



APPLICATION NOTE 4244

# Secure Supervisors Provide Multifaceted Monitoring to Ensure System Security

*Abstract: This article describes many of the embedded security features in the various DS36xx secure supervisor products.*

## Introduction

Intrusion prevention in many systems had traditionally been left to the specific demands of that application and to the individual creativity of the system designer. To provide enhanced security in an ever-more-interconnected society, various entities have defined specific standards to eliminate potential holes in the creation of a "secure system." Whether the system is a cash register or a file server, the task of security is essentially identical: prevent any open path for a hacker trying to compromise that system security.

## Secure Supervisors

The DS36xx secure supervisor products integrate a CPU supervisor, NVSRAM controller, real-time clock (RTC), temperature sensor, analog-to-digital converter (ADC), random number generator (RNG), and the I/Os and support circuitry necessary to operate this monitoring device on either system power or a battery. These products reduce component count and unload the continuous system monitoring requirements that would otherwise be placed on the processor in secure applications such as point-of-sale (PoS) terminals, PIN pads, secure communications, set-top boxes, alarm systems, or gaming systems. The secure supervisor products support the highest security level requirements of the FIPS-140.2, Common Criteria, PCI-PED, and EMV-4.1 certification entities. **Table 1** presents selection options presently available or in development.

**Table 1. Secure Supervisor Product Selection Guide**

Part Number	I/O	Analog Voltages Monitored <sup>1</sup>	Digital Inputs Monitored	Internal Key Memory	External Memory Control	Random Number Generator	Over-Voltage Monitor	Battery Monitor
DS3600	3-wire	4	1	64B	✓	✓		✓
DS3605	I <sup>2</sup> C	4	1	—	✓	✓		✓
DS3640	I <sup>2</sup> C	5	3	1024B		✓	✓	✓
DS3641	4-wire	5	3	1024B		✓	✓	✓
DS3645	I <sup>2</sup> C	12	4	4096B	✓	✓	✓	✓
DS3650	4-wire	2	—	—			✓	✓
DS3655	I <sup>2</sup> C	—	4	64B				

<sup>1</sup>Does not include V<sub>CCI</sub> and V<sub>BAT</sub> monitors.

The secure supervisor products are low-cost, space-efficient components that offer a premier security solution

for many applications. By using the high levels of integration in these devices, valuable system resources can be fully utilized for the principal application while the secure supervisor handles the generally mundane, but very critical, security monitoring chores.

## Tamper Response

All tamper inputs are constantly monitored in parallel. At the instant in which any tampering is detected, the following simultaneous actions are initiated:

1. Tamper latches record the monitor channel that initiated the tamper event
2. The tamper output asserts to alert the system processor
3. The current time is frozen in the Time Stamp registers
4. Encryption key memory is immediately erased (if applicable)
5. External SRAM memory is immediately erased (if applicable)

Recovery from a tamper event begins with identification of the source of the event. The tamper latches and the event time stamp will remain frozen until the condition causing the tamper event has been corrected and the latches have been reset.

## Power-Supply Monitoring

A traditional CPU supervisor function monitors the  $V_{CCI}$  power supply, providing a reset signal to the microprocessor when the supply is out of tolerance. A tamper reaction to an abnormally high  $V_{CCI}$  supply is also included in many of the products.

## Battery-Supply Monitoring

An ADC register monitors the battery voltage, which is readable through the I/O port. Tamper reaction to an abnormally low or high battery voltage is included in most of the product offerings.

## Time Keeping and Tamper-Event Time Stamp

The integrated RTC provides a time reference for tamper-event recording and recovery. Time-of-day alarm and CPU watchdog functions are also included in many of the product offerings.

## External Analog Supply Monitoring

Besides the internal  $V_{CCI}$  and  $V_{BAT}$  monitoring functions, the secure supervisor products offer multiple configurations of analog inputs. These inputs monitor external power supplies or other critical bias conditions, depending on specific application requirements.

## External Digital Signal Monitoring

Most of these devices also include digital input channel(s), which can be utilized for a tamper response to some user-defined conditions. Using standard TTL input thresholds, these inputs could be directly fed from other on-board logic controls. If needed, the inputs can be configured with a resistive-divider network to monitor additional bias sources.

## Internal Encryption Key Memory

Most of the devices include a nonvolatile encryption key memory array, accessible through the I/O port. In the event of a tamper, the encryption key memory is rapidly erased.

## External Memory Control and Security

Several of the secure supervisor products include a tamper-reactive nonvolatile SRAM controller, with provisions to supply battery-backed power and control logic for external memory support. When  $V_{CCI}$  power is within tolerance, the external SRAM is powered from that  $V_{CCI}$  supply. Should the external power supply fail, access to the SRAM is inhibited. The battery is automatically switched in to provide backup power to that external memory.

## Power for External Support Circuitry

A battery-backed power supply output is provided for any critical external support circuitry required for continuous operation. The output supply voltage is either the  $V_{CCI}$  supply, if within the defined tolerance, or  $V_{BAT}$ .

## Random Number Generator

Most of the secure supervisor products contain a pseudo-random number generator (RNG), which provides a seed value for the user to generate their own FIPS 140.2-compliant random number. Upon initial application of  $V_{CCI}$  power, the RNG is seeded using several natural sources of randomness. Until the device is ready, the RNG will output zeros data. Once a non-zero byte is read, any number of additional random bytes can be read in 128-byte blocks. This read cycle can be repeated any number of times until the user has retrieved sufficient random data to seed a software-controlled random number generation.

## Thermal Monitoring

An on-chip temperature sensor monitors the system environment. High- and low-temperature limits, and appropriate tamper reaction if those operational limits are violated, counter any intended thermal attack.

## Discrete System Identification

Each device contains a unique serial number, readable through the I/O port. This silicon serialization allows for discrete end-item system identification. The products are manufactured so that no two devices will ever contain the same serial number.

## BGA Packaging

The product family is offered in chip-scale ball grid array (CSBGA) packages. By minimizing exposed pins, this packaging further enhances the security of the data and control signals.

---

Application note 4244: [www.maxim-ic.com/an4244](http://www.maxim-ic.com/an4244)

### More Information

For technical support: [www.maxim-ic.com/support](http://www.maxim-ic.com/support)

For samples: [www.maxim-ic.com/samples](http://www.maxim-ic.com/samples)

Other questions and comments: [www.maxim-ic.com/contact](http://www.maxim-ic.com/contact)

---

### **Automatic Updates**

Would you like to be automatically notified when new application notes are published in your areas of interest?

[Sign up for EE-Mail™](#).

---

### **Related Parts**

DS3600: [QuickView](#)

DS3605: [QuickView](#)

DS3640: [QuickView](#)

DS3641: [QuickView](#)

DS3645: [QuickView](#)

DS3650: [QuickView](#)

DS3655: [QuickView](#)

AN4244, AN 4244, APP4244, Appnote4244, Appnote 4244

Copyright © by Maxim Integrated Products

Additional legal notices: [www.maxim-ic.com/legal](http://www.maxim-ic.com/legal)