How to Provide Secure Tracking and Validation in Attachable/Add-On Peripherals

Summary

Part 1 of this article described several applications that can benefit from single-wire memory. This second part shows how it can easily be implemented with existing technology in a variety of packages and available tools.

A Single-Wire Serial EEPROM IC Provides the Answer

The AT21CSx1 family is a single-wire 1-Kbit (128 × 8) Serial EEPROM with a factory-programmed 64-bit serial number. Only two pins are needed to access the device and its stored information: a serial input/output (SI/O) and ground (GND). Figure 4 shows the available packages for single-wire memory.

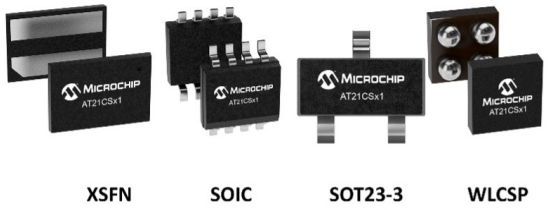

Figure 4. eXtra (thin) Single, Flat No-lead (XSFN) packages have two terminals for easily implementing single-wire memory. Other available packages include: 8-pin SOIC, 3-pin SOT23-3 and WLCSP.

The XSFN package (5 × 3.5 × 0.35 mm) has flat insertion bar contacts and is specifically designed to be a no-solder package. The encasing plastic connector end has one flat side and is formed of hard plastic. Simply epoxying the device into place allows both the SI/O and GND pins to connect on contact. The other packages in the lineup are suitable for soldering to a printed circuit board.

The SI/O signal is a modified I^2C interface, a combination data and power line that allows the device to extract power (V_{CC}) from the reading and writing sequences and provide power to the device with a parasitic power scheme. Other available packaging includes: an 8-pin SOIC (150 mil), 3-pin SOT-23 and a 4-ball wafer-level chip scale package (WLCSP). The WLCSP is the smallest form factor at less than 1 mm squared and 0.3 mm thick.

The AT21CS01 is self-powered via the 1.7V to 3.6V pull-up voltage on the SI/O line. The AT21CS11 lithium-ion battery version is self-powered via the 2.7V to 4.5V pull-up voltage on the SI/O line.

Both devices are organized as one block of 128 × 8 bits and optimized for use in consumer and industrial applications where reliable and dependable nonvolatile memory storage is essential. They have a 256-bit security register which includes a 64-bit serial number. The device also features manufacturer ID support in which the device responds with a unique value for density and revision information. The user

can choose to make all five EEPROM zones (128-bit writable space and four 256-bit blocks) permanently write protected at any time so they cannot be hacked or accidentally changed.

Cryptography

The need for security impacts any attachable product that could affect a system's security and damage the brand's reputation. In contrast to having no security, a variety of secure options can be implemented. With the AT21CS Series, basic authentication and identification are easily provided (see Figure 5). For users uncertain about the extent of security required for a specific product, this provides a good starting point that can always migrate to a more complex scheme such as full crypto authentication, also available from Microchip. However, everything does not require full cryptography. For example, storing the number of insertions of a connector or how much of a product is left in a cartridge, do not require authentication or encryption. It simply uses a block of memory for storing a stock-keeping unit (SKU) number or any other product data and verifying that it has not been tampered with. The cryptography could be done in the system microcontroller, or for extra security also use one of Microchips cryptographic devices.

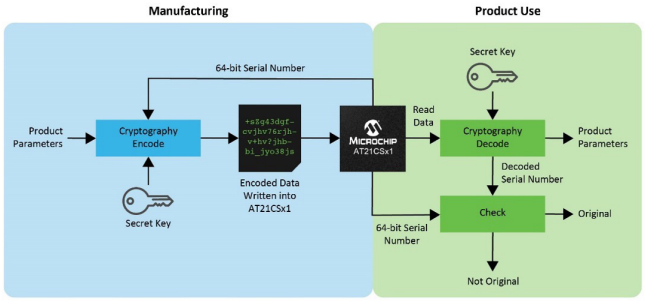

Figure 5. Encoded data written into an AT21CSx1 during the manufacturing process is decoded and checked by the end user's product. Cryptography could be performed via software inside an MCU or via a dedicated secure cryptographic element.

Implementation and Contact Optimization

Systems that have previously had some sort of memory and identification may potentially see a cost reduction from a single-wire memory system, especially if they used more than one wire to communicate or had more memory than required to store a small message that can easily be stored in a 1-kbit single-wire memory device. For example, traditional printer cartridges have four wires to communicate with the printer/computer. The connectors are expensive and if the number of pins can be reduced, a cost savings can be realized.

If a device already has some contacts or if reducing the number of connections is important, placing the identifying device across existing circuitry is one of the ways to add single-wire memory to the system. However, it is not the only approach. Figure 6 shows four implementation methods for contact optimization.

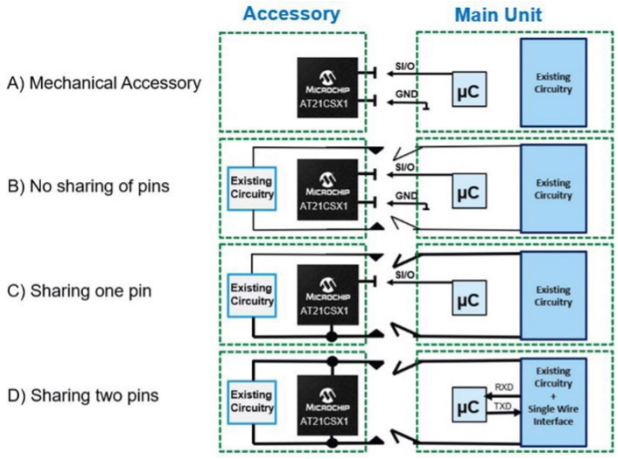

Figure 6. Four types of contact optimization: (a) Mechanical accessory with added ID, (b) adding ID to an existing accessory with electronics (c) hybrid, sharing the ground return wire, (d) Fully integrated requiring no extra contacts for ID function.

Figure 6a shows how the XSFN packaged AT21CSx1 could be added to a purely mechanical attachable that has no electronic content. The XSFN package is a contact package requiring no electronics assembly on the attachable accessory. Contacts in the main unit would connect directly to the XSFN package for identification. A potential use case for this could include disposable medical products such as ventilator tubes.

Figure 6b shows a potential with an existing connector or accessory. In this case, an external package is easily added to the product. The device is epoxied into place, allowing both pins (SI/O and GND) to connect on insertion. The XSFN package can be molded or glued onto the accessory.

In contrast, Figure 6c shows the type of connection for a battery charger or drill battery. In this case, the system is a hybrid sharing the ground return pin of the accessory's circuitry with single-wire memory. It requires only one contact to the authentication device. However, it is slightly more complex to add authentication to the accessory and requires electronics assembly.

Figure 6d shows the third type of connection. Printer cartridges or any other consumable that has existing simple

passive circuitry are candidates for this approach. Adding the authentication device across the accessory circuitry requires no external contacts to the single-wire device since it reuses the existing accessory contacts. This approach adds more complexity for both the main unit and accessory and requires electronics assembly. This solution works with simple loads such as lamps, heaters and more.

Getting Started

Any device that needs to identify a peripheral attached to it is a candidate for single-wire memory. AT21CSx1 design support includes a portable demo and an evaluation kit.

The Single-Wire Connector Demo for the AT21CSx1, shown in Figure 7, is a portable demo that uses the Curiosity Development Board for 8-bit MCUs. The demo shows how to use AT21CSx1 parts to identify attachments providing the ability to distinguish between genuine and fake connectors. The connector represents any kind of attachable to a system such as cartridges, connectors or any other attachable accessories. With the demo, users can clone a connector and test if the system recognizes the clone as genuine or fake. The demo has the ability to erase a connector as well as make it genuine and also counts the number of connector insertions.

An animation of the demo showing how easy it is to add identification into a product and the source files are available online at Microchip's GitHub repository (SWI Connector Demo).

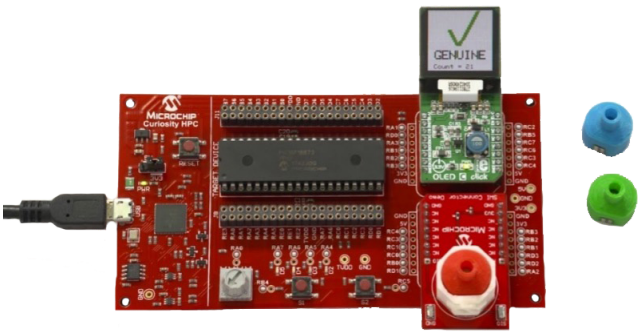

Figure 7. AT21CSx1 ID and tracking demo.

As shown in Figure 8, a Serial Memory Single-Wire Evaluation Kit (DM160232) provides an easy-to-use, interactive user tool that demonstrates the best-in-class features, functionality and low-power operation of the AT21CS Series Serial EEPROM devices. The included Graphical User Interface (GUI) makes it easy for engineers and developers to configure and evaluate single-wire Serial EEPROMs, shortening the overall development time needed to bring new designs from prototype to production.

Figure 8. The DM160232 evaluation kit demonstrates the capabilities of the AT21CSx1.

Design support files for the AT21CSx1 single-wire devices are available and include IBIS signal integrity and Verilog behavior models.

Summary

If an application requires a technique to easily implement a small amount of memory for a variety of purposes, address basic security, require small space constraints or require a large expensive connection and several wires to implement, a single-wire memory device is the answer. This capability is provided by AT21CS Series products that are easy to implement with several design tools to assist the system designer. More information can be found on the Microchip website.