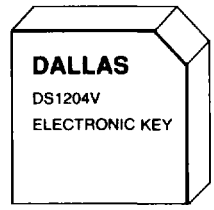
DALLAS SEMICONDUCTOR

DS1204V
Electronic Key

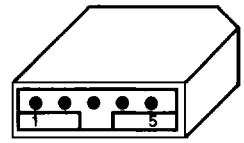
FEATURES

- Cannot be deciphered by reverse engineering
- Partitioned memory thwarts pirating
- User-insertable packaging allows personal possession
- Exclusive blank keys on request
- Appropriate identification can be made with a 64-bit reprogrammable memory
- Unreadable 64-bit security match code virtually prevents deciphering by exhaustive search with over 10^{19} possibilities
- 128 bits of secure read/write memory create additional barriers by permitting data changes as often as needed
- Rapid erasure of identification security match code and secure read/write memory can occur if tampering is detected
- Low-power CMOS circuitry
- Four million bps data rate
- Durable and rugged
- Applications include software authorization, gray market software protection, proprietary data, financial transactions, secure personnel areas, and system access control

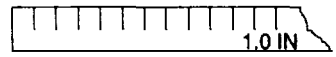
PIN ASSIGNMENT



SIDE



BOTTOM: PIN VIEW



See Mech. Drawings Section

PIN DESCRIPTION

Pin 1 - V_{CC}	+5 Volts
Pin 2 - $\overline{RST}$	Reset
Pin 3 - DQ	Data Input/Output
Pin 4 - CLK	Clock
Pin 5 - GND	Ground

DESCRIPTION

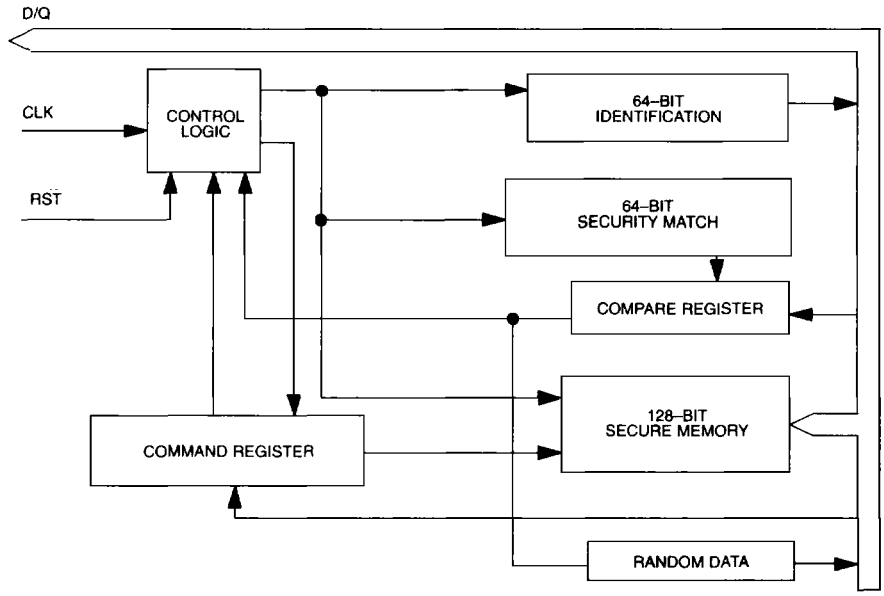
The DS1204V Electronic Key is a miniature security system that stores 64 bits of user-definable identification code and a 64-bit security match code that protects 128 bits of read/write nonvolatile memory. The 64-bit identification code and the security match code are programmed into the key via a special program mode operation. After programming, the key follows a procedure with a serial format to retrieve or update data. Interface cost to a microprocessor is minimized by on-chip circuitry that permits data transfer with only three signals: Clock (CLK), Reset ($\overline{RST}$), and Data Input/Output (DQ). Low pin count and a guided entry for mating receptacle overcome mechanical problems normally encountered with conventional integrated circuit packaging, making the device transportable and user-insertable.

OPERATION - NORMAL MODE

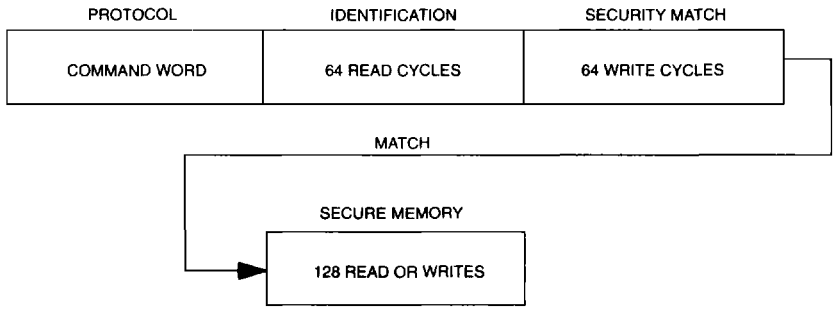
The Electronic Key has two modes of operation: normal and program. The block diagram (see Figure 1) illustrates the main elements of the key when used in the normal mode. To initiate data transfer with the key, $\overline{RST}$ is taken high and 24 bits are loaded into the command

register on each low-to-high transition of the CLK input. The command register must match the exact bit pattern that defines normal operation for read or write, or communications are ignored. If the command register is loaded properly, communications are allowed to continue. The next 64 cycles to the key are reads. Data is clocked out of the key on the high-to-low transition of the clock from the identification memory. Next, 64 write cycles must be written to the compare register. These 64 bits must match the exact pattern stored in the security match memory. If a match is not found, access to additional information is denied. Instead, random data is output for the next 128 cycles when reading data. If write cycles are being executed, the write cycles are ignored. If a match is found, access is permitted to a 128-bit read/write nonvolatile memory. Figure 2 is a summary of normal mode operation and Figure 3 is a flow chart of the normal mode sequence.

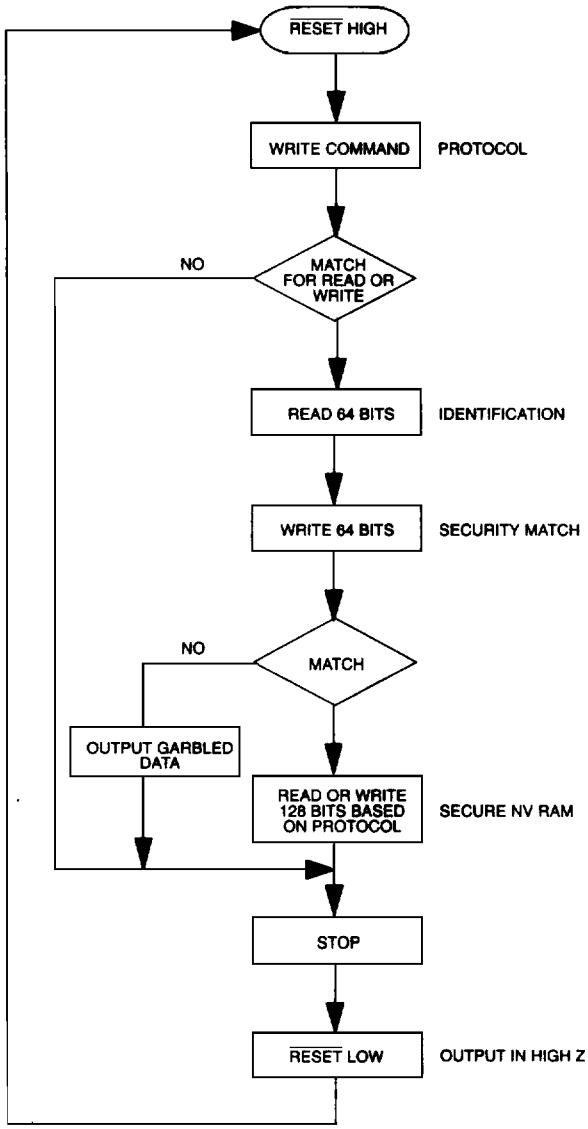
BLOCK DIAGRAM - NORMAL MODE Figure 1



SEQUENCE - NORMAL MODE Figure 2



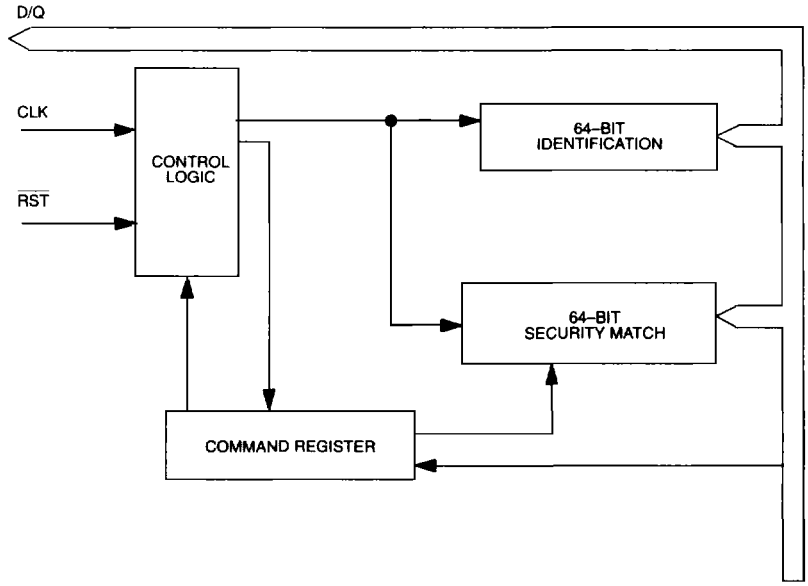
FLOW CHART - NORMAL MODE Figure 3



PROGRAM MODE

The block diagram in Figure 4 illustrates the main elements of the key when used in the program mode. To initiate the program mode, $\overline{RST}$ is driven high and 24 bits are loaded into the command register on each low-to-high transition of the CLK input. The command register must match the exact pattern that defines program operation. If an exact match is not found, the remainder of the program cycle is ignored. If the command register is properly loaded, then the 128 bits that follow are written to the identification memory and the security match memory. Figure 5 is a summary of program mode operation and Figure 6 is a flow chart of program mode operation.

BLOCK DIAGRAM - PROGRAM MODE Figure 4



SEQUENCE - PROGRAM MODE Figure 5

PROTOCOL	IDENTIFICATION	SECURITY MATCH
COMMAND WORD	64 WRITE CYCLES	64 WRITE CYCLES

COMMAND WORD

Each data transfer for the normal and program mode begins with a three-byte command word as shown in Figure 7. As defined, the first byte of the command word specifies whether the 128-bit nonvolatile memory will be written into or read. If any one of the bits of the first byte of the command word fails to meet the exact pattern of read or write, the data transfer will be aborted.

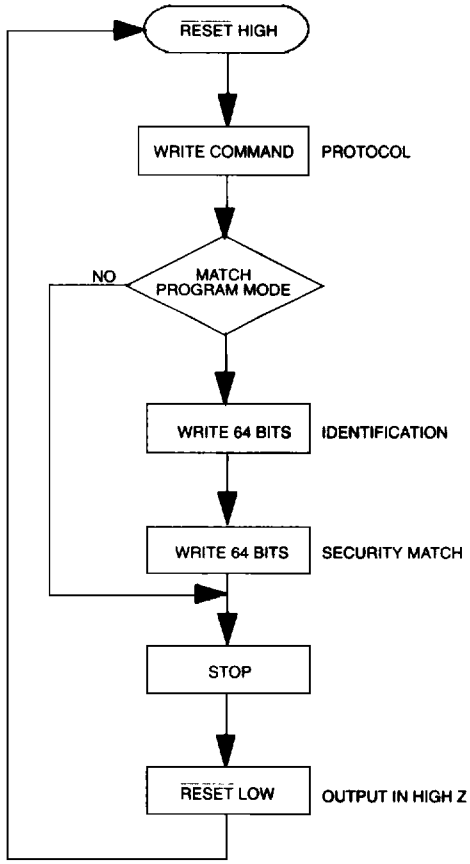
The 8-bit pattern for read is 01100010. The pattern for write is 10011101. The first two bits of the second byte of the command word specify whether the data transfer to follow is a program or normal cycle. The bit pattern for program is 0 in bit 0 and 1 in bit 1. The program mode can be selected only when the first byte of the command word specifies a write. If the program mode is specified and the first byte of the command word does not specify a write, data transfer will be aborted. The bit pattern that selects the normal mode of operation is 1 in bit 0 and 0 in bit 1. The other two possible combinations for the first two bits of byte 2 will cause data transfer to abort.

The remaining six bits of byte 2 and the first seven bits of byte 3 form unique patterns that allow multiple keys to reside on a common bus. As such, each respective code pattern must be written exactly for a given device or data transfer will abort. Dallas Semiconductor has five patterns available as standard products per the chart in Figure 7. Each pattern corresponds to a specific part number. Under special contract with Dallas Semiconductor, the user can specify any bit pattern other than those specified as unavailable. The bit pattern as defined by the user must be written exactly or data transfer will abort. The last bit of byte 3 of the command word must be written to logic 1 or data transfer will abort.

NOTE:

Contact the Dallas Semiconductor sales office for a special command word code assignment that makes possible an exclusive blank key.

FLOW CHART - PROGRAM MODE Figure 6

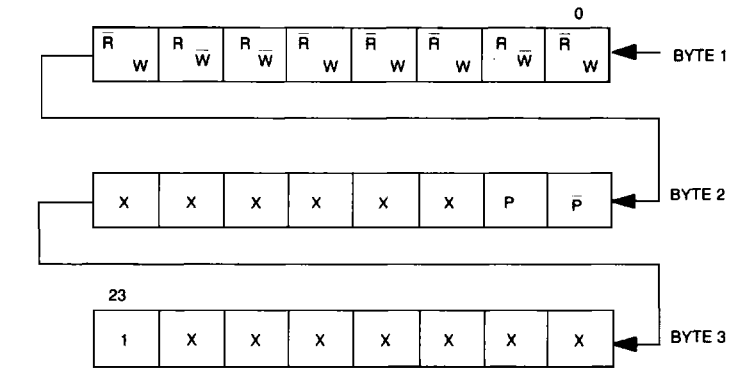


RESET AND CLOCK CONTROL

All data transfers are initiated by driving the $\overline{RST}$ input high. The $\overline{RST}$ input serves three functions. First, it turns on control logic, which allows access to the command register for the command sequence. Second, the $\overline{RST}$ signal provides a power source for the cycle to follow. To meet this requirement, a drive source for $\overline{RST}$ of 2 mA @ 3.5 volts is required. However, if the V_{CC} pin is connected to a 5-volt source within nominal limits, the $\overline{RST}$ is not used as a source of power and input levels revert to normal V_{IH} and V_{IL} inputs with a drive current requirement of 500 µA. Third, the $\overline{RST}$ signal provides a method of terminating data transfer.

A clock cycle is a sequence of a falling edge followed by a rising edge. For data inputs, the data must be valid during the rising edge of a clock cycle. Command bits and data bits are input on the rising edge of the clock and data bits are output on the falling edge of the clock. The rising edge of the clock returns the DQ pin to a high impedance state. All data transfer terminates if the $\overline{RST}$ pin is low and the DQ pin goes to a high impedance state. When data transfer to the key is terminated using $\overline{RST}$, the transition of $\overline{RST}$ must occur while the clock is at a high level to avoid disturbing the last bit of data. Data transfer is illustrated in Figure 8 for normal mode and Figure 9 for program mode.

COMMAND WORD Figure 7

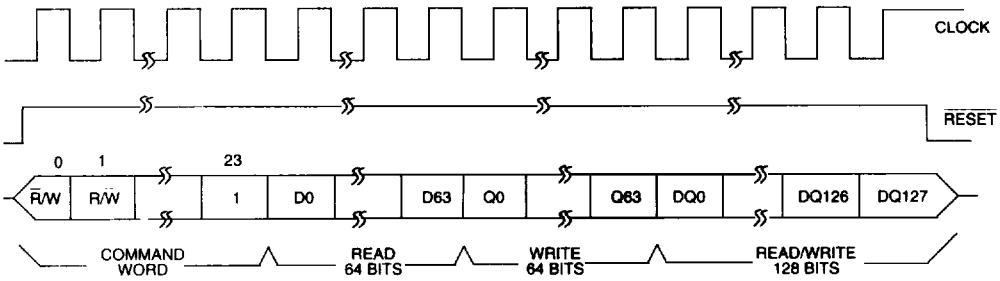


DS1204U-G01	0	0	0	0	0	0	P	$\overline{P}$	BYTE 2
	1	0	1	0	0	0	0	0	BYTE 3
DS1204U-G02	0	0	0	0	0	1	P	$\overline{P}$	BYTE 2
	1	0	1	0	0	0	0	0	BYTE 3
DS1204U-G03	0	0	0	0	1	0	P	$\overline{P}$	BYTE 2
	1	0	1	0	0	0	0	0	BYTE 3
DS1204U-G04	0	0	0	0	1	1	P	$\overline{P}$	BYTE 2
	1	0	1	0	0	0	0	0	BYTE 3
DS1204U-G05	0	0	0	1	0	0	P	$\overline{P}$	BYTE 2
	1	0	1	0	0	0	0	0	BYTE 3

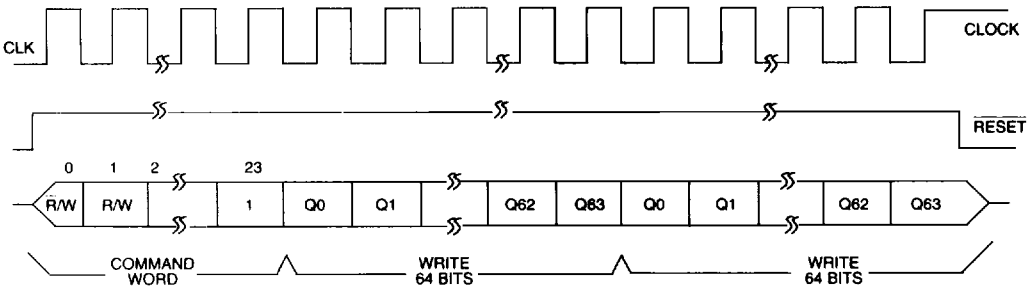
KEY CONNECTIONS

The key is designed to be plugged into a standard 5-pin, 0.1-inch center SIP receptacle (SAMTEC SS-105 or equivalent). A guide is provided to prevent the key from being plugged in backwards and aid in alignment of the receptacle. For portable applications, contact to the key pins can be determined to ensure connection integrity before data transfer begins. CLK, $\overline{RST}$, and DQ all have internal 20K ohm pulldown resistors to ground that can be sensed by a reading device.

DATA TRANSFER - NORMAL MODE Figure 8



DATA TRANSFER - PROGRAM MODE Figure 9



ABSOLUTE MAXIMUM RATINGS*

Voltage on any Pin Relative to Ground	-0.5V to +7.0V
Operating Temperature	0°C to 70°C
Storage Temperature	-40°C to +70°C

* This is a stress rating only and functional operation of the device at these or any other conditions above those indicated in the operation sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods of time may affect reliability.

RECOMMENDED DC OPERATING CONDITIONS

(0°C to 70°C)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Logic 1	V_{IH}	2.0			V	1, 8, 10
Logic 0	V_{IL}	-0.3		+0.8	V	1
$\overline{\text{RESET}}$ Logic 1	V_{IHE}	3.5			V	1, 9, 11
Supply	V_{CC}	4.5	5.0	5.5	V	1

DC ELECTRICAL CHARACTERISTICS

(0°C to 70°C; V_{CC} = 5V ± 10%)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Input Leakage	I_{IL}			+500	µA	4
Output Leakage	I_{LO}			+500	µA	
Output Current @2.4V	I_{OH}	-1			mA	
Output Current @0.4V	I_{OL}			+2	mA	
$\overline{\text{RST}}$ Input Resistance	Z_{RST}	10		60	K ohms	
D/Q Input Resistance	Z_{DQ}	10		60	K ohms	
CLK Input Resistance	Z_{CLK}	10		60	K ohms	
$\overline{\text{RST}}$ Current @3.0V	I_{RST}			2	mA	6, 9, 13
Active Current	I_{CC1}			6	mA	6
Standby Current	I_{CC2}			2.5	mA	6

CAPACITANCE

(t_A = 25°C)

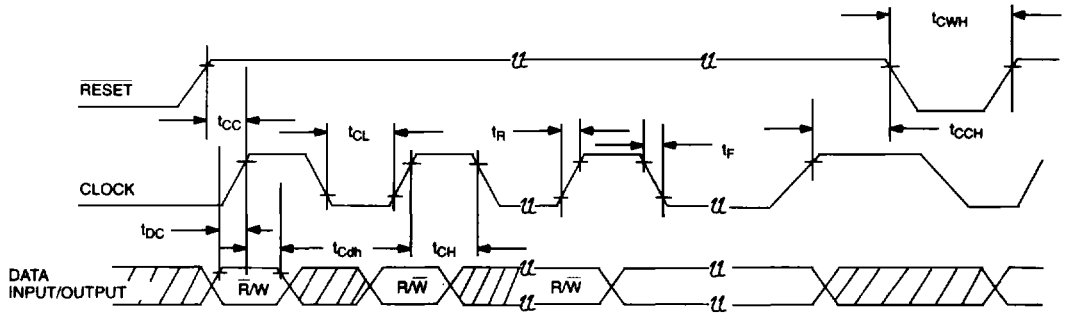
PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Input Capacitance	C_{IN}			5	pF	
Output Capacitance	C_{OUT}			7	pF	

AC ELECTRICAL CHARACTERISTICS

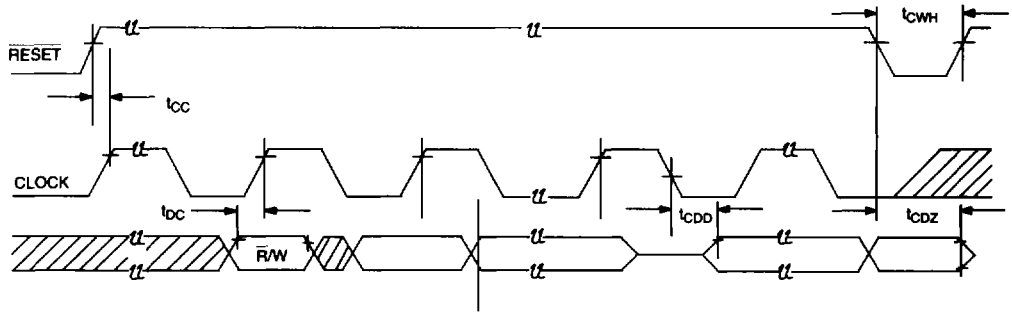
(0°C to 70°C, V_{CC} = 5V ± 10%)

PARAMETER	SYMBOL	MIN	TYP	MAX	UNITS	NOTES
Data to CLK Setup	t_{DC}	35			ns	2, 7
CLK to Data Hold	t_{CDH}	40			ns	2, 7
CLK to Data Delay	t_{CDD}			100	ns	2, 3, 5, 7
CLK Low Time	t_{CL}	125			ns	2, 7
CLK High Time	t_{CH}	125			ns	2, 7
CLK Frequency	f_{CLK}	DC		4.0	MHz	2, 7
CLK Rise & Fall	t_R, t_F	500			ns	2, 7
$\overline{RST}$ to CLK Setup	t_{CC}	1			µs	2, 7
CLK to $\overline{RST}$ Hold	t_{CCH}	40			ns	2, 7
$\overline{RST}$ Inactive Time	t_{CWH}	125			ns	2, 7, 14
$\overline{RST}$ to I/O High Z	t_{CDZ}			50	ns	2, 7

TIMING DIAGRAM: WRITE DATA



TIMING DIAGRAM: READ DATA



NOTES:

1. All voltages are referenced to GND.
2. Measured at V_{IH} = 2.0 or V_{IL} = .8V and 10ns maximum rise and fall time.
3. Measured at V_{OH} = 2.4 volts and V_{OL} = 0.4 volts.
4. For CLK, D/Q, and $\overline{RST}$.
5. Load capacitance = 50 pF.
6. Measured with outputs open.
7. Measured at V_{IH} of $\overline{RST} \geq$ 3.5V when $\overline{RST}$ supplies power.
8. Logic 1 maximum is V_{CC} + 0.3 volts if the V_{CC} pin supplies power and $\overline{RST}$ + 0.3 volts if the $\overline{RST}$ pin supplies power.
9. Applies to $\overline{RST}$ when V_{CC} < 3.5V.
10. Input levels apply to CLK, DQ, and $\overline{RST}$ while V_{CC} is within nominal limits. When V_{CC} is not connected to the key, then $\overline{RST}$ input reverts to V_{IHE}.
11. $\overline{RST}$ logic 1 maximum is V_{CC} + 0.3 volts if the V_{CC} pin supplies power and 5.5 volts maximum if $\overline{RST}$ supplies power.
12. Each DS1204V is marked with a 4-digit code AABB. AA designates the year of manufacture. BB designates the week of manufacture.
13. Average AC $\overline{RST}$ current can be determined using the following formula:
    $I_{TOTAL} = 2 + I_{LOAD\ DC} + (4 \times 10^{-3}) (CL + 140)^f$
    I_{TOTAL} and I_{LOAD} are in mA; C_L is in pF; f is in MHz.
    Applying the above formula, a load capacitance of 50 pF running at a frequency of 4.0 MHz gives an I_{TOTAL} of 5 mA.
14. When $\overline{RST}$ is supplying power t_{CWH} must be increased to100 ms average.