2009-12-24 Qemu PCI card emulation

Plan

- Make a PCI device with IRQ, IO and memory. Kind of ADC
- Find some suitable reference PCI device in hw/
- See details of bus interface. See used idioms
- ~~Design ADC command system~~
- Implement ADC and plug it into reference platform, e.g. PC

Worklog

- Make the following dummy device (qemu-0.12.1):

```
diff --git a/hw/iigp1.c b/hw/iigp1.c
new file mode 100644
index 0000000..c251dbe
--- /dev/null
+++ b/hw/iigp1.c
@@ -0,0 +1,48 @@
+
+#include "pci.h"
+
+#define PCI_CLASS_DA_DSP (0x1100)
+#define PCI_VENDOR_ID_II (0x8089)
+#define PCI_VENDOR_ID_II_GP1 (0x0001)
+
+typedef struct IIGP1State
+{
+    PCIDevice dev;
+} IIGP1State;
+
+static void iigp1_on_reset (void *opaque)
+{
+}
+
+static inline void pci_config_set_byte (void *config, int offset, uint8_t
byte)
+{
+    ((uint8_t*)config)[offset] = byte;
+}
+
+static int iigp1_initfn (PCIDevice *dev)
+{
+    pci_config_set_vendor_id (dev->config, PCI_VENDOR_ID_II);
+    pci_config_set_device_id (dev->config, PCI_VENDOR_ID_II_GP1);
+    pci_config_set_class (dev->config, PCI_CLASS_DA_DSP);
```

```
+    pci_config_set_byte (dev->config, PCI_INTERRUPT_PIN, 1);
+    pci_config_set_byte (dev->config, PCI_MIN_GNT, 0x0c);
+    pci_config_set_byte (dev->config, PCI_MAX_LAT, 0x80);
+
+    qemu_register_reset (iigp1_on_reset, dev);
+
+    return 0;
+}
+
+static PCIDeviceInfo iigp1_info = {
+    .qdev.name    = "IIGP1",
+    .qdev.desc    = "II GP 1",
+    .qdev.size    = sizeof (IIGP1State),
+    //.qdev.vmsd    = &vmstate_iigp1,
+    .init         = iigp1_initfn,
+};
+
+static void iigp1_register (void)
+{
+    pci_qdev_register (&iigp1_info);
+}
+device_init (iigp1_register);
```

- add it to PC platform:

```
diff --git a/hw/pc.c b/hw/pc.c
index db7d58e..d47573f 100644
--- a/hw/pc.c
+++ b/hw/pc.c
@@ -1251,6 +1251,10 @@ static void pc_init1(ram_addr_t ram_size,
         }
     }

+    if (pci_enabled) {
+        pci_create_simple(pci_bus, -1, "IIGP1");
+    }
+
     rom_load_fw(fw_cfg);
 }
```

- and add to makefile:

```
diff --git a/Makefile.target b/Makefile.target
index 7c1f30c..b2bd1b7 100644
--- a/Makefile.target
+++ b/Makefile.target
@@ -186,6 +186,8 @@ obj-y += pcnet.o
 obj-y += rtl8139.o
 obj-y += e1000.o

+obj-y += iigp1.o
```

```
+
 # Hardware support
 obj-i386-y = ide/core.o ide/qdev.o ide/isa.o ide/pci.o ide/piix.o
 obj-i386-y += pckbd.o $(sound-obj-y) dma.o
```

Code: ftp://kkv.spb.su/pub/home/dumb/ws/lted/20091224

Conclusion

- Too complex to complete in 2 hours;
- No clear infrastructure for PCI device plugging;
- Make a simple PCI device, modeled after es1370.

qemu, PCI, lted

From:
http://wiki.osll.ru/ - **Open Source & Linux Lab**

Permanent link:
http://wiki.osll.ru/doku.php/etc:users:jcmvbkbc:little-things:3?rev=1262564400

Last update: **2010/01/04 03:20**