gc-forever - Gamecube/Wii Forums

Gamecube/Wii support & news forums https://www.gc-forever.com/forums/

Open source Drivechip

https://www.gc-forever.com/forums/viewtopic.php?f=36&t=403

Open source Drivechip
by MrSporty
Posted: Sun Feb 13, 2011 1:35 pm

Ive created this thread to keep the "Show off your Cube!" thread on topic.

It will be an attempt to provide a free alternative to the drive chips currently available for the cube. Admittedly for most people a commercial chip like the XenoGC will of course be the best option (im told they will be coming to the GC-Forever webstores at a very reasonable price soon, so definately look there for one). This will be mainly for the people either interested in the lower level stuff of how the chip works or just plain like twiddling around with chips and bits and burning their fingers.

The initial work will be to dump the data from a XenoGC v1 and then a DuoQ (This is all i have at the moment). Im pretty sure the DuoQ is just a rip of the xeno anyway with a broken version of the setup screen. This ISNT me trying to dump either of the codes by reading the MCU on the modchip. I know they are both locked. This effort will be to dump the serial data that is read and written to the drive (drivecode) and recreate an open source mod to replicate that.

Here is my setup at the moment :



The 6 wires that the drivechip uses are brought out to the breadboard so i can intercept the signals using my logic analyser (the silver box with the yellow/orange wires).

The drives debug port is an SPI interface http://en.wikipedia.org/wiki/Serial_Per ... erface_Bus. So we can see that the 6 wires consist of 2 power and 4 for the SPI.

Ill post a bit more shortly as im just going to grab some data so you can see what im trying to do.

Re: Open source Drivechip

by emu_kidid Posted: Sun Feb 13, 2011 1:41 pm

You will need to have this done on all 4 drive revisions to dump the patch code data, but the basics should be the same (i.e. the way it checks the drive for the version and uploads the actual code, but the offsets will probably be different)

2001/06/08 (Very common original drive)

2002/04/02 (Pretty rare drive to find)

2002/08/23 (Last drive DOL-101 and late DOL-001 era)

2001/08/31 (Panasonic Q)

Re: Open source Drivechip

py yamaharacer Posted: Sun Feb 13, 2011 1:45 pm

will the code or the hex file be public so that we can flash it on our own atmel atmega 8l chip? i already have some here because of this i am asking.

Re: Open source Drivechip

by MrSporty Posted: Sun Feb 13, 2011 2:00 pm

@emu_kidid

Thanks for that info. It tallied with the info found by Tmbinc on his original wiki about the CN302 debug port.

As far as i can remember from some previous looks at the data, the drivechip reads the month byte to decide which drivecode block to upload. This is why you see the drives referred to as 04 06 and 08. I couldn't say for sure yet but maybe this mean that the same code is uploaded to the 08 and PanaQ drive.

@yamaharace

I would like to keep the code as agnostic as possible so that people could take it and port it to whatever MCU they found usefull to them. Unfortunately my C coding isn't all that crash hot so the initial code will probably be written in either PIC or AVR ASM.

Oh and yes, the code will be free for you to do with as you please.

Re: Open source Drivechip

by MrSporty Posted: Sun Feb 13, 2011 10:02 pm

Been having a play with the drive setup this afternoon and now have a little bit of data to play with. Luckily my Logic Analyser software has the ability to automatically decode SPI data so it took a bit of the donkey work out of it so far.

The SPI debug port is accessed by the modchip using a read and a write command. Borrowing from Tmbinc's wiki, they are structured as followed:

SERIAL_CMD_FF: Read Memory

RIO1 FF

R[1] 00

R[2] ADDRRESS MID

R[3] ADDR_LOW

R[4] 0 R[5] ADDR_HIGH

R[6] 0 R[7] 0

R[8] number of bytes to read

R[9] 0

SERIAL_CMD_FE: Writes one or two bytes to memory

R[0] FE

R[1] 00

R[2] ADDRRESS MID

R[3] ADDR_LOW

R[4] BYTE 1

R[5] ADDR_HIGH

R[6] BYTE_2

R[7] 0

R[8] 1 or 2: numberr of bytes to write

R[9] 0

In a normal transaction the modchip will output a 10 byte command to the drive and then clock a 4 byte response back in. The 4 bytes seem to be 0x00,0x00 then either the ones requested by a read or an echo of the bytes to be written.

To get a stable setup, the XenoGC initially clocks in a command packet of all FF's to which the drive returns a 2 byte response. It then clocks in 3 more commands.



Highlighted in red are the commands sent by the modchip, blue are the responses from the drive.

1.Sent: All FF's (flush SPI buffer?) Received: 0xEE,0xEE 2.Sent: Read 0x40D100 Received: 0x00,0x00,0xFF,0xFD 3.Sent: Write 0x40D000 Data written: 0xF7,0x10 4.Sent: Write 0x40D002 Data written: 0xFF,0xF7

The chip then has a bit of a rest for about 80ms and then proceeds to start writing a block of data beginning at 0x40D000 again.

Ill post that tomorrow.

Re: Open source Drivechip

by emu_kidid Posted: Sun Feb 13, 2011 10:06 pm

Nice work. I've seen that the 08 and Q patch block differs - perhaps the Panasonic Q isn't supported by the Xeno after all. (It'd be easy to do I suppose)

Re: Open source Drivechip

Posted: Sun Feb 13, 2011 10:33 nm

Could this be usefull for devoloping a patch for our Wii dvd drive mod'd cubes?

Re: Open source Drivechip

Posted: Sun Feb 13, 2011 10:44 pm

possibly but it'd require the early drive that could work with the debug port and it'd require someone to create a patch code - aka. too much work. :\

Re: Open source Drivechip

Posted: Mon Feb 14, 2011 12:05 am

MrSporty,

I have a .hex file that apparently you can flash on a Wilkey v1 to turn it into a XenoGC since it used the same efuse bits, but I have no idea if it's even valid (a couple of guys who looked at it didn't know wtf it was).

Re: Open source Drivechip

by MrSporty Posted: Mon Feb 14, 2011 6:35 am

If you upload it i can dissasemble it if its a valid Atmega8 dump.

The easy way to validate it is that it will contain the block of code i am about to post which is sent by the Xeno.

Re: Open source Drivechip

It is possible to dissassemble it? I heard it is impossible, cause of the fuse bits?

Though I dont have the source for this claim. Feel free to correct me, if I am wrong 😉

Re: Open source Drivechip

Posted: Mon Feb 14, 2011 10:15 am

y emu_kidid Posted: Mon Feb 14, 2011 12:55 pm

You know what really sucks? when I was in contact with the XenoGC dude, I received a XenoGC updater.dol (to make a 1.0 chip into a 2.0) but I've long since misplaced it 🥮 I will have to dig around for it soon.

I think this .rar i've attached is the opposite - it's to make a wiikey out of a Xeno (pointless)

Re: Open source Drivechip

by liquitt Posted: Mon Feb 14, 2011 1:13 pm

emu_kidid wrote:

You know what really sucks? when I was in contact with the XenoGC dude, I received a XenoGC updater.dol (to make a 1.0 chip into a 2.0)

well that sounds interesting! write access to a Xeno? 🥹

Re: Open source Drivechip

Posted: Mon Feb 14, 2011 1:19 pm

The fuse bits are not a concern other than when it comes to trying to dump the contents of an MCU. If its locked then other than a glitch attack, decapping and manually resetting the CP fuses is the only way of retrieving the contents. I have a company in china that i have used a number of times in the past for this service with great success. It is however not a cheap option.

Dissassembling the mcu dump on the other hand is pretty simple for the small scale MCU used in the Xeno.

Anyway, back to the task at hand. Here are the REGULAR debug commands sent by the Xeno V1. The first four are detailed in my previous post. The next block as you can see is written from 0x40D000-0x40D0D7

Then some code is written to 0x008674-0x008683, interesting that the payload for the second to last commands seem to be a pointer to our 0x40D000 code. This is probably where our main block gets hooked.

Finally a write of 0x86,0x00 to 0x00804D

0xFE.0x00.0xD0.0x00.0xF7.0x40.0x10.0x00.0x02.0x00 0xFE,0x00,0xD0,0x02,0xFF,0x40,0xF7,0x00,0x02,0x000xFE,0x00,0xD0,0x04,0xF5,0x40,0xD9,0x00,0x02,0x00 0xFE,0x00,0xD0,0x06,0xC8,0x40,0xFF,0x00,0x02,0x00 0xFE,0x00,0xD0,0x08,0xF4,0x40,0xC0,0x00,0x02,0x00 0xFE,0x00,0xD0,0x0A,0x00,0x40,0xD1,0x00,0x02,0x00 0xFE,0x00,0xD0,0x0C,0x40,0x40,0xF7,0x00,0x02,0x00 0xFE,0x00,0xD0,0x0E,0x48,0x40,0x44,0x00,0x02,0x00 0xFE,0x00,0xD0,0x10,0x44,0x40,0xE9,0x00,0x02,0x00 0xFE,0x00,0xD0,0x12,0x19,0x40,0xF4,0x00,0x02,0x00 0xFE,0x00,0xD0,0x14,0x74,0x40,0x00,0x00,0x02,0x00 0xFE.0x00.0xD0.0x16.0xD8.0x40.0x40.0x00.0x02.0x00 0xFE,0x00,0xD0,0x18,0xFD,0x40,0x1E,0x00,0x02,0x00 0xFE.0x00.0xD0.0x1A.0x00.0x40.0xA0.0x00.0x02.0x00 0xFE,0x00,0xD0,0x1C,0xF4,0x40,0x40,0x00,0x02,0x00 0xFE,0x00,0xD0,0x1E,0x00,0x40,0xD1,0x00,0x02,0x00 0xFE,0x00,0xD0,0x20,0x40,0x40,0xF4,0x00,0x02,0x00 0xFE,0x00,0xD0,0x22,0x74,0x40,0x74,0x00,0x02,0x00 0xFE,0x00,0xD0,0x24,0x0A,0x40,0x08,0x00,0x02,0x00 0xFE,0x00,0xD0,0x26,0xF7,0x40,0x20,0x00,0x02,0x00 0xFE,0x00,0xD0,0x28,0x4C,0x40,0x80,0x00,0x02,0x00 0xFE,0x00,0xD0,0x2A,0xF0,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x2C,0xF4,0x40,0x74,0x00,0x02,0x00 0xFE,0x00,0xD0,0x2E,0x00,0x40,0xC6,0x00,0x02,0x00 0xFE,0x00,0xD0,0x30,0x40,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x32,0x05,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x34,0xF4,0x40,0xE1,0x00,0x02,0x00 0xFE,0x00,0xD0,0x36,0xC7,0x40,0xF5,0x00,0x02,0x00 0xFE,0x00,0xD0,0x38,0xFF,0x40,0xF4,0x00,0x02,0x00 0xFE,0x00,0xD0,0x3A,0x70,0x40,0x80,0x00,0x02,0x00 0xFE,0x00,0xD0,0x3C,0xC0,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x3E,0xC0,0x40,0x80,0x00,0x02,0x00 0xFE,0x00,0xD0,0x40,0xFD,0x40,0x80,0x00,0x02,0x00 0xFE,0x00,0xD0,0x42,0x51,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x44,0x54,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x46,0xFD,0x40,0x6A,0x00,0x02,0x00 0xFE,0x00,0xD0,0x48,0x00,0x40,0x80,0x00,0x02,0x00 0xFE,0x00,0xD0,0x4A,0x43,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x4C,0x4C,0x40,0x00,0x00,0x02,0x00 0xFE.0x00.0xD0.0x4E.0xFD.0x40.0x62.0x00.0x02.0x00 0xFE,0x00,0xD0,0x50,0x00,0x40,0x81,0x00,0x02,0x00 0xFE,0x00,0xD0,0x52,0x95,0x40,0x95,0x00,0x02,0x000xFE,0x00,0xD0,0x54,0x95,0x40,0x95,0x00,0x02,0x00 0xFE,0x00,0xD0,0x56,0x95,0x40,0x95,0x00,0x02,0x00 0xFE,0x00,0xD0,0x58,0x95,0x40,0x95,0x00,0x02,0x00 0xFE,0x00,0xD0,0x5A,0x80,0x40,0x4F,0x00,0x02,0x00 0xFE,0x00,0xD0,0x5C,0xFD,0x40,0x3B,0x00,0x02,0x00 0xFE,0x00,0xD0,0x5E,0x00,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x60,0x51,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x62,0x91,0x40,0x80,0x00,0x02,0x00 0xFE,0x00,0xD0,0x64,0x44,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x66,0x32,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x68,0xFD,0x40,0x48,0x00,0x02,0x00 0xFE,0x00,0xD0,0x6A,0x00,0x40,0x84,0x00,0x02,0x00 0xFE,0x00,0xD0,0x6C,0xFD,0x40,0x2B,0x00,0x02,0x00 0xFE,0x00,0xD0,0x6E,0x00,0x40,0xAA,0x00,0x02,0x00 0xFE,0x00,0xD0,0x70,0xFD,0x40,0x40,0x00,0x02,0x00 0xFE,0x00,0xD0,0x72,0x00,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x74,0x24,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x76,0x10,0x40,0x92,0x00,0x02,0x00 0xFE,0x00,0xD0,0x78,0xFD,0x40,0x38,0x00,0x02,0x00 0xFE,0x00,0xD0,0x7A,0x00,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x7C,0x1C,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x7E,0xF5,0x40,0x10,0x00,0x02,0x00 0xFE,0x00,0xD0,0x80,0x01,0x40,0x92,0x00,0x02,0x00 0xFE,0x00,0xD0,0x82,0xD0,0x40,0x02,0x00,0x02,0x00 0xFE,0x00,0xD0,0x84,0xF7,0x40,0x1D,0x00,0x02,0x00 0xFE,0x00,0xD0,0x86,0x01,0x40,0x00,0x00,0x02,0x000xFE,0x00,0xD0,0x88,0xE9,0x40,0xE6,0x00,0x02,0x00 0xFE,0x00,0xD0,0x8A,0x88,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0x8C,0x25,0x40,0x00,0x00,0x02,0x00 0xFE,0x00,0xD0,0x8E,0xFD,0x40,0x09,0x00,0x02,0x00 0xFE.0x00.0xD0.0x90.0x00.0x40.0xD8.0x00.0x02.0x00 0xFE,0x00,0xD0,0x92,0x21,0x40,0xE9,0x00,0x02,0x00 0xFE,0x00,0xD0,0x94,0x37,0x40,0xF5,0x00,0x02,0x00 0xFE,0x00,0xD0,0x96,0xD9,0x40,0xC8,0x00,0x02,0x00 0xFE,0x00,0xD0,0x98,0xFF,0x40,0xFE,0x00,0x02,0x00 0xFE,0x00,0xD0,0x9A,0xF2,0x40,0x5A,0x00,0x02,0x00 0xFE,0x00,0xD0,0x9C,0xF4,0x40,0xC7,0x00,0x02,0x00 0xFE,0x00,0xD0,0x9E,0x83,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0xA0,0x00,0x40,0xF5,0x00,0x02,0x00 0xFE,0x00,0xD0,0xA2,0x03,0x40,0x80,0x00,0x02,0x00 0xFE,0x00,0xD0,0xA4,0xE8,0x40,0x09,0x00,0x02,0x00 0xFE,0x00,0xD0,0xA6,0xD2,0x40,0x01,0x00,0x02,0x00 0xFE,0x00,0xD0,0xA8,0xEE,0x40,0xD0,0x00,0x02,0x00 0xFE,0x00,0xD0,0xAA,0x07,0x40,0xE8,0x00,0x02,0x00 0xFE,0x00,0xD0,0xAC,0x1F,0x40,0xEA,0x00,0x02,0x00 0xFE,0x00,0xD0,0xAE,0xED,0x40,0xC4,0x00,0x02,0x00 0xFE,0x00,0xD0,0xB0,0x82,0x40,0xFD,0x00,0x02,0x00 0xFE,0x00,0xD0,0xB2,0xFE,0x40,0xF2,0x00,0x02,0x00 0xFE,0x00,0xD0,0xB4,0x5A,0x40,0xF4,0x00,0x02,0x000xFE,0x00,0xD0,0xB6,0xC7,0x40,0x83,0x00,0x02,0x00 0xFE,0x00,0xD0,0xB8,0xFD,0x40,0x00,0x00,0x02,0x00 0xFE.0x00.0xD0.0xBA.0xF5.0x40.0x03.0x00.0x02.0x00 0xFE,0x00,0xD0,0xBC,0x10,0x40,0xE9,0x00,0x02,0x00 0xFE,0x00,0xD0,0xBE,0x09,0x40,0xD2,0x00,0x02,0x00 0xFE,0x00,0xD0,0xC0,0x01,0x40,0xEE,0x00,0x02,0x00 0xFE,0x00,0xD0,0xC2,0xD0,0x40,0x07,0x00,0x02,0x00 0xFE,0x00,0xD0,0xC4,0xE8,0x40,0x06,0x00,0x02,0x00 0xFE,0x00,0xD0,0xC6,0xEA,0x40,0xED,0x00,0x02,0x00 0xFE,0x00,0xD0,0xC8,0xCC,0x40,0x82,0x00,0x02,0x00 0xFE,0x00,0xD0,0xCA,0xFD,0x40,0xFE,0x00,0x02,0x00 0xFE,0x00,0xD0,0xCC,0xF7,0x40,0x14,0x00,0x02,0x00 0xFE,0x00,0xD0,0xCE,0x00,0x40,0x08,0x00,0x02,0x00 0xFE,0x00.0xD0.0xD0.0xF4.0x40.0x74.0x00.0x02.0x00 0xFE,0x00,0xD0,0xD2,0x00,0x40,0x00,0x00,0x02,0x00 0xFE.0x00.0xD0.0xD4.0x08.0x40.0xF0.0x00.0x02.0x00 0xFE,0x00,0xD0,0xD6,0x00,0x40,0x00,0x00,0x02,0x00

 $\begin{array}{l} 0xFE,0x00,0x86,0x74,0xF4,0x00,0x74,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x76,0x74,0x00,0x0A,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x78,0x08,0x00,0xF7,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x7A,0x20,0x00,0x4C,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x7C,0x80,0x00,0xF4,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x7C,0x80,0x00,0x04,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x7E,0x74,0x00,0x00,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x80,0xD0,0x00,0x40,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x82,0xF0,0x00,0x00,0x00,0x02,0x00\\ 0xFE,0x00,0x86,0x41,0x86,0x00,0x00,0x00,0x02,0x00\\ 0xFE,0x00,0x80,0x41,0x86,0x00,0x00,0x00,0x02,0x00\\ \end{array}$

Now, above i stated that these were the REGULAR commands sent by the Xeno. As anyone who owns one of these mods knows, if you hold the start button when booting you get a nice info screen. But how can all that code for the menu be stored in about 200 or so bytes. Answer is it can't.

Immediately after the last command, the SPI lines from the xeno seem to go crazy with loads of non SPI data on them. What i think is happening is that the code above is basically a pre-loader. Its loaded and then jumped to to handle a higher speed data burst over the SPI lines.

I will post another picture tonight.

Re: Open source Drivechip

by **emu_kidid**

Posted: Mon Feb 14, 2011 1:37 pm

The code patches the apploader of a game (you can dump this if you just dump a blank disc straight out on a XenoGC modded GC), then based on a keypress, if it's the start button, it will download the credits binary from the XenoGC.

XenoGC Addons

The following commands are added by the XenoGC firmware. Bytes Description Versions 21 Disable audio fix 1.0 22 Disable DRE recovery 1.0 25 unload drive code/disable reset logic/Request credits binary 1.0

Re: Open source Drivechip

by **MrSporty**

Posted: Mon Feb 14, 2011 6:48 pm

Are those commands added to the debug port or commands that the GC can send to the drive?

GC can send to the drive - so look out for those when you're holding start. I have a DOL of the credits binary which I've dumped that way.

Re: Open source Drivechip

by MrSporty Posted: Mon Feb 14, 2011 10:10 pm

Thanks for that emu, ill keep an eye out for those. Any chance of that DOL btw?

Im just waiting on a replacement cube in the post, only gone and killed the laser on mine at the worst time 🥯 Can still sniff the SPI but wont boot disks now .. hey ho.

Re: Open source Drivechip

by MrSporty Posted: Tue Feb 15, 2011 7:00 am

Pictures paint a thousand words.

Heres the point where the SPI data transitions between the standard debug packets and into its new serial format.



Re: Open source Drivechip

Posted: Tue Feb 15, 2011 3:19 pm

Strange at all the XenoGC info popping up recently 😐

http://www.eurasia.nu/modules.php?name= ... =0&thold=0

Re: Open source Drivechip

by gtmtnbiker Posted: Tue Feb 15, 2011 4:26 pm

MrSporty wrote:

Strange at all the XenoGC info popping up recently 🤤

http://www.eurasia.nu/modules.php?name= ... =0&thold=0

Thanks for sharing that info. I'm also enjoying this thread and hope to see you make progress on it.

Re: Open source Drivechip

by liquitt Posted: Tue Feb 15, 2011 8:24 pm

MrSporty wrote:

Strange at all the XenoGC info popping up recently

http://www.eurasia.nu/modules.php?name= ... =0&thold=0

did you submit that story?

Re: Open source Drivechip

py MrSporty Posted: Tue Feb 15, 2011 8:50 pm

No, nothing at all to do with me.

Im a regular visitor to eurasia.nu cos its great for scene stuff but im not affiliated in any way. It did spook me out a bit though, within a day or so of me starting my posts that article popped up. Maybe modrobert saw my posts?

Interesting nonetheless.

Re: Open source Drivechip

yeah i was just going to say that - good read! 😉

by liquitt Posted: Tue Feb 15, 2011 9:20 pm

Re: Open source Drivechip

by emu_kidid Posted: Tue Feb 15, 2011 10:09 pm

Interesting that this pops up after I email them about the update DOL file $\stackrel{\textstyle \hookrightarrow}{=}$ coincidence?

Powered by phpB8® Forum Software ® phpB8 Limited

All times :

All times are UTC Page **1** of **3**