Niki2 cartridge reverse engineering

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).

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: loadable shift register
74ls05: six open-collector inverters

The 74ls74 in conjunction with the shift register is wired as a freezer logic. It's not the safest circuit, especially because certain (unused) inputs are not pulled high or low, but 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 shift register from shifting. Pressing the freeze button brings IRQ and NMI to low. Also, the Q output of U3b is pushed high, which lets the shift register shift, if it is not held by the BA signal. After three cycles, the flipflop U3a is set, bringing the Q output high, enabling the 6-bit flipflop. At the same time, the inverted Q output pulls the GAME line low, enabling the Ultimax mode and mapping in the cartridge's own IRQ vectors.

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 the Action Replay. 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.

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 shift register are not pulled to stable values. A capacitor on the $de00 select line seems to eat glitches, but the developer did not check when these glitches actually take place (man, look at phi2!). The diode logic that controls the shift-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.

The worst design 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.

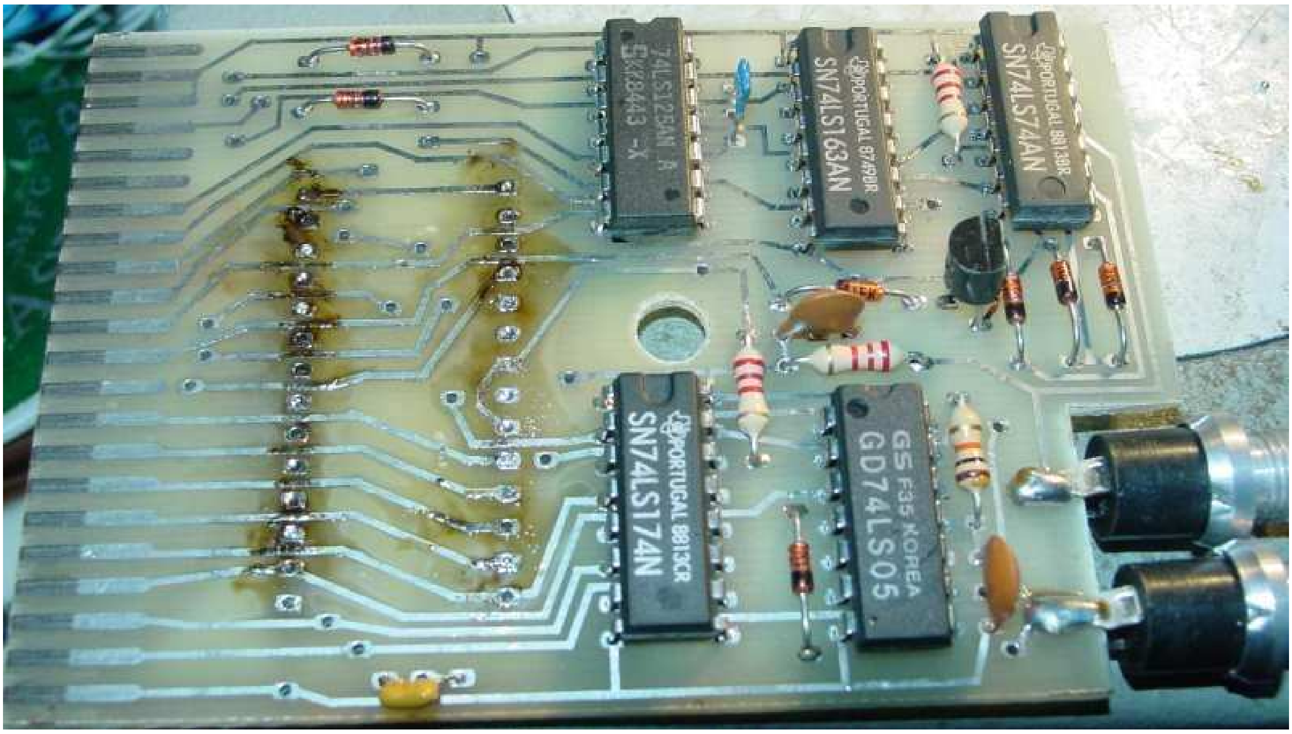
The R4/C3/Q1 combination seems like a waste of money with four unused open-collector inverters in the 74ls05.

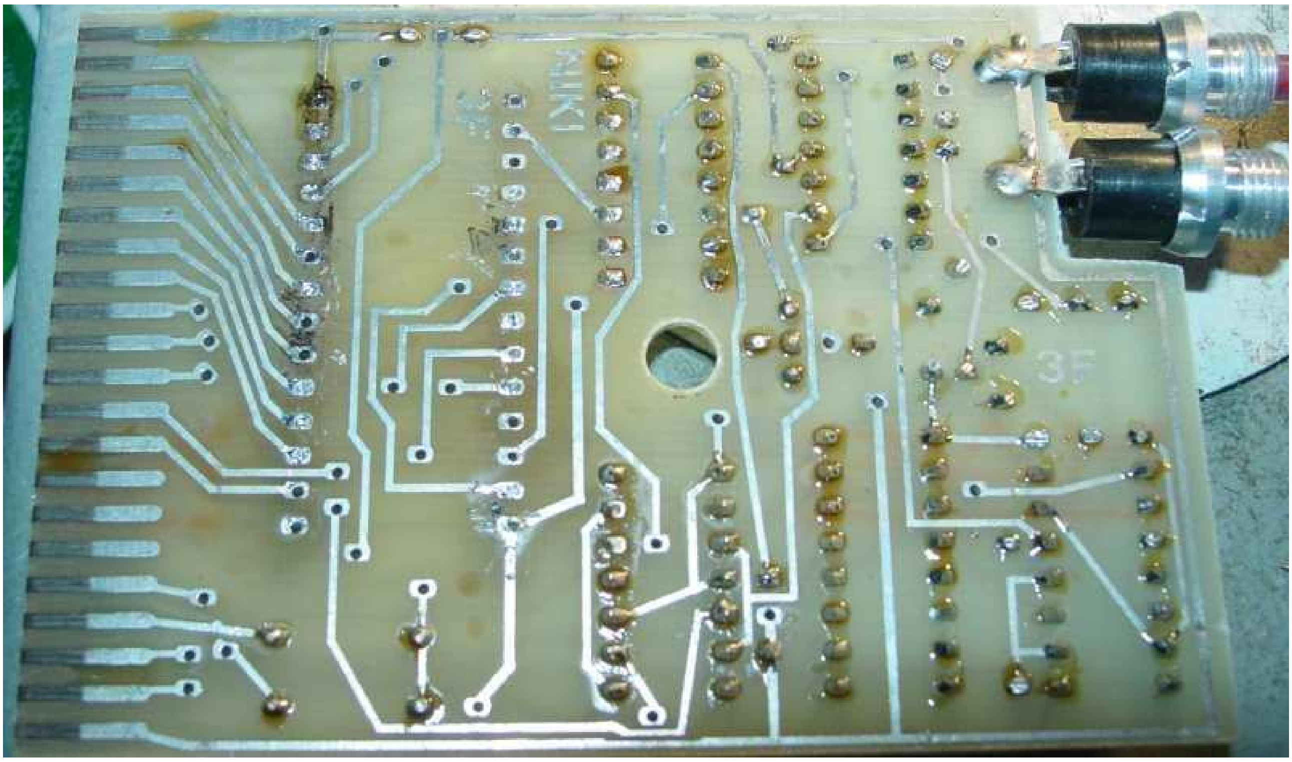
Last not least, the only blocking-capacitor is just 10nF. It is good design practise to have at least one 100nF ceramic capacitor per chip, but "good design practise" has not been practised here. I would not call this design, but a bad hack. I'll leave it up to others to comment the software.

February 1st, 2008: Jens Schönfeld

Pictures

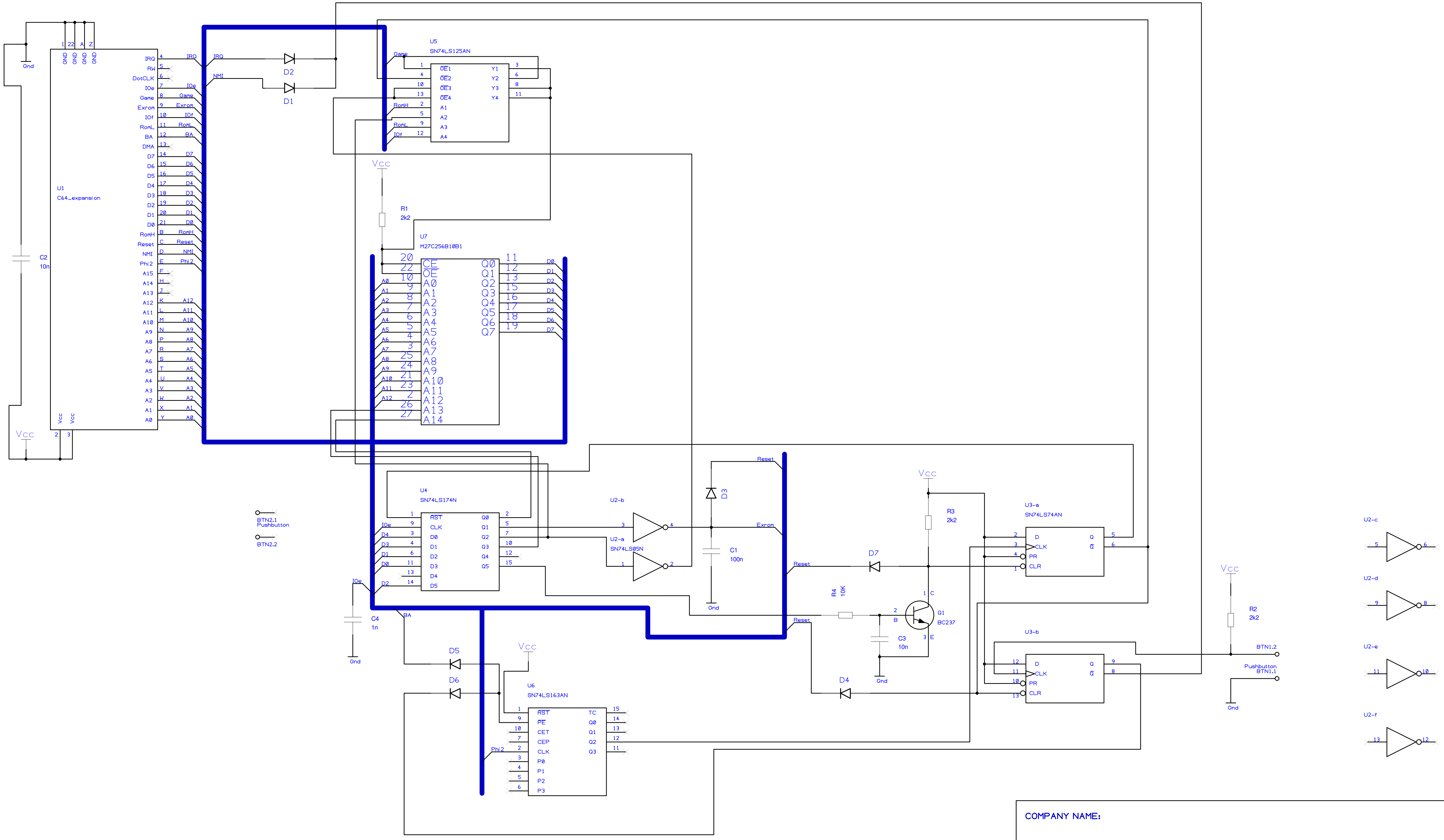
These pictures were taken after the Eprom was already removed. Over the course of reverse-eingineering, all other chips have been removed to follow the traces.





Schematics

drawn with Pulsonix



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

AUTHOR: Jens	LAST SAVED: 02.01.2008
CHECKED:	DATE:
ISSUED:	DATE: