Keywords: DS2703, DS2703 Communication, DS2703 Flowchart

APPLICATION NOTE 4080

Communication Flowchart for the DS2703

Jul 25, 2007

Abstract: The DS2703 SHA-1 battery-pack authentication IC provides a robust cryptographic solution for ensuring the authenticity of lithium-ion battery packs in a variety of portable applications. There are 11 function commands recognized by the DS2703, and each one has a particular sequence that must be followed in order to properly execute the command. This application note provides a description of a complete transaction sequence, as well as a flowchart of all possible communication sequences for the DS2703.

Introduction

The DS2703 SHA-1 battery-pack authentication IC provides a robust cryptographic solution for ensuring the authenticity of lithium-ion (Li+, Li-ion) battery packs in a variety of portable applications. This device utilizes the Secure Hash Algorithm (SHA-1) to authenticate a battery pack for a host system, such as a cell phone, PDA, or other portable computing device. Integrating the DS2703 in the battery pack allows the host to guard against unauthorized packs that could degrade system performance or even harm the user.

The DS2703 recognizes 11 function commands, and each one has a particular sequence that must be followed in order to properly execute the command. This application note provides a description of a complete transaction sequence, as well as a flowchart of all possible communication sequences for the DS2703.

Transaction Sequence

The protocol for accessing the DS2703 through its 1-Wire® port is as follows:
- Initialization
- Net Address Command
- Function Command(s)
- Data Transfer (not all commands have data transfer)

All transactions through the 1-Wire bus begin with an initialization sequence that consists of a reset pulse transmitted by the bus master, followed by a presence pulse simultaneously transmitted by the DS2703 and any other slaves on the bus. The presence pulse tells the bus master that one or more devices are on the bus and ready to operate.

Net Address Commands

Once the bus master has detected the presence of one or more slaves, it can issue one of the net

address commands: Read, Match, Search, or Skip. **Figure 1** presents a transaction flowchart for each of the net address commands.
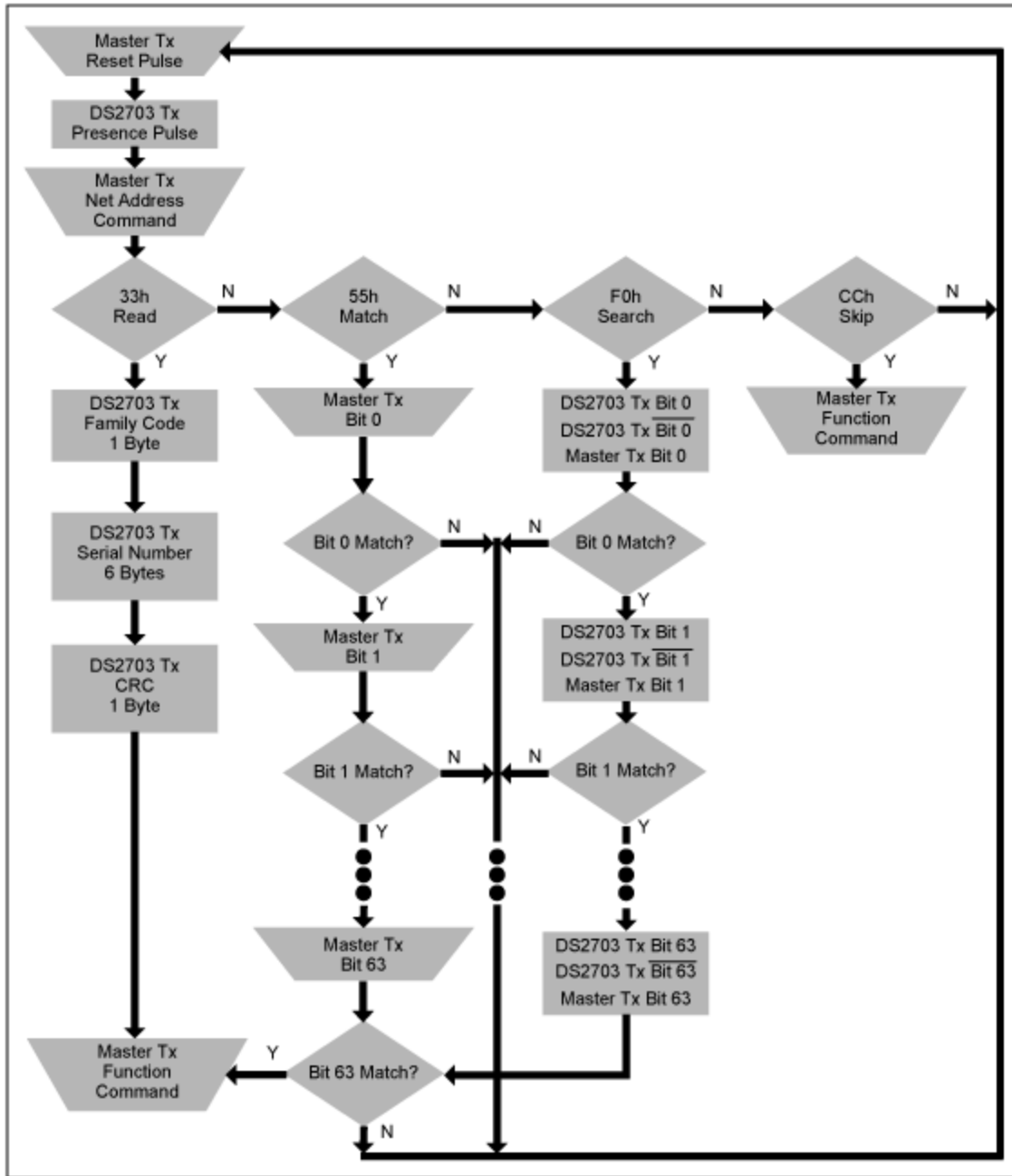

Figure 1. Net address commands flowchart for the DS2703.

Function Commands

Once the initialization and net address commands have been issued, the DS2703 is ready to receive a function command from the bus master. **Table 1** contains a list of the 11 function commands recognized by the DS2703, as well as a brief description of the function of each command. **Figure 2** then illustrates the flow required by the DS2703 to properly execute each command. Commands that require the same

sequence from the master have been combined into a single branch on the flowchart.

Table 1. All Function Commands

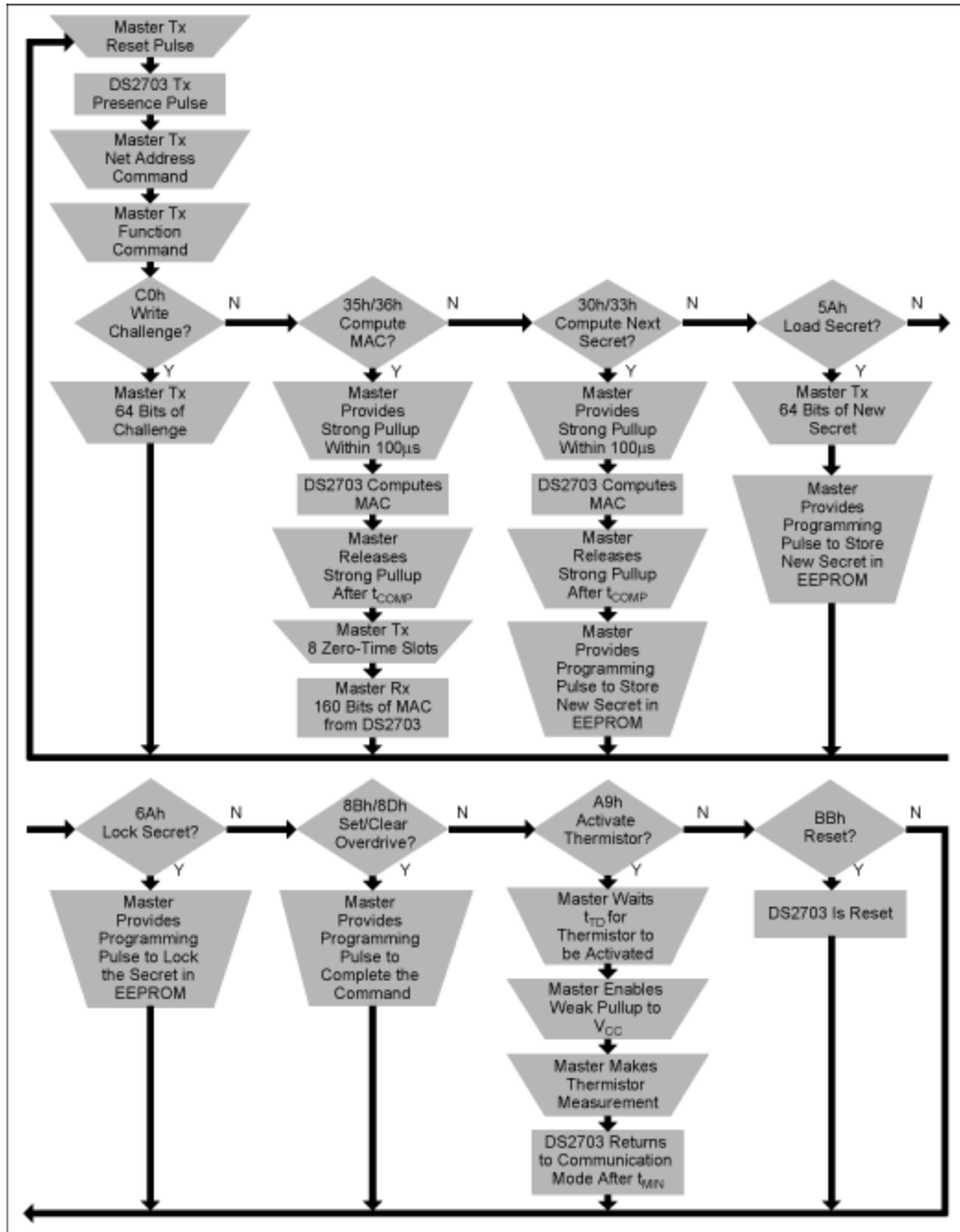| COMMAND	HEX	FUNCTION
Write Challenge	0C	Writes 64-bit challenge for SHA-1 processing; required prior to all Compute MAC and Compute Next Secret commands
Compute MAC *Without* ROM_ID and Return MAC	36	Computes hash of W0–W15 with logical 1's in place of the ROM_ID
Compute MAC *With* ROM_ID and Return MAC	35	Computes hash of W0–W15 with the ROM_ID
Load Secret	5A	Writes the 64-bit secret to supplied data; requires programming voltage on DQ
Compute Next Secret *Without* ROM ID	30	Generates new global secret; requires programming pulse
Compute Next Secret *With* ROM ID	33	Generates new unique secret; requires programming pulse
Lock Secret	6A	Sets lock bit to prevent changes to the secret; requires programming pulse
Set Overdrive	8B	Sets 1-Wire interface timings to OVERDRIVE; requires programming pulse
Clear Overdrive	8D	Sets 1-Wire interface timings to STANDARD; requires programming pulse
Activate Thermistor	A9	Activates the THM output for thermistor measurement; activation occurs within 50µs of command completion and continues until the VB capacitor is discharged
Reset	BB	Resets the DS2703 (software POR)

Figure 2. A flowchart of function commands for the DS2703.

Conclusion

The DS2703 requires a specific sequence, which must be executed under certain timing constraints, in order to properly execute the function commands. This application note has detailed the complete transaction sequence and presented a flowchart for all possible communication sequences.

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

Related Parts	
DS2703	SHA-1 Battery Pack Authentication IC

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 4080: http://www.maximintegrated.com/an4080
APPLICATION NOTE 4080, AN4080, AN 4080, APP4080, Appnote4080, Appnote 4080
Copyright © by Maxim Integrated Products
Additional Legal Notices: http://www.maximintegrated.com/legal