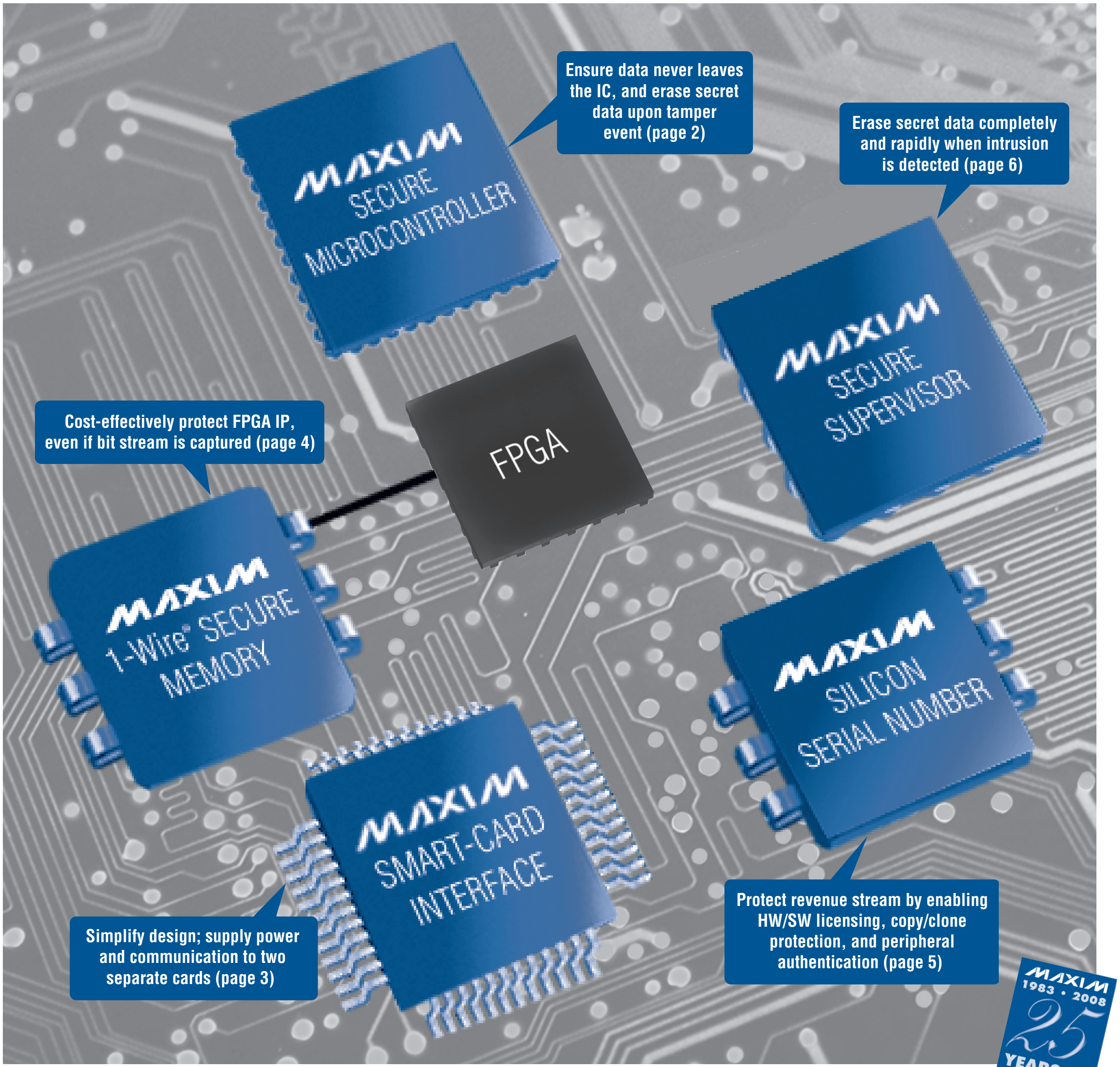
Authentication & Data Security
Design Guide

3rd Edition January 2009

Keep your IP designs, data, and revenue safe with Maxim's secure technologies


MAXIM SECURE MICROCONTROLLER
FPGA
MAXIM SECURE SUPERVISOR
MAXIM 1-Wire® SECURE MEMORY
MAXIM SILICON SERIAL NUMBER
MAXIM SMART-CARD INTERFACE

Ensure data never leaves the IC, and erase secret data upon tamper event (page 2)

Erase secret data completely and rapidly when intrusion is detected (page 6)

Cost-effectively protect FPGA IP, even if bit stream is captured (page 4)

Simplify design; supply power and communication to two separate cards (page 3)

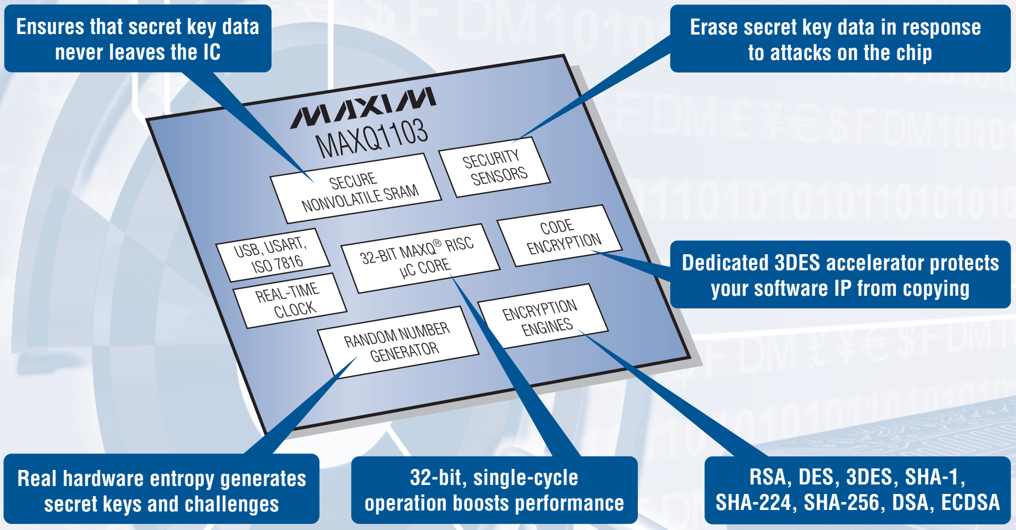
Protect revenue stream by enabling HW/SW licensing, copy/clone protection, and peripheral authentication (page 5)

MAXIM 1983 • 2008 25 YEARS OF ENGINEERING SUCCESS

MAXIM

Industry’s most secure 32-bit microcontroller

Advanced Security Features Protect Secret Data and IP



Ensures that secret key data never leaves the IC

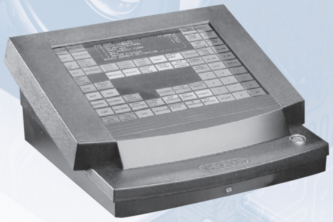
Erase secret key data in response to attacks on the chip

Dedicated 3DES accelerator protects your software IP from copying

Real hardware entropy generates secret keys and challenges

32-bit, single-cycle operation boosts performance

RSA, DES, 3DES, SHA-1, SHA-224, SHA-256, DSA, ECDSA



Maxim’s Secure Microcontroller Family

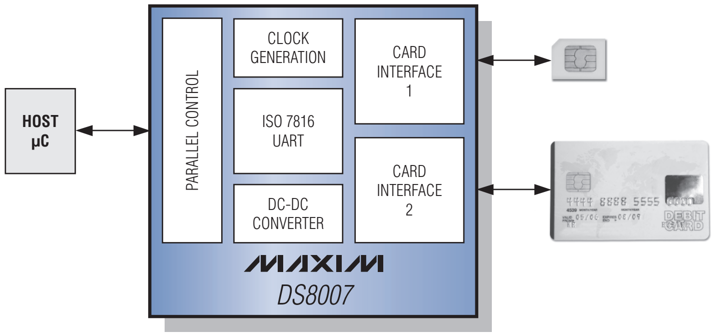
Part	Core	Address Space (Code/Data)	Integrated Security Supervisor	Code Encryption	User 3DES Engine	SHA-1, SHA-224, SHA-256 Engine	RSA, DSA, ECDSA Engine	Package
DS5002	8-bit 8051	64kB/64kB	✓	64-bit				80-MQFP
DS5230	8-bit 8051	64kB/64kB	✓	3DES				80-MQFP
DS5250	8-bit 8051	4MB/4MB	✓	3DES	✓		✓	80-/100-MQFP
MAXQ1103	**32-bit MAXQ30**	**8MB/8MB**	✓	**3DES**	✓	✓	✓	**144-LQFP, 144-CSBGA***

MAXQ is a registered trademark of Maxim Integrated Products, Inc.
*Future product—contact the factory for availability.

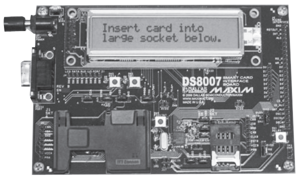
Simplify your smart-card interface design

DS8007 dual-slot interface IC provides power supply, level translation, and ESD protection for robust smart-card communication

Complete Interface Functions in One IC



- ISO 7816 UART
- Supplies up to 80mA for two cards
- EMV™-certified reference design at: **www.maxim-ic.com/DS8007-KIT**



Order your free DS8007 sample kit today
www.maxim-ic.com/DS8007-SKT

- Three DS8007 smart-card interface samples
- CD with complete software libraries
- CPU IC card

DS8113 single-slot interface is also available

- Low-power, 10nA stop mode
- ±8kV ESD protection

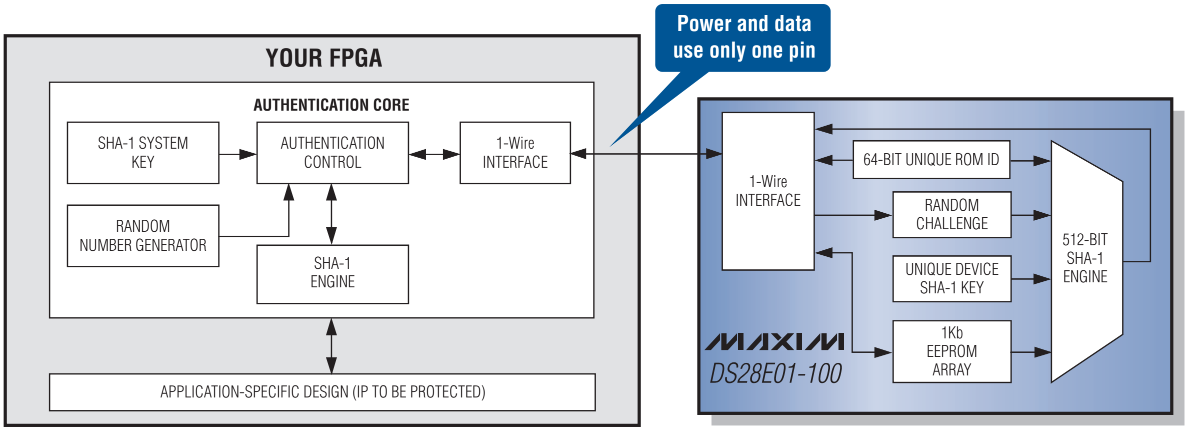
Part	Interfaces	Charge Pump	Stop Mode	Card Voltages (V)	ISO 7816 UART	Package	Auxiliary Contacts (C4, C8)
DS8023	1	✓	✓	5, 3, 1.8		28-TSSOP/SO	✓
DS8024		✓		5, 3, 1.8			✓
DS8113			✓	5, 3			✓
DS8007	2	✓		5, 3, 1.8	✓	48-TQFP	✓

EMV is a trademark owned by EMVCo LLC.

Cost-effective bit-stream protection for your FPGA design

The DS28E01-100** is 1-Wire® secure memory with crypto-strong, SHA-1, bidirectional challenge-and-response authentication security. It provides a low-cost,† world-class security and authentication solution to protect your design investment and IP.

Protect Your FPGA IP with 1-Wire Secure Memory



Power and data use only one pin

1-Wire secure memory protects FPGA designs from being cloned even if the configuration data bit stream is captured. The user design remains disabled until both the hash algorithm computation in the FPGA and in the secure memory match.

- **Protects the FPGA designer's IP**
- **Low-cost alternative to expensive encrypted FPGAs**
- **FPGA SHA-1 engine and 1-Wire interface supported by major FPGA vendors**
- **1-Wire interface requires only one FPGA pin to operate**
- **Data and power are multiplexed on the same pin**

For a tutorial on FPGA protection, go to: www.maxim-ic.com/FPGA

For more information about Maxim's authentication solutions, go to: www.maxim-ic.com/ProtectDG

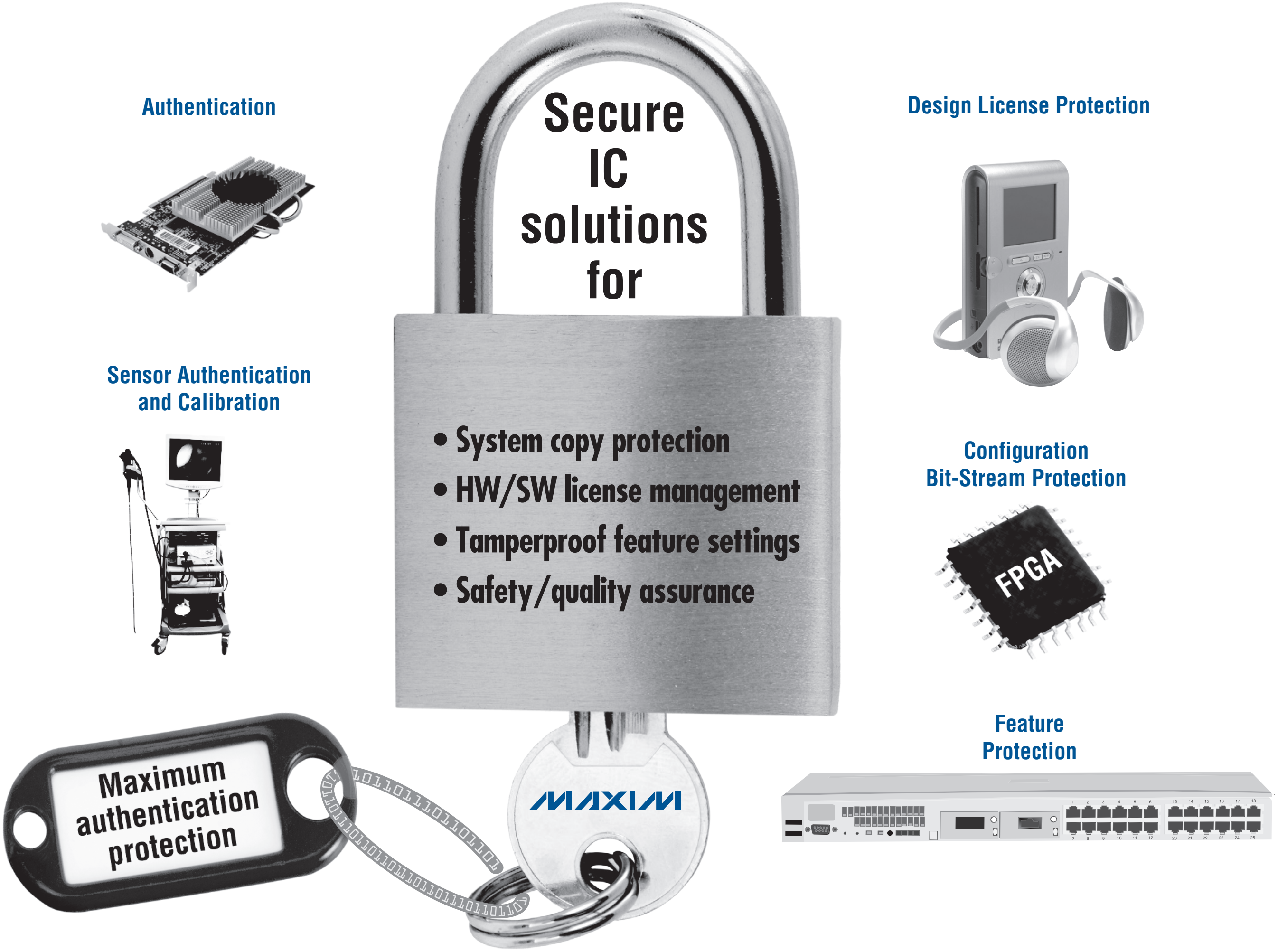
1-Wire is a registered trademark of Maxim Integrated Products, Inc.

†The DS28E01-100 is available for under $0.75 for consumer electronics volumes. Prices provided are for design guidance and are FOB USA.

**Data sheet available under NDA.

Protect IP development investments with proven electronic authentication solutions

Protect your R&D investment with a proven, low-cost† authentication solution. Options range from customization of the 64-bit, factory-lasered serial numbers to secure, crypto-strong, FIPS 180-1/2 and ISO/IEC 10118-3 SHA-1 based challenge and response for bidirectional authentication.



Secure IC solutions for

- System copy protection
- HW/SW license management
- Tamperproof feature settings
- Safety/quality assurance

Authentication

Sensor Authentication and Calibration

Design License Protection

Configuration Bit-Stream Protection

Feature Protection

Maximum authentication protection

Maxim's Authentication Solutions—the Key to Copy-Proofing Applications

Part	Description	Interface	Authentication Feature
DS28CN01**	1Kb EEPROM with SHA-1	I^2C/SMBus™	Bidirectional SHA-1 challenge and response
DS28E01-100**	1Kb EEPROM with SHA-1	1-Wire	Bidirectional SHA-1 challenge and response
DS2401/DS2411	64-bit ROM serial number	1-Wire	Customized 64-bit ROM
DS28CM00	64-bit ROM serial number	I^2C/SMBus	Customized 64-bit ROM
DS2431	1Kb EEPROM	1-Wire	Customized 64-bit ROM, WP/OTP modes
DS2460**	SHA-1 coprocessor	I^2C	Secure storage of system secrets

SMBus is a trademark of Intel Corporation.

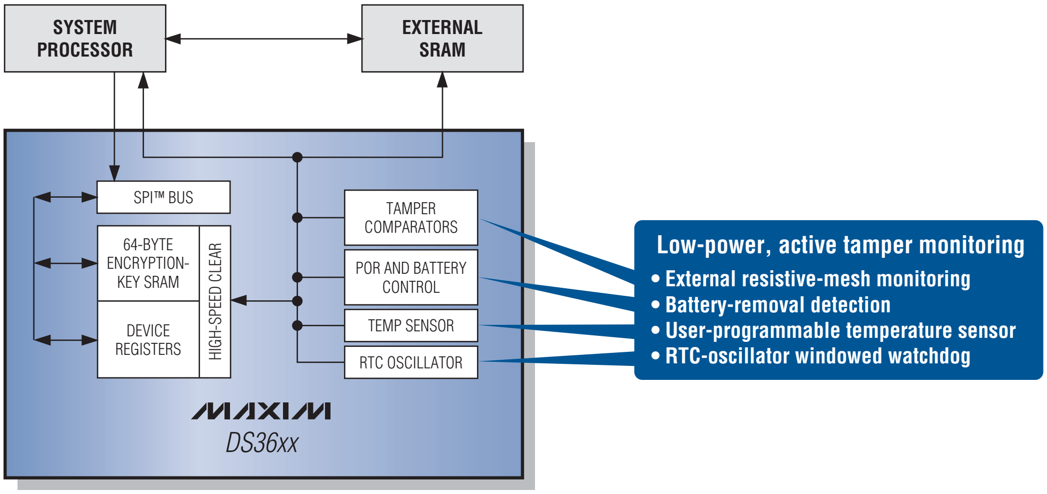
†Authentication solutions starting as low as $0.15 for consumer electronics volumes. Prices provided are for design guidance and are FOB USA.

**Data sheet provided under NDA.

Industry's first secure encryption-key supervisors

Replace up to 40 components and enhance key security

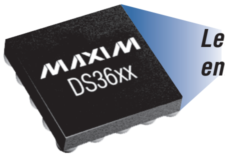
Maxim's secure supervisors are the industry's first ICs to integrate comprehensive features for encryption-key protection in POS terminals, secure servers, and software-defined radios. Packaged in a leadless CSBGA for added security, these devices provide active tamper detection and rapid erasure of key memory upon a tamper event. These supervisors support the highest security level of the FIPS 140-2, Common Criteria, PCI-PED, and EMV 4.1 certification entities.



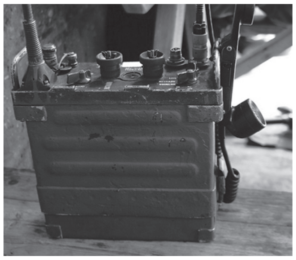
Low-power, active tamper monitoring

- External resistive-mesh monitoring
- Battery-removal detection
- User-programmable temperature sensor
- RTC-oscillator windowed watchdog

- **Nonimprinting, battery-backed encryption-key SRAM**
- **Low standby current (< 4µA at +25°C)**
- **Rapid erasure of internal and external SRAM upon a tamper event**
- **Low-profile, leadless CSBGA package**



Leadless CSBGA package enhances key security



Software-Defined Radios

Biometrics

POS Terminals

To learn about Maxim products in POS applications, go to: www.maxim-ic.com/POS-Solutions

SPI is a trademark of Motorola, Inc.

Secure encryption-key supervisors

Part	DS3600	DS3605	DS3640/ DS3641	DS3644*	DS3645	DS3650	DS3655	DS3665*
Package	25-CSBGA	25-CSBGA	25-CSBGA	49-CSBGA	49-CSBGA	16-CSBGA	16-CSBGA	49-CSBGA
Operating Temp (°C)	-40 to +85	-40 to +85	-40 to +85	-55 to +95	-55 to +95	-40 to +85	-40 to +85	-55 to +95
Power Consumption (µA, typ)	10	6	10	9	13	7	3	14
Encryption-Key Storage (Bytes)	64		1K	1K	4K		64	8K
RTC	✓	✓	✓	Counter	Counter		Counter	Counter
RTC Alarm	✓	✓		✓	✓			✓
Time Stamp	✓	✓	✓	✓	✓		✓	✓
Internal RAM Control and Erase	✓		✓	✓	✓		✓	✓
External RAM Control and Erase	✓	✓		✓	✓			✓
Battery Controller	✓	✓	✓	✓	✓	✓	✓	✓
Silicon Oscillator						✓		✓
CPU Supervisor	✓	✓	✓	✓	✓	✓		✓
Selective Memory Erase				2 levels				4 levels
Oscillator Monitor	✓	✓	✓	✓	✓			✓
Voltage-Defined Threshold Tamper Inputs	4	4	4	4	4	2	2	4
Logic-Level Tamper Inputs	1	1	3	2	2		1	2
Voltage Window Comparators				4	4			4
PCI/PED Voltage Monitoring			✓	✓	✓	✓	✓	✓
I^{2}C		✓	(DS3640)	✓	✓		✓	
SPI	3-wire		4-wire (DS3641)			4-wire		✓
Service Switch Input	✓	✓		✓	✓			✓
Analog/Digital Input	Temperature and battery							
Internal Temp Sensor	✓	✓	✓	✓	✓	✓	✓	✓
Silicon-Inscribed Serial Number	✓	✓	✓	✓	✓	✓	✓	✓
Random Number Generator	✓	✓	✓	✓	✓	✓	✓	✓
Glitch Filter	✓	✓	✓	✓	✓	✓		✓
Internal Voltage Reference	✓	✓	✓	✓	✓	✓	✓	✓

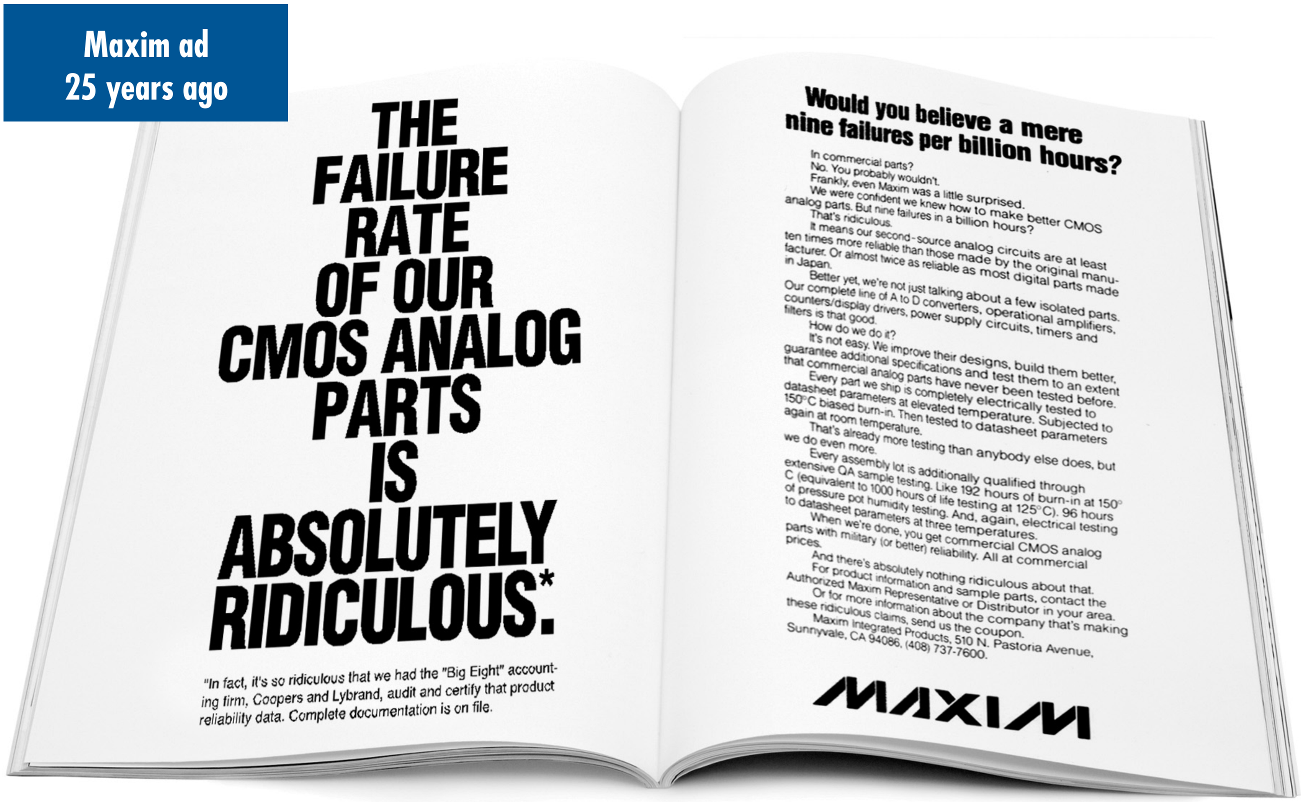
To learn more about Maxim's secure supervisors, go to: www.maxim-ic.com/SecureSupervisors

*Future product—contact the factory for availability. Specifications are preliminary.

Our failure rate is *still* absolutely ridiculous

One failure in over 2 billion hours

Maxim ad
25 years ago



THE FAILURE RATE OF OUR CMOS ANALOG PARTS IS ABSOLUTELY RIDICULOUS.*

*In fact, it's so ridiculous that we had the "Big Eight" accounting firm, Coopers and Lybrand, audit and certify that product reliability data. Complete documentation is on file.

Would you believe a mere nine failures per billion hours?

In commercial parts?

No. You probably wouldn't.

Frankly, even Maxim was a little surprised.

We were confident we knew how to make better CMOS analog parts. But nine failures in a billion hours?

That's ridiculous.

It means our second-source analog circuits are at least ten times more reliable than those made by the original manufacturer. Or almost twice as reliable as most digital parts made in Japan.

Better yet, we're not just talking about a few isolated parts. Our complete line of A to D converters, operational amplifiers, counters/display drivers, power supply circuits, timers and filters is that good.

How do we do it?

It's not easy. We improve their designs, build them better, guarantee additional specifications and test them to an extent that commercial analog parts have never been tested before.

Every part we ship is completely electrically tested to datasheet parameters at elevated temperature. Subjected to 150°C biased burn-in. Then tested to datasheet parameters again at room temperature.

That's already more testing than anybody else does, but we do even more.

Every assembly lot is additionally qualified through extensive QA sample testing. Like 192 hours of burn-in at 150° C (equivalent to 1000 hours of life testing at 125°C). 96 hours of pressure pot humidity testing. And, again, electrical testing to datasheet parameters at three temperatures.

When we're done, you get commercial CMOS analog parts with military (or better) reliability. All at commercial prices.

And there's absolutely nothing ridiculous about that.

For product information and sample parts, contact the Authorized Maxim Representative or Distributor in your area.

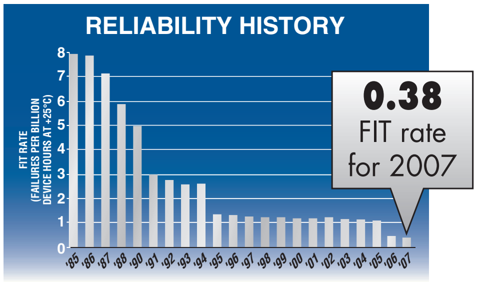
Or for more information about the company that's making these ridiculous claims, send us the coupon.

Maxim Integrated Products, 510 N. Pastoria Avenue, Sunnyvale, CA 94086, (408) 737-7600.

MAXIM

See our reliability tools at www.maxim-ic.com/qa

- Reliability reports on every product
- AEC-Q100 reports
- ISO 9001:2000 and ISO/TS 16949:2002 certificates
- Online reliability calculators (includes FIT rate, PPM with confidence interval, and LTPD calculators)



www.maxim-ic.com/ridiculous

MAXIM
www.maxim-ic.com
Maxim Integrated Products, Inc.
120 San Gabriel Drive
Sunnyvale, CA 94086