

Implementing remote tamper detection with wireless and capacitive sensing technologies

Parker Dorris, Senior Applications Engineer, Microcontroller Products, Silicon Labs



The advent of wireless connectivity in the home automation market has enabled developers to create many innovative products that make end users feel safer and more aware of their personal property. Remote tamper detection is one example of innovation made possible through wireless connectivity. By pairing a low-power wireless transceiver with a low-power capacitive sensing microcontroller (MCU), a developer can create an economical tamper detection node that can be discreetly located to detect movement of valuable objects on shelves or walls, as well as detecting when doors, windows or safes have been opened or otherwise manipulated.

The first step of a project development often requires the creation of a proof-of-concept to show to peers or potential investors. The emergence of crowdfunding sources such as Kickstarter has placed additional importance on creating a functional proof-of-concept that can generate excitement and funding. Although it might seem daunting to create a proof-of-concept for a project with components as complex as low-power wireless and capacitive sensing ICs, selecting the right semiconductor vendors and toolset can dramatically simplify development.

Design overview

This hypothetical remote tamper detection product has three main components:

- A capacitive sensing system on the detection node capable of detecting movement of one electrode relative to a conductive object
- A transmit-only RF system also on the detection node that can alert a receiver hub of tamper activity
- A receiver hub capable of monitoring for detection node alerts and reporting that activity.

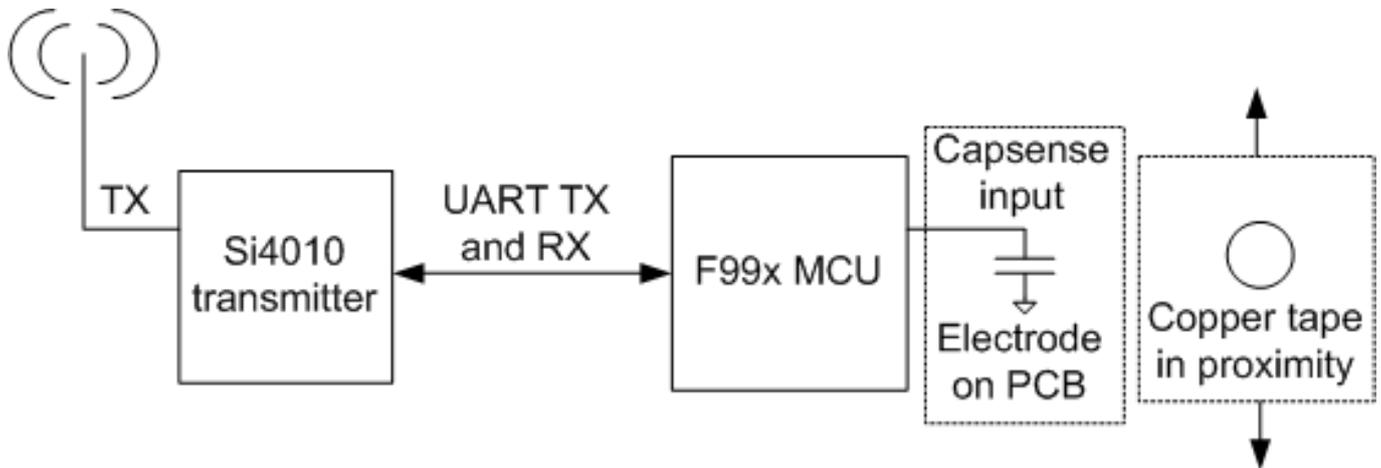
A few design constraints serve to define the product more narrowly:

- The combined transmitter and capacitive sensing components should be able to

operate using a battery for an extended period of time.

- The sensing and transmit node must be low profile and as small as possible to enable discreet placement in space-constrained areas.
- Some consideration must be paid toward future-proofing the design so that enhancements and “feature creep” won’t result in late-stage hardware and software re-design.

Figure 1 shows how the tamper detection design should work:



It can be advantageous to choose a single MCU and wireless IC vendor if that vendor provides a toolset that can support all components of a design. Many vendors offer similar toolsets and MCU and wireless connectivity features across their product lines, and so choosing a single vendor that can supply all the necessary embedded components can speed development by unifying tools and hardware.

Tamper detection overview

The tamper detection system’s capacitive sensing MCU uses charge timing technology to measure projected self-capacitance on an electrode connected to one of the MCU’s port pins. As a conductive object moves in proximity to the sensing electrode, the effects of that conductor on the electrode’s e-fields produces a change in the capacitance measured by the MCU. The technology’s sensitivity enables the firmware to detect very small changes in capacitance (less than 100 fF).

This system design uses the 1 mm diameter capsense button as the sensing electrode. A corresponding 1 mm circle cut from copper tape serves as the conductive object that will affect the sensor’s capacitance. The copper circle should be placed close to the electrode but attached to the object whose movement constitutes a tampering event to be reported. For instance, the tamper node with the MCU could be mounted on a wall, and the conductor could be mounted on the back side of a painting, for example. When the painting is hung and the conductor is situated in close proximity to the sensing electrode, small changes in the position of the painting will trigger a tamper detection event.

The tamper detection system periodically wakes from sleep state to take a

capacitance reading on the electrode. The sensing firmware compares this output to the capacitance that's expected with the conductive object in proximity to the sensor. If no change is detected, the MCU immediately switches back to its low-power sleep state. If the values don't match, the algorithm quickly takes a few more samples to verify that capacitance has changed. If the algorithm determines that the conductive object has moved based on additional readings, the firmware then toggles the port pin connected to the wireless transmitter, forcing an alert transmission.

Next steps

Once this system is up and running, a developer could start field testing the hardware in use cases such as detecting tampering to wall-mounted paintings, jewelry box lids and countless other in-home areas where homeowners might want to monitor activity.

When development progresses past the proof-of-concept stage, the radio component of the system could be optimized to use custom firmware that could enable enhanced functionality. For instance, this firmware could transmit information about the battery level to the receiver. If a communications interface between the MCU and the wireless transmitter is added, firmware could also transmit more detailed information about the tampering event such as raw capacitive sensing output.

Capacitive sensing node calibration is another feature that could be implemented later in development. This feature would enable end users to place the node and position the object to be monitored before firmware begins sensing and determines the system's static state capacitance. This innovative cap-sense node calibration feature would provide an optimal setup time for the sensor.

Conclusion

Intimidating design challenges can be overcome by selecting vendors that provide reference designs, firmware, and documentation to bridge gaps between a developer's concept and a functional, real-world system. Reviewing vendor collateral offerings that surround an MCU or other IC, rather than just focusing on the datasheet specs exclusively, can help developers choose components that will give them a head-start on development and shorten design time.

Parker Dorris

Senior Applications Engineer, Microcontroller Products, Silicon Labs
Parker Dorris is a senior applications engineer supporting Silicon Labs' microcontroller product line. He joined Silicon Labs in 2003 when the company acquired Cygnal Integrated Products. Mr. Dorris specializes in the areas of human interface and USB embedded system design. He holds a BSEE from the University of Texas at Austin.

Source URL (retrieved on 12/19/2013 - 3:18pm):

<http://www.ecnmag.com/articles/2013/05/implementing-remote-tamper-detection->

[wireless-and-capacitive-sensing-technologies](#)