the detected COM port is the number 32, please digit into the relevant field COM32.



A SPYLOCK Management Software		
CONNECTING	READ/PROGRAM PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
PASSWORD		DEBUG BOX
PASSWORD 1 PASSWORD 2 DATA ID Product DATE DATE DATE DATE DATE DATE DATE		Directory 'File Events' is created Starting Prog Aggiorno data e ora con quelle di sistema Premuto Pulsante Connect Porta Disconnessa -> tento connessione Try to open port Porta COM aperta correttamente Set COM ok Set COM Timeouts ok
(DD/MM/YEAR) 9 7 2015 Non HOUR (HH/MM) 16 2 FW1 GET SYSTEM TIME FW1	REVISION	Through the debug window it is possible to get additional information about the status of the COM port. Here it is the log information showing that the COM port is properly open and that the device is connected.
MODIFY PASSWORD 1		800T
INSERT OLD PASSWORD 1	SEND	
MODIFY PASSWORD 2	SEND	ERASE MEMORY EVENTS
		EXIT

Figure 20 – Log information about COM Port opening

7.2 Password management

SPYLOCK security is guaranteed by a two-level password.

Security Password no. 1 is requested to access the standard settings of the device and of its main functional parameters. Security Password no. 2 is required for the management of advanced settings. These passwords are stored inside the SPYLOCK Flash Memory.

Default:000000 (6 zeros)Security passwordPSW1:000000 (6 zeros)000000 (6 zeros)000000 (6 zeros)

NOTE: In case you forgot the passwords, you need to contact the manufacturer back.

7.2.1 Security Password 1 and its functionality

To access "SPYLOCK Management Software " it is necessary to insert Security Password 1 and push the button SEND. Once inserted this password correctly, it will be possible, other than performing the parameters reading, to set date and time by sybchronising them with the PC ones, change Security Password 1, download registered events, etc.



COM PORT: Disconnect PROGRAM READ SPYLOCK15 PROGRAMMER VER 7 ASSWORD ASSWORD 1 SEND DEBUG BOX Sento 100000 Disconnect Porta Disconnect 1000000 Disconnect 10000000 Disconnect 10000000 D	ONNECTING	READ/PROGRAM	
ASSWORD PASSWORD 1 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 1 D POULT D POULT D POULT D D D D D D D D D D D D D D D D D D D	COM PORT : Com 98	Disconnect PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
PASSWORD 1 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 2 PATA DP roduct D D DOUCD	ASSWORD		DEBUG BOX
PASSWORD 2 SEND DATA Privatic of data e ora con quelle di sistema Premuto pulsante Connect Porta Disconessa -> tento connessione Try to open port Porta COM aperta correttamente Set COM Timeouts ok 'Check password Data to Program:000000 Dati multipuesto (CD/MM/YEAR) DATE ID Product 000000 DATE ID Product 000000 DATE (CD/MM/YEAR) 9 7 2015 NUMBER EVENTS HOUR (HH/MM) 17 GET SYSTEM TIME MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 SEND	PASSWORD 1	SEND	Directory 'File Events' is created Starting Prog
DATA DATA ID Product 000000 ID 000000 DATE (DD/MM/YEAR) 9 7 2015 NUMBER EVENTS CD/MM/YEAR) 17 10 FW REVISION GET SYSTEM (HH/MM) 17 10 FW REVISION GET SYSTEM INSERT OLD PASSWORD 1 SEND MODIFY PASSWORD 1 SEND MODIFY PASSWORD 2 SEND INSERT OLD PASSWORD 2 SEND DEVINE COMPARENT MODIFY PASSWORD 2 SEND ERASE MEMORY EVENTS ERASE DOWNLOAD	PASSWORD 2	SEND	Aggiorno data e ora con quelle di sistema Premuto Pulsante Connect Porta Disconnessa -> tento connessione
ID Product 000000 ID 000000 ID 000000 ID 000000 Consistence of the second secon	ATA		Porta COM aperta correttamente Set COM ok
DATE 9 7 2015 NUMBER EVENTS Dati invisit HOUR 17 10 PW REVISION GET SYSTEM INSERT OLD PASSWORD 1 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 SEND ERASE MEMORY EVENTS	ID Product 000000	- ID 000000	Set COM Timeouts ok 'Check password
COD/MM/YEAR) 9 7 2015 NOMEL CUTITS HOUR (HH/MM) 17 10 FW REVISION GET SYSTEM INSERT OLD PASSWORD 1 BOOTLOADER MODIFY PASSWORD 1 SEND INSERT OLD PASSWORD 2 SEND	DATE La La		Data to Program:00000 Dati inviati Birevuto OK
HOUR (HI/MM) 17 10 FW REVISION GET SYSTEM TIME PASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 SEND ERASE MEMORY ERASE DOWNLOAD	(DD/MM/YEAR) 9 7 201:	NOPIDER EVENTS	
GET SYSTEM TIME PASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 SEND ERASE MEMORY EVENTS EVENTS EVENTS	HOUR 17 10 (HH/MM)	FW REVISION	
ASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 SEND BOOT ERASE MEMORY ERASE ERASE DOWNLOAD	GET SYSTEM		
PASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 SEND BOOTLOADER BOOT	TIME		
MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 INSERT OLD PASSWORD 2 SEND ERASE MEMORY EVENTS EVENTS EVENTS	ASSWORD MANAGEMENT		BOOTLOADER
INSERT OLD PASSWORD 1 SEND ERASE MEMORY EVENTS EV	MODIFY PASSWORD 1		BOOT
MODIFY PASSWORD 2 INSERT OLD PASSWORD 2 SEND ERASE EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EVENTS EV	INSERT OLD PASSWORD 1	SEND	
INSERT OLD PASSWORD 2 SEND ERASE DOWNLOAD	MODIFY PASSWORD 2		ERASE MEMORY EVENTS
	INSERT OLD PASSWORD 2	SEND	ERASE DOWNLOAD

Figure 21 – Password 1: example of inserting

7.2.2 Reading of parameters

Push the READ button to get the working device parameters. The toolbar will show the progress of this operation.

ONNECTING	READ/PROGRAM	
COM PORT : com48	PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
ASSWORD		DEBUG BOX
PASSWORD 1 PASSWORD 2	SEND SEND	Dato RX estrapolato:9/7/15 Read Par:5 Dati inviati Attende risposta: Par 5
ATA		KX String:\$5.17.25#3
ID Product 000000	ID 000007	Data for sponsor 1723 Data inviati Attende risposta: Par 12 Data Science 100001281
DATE 09 07 2015	NUMBER EVENTS 0012	- Dato RX estrapolato:0012 Read PariZ
HOUR 17 25 (HH/MM) GET SYSTEM	FW REVISION Firmware v1.32	 Dati inviati Attender risposta: Par 13 Rx String:\$Z.Firmware v1.32#f Dato RX estrapolato:Firmware v1.32
1 IME		Read OK
		BOOTLOADER
INSERT OLD PASSWORD 1	SEND	воот
MODIFY PASSWORD 2		ERASE MEMORY EVENTS
INSERT OLD PASSWORD 2	SEND	ERASE

Figure 22 – Reading in progress



ONNECTING	READ/PROGRAM	
COM PORT : com48	Disconnect PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
ASSWORD		DEBUG BOX
PASSWORD 1	SEND	Dato RX estrapolato:9/7/15
PASSWORD 2	SEND	Read Par:5 Dati inviati
		Attende risposta: Par 5 Rx String:\$5.17.25#§
ATA		Dato RX estrapolato:17.25
ID Product 000000	ID Program Spy-Lock15	Read Partu Dati inviati Attende richocta: Par 12
NATE In Int		Rx String:\$D.0012#]
(DD/MM/YEAR) 09 07 201		Dato RX estrapolato:0012 Read Par:Z
HOUR 17 25	FW REVISION	Dati inviati Attende risposta: Par 13
GET SYSTEM		Rx String:\$Z.Firmware v1.32#f
TIME		Dato RX estrapolato:Firmware v1.32 Read OK
ASSWORD MANAGEMENT		BOOILOADER
INSERT OLD PASSWORD 1	SEND	BOOT
MODIFY PASSWORD 2		ERASE MEMORY EVENTS
INSERT OLD PASSWORD 2	SEND	ERASE DOWNLOAD



🍰 SPYLOCK Management Software	
CONNECTING READ/PROGRAM	SPYLOCK15 PROGRAMMER VEB 7
PASSWORD	N. eventi memorizzati
PASSWORD 1 SEND	Dato RX estrapolato: 10/7/15 Read P#:5 Dati inflati Attegde risposta: Par 5
ID O00000 ID 000007 DATE (DD/MM/VEBR) 9 07 2015 AUMBER EVENTS 0021 HOUR (HH/MM) 17 25 FW REVISION Firmware v1.32	R: tring:\$5.14.54#; Pato RX estrapolato:14.54 Read Par:D Dati inviati Attende risposta: Par 12 R: String:\$D.0021#] Dato RX estrapolato:0021 Read Par:2 Dati inviati Attende risposta: Par 13 R: String:\$2.Firmware V1.32#f
	Dato RX estrapolato:Firmware v1.32
PASSWURU MANAVEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 1 SEND	BOOTLOADER
MODIFY FASSWORD 2 INSERT OF PASSWORD 2 Data/ora	ERASE MEMORY EVENTS ERASE DOWNLOO Versione FW

Figure 24 – SPYLOCK parameters retrieved



7.2.3 Date and time update with system data

Push the button "GET SYSTEM TIME" to acquire date nad time currently set inside SPYLOCK.

CONNECTING	READ/PROGRAM	
COM PORT : com48	Disconnect PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
PASSWORD		
PASSWORD 1 PASSWORD 2 DATA DProduct D00000 DATE (D0/MM(YEAR) 10 7 20 HOUR (HH/MM) 15 1 GET SYSTEM TIME	ID 000007 ID 000007 IS NUMBER EVENTS 0021 FW REVISION Firmware v1.32	Read Par:5 Dati invitati Attender isposta: Par 5 R. String:55.14.54#; Dato RX estrapolato:14.54 Read Par:D Dati invitat Attender isposta: Par 12 R. String:30.0021#; Dato RX estrapolato:0021 Read Par:2 Dati invitat Attender isposta: Par 13 R. String:27.Firmware v1.32#; Dato RX estrapolato:Firme Aggiorno data e ora con quelle di sistema
PASSWORD MANAGEMENT MODIF PASSWORD 1 INSERT OLD PASSWORD 1	SEND	BOOTLOADER
MODIFY PASSWORD 2 INSERT OLD PASSWORD 2	SEND	ERASE MEMORY EVENTS
		EXIT

7.2.4 Download of the stored log

Push the "DOWNLOAD" button to download all the events stored in the SPYLOCK memory. The log is automatically retrieved and saved as cvs file in the folder "File Events", at the same where is the folder of the application SW "SPYLOCK Management Software".

ONNECTING	READ/PROGRAM	
COM PORT : com48	PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
ASSWORD		DEBUG BOX
PASSWORD 1 PASSWORD 2	SEND	Read Par:C Del mwel Rx: String:\$C.0004CLOS24384209-07-15 12:08#** Dato RX: estrapolato:0004CLOS24384209-07-15 12:08 Read Par:C Dati mvelat Rx: String:\$C.00030PEN05025309-07-15 12:08#*
ID Product 000000 DATE (D0)PMM/YEAR) 10 7 2015 HOUR (HH/MM) 15 1 GET SYSTEM TIME	ID Program Spy-Lock15 X NUMBER EVEN DOWNLOAD OKI FW REVISION OK	Dato RX estrapolato:0003OPEN05025309-07-15 12:08 Read Par:C Dati Nivát RX: String:\$C.0002CL0573154709-07-15 12:014# Dato RX: estrapolato:0002CL0573154709-07-15 12:014 Dato RX: estrapolato:0002CL0573154709-07-15 12:04 Dati Niváti RX: String:\$C.00010PEN97457509-07-15 12:04#i Dato RX: estrapolato:00010PEN97457509-07-15 12:04 Dato RX: estrapolato:00010PEN97457509-07-15 12:04 Dato RX: estrapolato:00010PEN97457509-07-15 12:04
ASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 1	SEND	BOOTLOADER
MODIFY PASSWORD 2 INSERT OLD PASSWORD 2	SEND	ERASE MEMORY EVENTS

Figure 26 – Events download completed





Figure 27 – "File Events" folder storing different Download files

"SPYLOCK Management software" automatically generates event log files downloaded from the SPYLOCK device. At each download operation a new file is generated and labelled with date and tiem at which the operation occurred.

1	Data:	01/07/2015			
2	Ora:	13.24.44			
3					
4	ID Product :	123456			
5	ID :	2			
6					
7	NUMBER EVENT	ТҮРЕ	NUMBER RANDOM	DATE	HOUR
8	84	OPEN	218460	01/07/2015	11.35
9	83	CLOSE	598004	30/06/2015	18.28
10	82	OPEN	325501	30/06/2015	18.28
11	81	CLOSE	976482	30/06/2015	18.28
12	80	OPEN	141181	30/06/2015	18.28
13	79	CLOSE	125611	30/06/2015	18.28
14	78	OPEN	25670	30/06/2015	18.28
15	77	CLOSE	471589	30/06/2015	16.59
16	76	TACL	109769	30/06/2015	16.56
17	75	TAOP	50519	30/06/2015	16.55
18	74	TACL	766496	30/06/2015	16.55
19	73	OPEN	180768	30/06/2015	16.54
20	72	CLOSE	314847	30/06/2015	16.54
21	71	OPEN	544492	30/06/2015	16.54
22	70	CLOSE	776871	30/06/2015	16.54
23	69	OPEN	359630	30/06/2015	16.54
24	68	CUT	38776	30/06/2015	16.54
25	67	CLOSE	125873	30/06/2015	16.54

Figure	28 –	LOG	File:	an	example
--------	------	-----	-------	----	---------



7.2.5 How to change Password 1

To change Security Password 1 please follow the next steps:

1 Insert the current Security Password into the textbox "INSERT OLD PASSWORD 1" and press "SEND" button

CONNECTING	READ/PROGRAM	
COM PORT : com48	PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
PASSWORD		DEBUG BOX
PASSWORD 1 PASSWORD 2	SEND	 Dato RX estrapolato:0004CL0524384209-07-15 12:08 Read PartC Dati inviati Rx String:\$C.0003OPEN05025309-07-15 12:08#¹
DATA ID Product 000000 DATE (DD/MM/YEAR) 10 7 2015 HOUR (HH/MM) 15 1 GET SYSTEM TIME	ID 000007 NUMBER EVENTS 0021 FW REVISION Firmware v1.32	Date RX estrapolate:00030PEN05025309-07-15 12:08 Read Par:C Dati inviati R:String:\$C.0002CL0573154709-07-15 12:04#— Dato RX estrapolate:0002CL0573154709-07-15 12:04 Read Par:C Dati inviati R:String:\$C.00010PEN97457509-07-15 12:04#I Dato RX estrapolate:00010PEN97457509-07-15 12:04#I Dato RX estrapolate:00010PEN97457509-07-15 12:04 Modify PW0 1 Data to Program:000000 Data inviati Ricevuto OK
PASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT NEW PASSWORD 1	SEND	BOOTLOADER
MODIFY PASSWORD 2	SEND	ERASE MEMORY EVENTS

Figure 29 – Inserting the current Security Password 1

2 Insert the new Security Password into the textbox "INSERT NEW PASSWORD 1" and press "SEND" button

PROGRAM	SPYLOCK15 PROGRAMMER VER 7
	DEBUG BOX
SEND	▲ Dato RX estrapolato:0004CLOS24384209-07-15 12:08 Read Par:C Dati inviat RX String:\$€.0003OPEN05025309-07-15 12:08#
	Dato RX estrapolato:00030PEN05025309-07-15 12:08 Read Par:C Dati inviati Rx String:\$C.0002CL0573154709-07-15 12:04#- Dato RX estrapolato:0002CL0573154709-07-15 12:04 Read Par:C Dati inviati
EVISION Firmware v1.32	Rx String:\$C.00010PEN97457509-07-15 12:04#i Date RX estrapolate:00010PEN97457509-07-15 12:04 Download is finished! Modify PWD 1 Data to Program:000000 Data in Visit Ricevuto OK
SEND	BOOTLOADER
SEND	ERASE MEMORY EVENTS ERASE DOWNLOAD
	SEND 0000007 ER EVENTS 0021 EVISION Firmware v1.32

Figure 30 – Inserting the new Security Password 1



3

CONNECTING	READ/PROGRAM	
COM PORT : com48 💌 _ C	PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
PASSWORD		DEBUG BOX
PASSWORD 1	SEND	Dato RX estrapolato:0003OPEN05025309-07-15 12:0
PASSWORD 2	SEND	Read Par:C Dati inviati Rx String:\$C.0002CLOS73154709-07-15 12:04#—
DATA		Dato RX estrapolato:0002CLOS73154709-07-15 12:0 Read Par:C
ID Product	D Drogram Soy Lock 15	Dati inviati Rx String:\$C.00010PEN97457509-07-15 12:04#i
		Dato RX estrapolato:00010PEN97457509-07-15 12:0
DATE 10 7 2015 (DD/MM/YEAR)	NUMBER EVE Password 1 modified!	Modify PWD 1 Data to Program:000000
HOUR 15 1	FW REVISION OK	Dati inviati Ricevuto OK
GET SYSTEM		Modify PWD 1 Data to Program:000000
TIME		Ricevuto OK
PASSWORD MANAGEMENT		BOOTLOADER
MODIFY PASSWORD 1		BOOT
INSERT AGAIN NEW PASSWORD 1	* SEND	
MODIFY PASSWORD 2		ERASE MEMORY EVENTS
INSERT OLD PASSWORD 2	SEND	ERASE DOWNLOAD

Figure 31 – Security Password 1 modified

7.2.6 Security Password 2 and its functionality

Security Password 2 enables accessing advanced operations, as described in section 7.2 and in particular:

- Permanently erasing SPYLOCK memory
- Enabling FW upgrade
- Change Security Password 2

The level of Security Password 2 is accessed only after inserting properly security Password 1.

ONNECTING		READ	PROGRAM		
COM PORT :	com48 💌 Di	connect PR	OGRAM READ	SPYLOCK15 PROGRAMM	IER VER 7
ASSWORD				DEBUG BOX	
PASSWORD 1 PASSWORD 2			SEND SEND	Attende risposta: Par 5 Rx String:\$5.16.48#« Dato RX estrapolato:16.48 Read Par:D	
АТА				Attende risposta: Par 12 Rx String:\$D.0021#	
ID Product DATE (DD/MM/YEAR)	000000	ID NUMBER EVENTS	000007	Dato RX estrapolato:0021 Read Par:2 Dati invlati Attende risposta: Par 13 Rx String:\$2.Firmware v1.32#f	
Hour (hh/mm)	GET SYSTEM TIME	FW REVISION	Firmware v1.32	Dato RX estrapolato:Firmware v1.32 Read OK C'heck password Data to Program:000000 Data to triogram:000000 Ricevuto OK	
ASSWORD M	ANAGEMENT			BOOTLOADER	
INSERT OLD PA	SSWORD 1		SEND	BOOT	
MODIFY PAS	SSWORD 2			ERASE MEMORY EVE	NTS
INSERT OLD PA	SSWORD 2		SEND	ERASE	DOWNLOAD

Figure 32 – Inserting Security Password 2



7.2.7 Erasing memory

Push the "ERASE MEMORY" to format the device memory. **ATTENTION: all the stored events will be deleted !!!**

nnect PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
ID Program Spy-Lock15 NUMBER FW REVI Si No	Attende risposta: Par 5 Rx String:\$5.16.48#< Dato RX estrapolato:16.48 Read Par:D Deti mviati Attende risposta: Par 12 Rx String:\$0.0021#] Deto RX estrapolato:10021 Read Par:2 Dati mviati Attende risposta: Par 13 Rx String:\$2.Firmware v1.32#f Dato RX estrapolato:Firmware v1.32 Read OK 'Check password Data to Program:000000 Data to Program:000000 Data to KK
SEND	BOOTLOADER
SEND	ERASE MEMORY EVENTS
	ID ID ID IV IVINISER FW REVIS SEND SEND SEND SEND SEND SEND SEND SEN

Figure 33 – Erase memory: confirm operation

📆 SPYLOCK Management Software	🛛
CONNECTING COM PORT : com48 Jisconnect PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
PASSWORD	DEBUG BOX
PASSWORD 1	Attende risposta: Par 12 Rx String:\$D.0021#
PASSWORD 2	Dato RX estrapolato:0021 Read Par:Z Dati invisti Attende riposta: Par 13 Rx String:\$Z.Firmware v1.32#f
ID Product 000000 ID Program Spy-Lock15 X DATE (DD/MM/YEAR) 10 07 2015 NUMBER EVER Erased memory okl HOUR (HH/MM) 16 48 FW REVISION OK GET SYSTEM	Dato RX estrapolato:Firmware v1.32 Read OK 'Check password Data to Program:000000 Dati inviati Ricevuto OK Premuto pulsante Erase Program Par n.E Dati inviati Attende risposta: erasing memory Ricevuto OK Erased Memory OK
PASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 1 SEND	BOOTLOADER
MODIFY PASSWORD 2 INSERT OLD PASSWORD 2 SEND	ERASE MEMORY EVENTS
	EXIT

Figure 34 – Erase memory performed



7.2.8 How to enable firmware upgrade

Push the "BOOT" button; SPYLOCK display turns into "blank", the device exits the operational mode and enters Boot Loader mode to upgrade the firmware. Please refer also to section 8 – *Firmware upgrade*.

ONNECTING	READ/PROGRAM	
COM PORT : com48	PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
ASSWORD		
PASSWORD 1 PASSWORD 2	SEND SEND	Premuto Pulsante Connect Porta Disconnessa -> tento connessione Try to open port Porta COM aperta correttamente Set COM ok
ID Product 000000	ID Program Spy-Lock15	Det Corn Intelocus Vic 'Check password Data to Program:000000 Dati nvlati Ricevuto OK 'Check password Data to Program:000000
DATE (DD/MM/YEAR) 10 07 2015 HOUR (HH/MM) 16 48 GET SYSTEM TIME	NUMBER EVE Device in Bootloader	1 Dati inviati Ricevuto OK Premuto pulsante Boot Data to Program:boot Dati inviati Attender isposta: entry in boot Ricevuto OK
ASSWORD MANAGEMENT		BOOTLOADER
INSERT OLD PASSWORD 1	SEND	BOOT
MODIFY PASSWORD 2		ERASE MEMORY EVENTS
INSERT OLD PASSWORD 2	SEND	ED ASE DOWNLOAD

Figure 35 – Device in Boot Loader mode and ready to upgrade

7.2.9 How to change Password 2

To change Security Password 2 please follow the next steps:

1 Insert the current Security Password into the textbox "INSERT OLD PASSWORD 2" and press "SEND" button

ONNECTING		READ/PROGRAM		
COM PORT : com48	Disconnect	PROGRAM	SPYLOCK15 PR	OGRAMMER VER 7
ASSWORD			DEBUG BOX	
PASSWORD 1		SEND	Ricevuto OK Modify PWD 2	
PASSWORD 2		SEND	Data to Program:000000 Dati inviati Ricevuto OK	
ATA			Premuto Pulsante Connec Porta connessa -> tento Premuto Pulsante Connec	t disconnessione t
ID Product	ID	000007	Porta Disconnessa -> ten Try to open port	to connessione
000000		000007	Porta COM aperta corrett Set COM ok	amente
DATE 10 07	2015 NUMBER	EVENTS 0021	Set COM Timeouts ok 'Check password	
HOUR IS IS	EW DEVI	STON Gineman ut 22	Data to Program:000000 Dati inviati	
(HH/MM) 10 40	1.11.14	Finisher V1.32	Ricevuto OK 'Check password	
GET SYSTEM			Data to Program:000000 Dati inviati	
11ME			Ricevuto OK	
ASSWORD MANAGEMEN	r		BOOTLOADER	
MODIFY PASSWORD 1				1 TOO
INSERT OLD PASSWORD 1		SEND		
MODIFY PASSWORD 2			ERASE MEMORY	EVENTS
INSERT OLD PASSWORD 2	[******]	SEND	ERASE	DOWNLOAD

Figure 36 – Inserting the current Security Password 2



2 Insert the new Security Password into the textbox "INSERT NEW PASSWORD 2" and press "SEND" button

UNNECTING	READ/PROGRAM	
COM PORT : com48	PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
ASSWORD	DEB	UG BOX
PASSWORD 1	SEND	Ricevuto OK Modify PWD 2
PASSWORD 2	SEND	Data to Program:000000 Dati inviati Ricevuto OK Premuto Pulsante Connect
АТА		Porta connessa -> tento disconnessione Premuto Pulsante Connect
ID Product ID	000007	Try to open port Porta COM aperta correttamente
DATE 10 07 2015 NUMBE	REVENTS 0021	Set COM ok Set COM Timeouts ok 'Check password
HOUR 16 48 FW RE	ISION Firmware v1.32	Data to Program:000000 Dati inviati
(HH/MM)		Ricevuto OK 'Check password Data to Program:000000
GET SYSTEM TIME		Dati inviati Ricevuto OK
ASSWORD MANAGEMENT	BOO	JTLOADER
MODIFY PASSWORD 1		BOOT
	SEND	
MODIFY PASSWORD 2	ERA	SE MEMORY EVENTS
	CENID	

Figure 37 – Inserting the new Security Password 2

3 Confirm the new password

COM PORT: com48 Disconnect PROGRAM READ SPYLOCK15 PROGRAMMER VER 7 ASSWORD pASSWORD 1 SEND PROGRAM READ PROGRAMMER VER 7 ASSWORD 2 SEND SEND PROGRAM REVER 7 PROGRAMMER VER 7 DATA SEND SEND Data to Program.000000 Data to Program.000000 DATA DD 000007 Proto disconnessione Proto disconnessione DATA DProduct 000000 DD 000007 Proto Disconnessione DATE ID 000007 Proto Disconnessione Proto Disconnessione DATE ID 000007 Proto Disconnessione Proto Disconnessione DATE ID 000007 Proto Disconnessione Proto Disconnessione MOUR IE FW REVISION Firmware v1.32 Proto Disconnessione GET SYSTEM EXEND SEND Del Windi Reveto OK Proto Disconnessione SSWORD 1 SEND SEND Dott Dott Dott INSERT OLD PASSWORD 2 SEND ERASE DOWNLOAD DOWNLOAD	COM PORT: com48 Disconnect PROGRAM READ SPYLOCK15 PROGRAMMER VER 7 ASSWORD pASSWORD 1 SEND PROGRAM FREAD PEBUG BOX PASSWORD 2 SEND SEND Data to Program.000000 Data to Program.000000 DATA ID D00007 Prevalue Vision Connect. Prevalue Vision Connect. DATE ID D00007 Prevalue Vision Connect. Prevalue Vision Connect. DATE ID 000007 Prevalue Vision Connect. Prevalue Vision Connect. DATE ID 000007 Prevalue Vision Connect. Prevalue Vision Connect. HOUR 16 48 PW REVISION Pirmware v1.32 OH (Not Connect.) ASSWORD 1 SEND ERASE BOOT Data to Program.000000 Data invisiti SEND BOOT ERASE BOOT	CONNECTING	READ/PROGRAM	
ASSWORD PASSWORD 1 PASSWORD 2 PASSWORD 2 DATA DATA DProduct 000000 D D D D D D D D D D D D D D D D	ASSWORD PASSWORD 1 PASSWORD 2 PASSWORD 2 DATA DATA DProduct DO00000 Dot invide Permuto Pulsarite Connect Permuto Pulsarite Permuto P	COM PORT : com48	Disconnect PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7
PASSWORD 1 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 2 PASSWORD 1 Product Preduct P	PASSWORD 1 PASSWORD 2 PASSWORD 1 Product Preduct 000000 D PassWord Cornect Preduct Disonnessione Preduct Dison	PASSWORD		
PASSWORD 2 SEND DATA SEND DATA Deals to Program:000000 Data invisit Revuto OK DATA Docome DATA Docome DATA Docome DATA Deals to Program:000000 Data invisit Revuto OK DATA Docome DOCOT	PASSWORD 2 SEND DATA SEND DATA Revuto 0K DATA District Connect DATE District Connet	PASSWORD 1	SEND	Ricevuto OK
DATA Porta consesta >> tento a sconnessione DATA Deroduct 000000 ID Product 000007 DATE (DD/MM(YEAR) 10 07 DATE (DD/MM(YEAR) 10 07 DATE (DD/MM(YEAR) 10 07 DATE (DD/MM(YEAR) 16 48 PW REVISION Firmware v1.32 MOUIFY PASSWORD 1 SEND INSERT OLD PASSWORD 2 SEND INSERT AGAIN NEW PASSWORD 2 SEND	DATA PRASWORD MANAGEMENT INSERT OLD	PASSWORD 2	SEND	Data to Program:00000 Dati inviati Ricevuto OK
ID Product 000000 ID 000007 Porta Disconnessa -> tento connessione Porta Disconnessa -> tento connessa -> tento connessione Porta Disconnessa -> tento connessa -> tento connessione Porta Disconnessa -> tento connessa -> tento connes connessa ->	ID Product 000000 ID 000007 Porta Disconnessa -> tents connessione Porta Disconnessa -> tents connessine Porta Disconnessa -	DATA		Porta connessa -> tento disconnessione Premuto Pulsante Connect
DATE (DD/MM/YEAR) 10 07 2015 NUMBER EVENTS 0021 Set COM Timeouts ok "Check password HOUR 16 48 FW REVISION Firmware v1.32 CM Timeouts ok "Check password Dati riviati is revulue of the company of the	DATE (DD/MM/YEAR) 10 07 2015 NUMBER EVENTS 0021 Set COM Timeouts ok "Check password" HOUR 16 48 FW REVISION Firmware v1.32 BASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT AGAIN NEW PASSWORD 2 ****** SEND	ID Product 000000	ID 000007	Porta Disconnessa -> tento connessione Try to open port Porta COM aperta correttamente
HOUR 16 48 PW REVISION Pirmware v1.32 Data to Program:000000 HOUR GET SYSTEM GET SYSTEM Data to Program:000000 GET SYSTEM GET SYSTEM Data to Program:000000 TIME BOOT MODIFY PASSWORD 1 SEND INSERT OLD PASSWORD 2 SEND INSERT AGAIN NEW PASSWORD 2 SEND	(dot r, plany) 16 48 PW REVISION Pirmware v1.32 (H+I)MM) 16 48 PW REVISION Pirmware v1.32 (H+I)MM) GET SYSTEM Data to Program:00000 Data to Program:00000 (H+I)MM) GET SYSTEM Pirmware v1.32 Data to Program:00000 (H+I)MM) GET SYSTEM Pirmware v1.32 Data to Program:00000 (H+I)MM) GET SYSTEM Pirmware v1.32 Pirmware v1.32 (H)MOURY PASSWORD 1 SEND BOOT BOOT INSERT OLD PASSWORD 2 SEND ERASE MEMORY INSERT AGAIN NEW PASSWORD 2 SEND DOWNLOAD	DATE 10 07 201	5 NUMBER EVENTS 0021	Set COM Timeouts ok
PASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 1 BOOT MODIFY PASSWORD 2 INSERT AGAIN NEW PASSWORD 2 ERASE MEMORY ERASE DOWNLOAD	PASSWORD MANAGEMENT MODIFY PASSWORD 1 INSERT OLD PASSWORD 1 MODIFY PASSWORD 2 INSERT AGAIN NEW PASS	HOUR (HH/MM) 16 48 GET SYSTEM TIME	FW REVISION Firmware v1.32	Deta to Program:00000 Deti mvati Ricevuto OK "Check password Deta to Program:00000 Deti mvati Ricevuto OK
MODIFY PASSWORD 1 INSERT OLD PASSWORD 1 BOOT BOOT BOOT BOOT BOOT BOOT BOOT BOO	MODIFY PASSWORD 1 INSERT OLD PASSWORD 2 INSERT AGAIN NEW P	PASSWORD MANAGEMENT		BOOTI OADEB
INSERT OLD PASSWORD 1 SEND BOUT	INSERT OLD PASSWORD 1 SEND EVENTS ERASE MEMORY EVENTS ERASE DOWNLOAD	MODIFY PASSWORD 1		POOT
MODIFY PASSWORD 2 INSERT AGAIN NEW PASSWORD 2 EVENTS ERASE DOWNLOAD	MODIFY PASSWORD 2 ERASE MEMORY EVENTS INSERT AGAIN NEW PASSWORD 2 ****** SEND ERASE DOWNLOAD	INSERT OLD PASSWORD 1	SEND	
INSERT AGAIN NEW PASSWORD 2 ****** SEND ERASE DOWNLOAD	INSERT AGAIN NEW PASSWORD 2 ****** SEND ERASE DOWNLOAD	MODIFY PASSWORD 2		ERASE MEMORY EVENTS
		INSERT AGAIN NEW PASSWORD 2	** SEND	ERASE

Figure 38 – Confirming the new Security Password 2



YLOCK Management Software	2
OMPORT: com48 Disconnect	AD/PROGRAM PROGRAM READ SPYLOCK15 PROGRAMMER VER 7
SSWORD	DEBUG BOX
ASSWORD 1	SEND Ricevuto OK Premuto Pulsante Connect
ASSWORD 2	SEND Porta connessa -> tento disconnessione Premuto Pulsante Connect Porta Disconnessa -> tento connessione Try to open port Porta COM ok Set COM ok
D Product 000000 ID	Program Spy-Lock15 X Set COM Timeouts ok Check password Data to Program:000000
ATE 10 07 2015 NUMBER EVE	Dati inviati Ricevuto OK Vickerk password 2 modified!
OUR 16 48 FW REVISIO	Data to Program:000000 Det inviati
HH/MM)	OK Ricevuto OK Modify PWD 2 Deta to Program:000000
GET SYSTEM TIME	Dati inviti Ricevuto OK
SSWORD MANAGEMENT	BOOTLOADER
INSERT OLD PASSWORD 1	SEND BOOT
MODIFY PASSWORD 2	ERASE MEMORY EVENTS
INSERT AGAIN NEW PASSWORD 2 ******	SEND ERASE DOWNLOAD

Figure 39 – Security Password 2 modified

8. FW Upgrade

ATTENTION – in case of firmware upgrade operation it is important to remember that:

- The FW upgrade must be necessarily performed by qualified personnel;
- The FW upgrade will erase any data previously configured on the device, so you will need to save your settings and data before proceeding withr the reconfiguration of the device;
- Upon the occurrence of errors during the procedure, you must perform a hard reset of the device (please refer to Section 9– *Hard Reset*).

From "SPYLOCK Management Software" application software user interface push the "BOOT" button.

ONNECTING	READ/PROGRAM		
COM PORT : com48	PROGRAM READ	SPYLOCK15 PROGRAMMER VER 7	
ASSWORD		DEBUG BOX	
PASSWORD 1 PASSWORD 2	SEND SEND	Prenuto Pulsante Connect Porto Siscomessa -> tento connessione Try to open port Porto Connessione Set COM ok Set COM ok Set COM teneu to ok	
DATA 000000 ID DATE 000000 ID ID DATE 10 07 2015 NUL	MEER EVE	Check password Data Check Park Check Park Park Park Park Park Park Park Par	
HOUR 16 48 FW	REVISION	Deta to Programibost Deti invidei Attende rispotari entry in boot Risevedo OK	
ASSWORD MANAGEMENT		BOOTLOADER	
MODIFY PASSWORD 1 INSERT OLD PASSWORD 1	SEND	BOOT	
MODIFY PASSWORD 2		ERASE MEMORY EVENTS	
INSERT OLD PASSWORD 2	SEND	ERASE DOWINLOAD	

Figure 40 – Device in Boot Loader mode and ready for FW upgrade



When the device completes its entering into the Boot Loader mode the display automatically switches off.

Firmware upgrade steps:

- 1. Close the application "SPYLOCK Management software";
- 2. Start the application "Bootloader_Host" (Figure 41);
- 3. Select the item "USB Human Interface device" in the program window (Figure 42); it is not necessary to install any driver to carry out this operation.
- Select from the menu File -> Open the location where the firmware file to be uploaded on the device was saved (Figure 43);
- 5. Click the "PROGRAM" button and wait to the completion of the uploading process (Figure 46).

Bootloader Host		
File Actions Help		
🖆 🕽 BB 🛇		
File: C:\Documents and Settings\utente\Desktop		
Ports:	Filters Port Configuration Port Information	
Log:		
Ready		

Figure 41 – Bootloader host



🖹 Bootloader Host	t .	
File Actions Help	2	
🖆 🍹 BE		
File: C:\Documents and Settings\utente\Desktop		
Ports:	Filters Port Configuration USB Port Information face Device No configuration necessary for this port. VID: 0484 PID: 871D	
03:47:01 PM - Selected	nd device: USB Human Interface Device (0484_871D)	
Ready		.:

Figure 42 – USB Human Interface Device class to be selected



Figure 43 – Selection of FW upgrade file



📱 Bootloader Host		
File Actions Help		
🖆 🔁 🔁 📎 🔘 🔘		
File: \\N23 Program lech\Cd Eprojete	ch v1.3_ interno EPRO\Cd Eprojetech\Firmware\S	pylock15 v1.27.cyacd
Ports: Fi	Iters Port Configuration USB No configuration necessary for this port.	Port Information VID: 0484 PID: 871D
Log: 05:37:44 PM - Selected device: USB H 05:37:44 PM - Selected device: USB H	uman Interface Device (0484_871D) uman Interface Device (0484_871D)	
Ready 🗌		

Figure 44 – FW flashing operation activated

🖀 Bootloader Host 📃 🗖 👗
File Actions Help
📂 🔪 66 📎 🔕
File: \\\\\\2310\eprojetech\\Cd Eprojetech v1.3_ interno EPR0\\Cd Eprojetech\Firmware\Spylock15 v1.27.cyacd
Ports: Filters Port Configuration USB V Port Information
Vic USB Human Interface Device No configuration necessary for this VID: 0484
Log:
05:37:44 PM - Selected device: USB Human Interface Device (0484_B71D) 05:37:44 PM - Selected device: USB Human Interface Device (0484_B71D) 05:40:09 PM - Programming Started
Programming

Figure 45 – Firmware upgrade started



😫 Bootloader Host 📃 🗖 🔀
File Actions Help
File: \\N2310\eprojetech\Cd Eprojetech v1.3_ interno EPRO\Cd Eprojetech\Firmware\Spylock15 v1.27.cyacd
Ports: Filters Port Configuration Port Information
05:37:44 PM - Selected device: USB Human Interface Device (04B4_B71D)
05:37:44 PM - Selected device: USB Human Interface Device (04B4_B71D) 05:40:09 PM - Programming Finished Successfully 05:40:17 M - Programming Finished Successfully Programming completed in 8048ms.
Ready

Figure 46 – Firmware upgrade completed

NOTE: the Upgrade Firmware procedure does not require the installation of any driver: Windows OS automatically detects the SPYLOCK device.

The display automatically switches on again at the completion of the firmware upgrade process.

9. Hard Reset

When a harware resti s requierd the following procedure has to be followed:

- Open the SPYLOCK cable;
- Keep the navigation button pressed for 15 sec.;
- At the button release the display will show "Spylock 15 Firmware X.XX" to confirm that the reset operation has compelted successfully;
- SPYLOCK automatically goes back into its operational mode.

NOTA: Hard Reset of the device does not cause data loss.

10. SPYLOCK battery recharge

SPYLOCK is supplied by a USB rechargeable battery. At its very first use a 8-hours battery charge is recommended. To recharge SPYLOCK battery:

• Open the SPYLOCK cable;



- Remove USB port plastic protection;
- Connect the USB cable to the SPYLOCK on one end and to the main at the other end, via the universal power adapter supplied with the device;
- The display shows for 6 sec. "Charging" and then it automatically switches off.





11. Warranty and liability conditions

LEGHORN srl ensures that the SPYLOCK product is free from defects in materials and workmanship and also ensures that the product is fully compliant with the declared specifications.

However, in case of claimed product defects or non-compliances LEGHORN srl guarantees a warranty period of twelve (12) months in accordance with the regulation of the manufacturing country. The period of warranty starts from the date of purchase. During the warranty period it will be up to LEGHORN srl to decide whether to repair or replace the returned product. The above warranty does not cover defects from improper or inadequate maintenance, repairs or calibrations performed by the customer or by a third party not authorized by the manufacturer; hardware, software, interfaces or materials supplied by the customer or by third parties; use or operation outside the product's specifications; damage, negligence in use, accidents, loss or damage during travel.

THE ABOVE WARRANTIES ARE EXCLUSIVE AND EXCLUDE ALL OTHER WARRANTIES, WRITTEN OR ORAL, EXPRESS OR IMPLIED.

This device complies with the safety requirements required by law. Anyhow the equipment and the related documentation should be carefully examined to familiarize yourself with the safety instructions before starting with the operating procedures. To ensure a proper and safe use, the user of this apparatus will have to follow all the information and warnings contained in this document.

During the recharging operation this device must be connected to an electrical system which respects the national legislation force.

The information in this document is subject to updates without notice.

LEGHOR srl is not liable on any improper use of the product that breaches the rules of law, civil, criminal and labour code.

In the event that the device is not functioning or gives evidence of functional anomalies, please contact your local distributor or the manufacturer.