Niki 2 cartridge reverse engineering *which came to be AR3 reversing – read on!*

by Jens Schönfeld

Niki2 is a multi-functional C64 cartridge that was supposedly very popular in Italy. As a little background info, you have to know that copyright laws were very "open" in Italy back in the 80s. Friends of mine who returned from summer vacation in Italy often told storys of shops where they officially bought 60-minute tapes with lots of games on them. Niki2 seems to be the preferred tool for making such tapes, and the cartridge itself also feels like it is not 100% compliant with the common perception of what copyright is (I can't help myself, but that fastload reminds me of Action Replay).

This cartridge was given to me during the 0xAA party in summer 2006 by Ready./Level 64, who also won the combined competition with his Bike64 contribution.

outer appearance

The cartridge comes in a black case with a sticker on it. The sticker has been printed with a typewriter or a typewheel printer. It just says "Niki 2". Two buttons are in about the same place as the two buttons on an Action Replay. On the cartridge that was given to me, these buttons are red, but it might be different on other cartridges.

inner values

The cartridge is closed with a single screw. After opening, a low-quality circuit board becomes visible. There is no solderstop on the board, the contacts to the C64 are not gold-plated, and the board seems to be fully hand-soldered. None of the parts has a socket. Some TTL chips and a 32KByte Eprom with a handfull of discrete parts make the circuit. Although the cartridge has a freezer function, it does not feature any memory.

Used chips

27256: 32KByte Eprom
74ls74: Two D-type flipflops with async set and reset
74ls174: 6-bit D-type flipflop with async reset
74ls125: four tri-statable drivers
74ls163: 4-bit syncronous binary counter
74ls05: six open-collector inverters

The 74ls74 in conjunction with the counter is wired as a freezer logic. It's not the safest circuit, especially because certain (unused) inputs are not pulled high or low, but are simply left floating. Think of this as "uninitialized variables" if you're a programmer.

Flipflop U3b is reset on power-up, which brings output Q to low. This in turn keeps the counter from counting. Pressing the freeze button brings IRQ and NMI to low. Also, the Q output of U3b is pushed high, which lets the counter count, if it is not held by the BA signal. After five continuous free cycles, the flipflop U3a is set, bringing the Q output high, enabling the 6-bit flipflop. At the same time, IRQ and NMI are cleared and the inverted Q output pulls the GAME line low, enabling the Ultimax mode and mapping in the cartridge's own IRQ vectors (ROM at $e000, bank 0 of the Eprom).

The register is now enabled and has the contents $00. While the register is enabled, freezing is not possible – the freeze button is disabled.

The 6-bit flipflop forms the only register of the cartridge. It is mirrored over $de00 to $deff. Only five bits of the register are used:

bit 0: Eprom banking bit 0 (bank address 13)
bit 1: controls the GAME line (0 sets GAME low, 1 sets GAME high)
bit 2: Freeze-end bit (disables the register and hides any rom bank)
bit 3: controls the Exrom line (1 sets EXROM low, 0 sets EXROM high)
bit 4: Eprom banking bit 1 (bank address 14)
bit 5 to 7: unused.

Notice that bits 2 and 4 are the same as on the Action Replay. Also notice that EXROM and GAME bits are in different locations, and they are inverted compared to the polarity on Action Replay V6. Just like on Action Replay, reading the $de00 register will trash it.

Four memory configurations can be set in te $de00 register, where each of the four configurations can use one of the four Eprom banks:

x: bit can be any value
b: banking bit
0/1: fixed value

%xxxb000b
memory map:

$0000 - $0fff:	C64 memory
$1000 - $cfff:	nothing – random read value, writes go nowhere.
$d000 - $dfff:	standard C64 IO with no changes
$e000 - $ffff:	8K Eprom bank

This memory map cannot be affected by the processor register $0001. No matter what value has been written to $0001, the above memory map is active.

%xxxb001b
This value sets the normal C64 memory map. All ram/rom/IO switching with $0001 is possible. Only $df00-$dfff carries a mirror of the last page of the selected 8K bank.

%xxxb101b
This value activates an 8K bank in $8000-$9fff and a mirror page of that bank in the IO area $df00-$dfff. Ram/rom/IO banking with $0001 is possible with this setting.

%xxxb100b
This setting maps an Eprom bank to $a000-$bfff. Caution: With the standard $0001 value of $37, the memory area between $8000 and $9fff is empty for reading (writing reaches C64 memory). A $0001 value of $36 maps memory to that block, but leaves an Eprom bank between $a000 and $bfff. The $df00 mirror does not exist with this setting.

A value of **%xxxxx1xx** will disable the cartridge completely until the next freeze. As you might have guessed, the freeze button is put back to function with this write access.

Specialties of the hardware

It should be noted that the cartridge has serious design flaws. The reset line pulls several lines low through diodes, where one of the lines is a push-pull line (inverted Q of U3a). Sooner or later, this could result in a defective U3 chip. Further, input signals of the counter are not pulled to stable values. A capacitor on the $de00 select line seems to eat glitches. The diode logic that controls the count-enable of the 74ls163 is not properly pulled high – the circuit will probably not work if different vendors of the TTL ICs are used.

The Capacitor/diode combination C1 and D3 seems to pull Exrom low for a short period of time after reset. This will probably get around the software-anti-reset with the CBM80 magic, but 100nF seems a little small for this. It might work in one case, but won't be reliable over the full temperature range. Also, the delaying property of the C1 capacitor is also active when releasing the Exrom line with the register. In other words: You release the line with a write to the register, but memory in the $8000 area is not available right away. It'll take a few cycles until the change takes effect, and the time is not predictable, as the pull-up resistor is in the computer, not the cartridge.

Another flaw is that the GAME line is pulled low during a reset, but it is left floating again with the end of the reset pulse. This is a classic race condition: It is totally unpredictable how the cartridge will behave in different versions of the C64 or the C128, which is probably the reason why I've had different beaviour on power-up: Most of the times, the computer starts with the known 38911 basic bytes free, but sometimes it does not start at all. In any case, there is no startup-screen. The fastload utility must be activated through the freeze menu.

The R4/C3/Q1 combination seems like a waste of money with four unused open-collector inverters in the 74ls05. What is C3, a delay element?? Are you kiddin'? This is supposed to be a digital circuit!

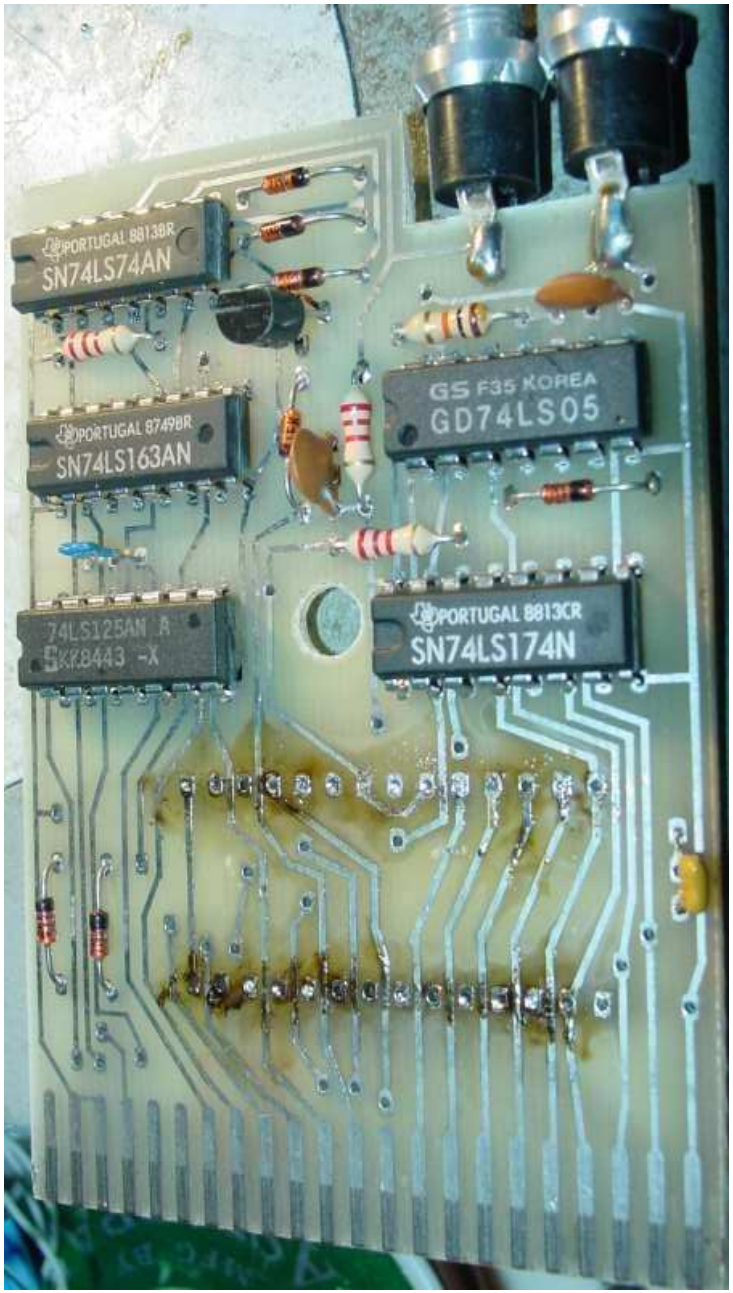
The freezer circuit is totally funny – the number of cycles to wait is a plain guess with no relation to what the CPU actually does when serving an IRQ or NMI. Also, the counter is reset when the VIC is accessing the bus, which is plain wrong. The freezer circuit can be challenged with programs that have sprites activated and more than one freeze-attempt might be necessary to get it right – I'd expect it to fail in 90% of the cases when FLI is displayed.

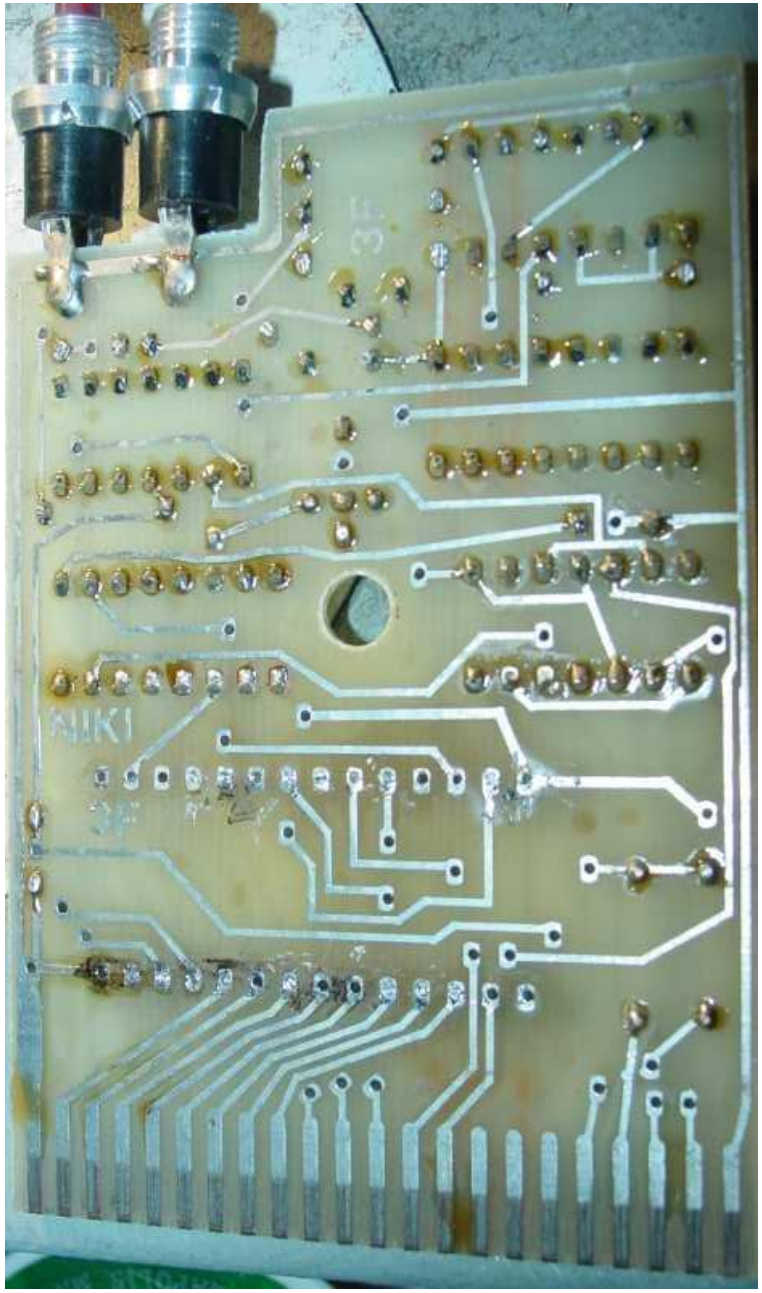
The wired-AND on the outputs of the 74ls125 is also plain wrong. Outputs 1, 3 and 4 are wired together, they might be enabled at the same time, but the inputs are intended to have different input values. In other words: Three totem-pole outputs are working against each other. The circuit only works, because the LS-TTLs can sink more than they source.

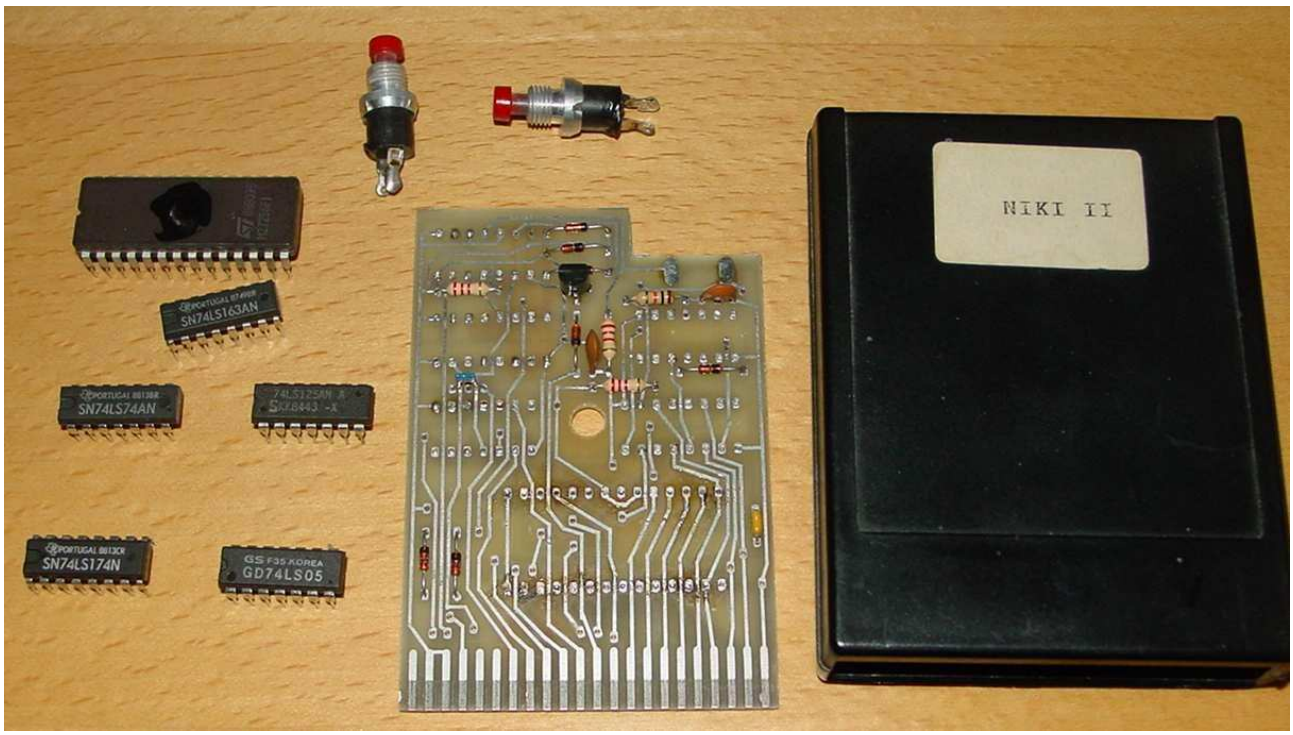
Last not least, the only blocking-capacitor is just 10nF. It is good design practise to have at least one 100nF ceramic capacitor per chip, but "good design practise" has not been practised here. I would not call this design, but a bad hack. I'll leave it up to others to comment the software.

Pictures

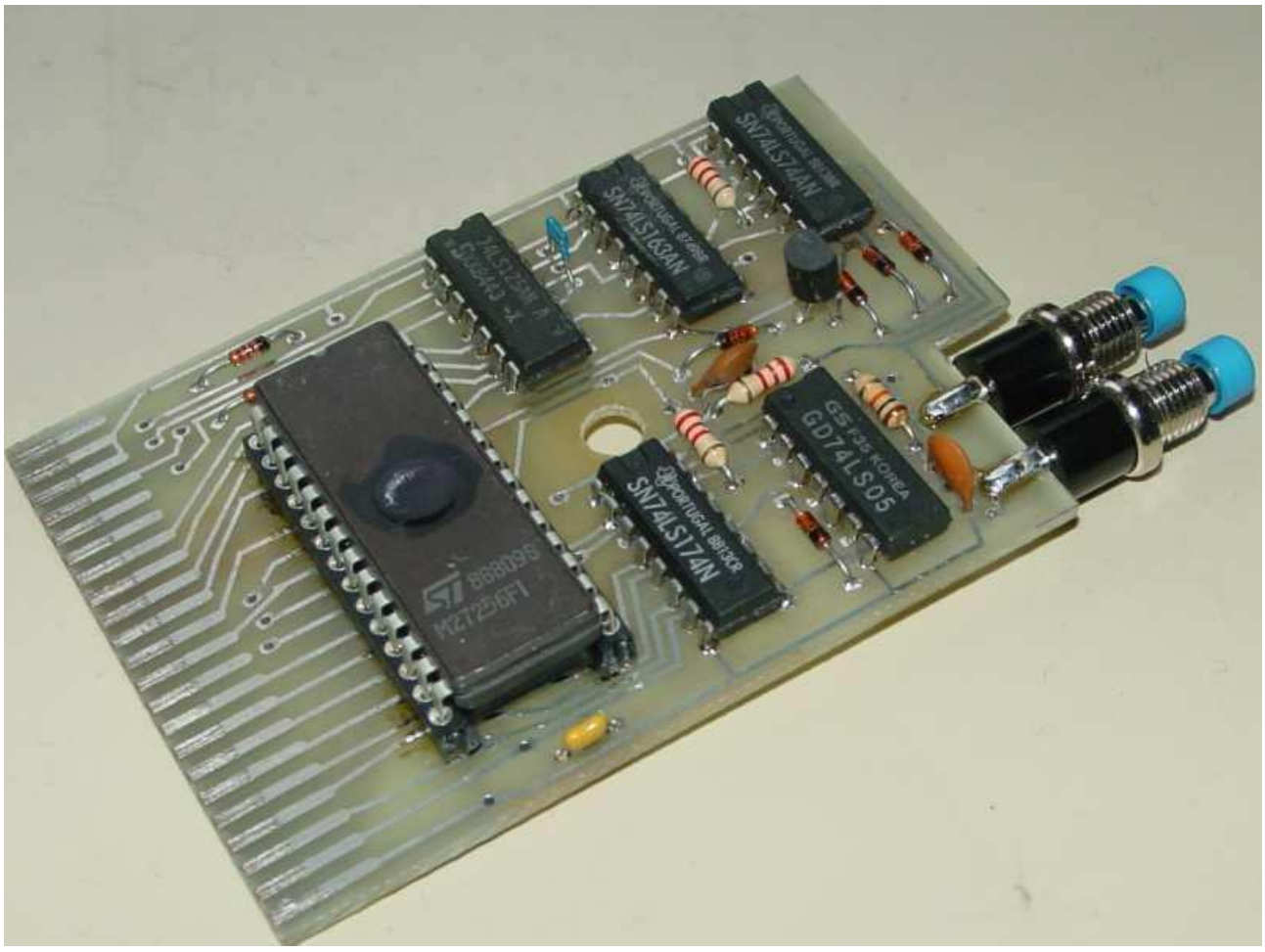
Over the course of reverse-eingineering, all chips have been removed to follow the traces, then all the parts have been put back together to get them in a working order. The buttons died at some point, so I replaced them with the new light-blue MMC Replay buttons.


PORTUGAL 8813BR
SN74LS74AN
GS F35 KOREA
GD74LS05
PORTUGAL 8749BR
SN74LS163AN
74LS125AN A
PORTUGAL 8813CR
SN74LS174N


NIKI

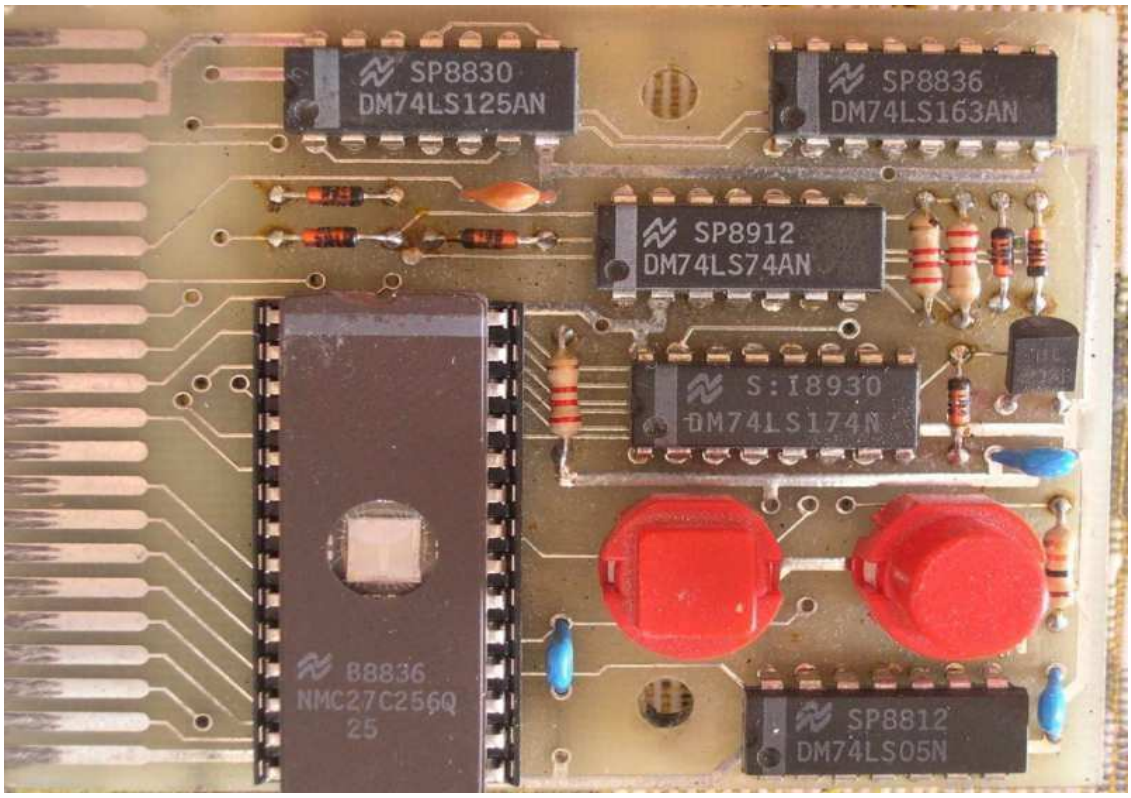


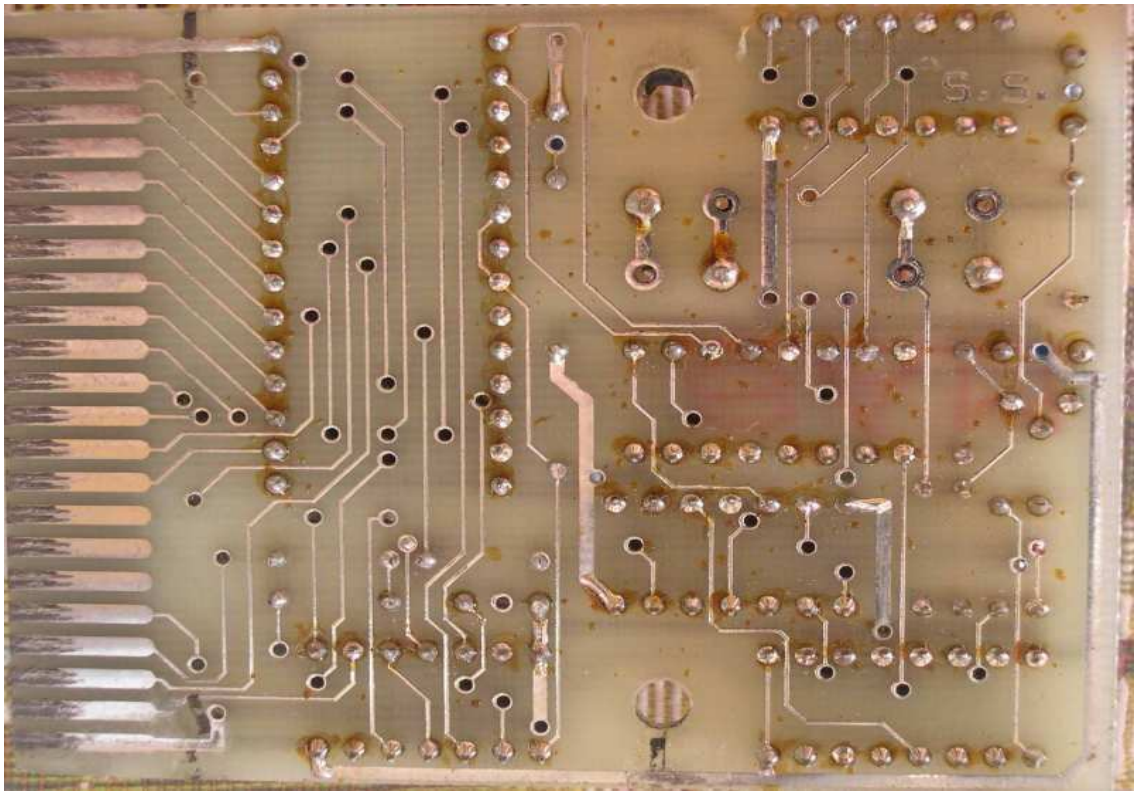
...and everything back in working condition:



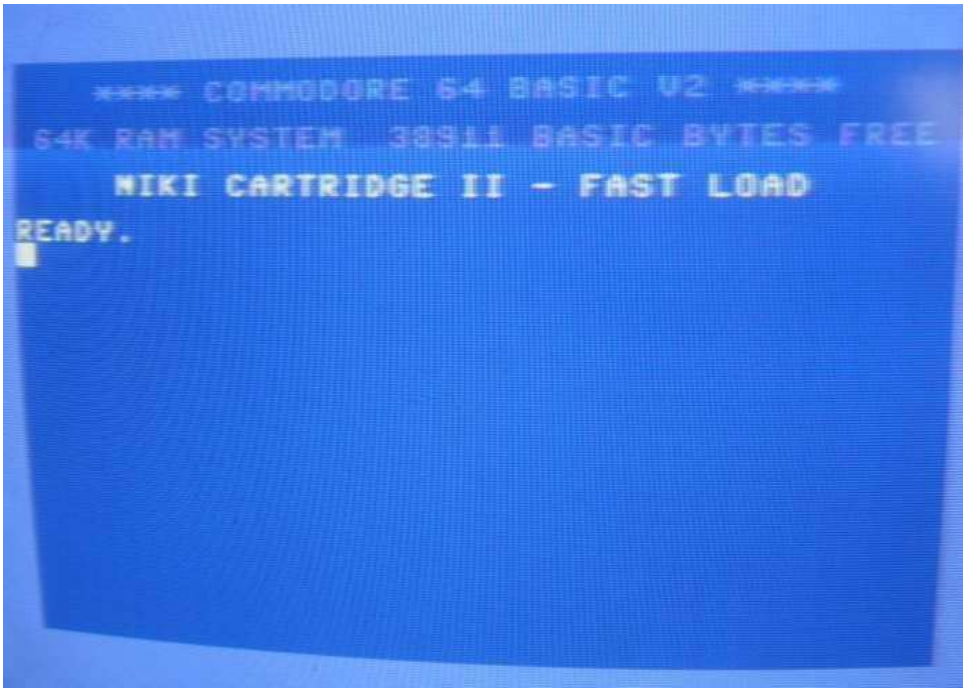
Captain Miky 2 cartridge

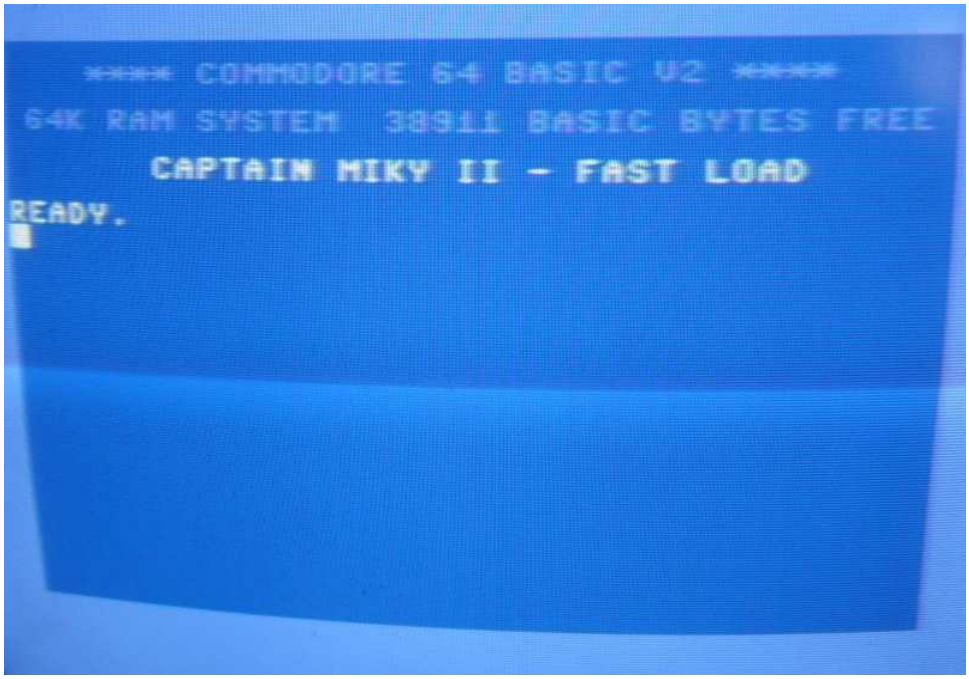
Groepaz sent an archive to me that was forwarded by iAN CooG/HokutoForce. The name of the original supplier is unknown at this point. The contents showed an Italian cartridge called "Captain Miky 2".





With this amazing likeliness, I immediately tried burning the 32K Eprom image into a new Eprom and put it into the (new) socket of my Niki2 cartridge. What can I say, it works! Here are the two fastload-pictures:



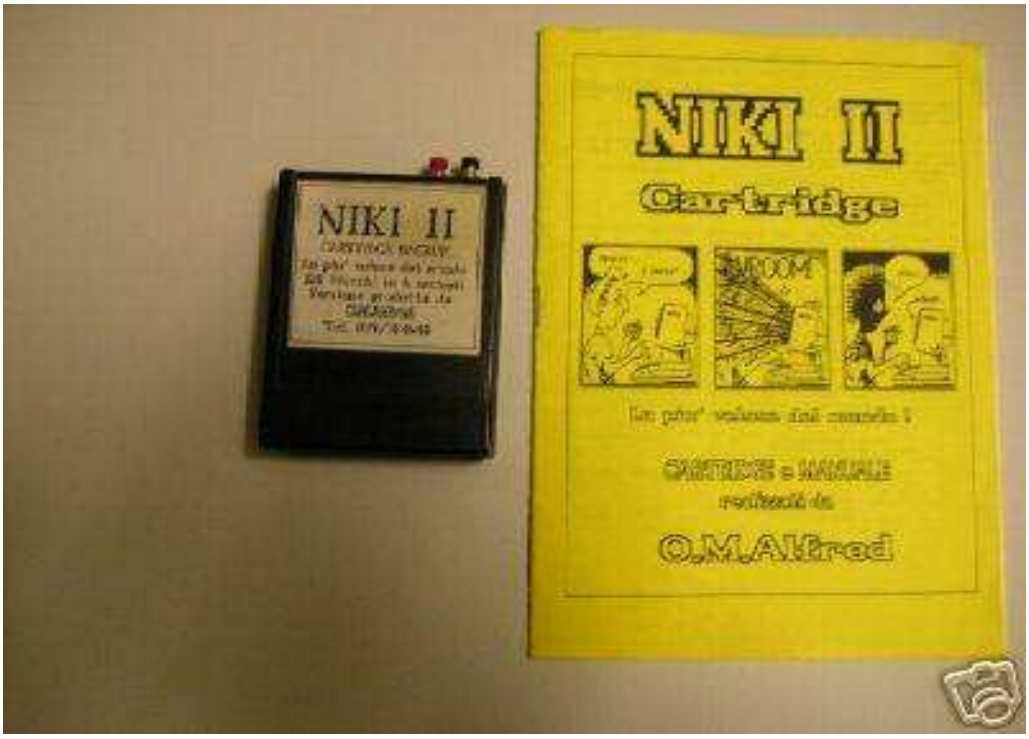


Remember that the cartridge starts with the normal 38911 basic bytes screen. You only get into a menu screen by pressing freeze. All menus are Italian, so I don't understand a single word.

More derived carts

Browsing through eBay Italy, I have found one more cartridge that seems to be based on the same hardware. The name is "Final Turbo IV". The buttons are in the same spot as the buttons on Captain Miky 2, and the name points to, well, "borrowing ideas from other products". The "IV" might have been borrowed from the real source of the software, which is presumably AR4 (the last update that works on this hardware).
I'm probably violating copyrights myself here, but here's the picture from the auction:

Other versions of the Niki 2 cartridge were equipped with a nicer sticker, as this eBay photo shows:



The original: Action Replay 3 by Datel

User Mangelore (Fotios) posted this picture of an AR3 on the forum of lemon64.com:

It should now be obvious that all the Italian cartridges are derived from the Action Replay V3 hardware. Further, it's more than obvious why Datel started to protect their hardware design with a custom chip. They already did some interesting protection by using capacitors that look like resistors to a an electrically iliterate person (fairly uncommon axial types).

I still don't understand why they used an open-collector transistor circuit for the local reset/disable, but used a (fairly expensive) 74ls05 open-collector inverter for driving the EXROM and GAME lines. I bet that two transistors and base-resistors would have been cheaper than a 74ls05 back in the days. The delay property of C3 would have surely worked on the input of the 74ls05. Maybe I'll meet the original designer one day and he'll explain all his reasons to me...

The Eprom on an AR3 cart is a 27128 (16KByte), and it works fine on the Niki2 hardware, which is the final proof that the hardware is really identical. An AR4 rom dump (32K) also works fine and has the look&feel of the Italian cartridges. If you downloaded this PDF only, go to www.c64upgra.de to download the full archive including all rom dumps that are known to work on this type of hardware and a scan of the Italian Captain Miky2 manual, taken from Ready64.

Schematics (drawn with Pulsonix)

U1
C64_expansion

U5
SN74LS125AN
funny wired-AND

this line shoulde be pulled high.

R1
2k2

U7
M27C256B10B1

U4
SN74LS174N
ethex register, Not read-proof.

U2-b
U2-a
SN74LS05N

C1
100n

D3

D7

D4

D5

D6

R3
2k2

R4
10K

Q1
BC237

C3
10n

U3-a
SN74LS74AN

U3-b

R2
2k2

BTN1.2
Pushbutton
BTN1.1
Freeze button

BTN2.1
Pushbutton
reset button
BTN2.2

C4
1n

U6
SN74LS163AN
so many input pins floating??

Spare
U2-c
U2-d
U2-e
U2-f

C2
10n
One 10nF blocking cap. Wow.

AUTHOR: Jens	LAST SAVED: 04.02.2008
CHECKED:	DATE:
ISSUED:	DATE:

COMPANY NAME:		
DESIGN TITLE:		
PAGE: Page1	DRAWING NO.	REVISION:
SCALE:	SIZE: A3	SHEET 1 OF 1