Протокол управления объективами Canon EF

24 марта 2016 г.

1 Методика «взлома»

Для работы со SPI–интерфейсом объектива использовался микроконтроллер PIC16F873a, подключенный к персональному компьютера через интерфейс RS–232. Так как кварцевый резонатор контроллера имел частоту $f_{osc} = 4\,\text{МГц}$, пришлось ограничиться довольно медленной скоростью — 19.2 кбит/с.

SPI–интерфейс контроллера был настроен на скорость передачи сообщений $f_{osc}/64$ (62.5 кГц). SPI работал в третьем режиме (высокий уровень CLK, передача информации на падающий фронт CLK, прием в середине такта – на возрастающий фронт CLK), регистры:

```
SSPCON = 0x32; TRISC = 0xD0; CKE = 0; SSPIE = 1; SMP = 0;
```

Для анализа сообщений, отсылаемых фотоаппаратом объективу, SPI переключался в пассивный режим:

```
SSPCON = 0x35; TRISC = 0xD8; CKE = 0; SSPIE = 1;  SMP = 0;
```

Однако, поток данных в обычном режиме работы фотоаппарата довольно велик, а скорость RS–232 слишком мала, чтобы контроллер успевал за промежуток между посылками отсылать их на ПК. Для буферизации посылок использовался массив данных из 95 элементов. Полученные по SPI–интерфейсу данные буферизовались контроллером в этот массив, а затем, при заполнении буфера или по команде пользователя, буфер передавался на ПК. Однако, и в этом случае оказалось очень много дополнительных команд, не имеющих отношения к управлению объективом.

Для подбора команд, вызывающих изменение фокусного расстояния объектива было принято решение отсылать поочередно объективу ненулевую однобайтную посылку, за которой следовало восемь нулевых посылок (как оказалось, нулевые посылки используются фотоаппаратом для считывания информации с объектива).

Методом последовательного перебора были определены основные управляющие команды. Временны́е интервалы между командами могут быть довольно велики. Если объектив должен ответить на какой-нибудь запрос, а после запроса никаких посылок не отсылалось, объектив будет ждать очередных посылок, чтобы выдать запрашиваемые данные. Поэтому стоит каждую команду завершать последовательностью нулевых посылок.

2 Команды EF 200

Некоторые команды не требуют от объектива ответа, поэтому их можно не завершать нулями, однако, некоторые запросы подразумевают достаточно длинный ответ, и требуют до восьми последующих нулевых сообщений.

Для перехода в ручной режим управления используется команда **94** или ее эквивалент **30** (все команды записываются здесь в десятичной системе). За этой командой должны следовать одна или две нулевых посылки. Некоторые команды для изменения фокусного расстояния требуют предварительного перехода в ручной режим управления.

Для увеличения фокусного расстояния объектива используются следующие команды (объектив EF 200, для EF 85 скорости не изменяются).

5 плавное увеличение фокусного расстояния (если за ней не следует других команд).

37 быстрый переход в ∞, за этой посылкой должны следовать две нулевые.

Для уменьшения фокусного расстояния используются команды

6 плавное перемещение на отметку 2.5 м.

22 быстрый переход на отметку 2.5 м. За этой командой следуют две нулевых. Эта команда имеет полные эквиваленты: **38, 70, 86**.

68 поворот привода объектива на заданный угол. Угол задается двумя следующими байтами (short int, старший байт первый). Узнать текущее угловое положение можно командой 192.

Для останова используется команда **4**. Таким образом, манипулируя командами **5**/**6** и **4** можно добиться постепенного изменения фокусного расстояния. Помимо ожидания для изменения фокусного расстояния на нужную величину после команд **5** или **6** можно отсылать нулевые посылки.

Кроме этой команды есть следующие информационные команды, чье предназначение пока не расшифровано (для EF 200, EF 85 см. в сводной таблице):

31 имеет двухбайтный ответ, оба байта содержали комбинации из единицы и тройки.

79 имеет трехбайтный ответ, являющийся комбинацией единиц и нулей.

95 ведет себя аналогично **31**.

111 имеет однобайтный ответ — единицу.

120 имеет однобайтный ответ — восьмерку.

239 имеет однобайтный ответ — 224 или 225.

247 однобайтный ответ 240.

250 однобайтный ответ 130 или 128.

251 однобайтный ответ 248.

252 однобайтный ответ (разные числа).

128 ответ из семи или восьми байт, возможно — запрос статуса объектива.

Было обнаружено еще несколько подозрительных запросов, ответом на которые был один байт с постоянным значением 128 или 192 (при любых манипуляциях с объективом).

2.1 Небольшое дополнение

команды (EF 85):

10 — **инициализация**, без этой команды EF85 не работает.

194 — узнать расстояние фокусировки (в метрах). Ответ — четыре байта, первые два — текущее расстояние, вторые два — предыдущее положение. В паре чисел первое умножаем на 2.5 м и складываем со вторым (в сантиметрах).

192 — узнать угловое положение лимба (от некоторого условного нуля). Ответ — два байта (short int, старший байт первый).

Управление диафрагмой: два байта число 18 (собственно команда) и байт — на сколько изменить текущее состояние диафрагмы (signed char) положительное число для закрытия, отрицательное – открыть.

При небольшом изменении состояния диафрагмы каждая команда 2 или 3 повторяет это изменение. Плюс объектив входит в режим пошаговой подстройки фокусировки. Выход из этого режима — команда 8 (или ее эквиваленты 11, 27, 43, 75).

3 Сводный перечень команд для EF 85

Расшифровка обозначений столбцов:

cmd команда;

N минимальная длина ответа в байтах;

ans ответ (в случае изменяющегося ответа — диапазон);

desc краткое описание команды.

Команды, чье предназначение не выявлено, имеют пустое поле описания. Если действие команды аналогично другой команде, в описании пишется эта команда. Под F подразумевается значение расстояния до объекта, чье изображение четко сфокусировано. Буква «о» в описании означает, что назначение команды неизвестно, но она приводит к отключению ручного управления F. Если в ответах встречаются записи через слеш, значит, в разные моменты времени появляется то одна, то другая из приведенных команд без видимой зависимости.

Таблица 1: Сводка команд

cmd	N	ans	desc
0	1	0	«пустышка» для получения ответа от объектива
1	1	1	
2	1	2	повтор предыдущего изменения величины диафрагмы, режим коротких шагов перемещения

Таблица 1: (продолжение).

cmd	**N**	**ans**	**desc**
3	1	3	2
4	1	4	остановить изменение F
5	1	5	увеличить F
6	1	6	уменьшить F
7	1	7	o
8	2	255/0, 170	отмена действия команды 2
9	1	9	o
10	1	10	инициализация объектива EF85 (без этой команды он не выходит из спящего режима)
11	1	11	8
12	1	12	
13	1	13	
14	1	14	
15	1	15	
16	2	16, 16	
17	2	17, 17	
18	2	18, 18	управление затвором, вторым байтом (signed char) отсылается степень изменения диаметра отверстия (положительным значениям соответствует уменьшение диаметра)
19	2	19, 19	18
20	2	20, 20	4
21	2	21, 21	5
22	2	22, 22	6
23	2	23, 23	o
24	3	24, 0/255, 170	
25	2	25, 25	o
26	2	26, 26	
27	2	27, 27	8
28	2	28, 28	
29	2	29, 29	
30	2	30, 30	(для EF 200 эквивалент команды 94)
31	2	31, 31	
32	2	32, 32	
33	2	33, 33	
34	2	34, 34	
35	2	35, 35	
36	2	36, 36	4
37	2	37, 37	5
38	2	38, 38	6
39	2	39, 39	o
40	3	40, 255/0, 170	
41	2	41, 41	o
42	2	42, 42	

Таблица 1: (продолжение).

cmd	N	ans	desc
43	2	43, 43	8
44	2	44, 44	
45	2	45, 45	
46	2	46, 46	
47	2	47, 47	
48	1	48	
49	1	49	
50	1	50	
51	1	51	
52	1	52	
53	1	53	
54	1	54	
55	1	55	
56	1	56	
57	1	57	
58	1	58	
59	1	59	
60	1	60	
61	1	61	
62	1	62	
63	1	63	
64	3	64, 64, 64	
65	3	65, 65, 65	
66	3	66, 66, 66	
67	3	67, 67, 67	
68	3	68, 68, 68	прокрутить мотор фокуса на заданное кол-во шагов (2 байта, int16, hi-low)
69	3	69, 69, 69	5
70	3	70, 70, 70	6
71	3	71, 71, 71	o
72	4	72, 72, 255/0, 170	
73	3	73, 73, 73	o
74	3	74, 74, 170	
75	3	75, 75, 75	8
76	3	76, 76, 76	
77	3	77, 77, 77	
78	3	78, 78, 78	(для EF 200 эквивалент команды 94)
79	3	79, 79, 79	
80	2	80, 80	
81	2	81, 81	
82	2	82, 82	
83	2	83, 83	
84	2	84, 84	4
85	2	85, 85	5

Таблица 1: (продолжение).

cmd	**N**	**ans**	**desc**
86	2	86, 86	6
87	2	87, 87	o
88	3	88, 255/0, 170	
89	2	89, 89	o
90	2	90, 170	
91	2	91, 91	
92	2	92, 92	
93	2	93, 93	
94	2	94, 94	включить ручное управление F
95	2	95, 95	
96	1	96	
97	1	97	
98	1	98	
99	1	99	
100	1	100	
101	1	101	
102	1	102	
103	1	103	
104	1	240	
105	1	35	
106	2	35, 253	
107	2	232, 103 ÷ 215, 185	
108	2	108, 236 ÷ 112, 0	
109	2	220, 80 ÷ 103, 56	
110	2	112, 108 ÷ 113, 62	
111	1	0/16	
112	1	112	
113	1	113	
114	1	114	
115	1	115	
116	1	116	
117	1	117	
118	1	118	
119	1	119	
120	1	120	
121	1	121	
122	1	122	
123	1	123	
124	1	124	
125	1	125	
126	1	126	
127	1	127	
128	6	129, 239, 0, 85, 0, 85	модель объектива ?
129	1	129	

Таблица 1: (продолжение).

cmd	**N**	**ans**	**desc**
130	1	130	
131	1	131	
132	1	132	
133	1	133	
134	1	134	
135	1	135	
136	1	136	
137	1	137	
138	1	138	
139	1	139	
140	1	140	
141	1	141	
142	1	142	
143	1	143	
144	2	0/32, X	старший бит X — значение переключателя «AF/MF» (нулю соответствует AF); у EF200 первый байт 0 или 32 (если крутить кольцо управления F), второй байт см. во второй таблице
145	1	145	
146	1	146	
147	1	147	
148	1	255	
149	1	149	
150	1	150	
151	1	151	
152	1	152	
153	1	153	
154	1	154	
155	1	155	
156	1	156	
157	1	157	
158	1	158	
159	1	159	
160	2	0, 85	фокусное расстояние объектива
161	1	161	
162	1	162	
163	1	163	
164	1	164	
165	1	165	
166	1	166	
167	1	167	
168	1	168	
169	1	169	

Таблица 1: (продолжение).

cmd	**N**	**ans**	**desc**
170	1	170	
171	1	171	
172	1	172	
173	1	173	
174	1	174	
175	1	175	
176	3	13, 13, 72	
177	2	91, 92	
178	3	96, 2, 71	
179	2	104, 92	
180	1	180	
181	1	181	
182	1	182	
183	1	183	
184	1	184	
185	1	185	
186	1	186	
187	1	187	
188	1	188	
189	1	189	
190	1	190	
191	1	191	
192	2	short int	угловое положение лимба F, первый байт — старший, нуль около бесконечности (чуть левей), отрицательные числа — движение к 2.5m, чем больше модуль числа, тем ближе к 2.5m
193	1	193	
194	4	X_1, X_2, Y_1, Y_2	значение F в метрах; X – текущее F, Y – предыдущее F; $F(\text{метр}) = 2.5 \cdot X_1 + X_2/100$ (не работает у EF200!)
195	1	195	
196	2	0, 9 ÷ 10, 1	
197	1	197	
198	1	198	
199	1	199	
200	1	200	
201	1	201	
202	1	202	
203	1	203	
204	1	204	
205	1	205	
206	1	206	
207	1	207	
208	1	208	

Таблица 1: (продолжение).

cmd	**N**	**ans**	**desc**
209	1	209	
210	1	210	
211	1	211	
212	1	212	
213	1	213	
214	1	214	
215	1	215	
216	1	216	
217	1	217	
218	1	218	
219	1	219	
220	1	220	
221	1	221	
222	1	222	
223	1	223	
224	2	61, 186 ÷ 61, 172	
225	1	225	
226	1	226	
227	1	227	
228	2	30, 84	
229	1	229	
230	1	230	
231	1	231	
232	2	163, 203 ÷ 162, 105	
233	1	233	
234	2	157, 166 ÷ 163, 205	
235	1	235	
236	1	236	
237	1	237	
238	1	238	
239	1	239	
240	1	10	
241	1	241	
242	1	242	
243	1	243	
244	1	244	
245	1	245	
246	1	246	
247	1	247	
248	1	185 ÷ 188	
249	1	3 ÷ 7	
250	1	192 ÷ 194	
251	1	251	
252	1	198 ÷ 201	

Таблица 1: (продолжение).

cmd	N	ans	desc
253	1	0	
254	1	207 ÷ 208	
255	1	255	

Команды можно условно разделить на две половины: если старший бит команды равен нулю, объектив выполняет определенные действия. Когда старший бит команды равен единицы, у объектива запрашиваются определенные данные.

Команды изменения F аналогичны (за исключением разрядности ответа). Младшие 4 байта принимают значения 0100 (стоп), 0101 (F+), 0110 (F−), самый старший бит — обязательно 0. Биты 4 ÷ 6 принимают любые значения, кроме 110, 011 и 111.

4 Сводный перечень команд для EF 200

В марте 2016 г. при помощи цифрового логического анализатора были сняты логи протоколов общения фотоаппарата и объектива, в результате чего выявлены используемые команды. В таблице представлены только те команды, которые использовал фотоаппарат[1].

Таблица 2: Сводка команд EF 200

hex	dec	N	ans	desc
0x01	1	6	0xc8,0,0xc8,0,0,0	lens ID, min/max zoom, proto, brand ?
0x05	5	1	0x05	установка фокуса в положение минимума (отменяет действие 94)
0x06	6	1	0x06	установка фокуса в положение максимума (отменяет действие 94)
0x07	7	1	0x07	включить напряжение на двигателях объектива
0x08	8	1	0x08	отключить напряжение
0x0a	10	2	0xaa,0	busy poll
0x0c	12	1	0x0c	конец инициализации, за командой следует пауза
0x0e	14	1	0x0e	? встречается при включении, автофокусе, экспозиции, за ней обычно следует 0x0f
0x0f	15	1	0x0f	аналогично предыдущей, за ней обычно следует что-нибудь из 0xf0, 0x0a, 0xc0, 0x90
0x13	19	2	0x13,0x13	установка диафрагмы, второй байт – степень открытия (max: 0x80; F/2.5: 0x07; F/4.0: 0x12; F/8.0: 0x22; F/16.0: 0x32; за аргументом обычно идет 0x90, для некоторых объективов перед этой командой надо дать 0x07

[1] В расшифровке команд также использовались данные из `https://pickandplace.wordpress.com/2011/10/05/canon-ef-s-protocol-and-electronic-follow-focus/` и `http://www.rwpbb.ru/test/canonautosonyl.html`

Таблица 2: (продолжение).

hex	dec	N	ans	desc
0x50	80	2	0x50, 0x50	имеет аргумент: 0x2c..0x2f; 0x2c встречается при нажатии кнопки «set focus» и иногда при автофокусировке; 0x2d — при автофокусе и экспозиции на бесконечность; 0x2e — автофокус и экспозиция на F2.5m; в остальных случаях — 0x2f
0x80	128	x	0x81,0x87,0x00	с этого байта начинается стартовая последовательность 0x80,0x0a,0x99 (третий байт для других объективов — 0x97), видимо, узнать модель или протокол объектива
0x90	144	3	a,b,0	Состояние регуляторов объектива. Первый байт при вращении кольца управления фокусом равен 0x20 (и некоторое время после окончания вращания), иначе нуль; второй байт: биты 0 и 1 равны единице, если диафрагма не полностью открыта; бит 2 равен единице, если в данный момент кольцо вращают; бит 4 равен единице, если достигнут нижний или верхний предел F; бит 7 равен единице при положении переключателя AF/MF в MF
0xa0	160	2	0x00,0xc8	входит в состав порции данных при периодическом опросе (после инициализации), за ней идет 0xe4
0xb0	176	3	0x16,0x16,0x50	идет после 0xf0 или 0x0a; за ней бывают либо 0,0,a0, либо 0,0,c0, либо 7f,ff,0a -> ответ не меняется; min/max aperture?
0xb2	178	4	0x5a,a,b,0	? ответ зависит от положения фокуса
0xc0	192	3	a,b,0	положение лимба (в режиме «ручной фокус» возвращает нули, если подключен к фотоаппарату)
0xe0	224	2	0xc2,a	? за ней обычно следует 0xea
0xe4	228	2	0x9c, 0x6a	? за ней обычно следует 0xb2
0xe8	232	7	x	(меняются лишь первые 2 байта ответа, остальные — нули) меняется при изменении фокуса в автофокусе, за ней обычно следуют 0xf8, 0xfc; ответы при разных положениях MF: ∞,20m,10m — 0x22,0x16; 5m — 0x21,0x66; 2.5m — 0x20,0xed
0xea	234	6	x	(меняются лишь первые 2 байта ответа, остальные — нули) меняется при изменении фокуса в автофокусе, встречается и в экспозиции при ручном фокусе
0xf0	240	1	x	зависит от фокуса (0x11 — ∞,20m,10m, 0x0d — 5m, 0x12 — 2.5m), за ней всегда следует 0xb0

Таблица 2: (продолжение).

hex	dec	N	ans	desc
0xf8	248	x	x	начало последовательности 0xf8,0xfc,0xfa,0xfe, следующей после команды 0xe8 — при фокусировке и экспозиции, ответы меняются: 2.5m — 0xbd, 0xcb, 0xbe, 0xcd; 5m — 0xba, 0xc6, 0xbd, 0xca; 10m, 20m, ∞ — 0xb3, 0xbe, 0xba, 0xc5

Анализ предыдущей и этой таблицы в двоичном коде позволяет сделать следующие выводы:

- в командах, приводящих к определенному действию, старший (седьмой) бит нулевой, в запрашивающих данные — единичный;
- некоторые команды «действия» имеют следующую особенность: в старший квартет могут добавляться 0x1, 0x2, 0x4, 0xa без изменения действий команды (исключение — команда 4, для нее 0x44 приводит к иному действию);
- команды 4, 5, 6 и 7 отменяют действие команды 94 (вручную фокус перестает регулироваться).