ACUMEN READING REMOTELY USING LOW SPEED BUS OVER ETHERNET

HP INC
ACUMEN READING REMOTELY USING LOW SPEED BUS OVER ETHERNET

This disclosure relates to the field of remote communication among devices, in this case cryptographic device, Acumen IC, which use low speed bus like I2C or similar.

A system is disclosed that presents a way to handle these security encrypted devices in a remote way, avoiding the usage of costly electronics and making use of Ethernet cable which is an extended and cheap communication infrastructure.

In an example 3D printing environment, the post-processing machine is in charge of cooling the printed bucket with the job buried in, un-cake it and refilling the build unit with new powder in order to process a new job in the printer.

The process of refilling the build unit involves mixing fresh and recycled powder which is stored inside the processing station. The mixture is then uploaded in the build unit following a predefined process.

Fresh powder is obtained from the powder supplies attached to the processing station. These supplies have an encryption device which currently is a four pin secured non-volatile memory device accessed over a two-wire serial interface.

This integrated circuit is used:

• To store the type of material loaded in the supply
• It handles a mechanism of encryption to guarantee that the information stored is valid
• Store and manage the information related to the remaining powder quantity
• Supply refilling prevention
• To store powder expiration date, additives, end of warranty and other relevant information needed by the system.

The two-wire serial interface is a communication protocol very similar to the popular I2C (Inter Integrated Circuit).

At physical level, the bus has two roles for nodes:

• Master, generates the clock signal and initiates the communication
• Slave, clock receiver, it should be addressed by the master and can send or received data synchronized with the clock

In the 3D printing system the master is located in the engine board in the processing station, which has the electronics that manages the two-wired signal. This electronics is composed in this case by an ASIC which implements all the hardware needed to control the two-wire bus interface. The receiver node is the encryption device (Acumen IC) in the supply (see Fig 1).
The two-wire serial interface is a bus intended for local communications, usually no longer than one meter and basically focused on onboard communication among devices. This limitation forces that a controlling device with a master two-wire serial interface will be located close to the security integrated device (aka Acumen in 3D printers).

On the other hand, there should be another communication path between the master two-wire serial interface with the security protocol controller which is in charge of starting top level protocol communication, manage the keys stored in Acumen, etc. These functionality usually is implemented in the top level firmware running in the engine board or formatter board which controls the whole system (Fig 2).

In the case of the 3D printers the communication bus between the Security Protocol Controller and the Master TWD Controller is carried out through a PCI-E bus.

In summary, in order to use the security encrypted device (Acumen), additional electronics is needed close to the Acumen IC, these electronics use to have a high cost compared with the cost of the Acumen IC itself.

This approach makes sense when there are few systems (usually supplies) which require the security encrypted device and they are by definition close to the printer or processing station like the supplies used for the agents in the 3D printer or the powder supplies in the processing station.

The problem comes up when the number of systems that needs Acumen is high and they don’t have to be located close to the printer or the processing station. Traditional approach will be adding those electronics (formatter board, engine board, main board, etc) to manage the Acumen in these systems just to control the Acumen ICs, making the system much more complex and more prone to failures increasing the overall cost of the solution (see Fig 3).

This disclosure presents a way to handle these security encrypted devices in a remote way, avoiding the usage of costly electronics and making use of LAN cable which is a extended and cheap communication infrastructure.

The system proposed is shown in Fig 4. Only one Master System (with Code in formatter and engine PCA) is used to manage all the Acumen devices. Fusion TWD or any device I2C is connected to the LAN cable using an I2C to Ethernet bus interface. At the other side of the LAN, another I2C to ethernet bus interface converts the ethernet traffic in I2C signals to handle the acumen.

The key element of the chain is the I2C-Ethernet bus interface. the main characteristics of this device are:

- it must arbitrate the bus interface. Ethernet speed is variable and depends on several factors like the traffic in the LAN, the length of the package to be sent, the device speed to process the request, etc. On the other hand the I2C communication could require fast and synchronized replies from any slave for example when an acknowledge has to be sent where times less than 1 m/sec are expected from the master. In order to do that the electronics in the I2C to ethernet bus interface has to use an I2C technique called Clock Stretching to hold the transmission from I2C master until a response from the slave is available
- from LAN perspective, it has to handle all the requirements related to the Ethernet-IP protocol
• it must translate the instructions, data, and address sent by I2C to ethernet packets and send them to the receiver through LAN
• it has to manage all diagnostics and error conditions like slave not detected or any transaction error
Figure 1 Diagram of Acumen reading in the processing station
Figure 2 Devices involved in bus transactions
Figure 3 Traditional way of implementing multiple acumen solutions
Figure 4 Multiple acumen solutions using I2C over Ethernet

Disclosed by Sergio de Santiago Dominguez, Abel Borras, Mayid Shawi and Michele Vergani, HP Inc.