Sitara™ AM438x processor: tamper protection

Texas Instruments

Carlos Betancourt,
Product marketing manager,
Sitara™ processors
Texas Instruments

Amrit Mundra,
System security architect,
Sitara processors
Texas Instruments

Carolyn England,
Technical sales engineer,
Sitara processors
Texas Instruments

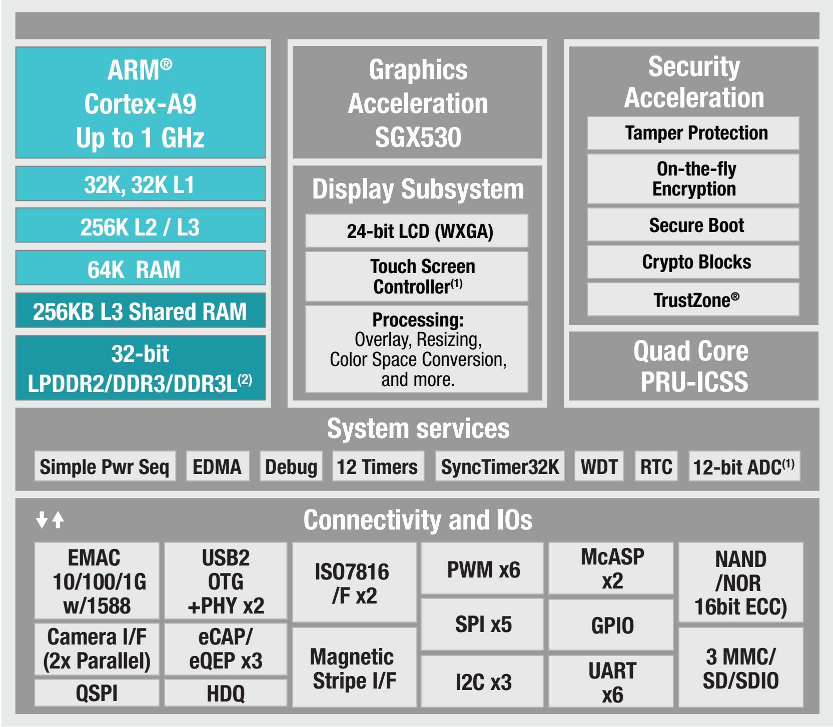
In today's Internet-of-things (IoT) infrastructure, security threats have become a prominent concern for electronic manufacturers. The seamless integration of devices and data opens the door for intruders looking to access private information to develop creative ways to tamper with devices.

Because of this, the need for physical protection is more necessary than ever before. This safeguard is immensely critical in applications such as point-of-sale, medical devices, navigation equipment, gateways, building security and automation, and biometric equipment.

The reality is—all devices can be compromised, thus there is a need for more security features to be taken into account in the early stages of product development. Today's applications requiring high security often rely on a two or more chips solution. Texas Instruments' (TI's) Sitara™ AM438x processor, based on the ARM® Cortex®-A9 integrates security features that help electronic manufacturers design products that can detect and react to physical attacks.

Sitara AM438x processor

The Sitara AM438x processor, a high-performance processor running up to speeds of 1 GHz, offers security features, connectivity, graphical interface and scalability. As the follow-on of TI's Sitara AM335x processor, the AM438x processor is designed with applications requiring security and more system performance in mind. The Sitara AM438x processor is an upgrade from the AM335x processor in that it supports additional cryptography, secure boot and now a new security feature called enclosure protection. Enclosure protection is the technology that helps customers design systems that can detect the physical tampering of a device and react immediately to such threats. See **Figures/Table 1** for a detailed layout of components and features for TI's AM438x processor.



(1) Use of TSC will limit availability of channels
(2) Max clock: LPDDR2 = 266 MHz; DDR3 = 400 MHz

***Figure 1**. Block diagram of TI's Sitara™ AM438x processor.*

Benefits	Features
Performance increase	• ARM® Cortex®-A9 at 1 GHz (25% more DMIPS than ARM Cortex-A8) • 32b LPDDR2/DDR3 at 266/400 MHz • Single cycle VFP (10× better than ARM Cortex-A8) • 512K of L2 plus L3 internal SRAM • Displaying subsystem with signal processing
Extensive integration and new peripherals	• Camera ×2 • Programmable Realtime Unit (PRU) • Magnetic card reader plus an additional 8-channel ADC • EMV compliant smart card interface
Security	• Secure boot • Enclosure (tamper) protection • Cryptography • JTAG / debug security monitoring and reacting • Trusted execution environment

***Table 1**. Benefits and features of TI's Sitara AM438x processor.*

During boot up, the Sitara AM438x processor activates secure boot. Secure boot outlines the procedure for helping designers validate encrypted software to prevent unauthorized users from stealing code and overwriting the Flash with unauthorized software updates.

The processor helps designers load the encrypted code from the device's Flash memory to verify its authenticity. After designers have deemed the code trustworthy, they can use enclosure protection to protect against physical attacks.

Enclosure protection

System designers can implement enclosure protection with two mechanisms—spring loaded open/close switches and wire mesh. The AM438x battery-backed tamper protection module, as shown in **Figure 2**, integrates enclosure protection capabilities, which allows designers to connect up to six pairs of wire mesh or open/close switches. The tamper protection module can also monitor voltage, temperature and crystal frequency, which helps customers further protect their systems. This feature is typically required for point-of-sale applications. However, that is beyond the scope of this paper which focuses on enclosure protection.

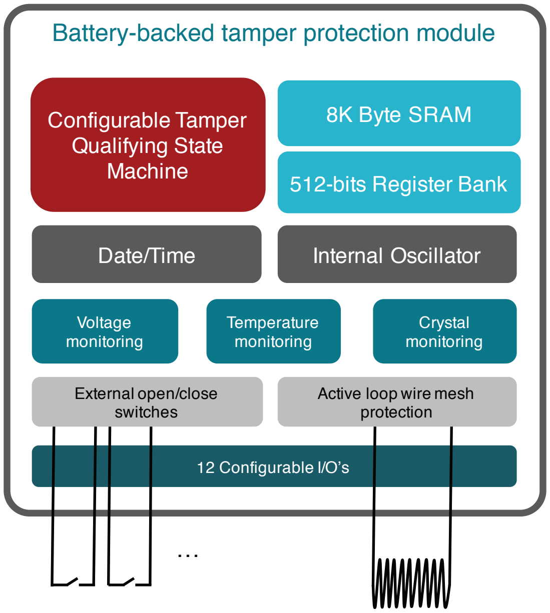


***Figure 2**. Enclosure Protection using the battery-backed tamper protection module.*

System designers can place spring-loaded switches to surround the plastic or metal casing of the electronic device being developed. These switches

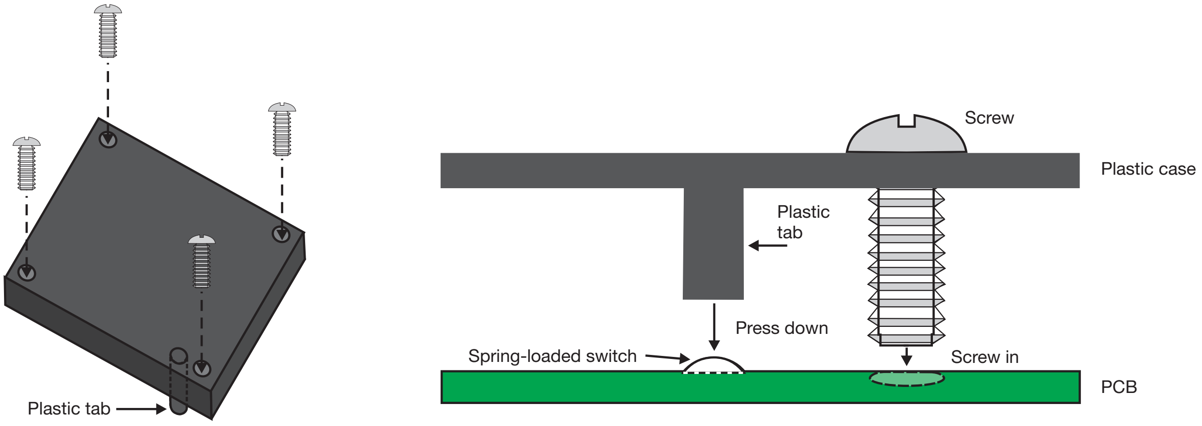


***Figure 3**. Spring-loaded switches can be activated by the loosening of screws sealing the device's casing.*

can then be connected to the tamper protection module in TI's Sitara AM438x processor, and when the device's case is opened without permission, the switches, if enabled correctly by system designers, can release a signal alerting the processor of the intrusion. For example, **Figure 3** illustrates these spring-loaded switches in their open and closed states. If a screw that holds the casing together is loosened, the surface bubbles indicating that the switch has been opened, thus alerting the tamper protection module. Electronic device manufacturers can use this feature to detect a physical attack and choose the appropriate action to protect the integrity of the device.

Wire mesh protection entails wrapping sensitive hardware of the device with a wire mesh that acts similar to an electric fence. System designers can embed the wire mesh on a PCB layer or separate PCB bolted around sensitive hardware. **Figure 4** shows an example of a wire mesh PCB.

If an intruder were to drill through the casing, severing the wire, the tamper protection module, if enabled correctly by system designers, can detect the breach within the circuit. Once again, electronic device manufacturers can use this feature to detect a physical attack and choose the appropriate action to protect the integrity of the device. This protection is credited to a random generated signal sent through the internal wire mesh which can be periodically monitored by the tamper protection module as configured by the system designer.

Figure 5 shows the flow of this process in detail; spring-loaded open/close switches follow the same flow.

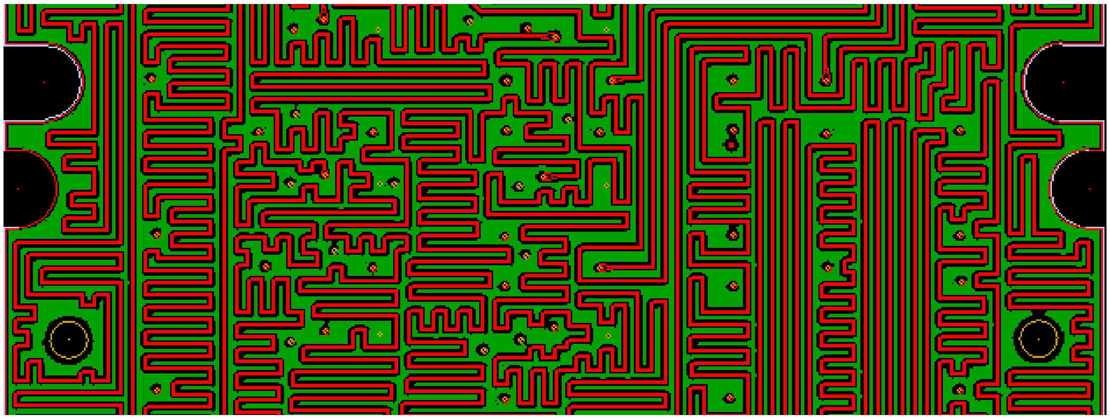


***Figure 4**. Wire mesh is wrapped around sensitive hardware, acting as a protective fence.*

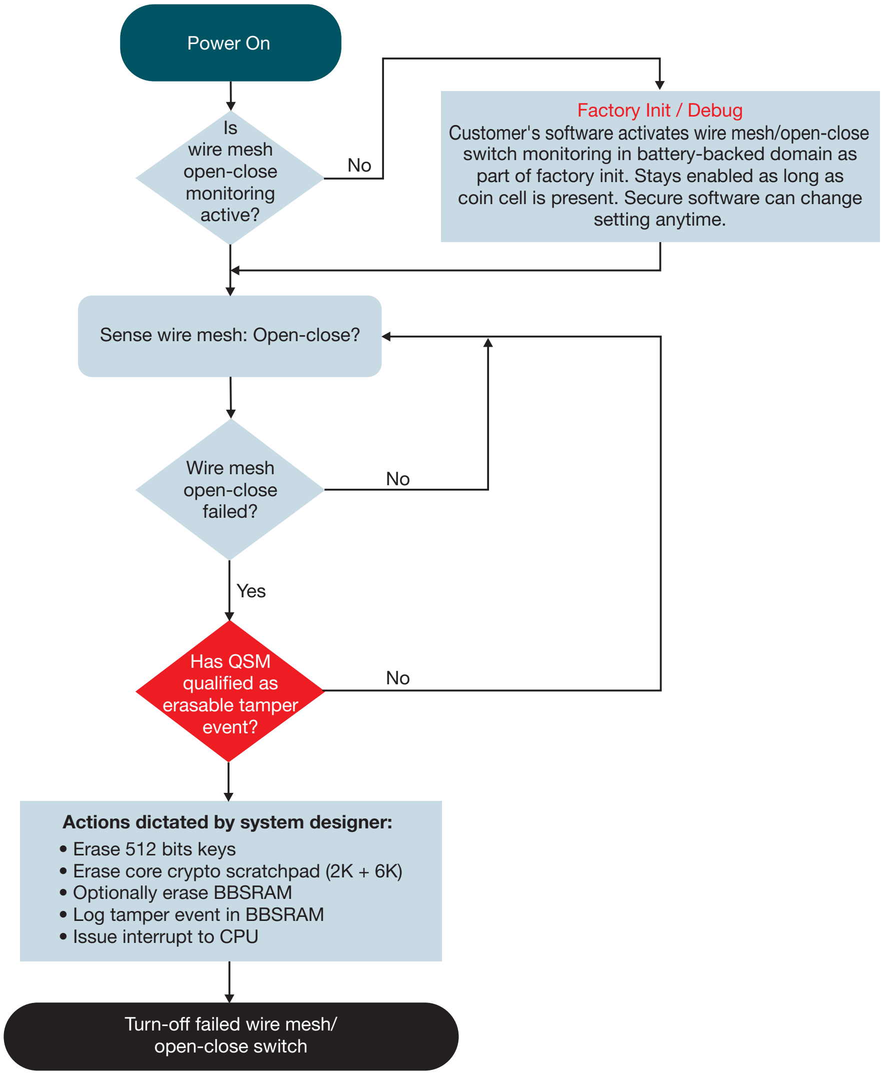

Power On
Is wire mesh open-close monitoring active?
No
Factory Init / Debug
Customer's software activates wire mesh/open-close switch monitoring in battery-backed domain as part of factory init. Stays enabled as long as coin cell is present. Secure software can change setting anytime.
Sense wire mesh: Open-close?
Wire mesh open-close failed?
No
Yes
Has QSM qualified as erasable tamper event?
No
Actions dictated by system designer:
• Erase 512 bits keys
• Erase core crypto scratchpad (2K + 6K)
• Optionally erase BBSRAM
• Log tamper event in BBSRAM
• Issue interrupt to CPU
Turn-off failed wire mesh/ open-close switch

***Figure 5**. Flow diagram for wire mesh.*

Balancing security with usability is critical for any product design. Security that is too sensitive gives false triggers, thereby erasing sensitive data on the device and rendering the device inoperable. TI has developed technology to counter false trigger via micro-coded qualification state machine (QSM) in hardware that enables system designers to qualify the tamper events and deem them true before reacting with hard tamper events. QSM also provides designers with the ability to adjust security sensitivity based on the operating environment.

Additionally, JTAG security monitoring and reacting is present in the Sitara AM438x processor. JTAG is a protocol describing the bidirectional communication between master and slave ports. To a manufacturer, JTAG is useful in real-time debugging and accessing memory registers. On the other hand, a physical attack could happen via JTAG to access, read, monitor and/or control data flowing through this link. As shown in **Figure 6**, the tamper protection module, if enabled correctly by system designers, can monitor the JTAG/TEST/ Boundary Scan, which enables designers to detect attacks and choose the appropriate actions.

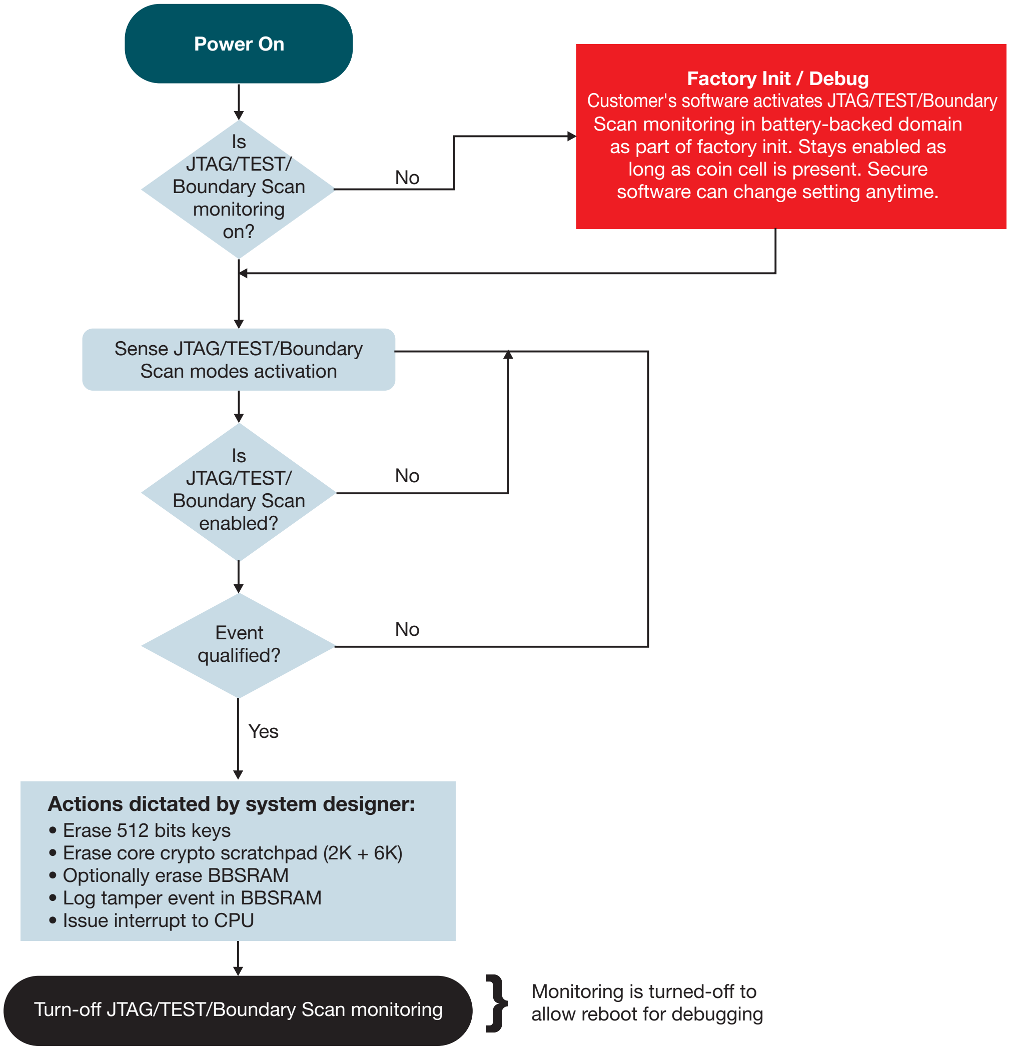

Power On
Is JTAG/TEST/ Boundary Scan monitoring on?
No
Factory Init / Debug
Customer's software activates JTAG/TEST/Boundary Scan monitoring in battery-backed domain as part of factory init. Stays enabled as long as coin cell is present. Secure software can change setting anytime.
Sense JTAG/TEST/Boundary Scan modes activation
Is JTAG/TEST/ Boundary Scan enabled?
No
Event qualified?
No
Yes
Actions dictated by system designer:
• Erase 512 bits keys
• Erase core crypto scratchpad (2K + 6K)
• Optionally erase BBSRAM
• Log tamper event in BBSRAM
• Issue interrupt to CPU
Turn-off JTAG/TEST/Boundary Scan monitoring
Monitoring is turned-off to allow reboot for debugging

Figure 6. *Flow diagram for JTAG monitoring and reacting.*

When the Sitara AM438x processor detects a physical intrusion, either from a wire mesh or open/close switch, it will react as the electronic manufacturer has defined. For example, the manufacturer can implement: (1) erasing sensitive memory or applications, (2) making the device inoperable, (3) sending an alert message over the network; and/or (4) voiding the manufacturer's warranty.

Conclusion

Looking to design with security in mind while seeking performance? Consider TI's Sitara AM438x processor. It's not only a processor running at speeds up to 1 GHz, but also has enclosure protection features that enable device manufacturers to protect against physical intrusion.

For more information on TI's AM438x processor: www.ti.com/am438x.

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265