Appunti sul protocollo SCS

Frame

Le informazioni vengono scambiate con 2 tipi di frame: frame ridotto e frame esteso-

Frame ridotto:

STX	DES	LOC	CMD	ARG	CKS	ETX

STX inizio del frame 0xA8

DES indirizzo di destinazione
0x01 destinazione gruppo (scenario)
0x.. indirizzo del singolo device
0xB1 broadcast
0xB3 indirizzo di ambiente o scenario
0xB4 broadcast allarme
0xB8 segnalatori stato dei dispositivi

LOC
per destinazione singolo device:	indirizzo di chi invia (00 = null)
Per destinazione 0xB1 broadcast:	00
Per destinazione 0xB3 ambiente:	codice ambiente o scenario
Per destinazione 0xB4 allarme:	probabilmente indirizzo centralina (0xC1)
Per destinazione 0xB8 segnalatori:	indirizzo dispositivo segnalato

CMD tipo di commando
0x12 comando di attuazione / risposta stato
0x14 comando di gruppo
0x15 interrogazione stato
0x17 conferma di gruppo / scenario
0x43 stato delle zone (accese/spente)
0x44 ….
0x49 comando/stato on/off allarme
0x4E stato delle zone (in allarme/tranquille)
0x60 comando/richiesta citofono o videocitofono
0x6F stato citofono o videocitofono

ARG argomento del comando / stato risposto
Comandi:
0x00 accendi
0x01 spegni
0x03 dimmer aumenta
0x04 dimmer diminuisci
0x08 tapparella su
0x09 tapparella giu
0x0A tapparella stop
0x1D-0x9D intensita (dimmer)
0x4n - Stati allarme vedi nota sotto.

CKS checksum (xor dei 4 bytes precedenti)

ETX fine frame 0xA3

Frame esteso:

STX	DES1	DES2	DES3	LOC1	LOC2	LOC3	CMD	ARG	CKS	ETX

STX inizio del frame 0xA8

DES1 DES2 DES3 indirizzi di destinazione

LOC1 LOC2 LOC3 indirizzi di chi invia

CMD tipo di comando

ARG argomento del comando

CKS checksum

ETX fine frame 0xA3

I frame sono trasmessi a 9600baud, ogni byte composto da 1 bit di start, 8 bits di dati, 1 bit di stop. Ogni bit dura 104uS, durata di 1 frame standard circa 7,3mS. I frame ripetuti hanno una pausa intermedia di **3,12mS**.

La collisione deve essere intercettata da chi trasmette e corrisponde alla situazione in cui si sta trasmettendo ed il bus assume uno stato non corrispondente a quello atteso in un qualunque istante. In tal caso il frame viene ripetuto dopo un periodo di attesa di bus libero di almeno 5,2mS.

I frame possono essere PP (point-to-point) o BB (brief broadcast).

I controlli possono essere di tre tipi:

Room controls: Controllo diretto a tutti gli attuatori identificati dallo stesso numero di ambiente.
Group controls: Controllo diretto a tutti gli attuatori identificati dallo stesso numero di gruppo anche se collegati ad ambienti differenti.
General controls: Controllo diretto a tutti gli attuatori del sistema.

I frame point-to-point (con un solo destinatario singolo) si aspettano un ACK (0xA5) ricevuto entro **1,66mS**, altrimenti vengono ripetuti 8 volte. Se nessun ACK è ricevuto il dispositivo si considera fuori servizio. Prima di ogni ripetizione il dispositivo origine aspetta il bus libero per 3,12mS.

Before each repetition, the transmitter MUST wait its free-Bus time before transmitting. Brief point to point
frame timing:

$9{:}56ms + TwaitF\ reeBus \Rightarrow 14{:}5ms < T < 46ms$

Brief Broadcasting frame(BB): A broadcasting frame is sent from a device without any confirm of the reception. The frame is repeated 3 times at a 3.12ms interval. Brief Broadcasting frame timing:

$30ms + TwaitF\ reeBus \Rightarrow 35ms < T < 62ms$

I tempi dei frame estesi invece sono:

43:5 + *TwaitF reeBus* => 48:5*ms* < *T* < 80*ms*

LOG comandi di ALLARME (e ipotesi)

I log che riporto risultano da una centrale di allarmi bTicino 3500N – le conclusioni che riporto sono delle IPOTESI. I messaggi hanno tutti destinazione 0xB4 (broadcast messaggi allarme) e provenienza 0xC1 (centralina allarme).

Il "tipo di comando" dei messaggi è sempre della "serie" 0x4n (0x43, 0x44, 0x49, 0x4E)

Per brevità nel log ogni messaggio è singolo, in realtà, come sempre nel broadcast, ogni messaggio è ripetuto 3 volte perché non c'è ackowledgement.

```
#############Inserimento con Zona 1 , Zona 3 , Zone 1-3 ed infine Zone 1-2-3


SCS[7]: A8 B4 C1 4E FA C1 A3 ############Inserimento con sola Zona 1
SCS[7]: A8 B4 C1 43 EA DC A3
SCS[7]: A8 B4 C1 49 00 3C A3

SCS[7]: A8 B4 C1 44 20 11 A3 #############Disinserimento
SCS[7]: A8 B4 C1 4E F8 C3 A3
SCS[7]: A8 B4 C1 43 E8 DE A3
SCS[7]: A8 B4 C1 49 01 3D A3

###############Inserimento con solo Zona 3

SCS[7]: A8 B4 C1 4E FA C1 A3 ##########Inserimento
SCS[7]: A8 B4 C1 43 BA 8C A3
SCS[7]: A8 B4 C1 49 00 3C A3

SCS[7]: A8 B4 C1 44 20 11 A3 #########Disinserimento
SCS[7]: A8 B4 C1 4E F8 C3 A3
SCS[7]: A8 B4 C1 43 B8 8E A3
SCS[7]: A8 B4 C1 49 01 3D A3

###########Inserimento da centrale con Zone 1 e 3

SCS[7]: A8 B4 C1 4E FA C1 A3 ###########Inserimento
SCS[7]: A8 B4 C1 43 AA 9C A3
SCS[7]: A8 B4 C1 49 00 3C A3

SCS[7]: A8 B4 C1 44 20 11 A3 #########Disinserimento
SCS[7]: A8 B4 C1 4E F8 C3 A3
SCS[7]: A8 B4 C1 43 A8 9E A3
SCS[7]: A8 B4 C1 49 01 3D A3

##########Inserimento e disinserimento con Zone 1-2-3

SCS[7]: A8 B4 C1 4E FA C1 A3 #######Inserimento
SCS[7]: A8 B4 C1 43 8A BC A3
SCS[7]: A8 B4 C1 49 00 3C A3

SCS[7]: A8 B4 C1 44 20 11 A3

SCS[7]: A8 B4 C1 4E F8 C3 A3 #######Disinserimento
SCS[7]: A8 B4 C1 43 88 BE A3
```

```
SCS[7]: A8 B4 C1 49 01 3D A3

SCS[7]: A8 B4 C1 44 31 00 A3 ########Innesco perimetrale Cucina

SCS[7]: A8 B4 C1 4E FB C0 A3
SCS[7]: A8 B4 C1 43 AB 9D A3
SCS[7]: A8 B4 C1 49 84 B8 A3

SCS[7]: A8 B4 C1 44 10 21 A3
SCS[7]: A8 B4 C1 44 20 11 A3

SCS[7]: A8 B4 C1 4E F9 C2 A3
SCS[7]: A8 B4 C1 43 A9 9F A3
SCS[7]: A8 B4 C1 49 85 B9 A3
```

```
################## Perimetrale Cucina - Zona 3 ######################


SCS[7]: A8 B4 C1 44 10 21 A3 ####Inserimento allarme con Zone 1-3
SCS[7]: A8 B4 C1 44 31 00 A3
SCS[7]: A8 B4 C1 4E FB C0 A3
SCS[7]: A8 B4 C1 43 AB 9D A3
SCS[7]: A8 B4 C1 49 84 B8 A3

SCS[7]: A8 B4 C1 4E FA C1 A3 ####Apertura perimetrale cucina-innesco allarme
SCS[7]: A8 B4 C1 43 AA 9C A3
SCS[7]: A8 B4 C1 44 31 00 A3
SCS[7]: A8 B4 C1 4E FB C0 A3
SCS[7]: A8 B4 C1 43 AB 9D A3
SCS[7]: A8 B4 C1 49 84 B8 A3
SCS[7]: A8 B4 C1 4E FA C1 A3
SCS[7]: A8 B4 C1 43 AA 9C A3

SCS[7]: A8 B4 C1 44 20 11 A3 ########Disinserimento
SCS[7]: A8 B4 C1 4E F8 C3 A3
SCS[7]: A8 B4 C1 43 A8 9E A3
SCS[7]: A8 B4 C1 49 01 3D A3


###############  Porta Ingresso  - Zona 1  ######################

SCS[7]: A8 B4 C1 4E F8 C3 A3 #########Inserimento allarme con Zone 1-3
SCS[7]: A8 B4 C1 43 A8 9E A3
SCS[7]: A8 B4 C1 4E FA C1 A3
```

```
SCS[7]: A8 B4 C1 49 00 3C A3

SCS[7]: A8 B4 C1 44 10 21 A3 #########Apertura porta con innesco allarme
SCS[7]: A8 B4 C1 44 11 20 A3
SCS[7]: A8 B4 C1 4E FB C0 A3
SCS[7]: A8 B4 C1 43 AB 9D A3
SCS[7]: A8 B4 C1 49 84 B8 A3
SCS[7]: A8 B4 C1 4E FA C1 A3
SCS[7]: A8 B4 C1 43 AA 9C A3

SCS[7]: A8 B4 C1 44 20 11 A3 ########Disinserimento
SCS[7]: A8 B4 C1 4E F8 C3 A3
SCS[7]: A8 B4 C1 43 A8 9E A3
SCS[7]: A8 B4 C1 49 01 3D A3

#################  Perimetrale Salone - Zona 3 ########################

SCS[7]: A8 B4 C1 4E FA C1 A3 #########Inserimento allarme con Zone 1-3
SCS[7]: A8 B4 C1 4E FA C1 A3
SCS[7]: A8 B4 C1 4E FA C1 A3
SCS[7]: A8 B4 C1 43 AA 9C A3
SCS[7]: A8 B4 C1 43 AA 9C A3
SCS[7]: A8 B4 C1 43 AA 9C A3
SCS[7]: A8 B4 C1 49 00 3C A3
SCS[7]: A8 B4 C1 49 00 3C A3
SCS[7]: A8 B4 C1 49 00 3C A3



SCS[7]: A8 B4 C1 44 31 00 A3 #####Apertura perimetrale salone innesco allarme
SCS[7]: A8 B4 C1 4E FB C0 A3
SCS[7]: A8 B4 C1 43 AB 9D A3
SCS[7]: A8 B4 C1 49 84 B8 A3
SCS[7]: A8 B4 C1 44 10 21 A3
SCS[7]: A8 B4 C1 4E FA C1 A3
SCS[7]: A8 B4 C1 43 AA 9C A3

SCS[7]: A8 B4 C1 44 20 11 A3 ##########Disinserimento
SCS[7]: A8 B4 C1 4E F8 C3 A3
SCS[7]: A8 B4 C1 43 A8 9E A3
SCS[7]: A8 B4 C1 49 01 3D A3
```

Ogni “inserimento” si articola in 3 messaggi di tipo 0x4E, 0x43 e 0x49. Il disinserimento ha in più il messaggio 0x44. Il messaggio con tipo 0x49 è certamente un on/off dato che è l’ultimo della serie di inserimento con valore 00 e anche l’ultimo del disinserimento con valore 01 (i valori tipici di on/off degli interruttori). Probabilmente i tipi 0x4E e/o 0x43 riguardano le zone da attivare o disattivare.

Attiva	zone	0x44	0x4E	0x43	0x49	
Attiva	1		1111 1010	1110 1010	0000 0000	
Attiva	3		1111 1010	1011 1010	0000 0000	
Attiva	1+3		1111 1010	1010 1010	0000 0000	
Attiva	1+2+3		1111 1010	1000 1010	0000 0000	

Azione	zone	0x44	0x4E	0x43	0x49	
Disattiva	1	0x20	1111 1000	1110 1000	0000 0001	
Disattiva	3	0x20	1111 1000	1011 1000	0000 0001	
Disattiva	1+3	0x20	1111 1000	1010 1000	0000 0001	
Disattiva	1+2+3	0x20	1111 1000	1000 1000	0000 0001	

Attiva	1+3	0x10				
Attiva	1+3	0x31	1111 1011	1010 1011	1000 0100	
Allarme	3		1111 1010	1010 1010		
		0x31	1111 1011	1010 1011	1000 0100	
			1111 1010	1010 1010		
Disattiva	1+3	0x20	1111 1000	1010 1000	0000 0001	
---						led--------
Attiva	1		1111 1010	1110 1010	0000 0000	spento
Fine ritardo		0X10				
Allarme		0x11	1111 1011	1110 1011	1000 0100	rosso
Disattiva	1	0x20	1111 1001	1110 1001	1000 0101	ambra

Attiva	1+3		1111 1000	1010 1000	1000 0100	
			1111 1010		0000 0000	
Fine ritardo		0x10				
Allarme	1	0x11	1111 1011	1010 1011	1000 0100	
			1111 1010	1010 1010		
Disattiva	1+3	0x20	1111 1000	1010 1000	0000 0001	

Attiva	1+3		1111 1010	1010 1010	0000 0000	
Allarme	3	0x31	1111 1011	1010 1011	1000 0100	
		0x10	1111 1010	1010 1010		
Disattiva	1+3	0x20	1111 1000	1010 1000	0000 0001	

Azione	zone	0x44	0x4E	0x43	0x49	
In allarme	1+3	0x31				
In allarme	1+3		1111 1011	1010 1011	1000 0100	
In allarme	1+3	0x10		| allarme momentaneo		
In allarme	1+3	0x20				
					| memoria |	
In allarme	1+3		1111 1001	1010 1001	1000 0101	
			||||	||||	|	
				Zone accese(0)	Centrale accesa(0)/spenta(1)	

Il valore del messaggio 0x4E in binario vale:
bit 7-6-5-4 sempre 1111 – potrebbero rappresentare l'attivazione (0) delle zone 8-7-6-5
bit 3 sempre 1.
bit 2 sempre 0.
bit 1 vale 1 a centrale inserita, 0 a centrale disinserita
bit 0 1 significa allarme momentaneo (ha senso solo se centrale inserita) **

Il valore del messaggio 0x43 in binario vale:
bit 7-6-5-4 potrebbero rappresentare l'attivazione (0) delle zone 4-3-2-1
bit 3 sempre 1.
bit 2 sempre 0.
bit 1 vale 1 a centrale inserita, 0 a centrale disinserita
bit 0 1 significa allarme momentaneo (ha senso solo se centrale inserita) **

Il valore del messaggio 0x49 in binario vale:
bit 7 0 significa che dall'accensione ad ora non è scattato allarme, 1 si (*)
bit 6-5-4-3 sempre 0.
bit 2 0 significa che dall'accensione ad ora non è scattato allarme, 1 si (*)
bit 1 sempre 0
bit 0 1 significa centrale spenta, 0 accesa

* in un caso il bit non si è azzerato all'accensione
** in un caso il bit non si è azzerato immediatamente all'accensione ma dopo qualche istante

Da notare anche che il semibyte basso dei messaggi 0x4E e 0x43 coincide sempre in ciascuna sequenza – ignoro se ci siano casi particolari in cui si possa differenziare.

Il valore del messaggio 0x43 (high-nibble) in binario riporta "0" per ogni zona attiva e "1" per ogni zona disattiva – il bit più a sinistra (bit7) riguarda la zona 4, il successivo la zona 3, poi la 2, poi la 1.

TUTTI i messaggi riportati nel log vengono inviati dalla centrale all'accensione o allo spegnimento – non ho a disposizione log di messaggi che possano attivare o disattivare la centrale.

Il messaggio 0x44 ha a che vedere con la rilevazione di allarme – in particolare un attimo prima della rilevazione dell'allarme è transitato un messaggio 0x44 con bit0 del valore a 1 – il valore 0x31 ha indicato una rilevazione di allarme in zona 3, il valore 0x11 in zona 1. Il valore 0x10 sembra rappresentare la fine del tempo di uscita (attiva i sensori) e 0x20 invece sembra che resettino i bits di allarme.

Esempi di comandi PP singoli

Spegni/accendi luce

A8 32 00 12 01 21 A3

32: indirizzo dispositivo
00: origine null
12: comando di attuazione
01: spegni

A8 32 00 12 00 20 A3

32: indirizzo dispositivo di destinazione
00: origine null
12: comando di attuazione
00: accendi

Risposta

A8 B8 32 12 00 20 A3

B8: indirizzo dei segnalatori di stato
32: origine dispositivo comandato
12: stato di attuazione
00: acceso

Accendi/aumenta dimmer

A8 21 00 12 00 33 A3

21: indirizzo dispositivo
00: origine null
12: comando di attuazione
00: accendi / aumenta

Risposta

A8 B8 21 12 9D 16 A3

B8: indirizzo dei segnalatori di stato
21: origine dispositivo comandato
12: stato di attuazione
9D: intensità di accensione

Spegni/diminuisci dimmer

A8 21 00 12 01 32 A3

21: indirizzo dispositivo
00: origine null
12: comando di attuazione
01: spegni / diminuisci

Risposta

A8 B8 21 12 8D 06 A3

B8: indirizzo dei segnalatori di stato
21: origine dispositivo comandato
12: stato di attuazione
8D: intensità di accensione

Imposta luminosita dimmer

A8 21 00 12 01 32 A3

21: indirizzo dispositivo
00: origine null
12: comando di attuazione
8D: luminosità – valori possibili 1D-2D-3D-4D-5D-6D-7D-8D-9D

Risposta

A8 B8 21 12 8D 07 A3

B8: indirizzo dei segnalatori di stato
21: origine dispositivo comandato
12: stato di attuazione
8D: intensità di accensione

Alza tapparella

A8 91 00 12 08 xx A3

91: indirizzo dispositivo
00: origine null
12: comando di attuazione
08: alza

Risposta

A8 B8 91 12 08 xx A3

B8: indirizzo dei segnalatori di stato
91: origine dispositivo comandato
12: stato di attuazione
08: in apertura

Ferma tapparella

A8 91 00 12 0A xx A3

91: indirizzo dispositivo
00: origine null
12: comando di attuazione
0A: stop

Risposta

A8 B8 91 12 0A xx A3

B8: indirizzo dei segnalatori di stato
91: origine dispositivo comandato
12: stato di attuazione
0A: ferma

Abbassa tapparella

A8 91 00 12 09 xx A3

91: indirizzo dispositivo
00: origine null
12: comando di attuazione
09: abbassa

Risposta

A8 B8 91 12 09 xx A3

B8: indirizzo dei segnalatori di stato
91: origine dispositivo comandato
12: stato di attuazione
09: in chiusura

Esempi di comandi di allarme

Attiva gruppo/scenario 1

A8 01 00 14 04 11 A3

01: indirizzo di gruppo/scenario
00: origine null
14: comando di attuazione di gruppo
04: numero gruppo / scenario

Esempi di comandi di gruppo (di ambiente?) (di scenario?)

Attiva gruppo/scenario 1

A8 01 00 14 04 11 A3

01: indirizzo di gruppo/scenario
00: origine null
14: comando di attuazione di gruppo
04: numero gruppo / scenario

Risposte

A8 B8 01 17 04 AA A3 chi risponde ?

B8: indirizzo dei segnalatori di stato
01: origine dispositivo comandato (indirizzo di gruppo)
17: conferma di gruppo
04: gruppo / scenario

A8 B1 00 12 01 A2 A3 prima spegne tutto - sempre uguale per qualunque gruppo/scenario – chi lo manda?

Non risponde nessuno

B1: indirizzo broadcast (tutti)
00: origine null
12: stato di attuazione
01: spegni tutto

A8 21 01 12 9D AF A3 un comando di stato per ogni singolo dispositivo che va acceso – chi lo manda?

21: indirizzo broadcast (tutti)
01: origine indirizzo di gruppo
12: stato di attuazione
9D: stato richiesto (intensità dimmer)

A8 B8 21 12 9D 16 A3 una risposta di stato per ogni singolo dispositivo che si accende

B8: indirizzo dei segnalatori di stato
31: origine dispositivo comandato
12: stato di attuazione
9D: stato o intensità di accensione

Comandi o report di antifurto

A8 B4 C1 4E F8 xx A3

A8 B4 C1 43 88 xx A3

Abbassa le tapparelle dell'ambiente 1

A8 B3 01 12 09 A9 A3

B3: indirizzo di ambiente
01: ambiente 1
12: comando di attuazione
09: abbassa le tapparelle

Alza le tapparelle dell'ambiente 1

A8 B3 01 12 08 A8 A3

B3: indirizzo di ambiente
01: ambiente 1
12: comando di attuazione
09: abbassa le tapparelle

Esempi di comandi globali

Spegni tutte le luci

A8 B1 00 12 01 A2 A3

B1: broadcast (a tutti)
00: origine null
12: comando di attuazione
01: spegni

Risposte

Accendi tutte le luci

A8 B1 00 12 00 A3 A3

B1: broadcast (a tutti)
00: origine null
12: comando di attuazione
00: accendi

Risposte

Giu tutte le tapparelle

A8 B1 00 12 09 AA A3

B1: broadcast (a tutti)
00: origine null
12: comando di attuazione
00: accendi

Risposte

Videocitofono

Pur essendo i videocitofoni bTicino formalmente dei dispositivi SCS, essi se ne differenziano per alcuni motivi:

1- Non vengono collegati sul bus SCS degli altri dispositivi ma su di un bus separato
2- Dal bus l'alimentazione viene prelevata solamente dal posto esterno, ogni posto interno ha invece un proprio alimentatore. Il bus viene alimentato dal posto interno "master"

3- Gli alimentatori non sono dei veri alimentatori stabilizzati SCS e di conseguenza la tensione sul bus non è così stabile come sugli impianti SCS.

Ne consegue una più delicata taratura ed una maggior difficoltà nell'uso di dispositivi autoalimentati dal bus come esp_scsgate e opt_scsgate, che pur tuttavia funzionano.

Le informazioni vengono scambiate con il classico frame SCS – qui mi limito a riportare un log di conversazione nelle varie situazioni – per brevità elenco ogni telegramma che transita sul bus una volta sola anche se vi appare per 3 o più volte di seguito.

Suonano dal posto esterno

```
A8 B0 A0 6F 88 F7 A3

A8 91 01 60 88 78 A3

A8 B2 A0 6F 88 F5 A3
```

Il posto interno 1 risponde (conversazione audio)

```
A8 B3 01 60 88 5A A3

A8 B4 A0 6F 88 F3 A3
```

Il posto interno 1 apre il cancellino

```
A8 96 A0 6F A4 FD A3

A8 96 A0 6F A0 F9 A3
```

Il posto interno 1 apre il cancello elettrico

```
A8 96 A1 6F A4 FC A3

A8 96 A1 6F A0 F8 A3
```

Il posto interno 1 preme il pulsante "luce"

```
A8 9D A0 6F A4 F6 A3

A8 9D A0 6F A0 F2 A3
```

Conversazione OFF

```
A8 B5 01 60 88 5C A3
```

Il posto interno 1 preme il pulsante "guarda"

```
A8 98 A0 6F A4 F3 A3

A8 A0 A0 6F 01 6E A3

A8 98 A0 6F A0 F7 A3

A8 A0 A0 6F 01 6E A3

A8 B0 A0 6F 98 E7 A3

A8 91 01 60 88 78 A3

A8 B2 A0 6F 88 F5 A3

A8 96 A1 6F A0 F8 A3
```

Il posto interno 1 chiama il posto interno 2

A8 B5 01 60 0C D8 A3

A8 B0 01 60 0C DD A3

A8 91 01 60 0C FC A3

A8 B2 01 60 0C DF A3

Il posto interno 2 chiama il posto interno 1

A8 B0 01 60 0C DD A3

A8 91 01 60 0C FC A3

A8 B2 01 60 0C DF A3

Citofono

Per i citofoni bTicino valgono le medesime considerazioni, i messaggi differiscono nei contenuti:

A8 B2 A0 6F 08 75 A3

A8 B5 A0 6F 08 72 A3

A8 B0 A0 6F 08 77 A3

A8 91 00 60 08 F9 A3