Read FAQ v.3.2

By Xzbir / UD

Tekst Oparty Na Faktach Autentycznych J

Ogólne Informacje :

To co tu napiszę nie jest nowością ale sobie napisałem bo jeszcze chyba nikt nie pisał :) Przedstawione rysunki i poniższy text mają na celu uświadomić tylko co można odczytać (bardziej co można napotkać podczas odczytywania) więc to tylko widok tego co 'zaobserwowała' głowica podczas odczytu. No poruszyłem tu również kilka innych, myślę że interesujących tematów. **Jeżeli są tu jakieś błędy to bardzo proszę o wskazanie i ewentualne propozycje!!!!!!!**
Zwróć uwagę, że rysunki przedstawiają trochę inny zapis (odczyt) niż powszechnie to się przyjęło. Są one po prostu odwrócone (lustrzane odbicie) tak jak to się widzi przy oryginalnym odczycie. **J**

Wstęp:

Na razie (jak wiadomo) w Polsce obsługiwane są dwa rodzaje kart magnetycznych:

- Czerwone

Karty te były nagrywane (oryginalnie przez Telefonice) 2 - ścieżkowo. Nie są one już produkowane, ponieważ ich zabezpieczenia wg tpsy były niewystarczające do potrzeb. ;)) Obsługiwane teraz jedynie przez automaty tzw. 'Niebieskie' (chociaż też nie we wszystkich przypadkach – nowy czytnik) a szkoda ;)
Karty czerwone można podzielić na dwa rodzaje :

- I Generacja (seria tylko od 0 do 1023)
- II Generacja (seria od 0 do 16383)

Produkujący karty „I Generacji" nie przewidzieli, że w przyszłości pojawią się automaty tzw. „Srebrne", które z danych na karcie będą wyciągały sobie większą serię, dlatego w miejscu dodatkowych bitów (emisja) pojawiały się przypadkowe dane (czyli Śmietnik) **J**. Powstała później „II Generacja", która nie miała już w miejscu emisji „bałaganu". Bity te nie były przypadkiem wyliczenia sumy kontrolnej przez algorytm 2 i 1, tylko przyjmowały określony porządek, określający większą serię (emisję) **J**.

Automaty TPE-97/U obsługiwały w 'pełni' możliwości kart II generacji. W sumie to II - Generacja powstała z myślą o 'Sreberkach'. Co nie oznacza, że 'Niebieski' ich nie widział, po prostu z tak dużej serii wycinał sobie tylko 10 bitów, a pozostałe służyły mu tylko do wyliczenia sumy kontrolnej.

- Zielone

Te karty funkcjonują obecnie na polskim rynku ;)) Zostały tak zaprojektowane że posiadają taki przedział serii jak karty 'Czerwone' II - Generacji. Mają dodatkowe zabezpieczenia w postaci danych wyliczonych dodatkowym algorytmem i trochę innego sposobu zapisu niektórych bitów. Zapis różni się tym od zapisu starszego, że jest on rozłożony na 5 ścieżek i zawiera dodatkowe informacje na karcie (np. rozpoznawanie czy karta 'Zielona' czy 'Czerwona'). Dane z karty odczytane przez głowicę środkową (obejmuje ona ścieżki 2, 3 i 4) są sprawdzane dodatkowym algorytmem z danymi odczytanymi przez głowicę obejmującą cały pasek magnetyczny. Ten dodatkowy zapis to tzw. 'nowe jedynki'.
Tymi kartami zajmę się w dalszej części tego tekstu..

Znaczenie poszczególnych bitów:

Tutaj rozpiszę dla przypomnienia znaczenie poszczególnych bitów i danych w kartach zielonych.

- tzw. I Algorytm to algorytm zawarty oryginalnie w sofcie czytnika niebieskiego i srebrnego automatu i opisany został przez Shadowa w „**shadow_faq.txt”**.
- tzw. II Algorytm to algorytm zawarty oryginalnie w sofcie płyty głównej niebieskiego i srebrnego automatu gdzie został rozszerzony o obsługę emisji.
- tzw. III Algorytm to algorytm zawarty oryginalnie w sofcie czytnika srebrnego automatu oraz od niedawna został użyty w nowych czytnikach automatu niebieskiego. Pozwala on określić pozycję „Nowych” jedynek.

Tabela danych (bajty A....H) odczytanych głowicą obejmującą 5 – ścieżek.

A							
7	6	5	4	3	2	1	0
1 – Bit Typu Karty	0 – Bit Typu Karty	B.S.K.K. I	B.S.K.K. I	B.S.K.K. I	B.S.K.K. I	2 – Bit Emisji Karty	

B							
7	6	5	4	3	2	1	0
12 – Bit Numeru Karty	7 – Bit Numeru Karty	2 – Bit Numeru Karty			15 – B.S.K.K. II	10 – B.S.K.K. II	3 – B.S.K.K. II

C							
7	6	5	4	3	2	1	0
	15 – Bit Numeru Karty	8 – B.S.K.K. II	5 – Bit Emisji Karty	0 – Bit Numeru Karty	13 – B.S.K.K. II	4 – Bit Emisji Karty	3 – Bit Emisji Karty

D							
7	6	5	4	3	2	1	0
8 – Bit Numeru Karty	9 – Bit Numeru Karty	0 – Bit Tax Value Karty	13 – Bit Numeru Karty	2 – B.S.K.K. II	3 – Bit Numeru Karty	4 – Bit Numeru Karty	2 – Bit I.D.T.D. Karty

E							
7	6	5	4	3	2	1	0
0 – B.S.K.K. II	9 – B.S.K.K. II	1 – Bit I.D.T.D. Karty	7 – B.S.K.K. II	14 – B.S.K.K. II	0 – Bit I.D.T.D. Karty	6 – B.S.K.K. II	

F							
7	6	5	4	3	2	1	0
1 – Bit Emisji Karty	1 – Bit Numeru Karty		0 – Bit Emisji Karty	6 – Bit Numeru Karty	11 – B.S.K.K. II	8 – Bit Serii Karty	11 – Bit Numeru Karty

G							
7	6	5	4	3	2	1	0
4 – B.S.K.K. II	7 – Bit Serii Karty	14 – Bit Numeru Karty		6 – Bit Serii Karty	5 – Bit Serii Karty	4 – Bit Serii Karty	5 – Bit Numeru Karty

H							
7	6	5	4	3	2	1	0
12 – B.S.K.K. II	3 – Bit Serii Karty	2 – Bit Serii Karty	1 – B.S.K.K. II		1 – Bit Serii Karty	10 – Bit Numeru Karty	5 – B.S.K.K. II

Bit I.D.T.D. Karty – Bit Indeksu do tablicy dzielników. Tablica(0, 1, 2, 5, 8, 10, 20).
B.S.K.K. I – Bit Sumy Kontrolnej Karty (w tym przypadku cały bajt „A” określa w jakiś sposób sumę kontrolną dla Algorytmu „I”).
B.S.K.K. II – Bit Sumy Kontrolnej Karty (dla Algorytmu „II”).
Puste pola są to bity pomocnicze, które biorą udział przy wyliczaniu sumy kontrolnej zarówno dla algorytmu „I” jak i „II”.

Bit Emisji Karty (2 .. 5) – są to bity istotne dla kart „Zielonych” i „Czerwonych” II – Generacji, ponieważ jak już wcześniej wspomniałem bity te określają większą serię i były one przypadkiem w „Czerwonych” I – Generacji. Pozostałe bity zawierają te same dane dla kart „Zielonych” jak i dla „Czerwonych” I i II – Generacji. Inaczej krótko mówiąc to że różnica między kartami „Czerwonymi” I – Generacji a „Czerwonymi” II – Generacji i „Zielonymi” zawarta jest tylko w bitach emisji (mowa jest oczywiście tylko o danych jakie odczytuje głowica obejmująca cały pasek magnetyczny).

Bity odpowiadające np. za serię, numer itd. są „porozrzucane”, ponieważ Drugi Algorytm na wstępie wszystkie bity miesza (albo jak kto woli układa) i w końcu ładnie te bity składa sobie do „kupy” w serię, numer itp. Na końcu poddaje je dalszej obróbce (czyli porównuje je z sumą kontrolną zapisaną na karcie). Na tym algorytmie w sumie nie kończy się sprawdzanie karty, ponieważ sprawdzany jest jeszcze bajt „A” (a dokładniej tylko dwa bity określające „Typ Karty”) czy karta Impulsowa (Typ Karty = 2) [ten kawałek dotyczył ściśle softu z Silvera]. A jeszcze sprawdzana jest czy istnieje na białej liście i czy przypadkiem nie widnieje na czarnej. Jeżeli te wszystkie testy karta przejdzie pomyślnie to zostanie zaakceptowana. Niżej zamieściłem opis dotyczący **2 – Algorytmu** żeby nie myśleć, że jestem gołosłowny i wszystkie te rzeczy opisuje z powietrza. **J**

Drugi Algorytm można podzielić na trzy części:

1.: Pierwsza miesza bajty oraz bity:

a: Na wstępie **bajty** zamieniane są miejscami i tu przykład:

```
X := ((Bajt_z_Karty[0] and $0F) or (Bajt_z_Karty[1] shl 4))
Y := ((Bajt_z_Karty[0] and $F0) or (Bajt_z_Karty[1] shr 4));
Bajt_z_Karty[0] := Bajt_z_Karty[2];
Bajt_z_Karty[1] := Bajt_z_Karty[3];
Bajt_z_Karty[2] := Bajt_z_Karty[4];
Bajt_z_Karty[3] := Y;
Bajt_z_Karty[4] := X;
```

b: Po takiej zamianie czas (na piknik ;)) na zamianę **bitów** miejscami:

```
X := 4;
For Z := 1 To 25 Do Begin
    Dec(X);
    A := Bajt_z_Karty[X];
    Y := 0;
    While X >= Y Do Begin
        B := (A shl 7) and $80;
        A := Bajt_z_Karty[Y];
        Bajt_z_Karty[Y] := (Bajt_z_Karty[Y] shr 1) or B;
        Inc(Y);
    End;
    A := Bajt_z_Karty[X + 1];
    Y := 7;
    While Y >= (X + 1) Do Begin
        B := (A shr 7) and 1;
        A := Bajt_z_Karty[Y];
        Bajt_z_Karty[Y] := (Bajt_z_Karty[Y] shl 1) or B;
        Dec(Y);
    End;
    If X = 0 Then X := 7;
End;
```

2.: Teraz czas na kolejny kawałek, czyli wyodrębnianie Typu, Serii, Numeru, i takich tam …..

```
Typ__Karty  :=  (Bajt_z_Karty[3] shr 5) and 3;
SeriaKarty  :=  ((Bajt_z_Karty[4] and $7F) shl 3) or ((Bajt_z_Karty[5] shr 5) and 7) or
                ((Bajt_z_Karty[3] and 1) shl 10) or ((Bajt_z_Karty[2] and $38) shl 8);
NumerKarty  :=  (Bajt_z_Karty[0] shl 8) or Bajt_z_Karty[1];
DzielKarty  :=  ((Bajt_z_Karty[3] shr 7) and 1) or ((Bajt_z_Karty[2] and 3) shl 1);
TaxVaKarty  :=  ((Bajt_z_Karty[2] shr 2) and 1) = 0;
```

3.: Heh… Teraz chyba trzeba by było opisać kawałek który odpowiada za wyliczanie sumy kontrolnej, no ale chyba jednak zostawię to na inną okazję ze względów logicznych. Co byście robili gdybym wszystko podał na przysłowiowej „Tacy", a tak trochę asemblera nigdy nie zaszkodzi ;))))

Tak na zakończenie chciałbym dodać że to co jest opisane wyżej można zobaczyć sobie w oryginalnej postaci w sofcie sreberka. Stamtąd właśnie to wyciągałem….

Jakiś czas temu zauważyłem kilka fajnych właściwości tych wszystkich algorytmów. Po odpowiednim „poprawieniu" tychże algorytmów uzyskałem kilka dodatkowych funkcji czyli: możemy generować dane dla karty tak żeby zawierały one stosunkowo mało „**Zer**", „**Jedynek**" lub „**Nowych Jedynek**". Jest to dość pożyteczna funkcja – która na pewno podniosłaby skuteczność nagranych kart (zrozumiałe ze względu na nowe stany które często przysparzają najwięcej kłopotów podczas nagrywania).
Dla przykładu podam, karta impulsowa o: **Numerze: 58948, Serii: 5165, Dzielniku 8.**

– Telefonica wygenerowała : **34 – Zera, 14 – Jedynek i 16 – Nowych Jedynek,**
– Taki algorytm jak używa połowa polski wygenerował : **40 – Zer, 13 – Jedynek i 11 – Nowych Jedynek,**
– Zmodyfikowany algorytm wygenerował : **36 – Zer, 23 – Jedynki i 5 – Nowych Jedynek,**

Algorytm był tak ustawiony żeby generował jak najmniejszą ilość nowych jedynek.

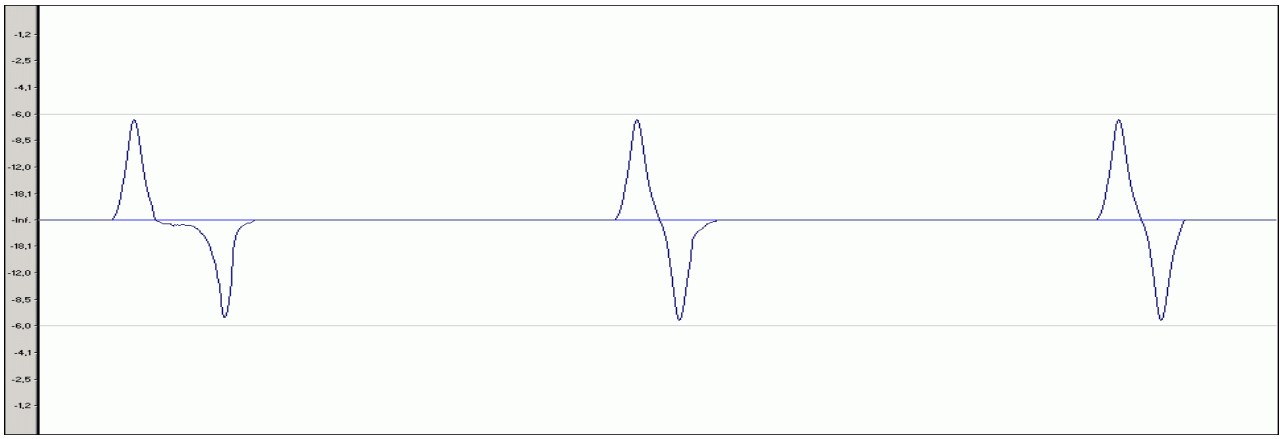
Dane z środkowej Głowicy:

Dane odczytane przez głowicę środkową są trochę inaczej traktowane niż dane odczytane głowicą kasującą (nie przenoszą one konkretnych danych dotyczących np.: numeru karty itp.). Głowica środkowa traktuje zapis w ten sposób, że jeżeli napotka na swej drodze nowy stan (nową jedynkę) to odczytuje ją jako „1” a pozostałe napotkane stany (bity) traktuje jako „0”. Następnie te dane testowane są algorytmem „III” z danymi odczytanymi przez głowicę kasującą. Jeżeli wynik jest poprawny to karta uznana jest za „Zieloną” a jeżeli nie to karta uznana jest jako „Czerwona”.

Nowy zapis :

Odczyt z poszczególnych głowic i obraz poszczególnych ścieżek można ogólnie przedstawić w ten sposób jak to zrobiłem poniżej:

1, 3, 5 Ścieżka w „Zielonych” :

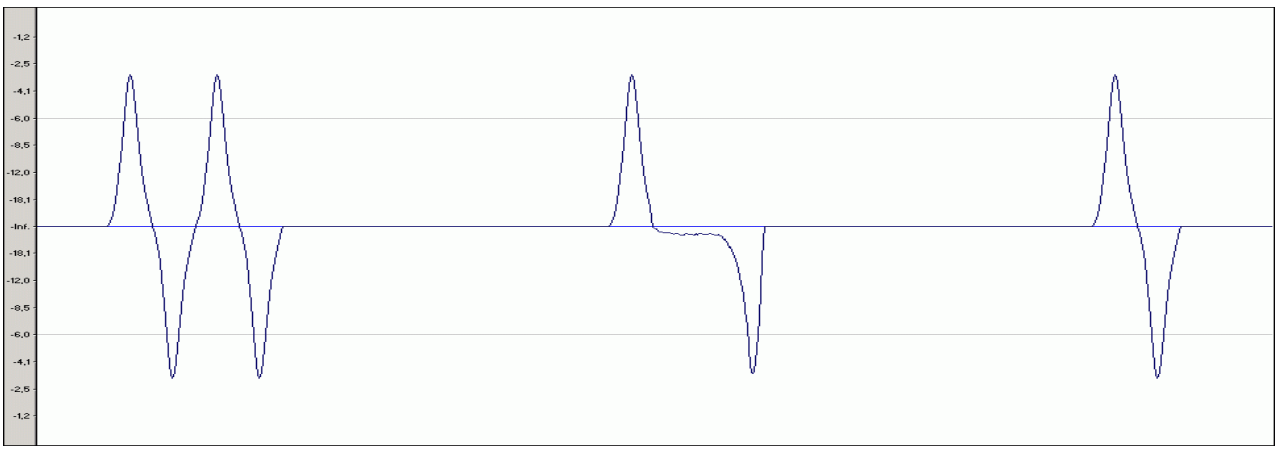


To jest cześć „**A**”
„Nowej 1”

To jest cześć „**A**”
„Zwykłej 1”

To jest cześć „**A**”
Zera

2, 4 Ścieżka w „Zielonych” :



To jest cześć „**B**”
„Nowej 1”

To jest cześć „**B**”
„Zwykłej 1”

To jest cześć „**B**”
Zera

Zauważ że odczyt z ścieżek 1,3,5 jest mniej wzmocniony w stosunku do odczytu z ścieżek 2 i 4 a to dlatego że ścieżki te są węższe. Głowica później sobie ładnie te ścieżki sumuje. Składając do kupy cześć „A” z częścią „B” otrzymamy zapis jaki pokazany jest poniżej. Czytnik Silvera dla odmiany od Niebieskiego posiada jedną głowicę ale z dwoma uzwojeniami (takie jakby 2 w 1). Jedno z tych uzwojeń nawiniętych na rdzeniu, to o mniejszej rezystancji, 'obejmuje' 5 ścieżek. Zastosowane w czytniku z zamysłem kasowania danych z karty jak również odczytu. Dane odczytane przez tę głowicę są istotne w dalszej 'obróbce' przez płytę główną automatu. Drugie uzwojenie (to o większej rezystancji) wykorzystywane jest do odczytu tylko środkowej części karty, czyli ścieżki 2, 3 i 4. Odczyt z tych dwóch głowic można przedstawić w przybliżony sposób tak:

Głowica Kasująca (wszystkie 5 - ścieżek):

„Nowa 1” „Zwykła 1” Zero

Głowica Środkowa (ścieżki 2, 3, 4):

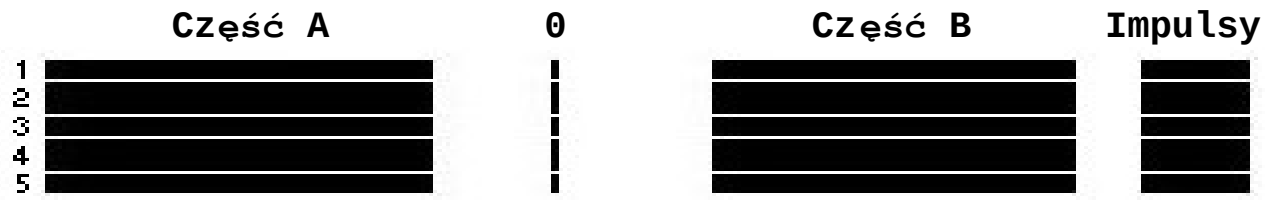
„Nowa 1” „Zwykła 1” Zero

W pierwszym odczycie (z głowicy kasującej) można zauważyć że wszystkie ścieżki zsumowały się i nowa jedynka zbytnio nie odbiega od zwykłej jedynki. Ścieżki po sczytaniu są w stosunku 2:3 ale stosunek sum wymiarów tych ścieżek jest jak 1:1 (bardzo istotne zjawisko). Dane z karty odczytane tą głowicą są brane pod uwagę podczas testowania trzecim (dodatkowym) algorytmem z danymi odczytanymi przy użyciu środkowej głowicy. Ten odczyt jest potrzebny do odczytu danych z karty czyli numer serii, numer karty, ilość pozostałych impulsów itd.

Drugi odczyt (z głowicy środkowej) jest bardzo istotny dla kart zielonych, ponieważ środek nowej jedynki przechodzi przez zero ale nie osiąga max wartości (pokazane na rys.) ten nowy stan potrzebny jest „Silver-kowi” (czytnik) do rozróżniania koloru karty (czerwona/zielona), również użyty po to by utrudnić ewentualne próby nagrywania poza firmą „Telefonica” **J J J J J J J J J J J J J**. Stosunek ścieżek w tym odczycie jest jak 2:1 ale stosunek zsumowanych wymiarów jest jak 3:1.

Wygląd fizyczny ścieżek :

No tutaj zamieszczam taki rysuneczek który **OGÓLNIE** pokazuje jak wygląda zapis magnetyczny na karcie i stosunek tych ścieżek (coś przybliżonego do tego pojawi się po posypaniu karty np.: Tonerem – więc zaoszczędziłem wam paprania się i brudzenia wszystkiego do około). Chciałbym tylko przypomnieć, że nie tylko wymiary wszystkich ścieżek są istotne ale również odległości między nimi (proszę się nie sugerować poniższymi wymiarami).:



Ten zapis pochodzi z karty która miała jeden kredyt (dzielnik 8) ;)))))))

Na zakończenie o hybrydce:

Myślę, że jest to interesująca sprawa nie wymyślona i rozpoczęta przeze mnie lecz przez innego fachowca. Chyba się nie obrazi jeżeli troszkę sprostuje to co wcześniej napisał (może nie ma czasu sam tego zrobić – dlatego zrobię to ja) chodzi tu o opis hybrydy z Niebieskiego czytnika autorstwa **Leer-a.**
Ten pomysł na 'odczytywarkę' zbudowaną na Hybrydzie wziął mnie ostatnio dość mocno, a tym bardziej, że w listach często padają pytania jak można odczytać kartę i jak zrobić sobie 'odczytywarkę'. Napiszę jeszcze raz dla pewności żeby takie pytania już raczej nie padały.

Może nie długo podam razem z tekstem program który będzie reagował na dane wysyłane przez hybrydę. Ale na razie ograniczę się do opisania krótko co można wycisnąć z takiego układu jakim jest hybryda.
Jest jeden istotny fakt że to urządzonko służy czytnikowi do rozpoznawania zapisu na karcie. Czyli to on podaje takie odpowiednie stany do procka żeby była możliwość wyeliminowania fałszywych, źle nagranych, bądź też rozpoznania czy głowica jest jeszcze w stanie używalności. Opisane wyjścia z hybrydy 1, 2 i 5 służą do detekcji stanów zapisanych na karcie. Na tych trzech pinach zawsze panuje stany wysoki (logiczna '**1**') a jakiekolwiek zmiany rejestrowane są w postaci przejścia ze stanu wysokiego w stan niski. Każdy stan na określonym pinie będzie trwał tyle ile trwa określony stan na karcie. Krótko mówiąc :

1 pin – Na nim zawsze pojawi się stan **niski** jeżeli głowica napotka na pierwsze 'wybrzuszenie' każdego bitu (czy to będzie jedynka nowa, stara lub zero).

2 pin – Na nim pojawi się stan **niski** jeżeli odczytywany bit będzie miał dołek może to być jedynka lub zero.
Testy dowiodły, że jeżeli karta została nagrana **niepoprawnie** czyli była za mała amplituda tych dwóch dołków w jedynkach (lub jeden z nich był za mały) to nie został on w ogóle uwzględniony na tym pinie, nie zmienił się stan z wysokiego na niski. No i właśnie żeby zaoszczędzić stanie pod automatem i testowania kart nagranych we własnym domowym zaciszu należy sobie testować karty na samej hybrydzie która powie nam gdzie jest błąd i będzie wiadomo co należy poprawić …

5 pin – Tutaj zawsze się pojawi stan **niski**, kiedy pod głowicą znajdzie się dołek przeciwny do tego, który zawsze jest wyłapywany na pinie 1. Krótko mówiąc ten stan pojawi się tylko wtedy gdy mamy do czynienia z zerem bo tylko ono ma taki dołek. Właśnie w tym jest istota całego układu, że gdyby nie było takiej detekcji poprzez pin 5 to jedynka mogła by mieć takie dołki jak zero, a zero natomiast mogło by mieć taki dołek jak jedynka i nic by się nie działo (czytnik rozpoznawał by to jako poprawny zapis). To właśnie ten pin odpowiada między innymi za prawidłowe rozróżnianie danego bitu jak również za to żeby jedynka nie przekraczała danego progu i zero nie schodziło poniżej tego progu.

Teraz po zrozumieniu tego kawałka tekstu nie powinno być żadnego kłopotu ze zbudowaniem sobie 'odczytywarki - Full wypas', która będzie nam podawała numer, zapis bitowy na karcie no i w ogóle super. Nasuwa się taka prosta myśl żeby to urządzenie wykorzystać do własnych potrzeb. Chodzi o to że można wykorzystać to urządzenie do testowania kart zaraz po nagraniu (wtedy dowiemy się od razu czy dana karta zostanie zaakceptowana przez automat czy też nie) Ja np. zrobiłem sobie to tak:

Zbudowałem całość na czytałce od Blue. Podłączyłem pod LPT przekaźnik przez tranzystory, który sterował mi wyborem głowicy. Potem każdy z wymienionych pinów połączyłem do wybranej nóżki w LPT i nie jest konieczne stosowanie dodatkowej elektroniki (krótko mówiąc zaoszczędzimy kasy i czasu na montaż elementów i co za tym idzie układ będzie szybszy - co jest wskazane). Całość zasilana 5V. No i to koniec całego układu.

A dodałem sobie dla bajeru przełącznik (chodź można byłoby sobie od razu zrobić za pomocą przekaźnika) który przełącza mi głowicę kasującą raz do zasilania (w celu kasowania kart) a w drugiej pozycji do odczytywania kart. Również nie widzę problemu żeby zmodyfikować troszkę program i użyć nowej głowicy z niebieskiego (tej czytającej tylko środek) i zrobić sobie odczytywarkę która rozpoznawałaby nowe jedynki.

P.S. Do wszystkich piszących e-maile proszę żebyście nie męczyli mnie pytaniami odnośnie nagrywarek itp. Ja nie piszę tego tekstu tylko po to żeby sobie napisać (bo nie mam co robić). Piszę, żebyście nie zadręczali mnie pytaniami np. jak nagrać nowe jedynki albo jak to jest że dzieci się nie rodzą na drzewach tylko wychodzą skąd indziej… . Przecież można wypożyczyć książkę i poczytać o budowie środowiska lub też przeczytać powyższy tekst i troszkę pomyśleć samemu dlaczego się tak dzieje.

Szczególne Podziękowania i Pozdrowienia dla :

- ***Kołnierzyk - a***
- ***Nol - a***
- ***Shadow - a***
- ***GoaT - a***
- ***... i pozostałych których zapomniałem wymienić…***

The End:

No i to na tyle ::::::::::
Najlepiej co można zrobić to samemu odczytać sobie kartę i zobaczyć jak to wszystko wygląda. :)
Ewentualne pytania i uwagi proszę przesyłać na adres:

e-mail:

Xzbir@poczta.onet.pl