CIRCUIT OF MULTIFUNCTIONAL ELECTRONIC KEY WITH DATA PROTECTION

(functional equvivalent DS1991 «Maxim-Dallas Semiconductor»)

IZ1991 – circuit of multifunctional electronic key with data protection is perposed for autonomos identification in systems of access control, registration and identification of object.

Circuit performs following functions:

- One-time data writing in to ROM;
- Data storage and reading out of ROM;
- CRC-code (Cyclic Redundancy Check) generation ;
- Data transfer via 1-wire interface;
- Data and password storage for three independent keys.

Main features:

- 1152-bit secure memory with read/write possibility;
- Secure memory can be decoded only on matching 64-bit password
- Memory is partitioned into 3 blocks of 384 bits each
- 64-bit password and ID fields for each memory block
- 512-bit scratchpad ensures data transfer integrity
- Supply voltage (battery supply), U_{DD}, from 2,7 to 3,3 V
- Operating temperature range from - 40 to +85°C

Table 1 - Contact pad description

Contact pad number	Symbol	Function
01	TEST1	Test pad
02	TEST2	Test pad
03	GND	Common pin
04	DATA	Data I/O
05	U_{DD}	Supply voltage
06	TEST3	Test pad
07	TEST4	Test pad
08	TEST5	Test pad
09	TEST6	Test pad
10	TEST7	Test pad
11	TEST8	Test pad
12	TEST9	Test pad
13	TEST10	Test pad
Note – Contact pads TEST1 – TEST10 are purposed for testing and not used by customer		

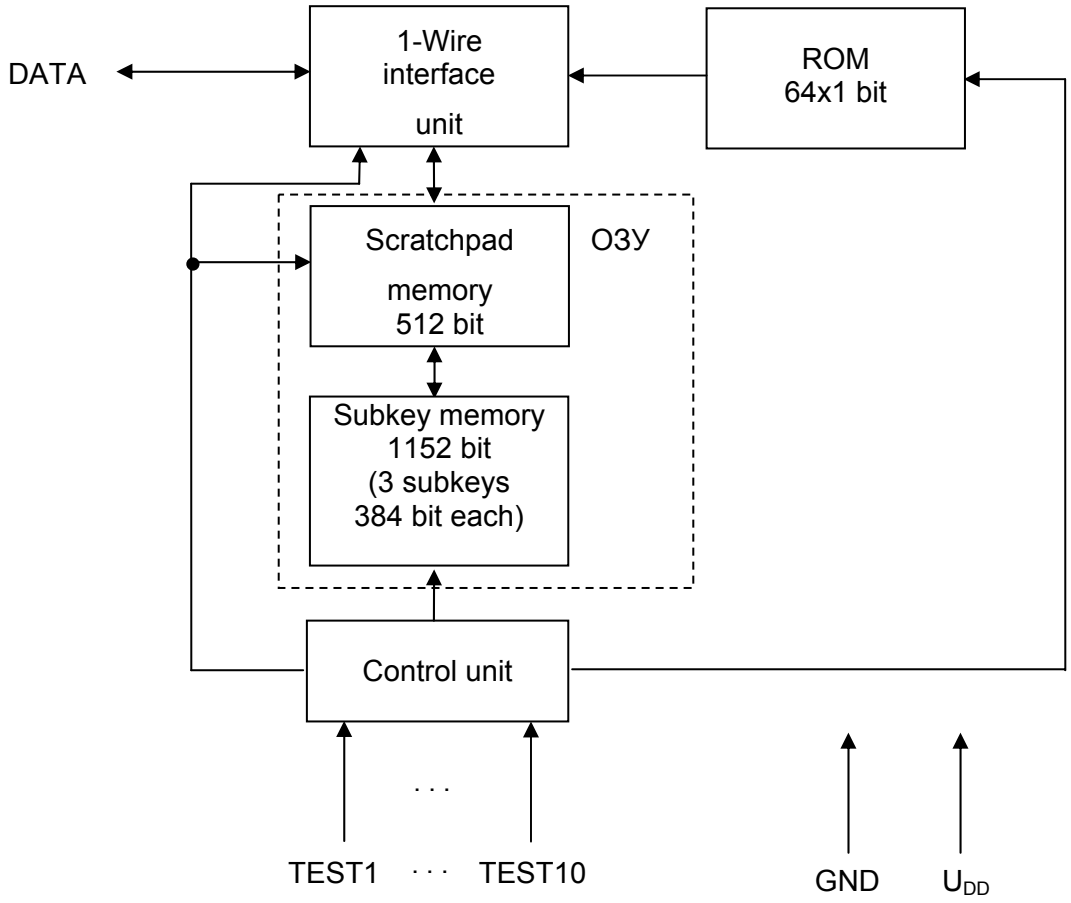


Fig. 1 – Block diagramm

Table 2 – Absolute maximum ratings

Symbol	Parameter	Norm		Unit
		Min	Max	
U_{CC}	Supply voltage (on external pullup resistor)	-0,5	7,0	V
U_{IL}	Low level input voltage	-0,3	-	V
U_{IH}	High level input voltage	-	U_{CC}+0,3	V
Ta	Ambient temperature	-60	125	°C
Note - All voltages are indicated relative to GND				

Table 3 – Recommended operation conditions

Symbol	Parameter	Norm		Unit
		Min	Max	
U_{CC}	Supply voltage (on external pullup resistor)	2,8	6,0	V
U_{DD}	Supply voltage (from battery cell)	2,7	3,3	V
U_{IL}	Low level input voltage	0	0,8	V
U_{IH}	High level input voltage	2,2	U_{CC}	V
Ta	Operating ambient temperature	-40	85	°C
Note - All voltages are indicated relative to GND				

Immunity to ESD potential 1000 V. Limiting value of the potential of static electricity 2000 V.

Table 4 – Electric parameters of IC

Symbol	Parameter	Measurement mode	Norm		Unit	Ambient temperature, °C
			Min	Max		
U_{OL}	Low level output voltage	U_{DD}=2,7 V U_{CC}=2,8 V U_{IL}=0 V U_{IH}= U_{CC} I_{OL}=4 mA	-	0,4 0,45	V	25±10 85 -40
U_{OH}	High level output voltage	U_{DD}=3,3 V U_{CC}=6,0 V U_{IL}=0 V U_{IH}= U_{CC}	-	6	V	25±10 85 -40
t_{PDL}	Low level presence pulse detection time	U_{DD}=2,7 V U_{CC}=2,8 V U_{IL}=0 V U_{IH}= U_{CC} and U_{DD}=3,3 V U_{CC}=6,0 V U_{IL}=0 V U_{IH}= U_{CC}	70 60	230 240	μs	25±10 85 -40

Type current consumption (I/O DATA) 6 μA (U_{DD}=3,3 V, U_{CC}=6,0 V).

General operation description

The IZ1991 multikey is read/write data carrier that acts as three separate electronic keys, and provide 1152 bits of secured memory to user.

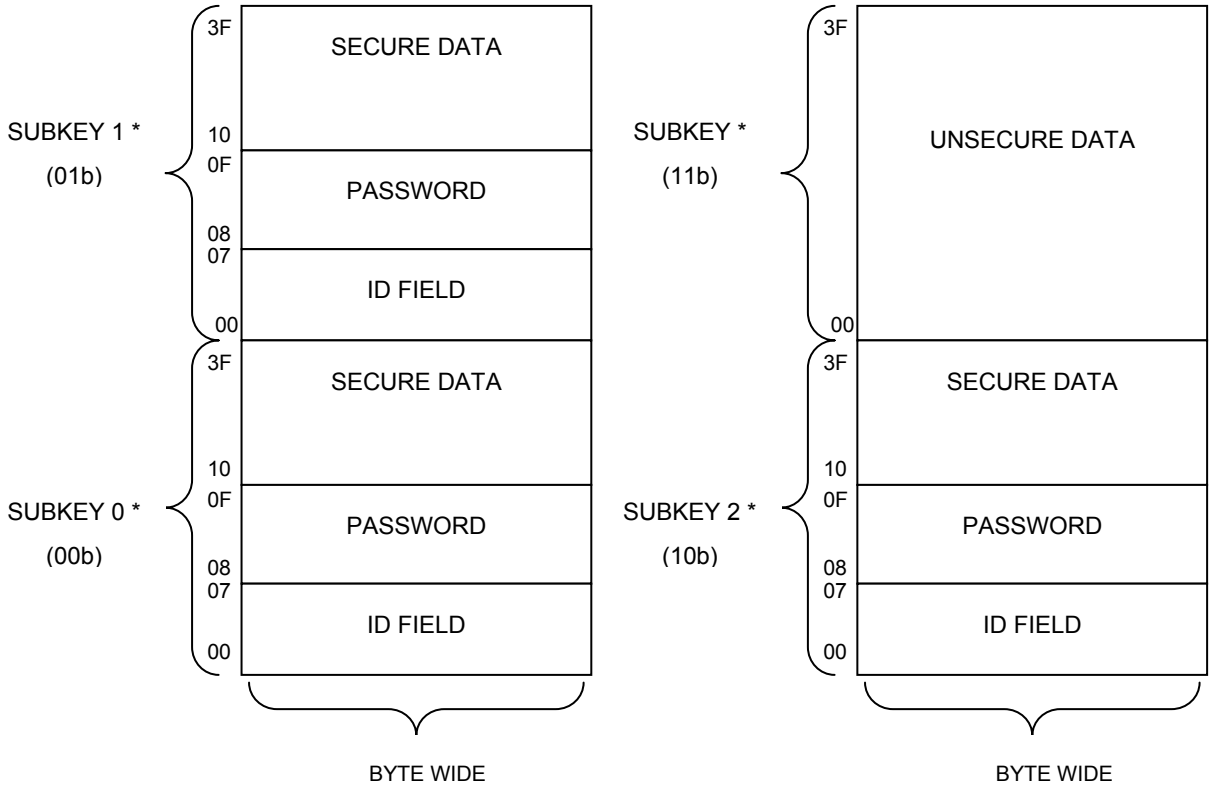
Each 384 bits key has 64-bit individual password and public ID fields . The password field must be matched in order to access the secure memory. Data is transferred serially via the 1-Wire protocol, which requires only a single data (signal) lead, a common (ground) & power supply leads.

The 512-bit scratchpad memory ensures integrity of data transfers to secure memory. Data should first be written to the scratchpad where it can be read back. After the data verification, a copy scratchpad memory command will transfer the data to the secure memory. This process ensures data integrity when modifying the memory. Constant power supply of device is requiered for data storage in scratchpad memory.

Fig.2 displays RAM map.

A 48-bit serial number is written into each IZ1991 during manufacturing process to guarantee unique identity which provide absolute control possibility.

Application fields include secure access control, debit tokens, work-in-progress tracking, electronic monitoring of goods transportation and proprietary (private) data storage.



* The scratchpad & each subkey or has its own unique address.

Fig. 2. RAM map

The IZ1991 is accessed via a single data line using the 1-Wire protocol. The bus master must first provide one of the four ROM function commands:

- Read ROM,
- Match ROM,
- Search ROM,
- Skip ROM.

These commands operate on the 64-bit ROM that present iside each chip. These commands can singulate a specific device if many are present on the 1-Wire line & also indicate to the bus master how many and what types of devices are present. After a ROM function command is successfully executed, the memory functions that operate on the secure memory and the scratchpad become accessible and the bus master can issue any one of the six memory function commands specific to the IZ1991. All data is read and written starting from lower bit.

64-bit ROM

Each IZ1991 contains a unique 64 bits ROM code. The first 8 bits are a 1-Wire family code. The next 48 bits are a unique serial number. The last 8 bits are a CRC of the first 56 bits. (Figure 3.) The CRC (Cyclic Redundancy Check) for 1-Wire bus is formed using a polynomial generator consisting of a shift register and XOR gates as shown in Fig. 4. The polynomial $X^8 + X^5 + X^4 + 1$ is used for all that. The shift register bits are initialized to zero. Then starting with the lower bit of the family code, 1 bit at a time is shifted in. After the 8th bit of the family code has been entered, then the serial number is entered. After the 48th bit of the serial number has been entered, the shift register contains the CRC value. Shifting in the 8 bits of CRC should return the shift register to all zeros.

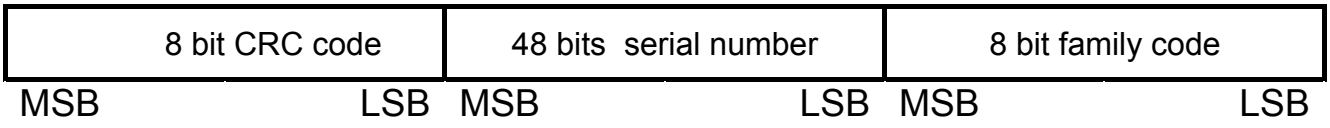


Fig. 3. 64-bit code structure

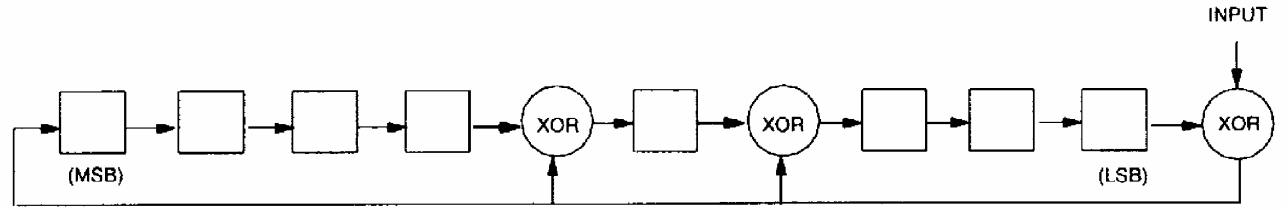


Fig. 4. 1-Wire bus CRC generator

Memory function commands

There are six device-specific for IZ1991 commands - three scratchpad memory commands(Write Scratchpad memory, Read Scratchpad memory , Copy Scratchpad memory) and three subkey commands (Write Password, Write Subkey and Read Subkey). After the device is selected, the memory function command is written to the IZ1991. The command is consist of three fields, each one byte long:

The first byte is the function code field. This field defines the six commands that can be executed.

The second byte is the address field. The first 6 bits of this field define the starting address of the command. The last 2 bits of this field are the subkey address code.

The third byte of the command is a complement of the second byte

The structure of command is shown in the table 5.

For the first use, the IZ1991 needs to be initialized.since the passwords actually stored in the device are unknown. This operation is done by directly writing (i. e., not through the scratchpad memory) the new identifier and and password for the selected subkey using the Write Password command. As soon as new identifier and password are stored in the device, further updates should be done through the scratchpad.

Table 5. IZ1991 Command structure

<table>
<tr><th rowspan="2">Command</th><th rowspan="2">1st byte</th><th colspan="8">2nd byte</th><th rowspan="2">3rd byte</th></tr>
<tr><th>B7</th><th>B6</th><th>B5</th><th>B4</th><th>B3</th><th>B2</th><th>B1</th><th>B0</th></tr>
<tr><td>Write scratchpad memory</td><td>96h</td><td rowspan="2">1</td><td rowspan="2">1</td><td colspan="6" rowspan="2">Any value from 00h to 3Fh</td><td rowspan="7">com-plement of 2nd byte</td></tr>
<tr><td>Read scratchpad memory</td><td>69h</td></tr>
<tr><td>Copy scratchpad memory</td><td>3Ch</td><td rowspan="5">Subkey number:
0 0
or
0 1
or
1 0</td><td rowspan="5">0</td><td rowspan="5">0</td><td rowspan="5">0</td><td rowspan="5">0</td><td rowspan="5">0</td><td rowspan="5">0</td></tr>
<tr><td>Read subkey</td><td>66h</td></tr>
<tr><td>Write subkey</td><td>99h</td></tr>
<tr><td>Write password</td><td>5Ah</td></tr>
<tr><td colspan="2">Any value from 10h to 3Fh</td></tr>
</table>

Scratchpad memory commands

The 64-byte read/write scratchpad memory of the IZ1991 is not protected by password. Its usual purpose is to build up a data structure to be verified and then copied to a secure subkey.

Write scratchpad memory [96h]

The Write Scratchpad command is used to enter data into the scratchpad. The starting address for the write sequence is specified in the command. Data can be continuously written until the end of the scratchpad memory is reached or until the IZ1991 is reset. The command sequence is shown in Fig. 5-1, left column.

Read scratchpad memory [69h]

The Read Scratchpad memory command is used to retrieve data from the scratchpad. The starting address is specified in the command word. Data can be continuously read until the end of the scratchpad is reached or until the IZ1991 is reset. The command sequence is shown in Fig. 5-1, center column.

Copy scratchpad memory [3Ch]

The Copy Scratchpad memory command is used to transfer specified data blocks from the scratchpad to a selected subkey. This command should be used when data verification is required before storage in a secure subkey. Data can be transferred in single 8-byte blocks or in one large 64-byte block. There are nine valid block selector codes that are used to specify which block is to be transferred. Block selector codes are presented in table 6. As a further precaution against accidental erasure of secure data, the 8-byte password of the destination subkey must be entered. If the password does not match, the operation is terminated. After the block of data is transferred to the secure subkey, the original data in the corresponding block of the scratch-pad is erased. The command sequence is shown in Fig. 5-1, right column

Subkey commands

Each of the subkeys within the IZ1991 is accessed individually. Transactions to read and write data to a secured subkey start at the address defined in the command and proceed until the device is reset or the end of the subkey is reached.

Write password [5Ah]

The Write Password command is used to enter the ID and password of the selected sub-key. This command erase all of the data stored in the secure area as well as overwriting the ID and password fields with the new data. The IZ1991 has a built-in check to ensure that the proper subkey was selected. The sequence begins by reading the ID field of the selected subkey; the ID of the subkey to be changed is the IDs do not match, the sequence is terminated. Otherwise, the subkey contents are erased and 64 bits of new ID data are written followed by a new 64-bit password. The command sequence is shown in Fig. 5-2, right column.

Write subkey [99h]

The write subkey command is used to enter data into the selected subkey. Since the sub-keys are secure, the correct password is required to access them. The sequence begins by reading the ID field; the password is then written back. If the password is incorrect, the transac-tion is terminated. Otherwise, the data following is written into the secure area. The starting ad-dress for the write sequence is specified in the command word. Data can be continuously written until the end of the secure subkey is reached or until the IZ1991 is reset. The command se-quence is shown in Figure 5-2, center column.

Read subkey [66h]

The Read Subkey command is used to retrieve data from the selected subkey. Since the subkeys are secure, the correct password is required to access them. The sequence begins by reading the ID field; the password is then written back. If the password is incorrect, the IZ1991 will transmit random data.

Otherwise the data can be read from the subkey. The starting address is specified in the com-mand. Data can be continuously read until the end of the subkey is reached or until the IZ1991 is reset. The command sequence is shown in Figure 5-2, left column.

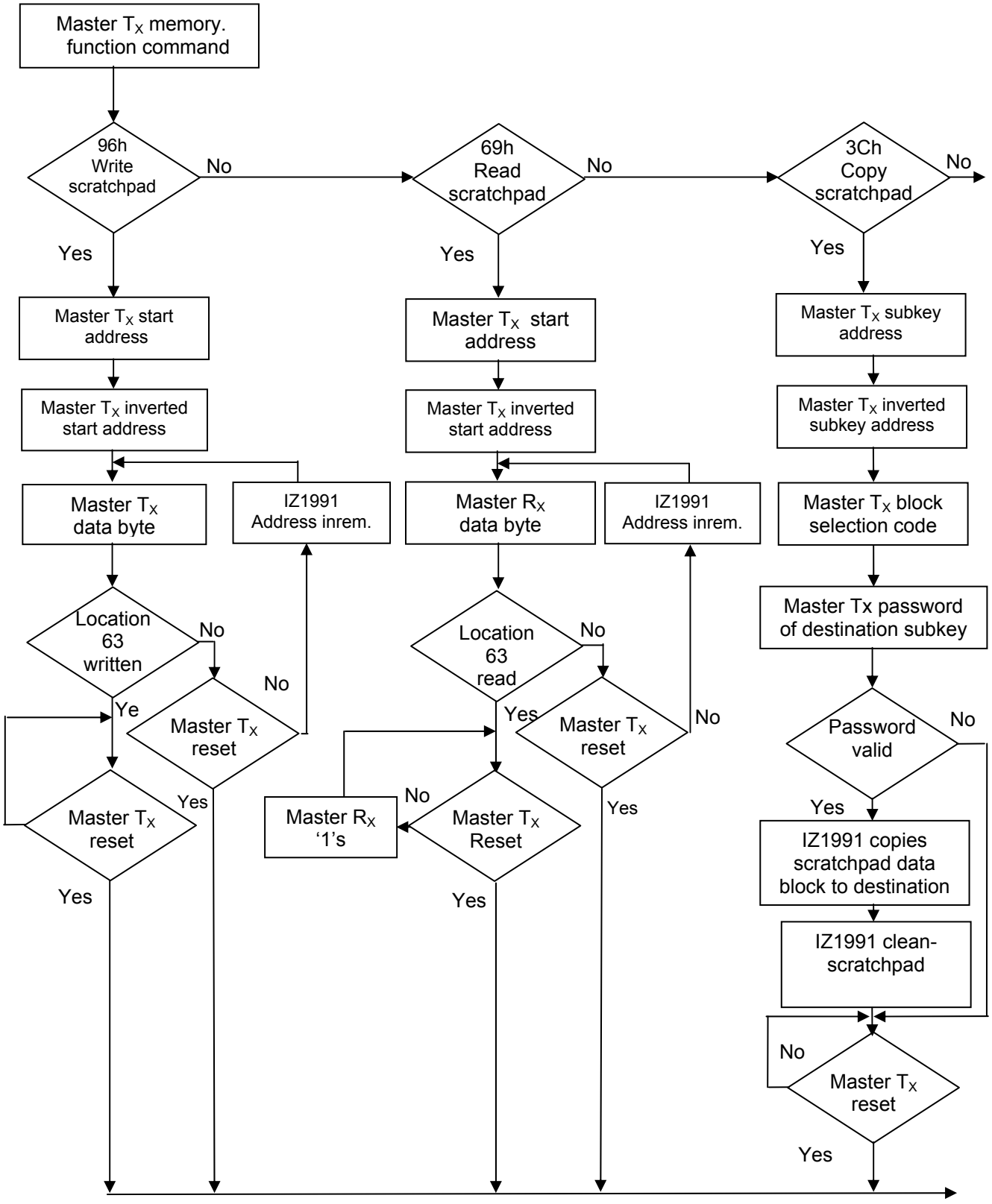


Fig. 5-1. Memory function block-diagram (Part 1)

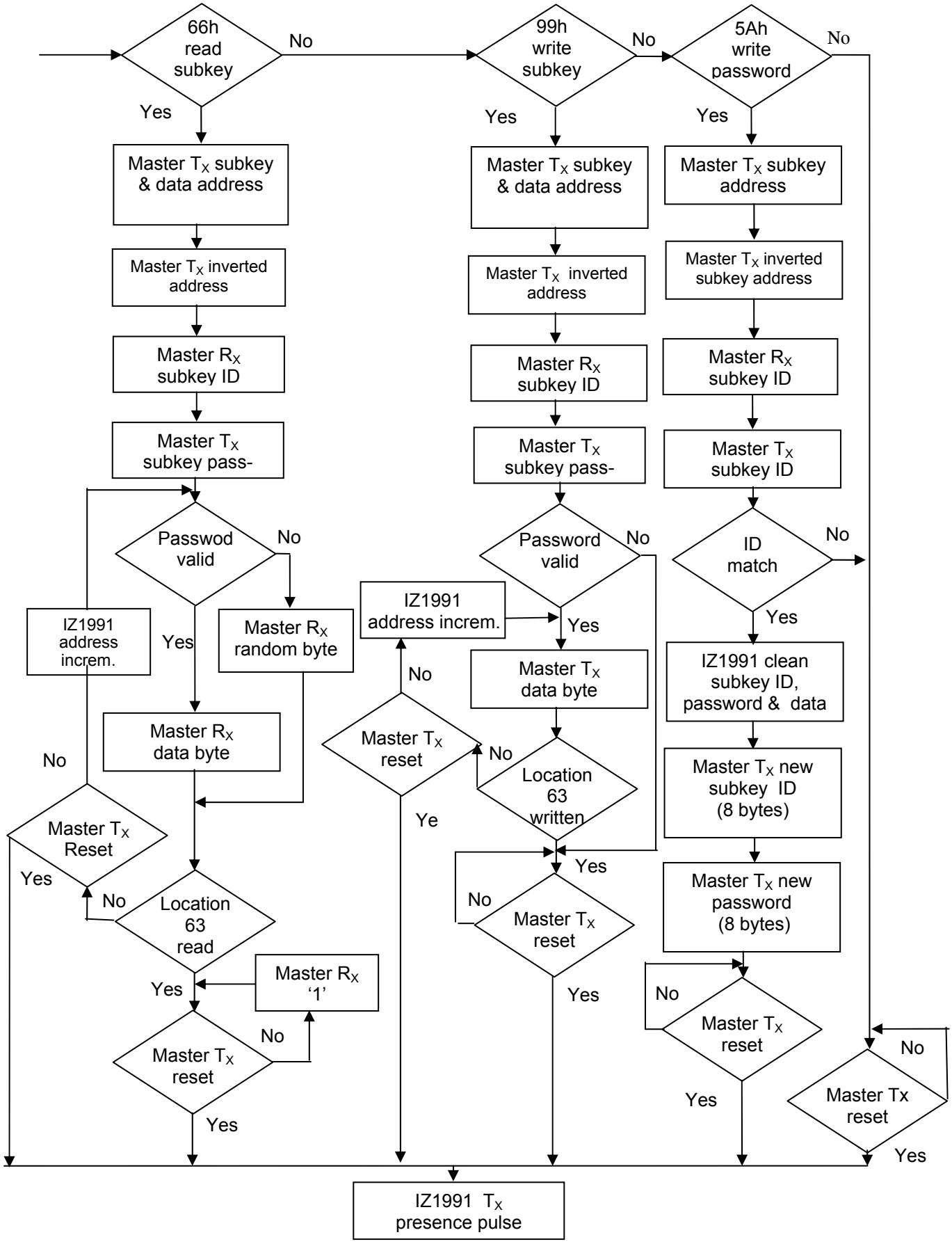


Fig. 5-2. Memory function block-diagram (part 2)

Table 6

Block number	Address range	Codes							
		LSB							MSB
0 to 7	00 to 3Fh	56	56	7F	51	57	5D	5A	7F
0	ID	9A	9A	B3	9D	64	6E	69	4C
1	Password	9A	9A	4C	62	9B	91	69	4C
2	10h to 17h	9A	65	B3	62	9B	6E	96	4C
3	18h to 1Fh	6A	6A	43	6D	6B	61	66	43
4	20h to 27h	95	95	BC	92	94	9E	99	BC
5	28h to 2Fh	65	9A	4C	9D	64	91	69	B3
6	30h to 37h	65	65	B3	9D	64	6E	96	B3
7	38h to 3Fh	65	65	4C	62	9B	91	96	B3

1-wire bus system

The 1-Wire bus is a system which has a single bus master and one or more slaves. In all instances, the IZ1991 is a slave device. The bus master is typically a micro-controller. The discussion of this bus system is broken down into three topics: hardware configuration, transaction sequence, and 1-Wire signaling (signal types and timing). A 1-Wire protocol defines bus transactions interms of the bus state during specified time slots that are initiated on the falling edge of sync pulses from the bus master.

Hardware configuration

The 1-Wire bus has only a single line by definition; it is important that each device on the bus be able to drive it at the appropriate time. To facilitate this, each device attached to the 1-Wire bus must have an open drain connections or tri-state outputs. The 1-Wire port of the IZ1991 is an open drain part with an internal circuit equivalent to that shown in Fig. 6. The bus master can be the same equivalent circuit. If a bidirectional pin is not available, separate output and input pins can be tied together.

The bus master requires a pullup resistor at the master end of the bus, with the bus master circuit equivalent to the one shown in Fig. 7. The value of the pullup resistor should be approximately 5 kΩ for short line lengths.

A multidrop bus consists of a 1-Wire bus with multiple slaves attached. The 1-Wire bus has a maximum data rate of 16.3 kbits per second. The idle state for the 1-Wire bus is high. If, for any reason a transaction needs to be suspended, the bus must be left in the idle state if the transaction is to resume. If this does not occur, and the bus is left low for more than 120 μs, one or more of the devices on the bus may be reset.

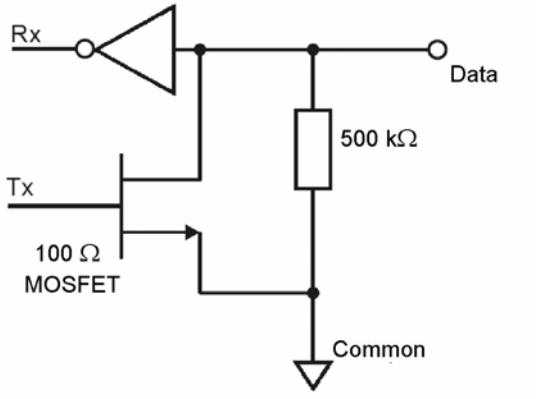
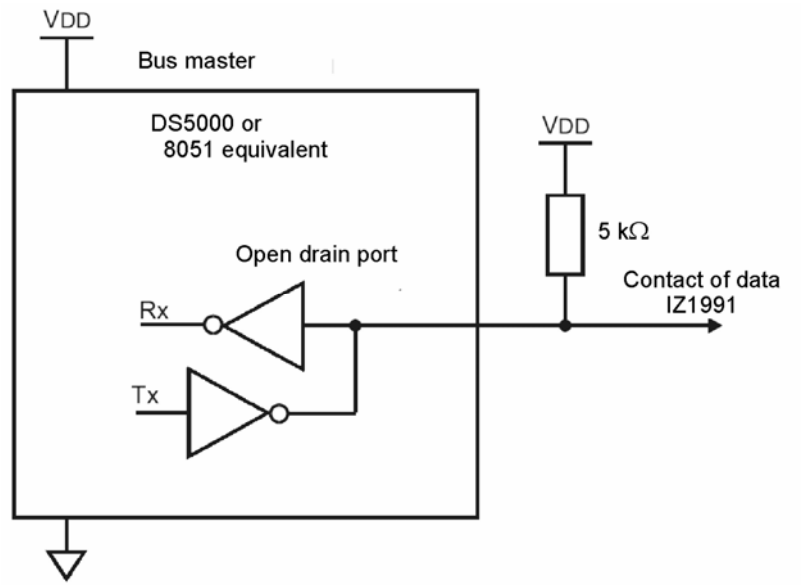
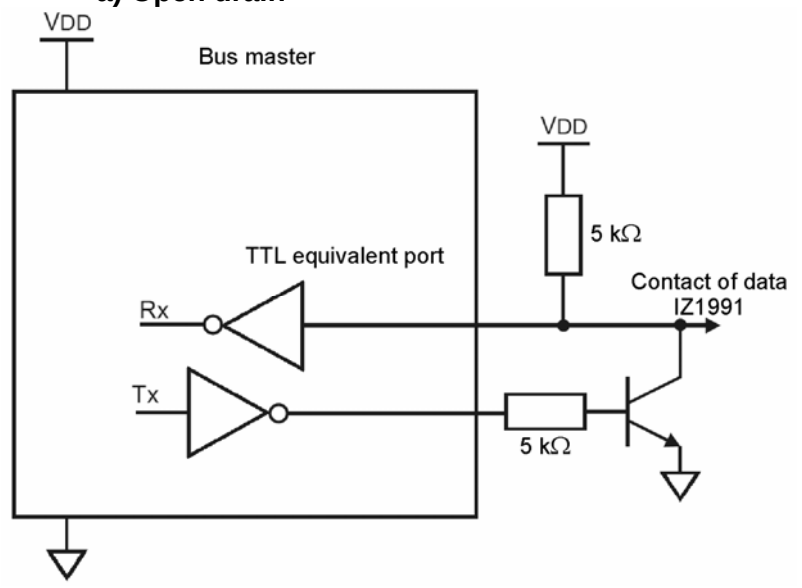


Fig. 6 – Equvivalent circuit of port



a) Open drain



b) Standard TTL

Fig. 7 – Equvivalent circuit of bus master

Transaction sequence

The protocol for accessing the IZ1991 via the 1-Wire port is as follows:

- Initialization
- ROM functions command
- Memory function command
- Transaction/data

Initialization

All transactions on the 1-Wire bus begin with an initialization sequence. The initialization sequence consists of a reset pulse transmitted by the bus master followed by presence pulse(s) transmitted by the slave(s). The presence pulse lets the bus master know that the IZ1991 is on the bus and is ready to operate.

ROM functions commands

Once the bus master has detected a presence of device, it can issue one of the four ROM functions commands that the IZ1991 supports. All ROM function commands are 8 bits long. A flowchart ROM functions commands is shown at Fig. 8. Description of these commands is indicated below.

Read ROM [33h]

This command allows the bus master to read the IZ1991's 8-bit family code, unique 48-bit serial number and 8-bit CRC. This command should only be used if there is a single IZ1991 on the bus. If more than one slave is present on the bus, a data collision will occur when all slaves try to transmit at the same time (open drain will produce a wired-AND result).

Match ROM [55h]

The match ROM command, followed by a 64-bit ROM sequence, allows the bus master to address a specific IZ1991 on a multidrop bus. Only the IZ1991 that exactly matches the 64-bit ROM sequence will respond to the subsequent memory function command. All slaves that do not match the 64-bit ROM sequence will wait for a reset pulse. This command can be used with a single or multiple devices on the bus.

Skip ROM [CCh]

This command can save time in a single drop bus system by allowing the bus master to access the memory functions without providing the 64-bit ROM code. If more than one slave is present on the bus and, for example, a read command is issued following the Skip ROM command, data collision will occur on the bus as multiple slaves transmit simultaneously (open drain will produce a wired-AND result).

Search ROM [F0h]

When a system is initially brought up, the bus master might not know the number of devices on the 1- Wire bus or their 64-bit ROM codes. The search ROM command allows the bus master to use a process of elimination to identify the 64-bit ROM codes of all slave devices on the bus. The ROM search process is the repetition of a simple 3-step routine: read a bit, read the complement of the bit, then write the desired value of that bit. The bus master performs this simple 3-step routine on each bit of the ROM.

After one complete pass, the bus master knows the contents of the ROM in one device. Additional passes will identify the ROM codes of the remaining devices.

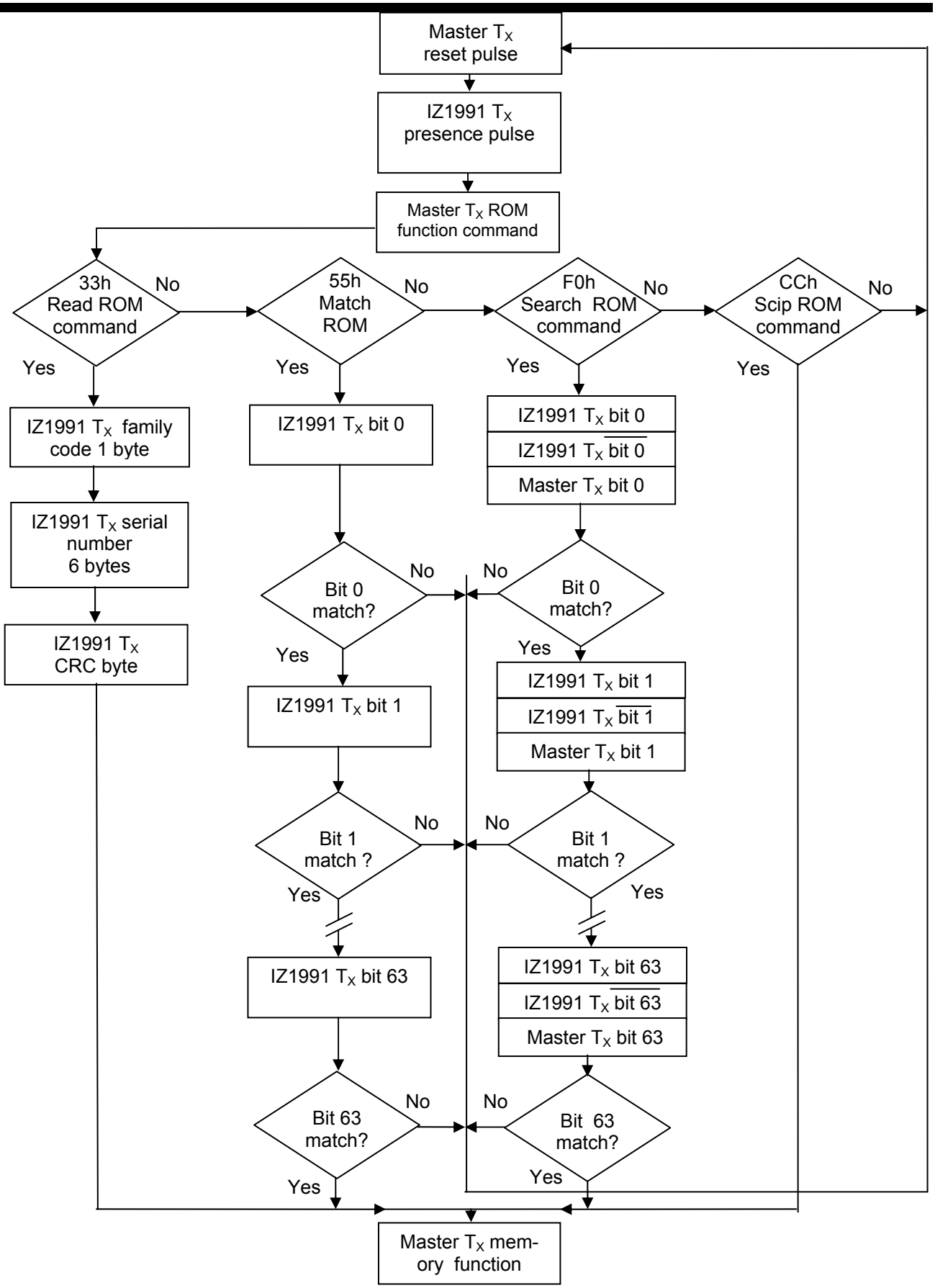
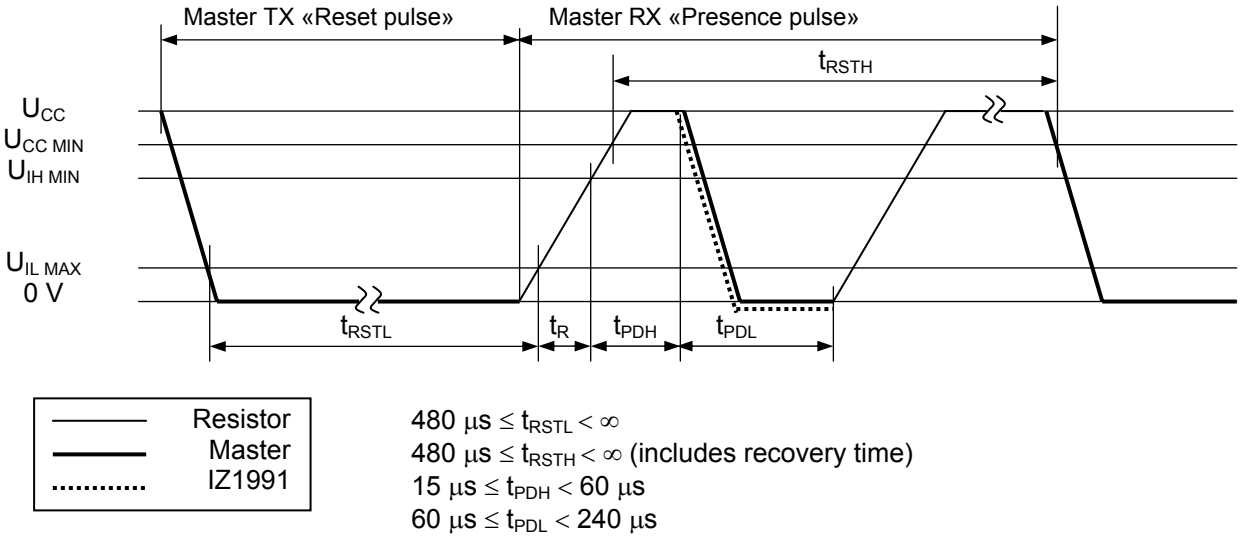


Fig. 8. ROM function flow chart

1-WIRE SIGNALING

The IZ1991 requires strict protocols to ensure data integrity. The protocol consists of four types of signaling on one line: reset sequence with reset pulse and presence pulse, write 0, write 1 and read data. All these signals except presence pulse are initiated by the bus master. The initialization sequence required to begin any communication with the IZ1991 is shown in Fig. 9. A reset pulse followed by a presence pulse indicates the IZ1991 is ready to send or receive data given the correct ROM command and memory function command. The bus master transmits a reset pulse (t_{RSTL}, minimum 480 us).

Then the bus master releases the line and goes into receive mode. The 1-Wire bus is pulled to a high state via the pullup resistor. After detecting the rising edge on the data pin, the IZ1991 waits (t_{PDH}, 15-60 us) and then transmits the presence pulse (t_{PDL}, 60-240 us).



In order not to mask interrupt signaling by other devices on the 1-Wire bus, $t_{RSTL} + t_R$ should always be less than 960 μs.

Fig. 9. Initialization time diagramm

Read/write time slots

Write and read time diagramms are illustrated in Fig. 10-12. Description of dynamic parameters is given in table 7. All time slots are initiated by the master driving the data line low. The falling edge of the data line synchronizes the IZ1991 to the master by triggering a delay circuit in the IZ1991. During write time slots, the delay circuit determines when the IZ1991 will sample the data line. For a read data time slot, if a “0” is to be transmitted, the delay circuit determines how long the IZ1991 will hold the data line low overriding the 1 generated by the master. If the data bit is a “1”, the IZ1991 will leave the read data time slot unchanged.

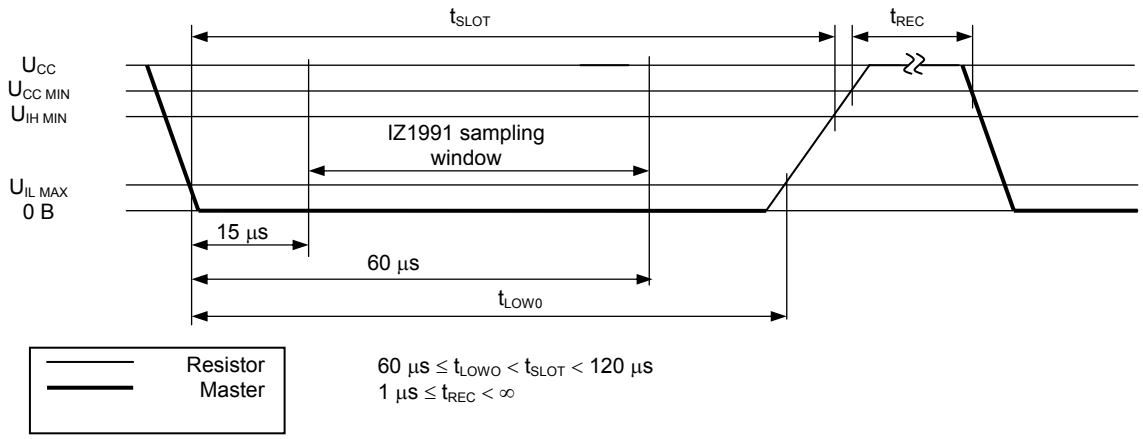


Fig. 10. Write “0” time diagramm

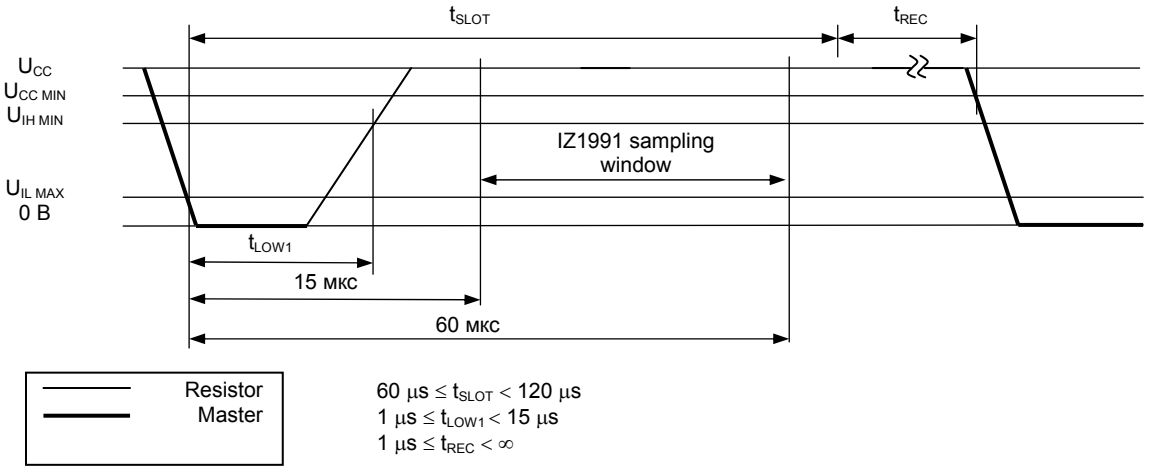


Fig. 11. Write “1” time diagramm

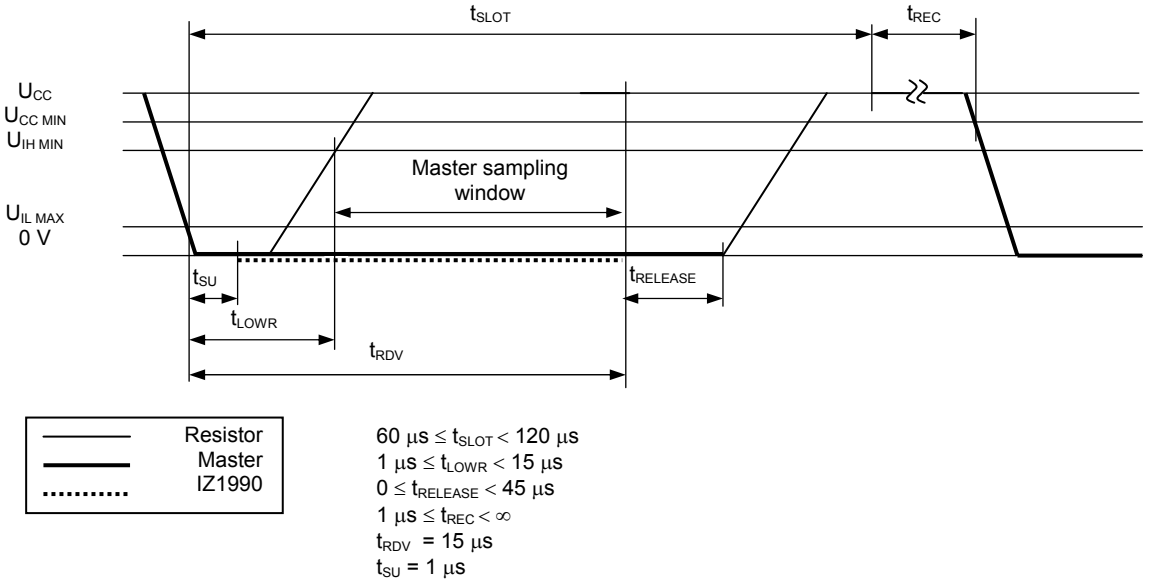


Fig. 12. Read time diagramm

Table 7 – Dynamic parameters (Ta = -40 ÷ 85 °C)

Parameter, unit	Symbol	Norm		Note
		Min	Max	
1-wire interface protocol time slot period, μs	t_{SLOT}	60	120	-
Write “1” low time, μs	t_{LOW1}	1	15	-
Write “0” low time, μs	t_{LOW0}	60	120	-
Read data valid time, μs	t_{RDV}	15		-
Bus release time, μs	$t_{RELEASE}$	0	45	-
Read data setup time, μs	t_{SU}	1		1
Recovery time, μs	t_{REC}	1	-	-
Reset high time, μs	t_{RSTH}	480	-	2
Reset low time, (s	tRSTL	480	-	-
Presence detect high time, μs	t_{PDH}	15	60	-
Presence detect low time, μs	t_{PDL}	60	240	-
Rise time, μs	t_R	-	-	3

Notes

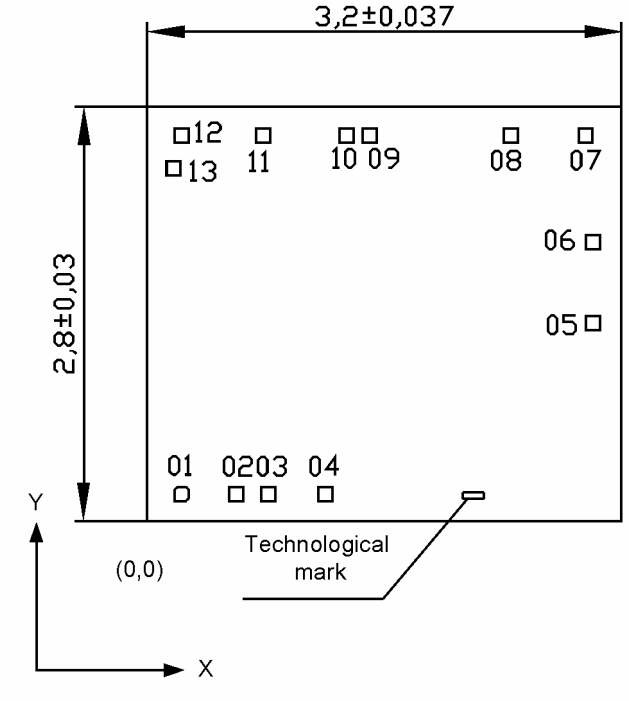
1 Read data setup time refers to the time the host must pull the 1-Wire bus low to read a bit. Data is guaranteed to be valid within 1 μs of this falling edge and will remain valid for 14 μs minimum. (15 μs total from falling edge on 1-Wire bus.)

2 An additional reset or communication sequence cannot begin until the reset high time has expired.

3 In order not to mask interrupt signaling by other devices on the 1-Wire bus, $t_{RSTL} + t_R$ should always be less than 960 μs

Chip and contact pad layout diagram

ICs are available for shipment in chip form (not diced wafer)
Weight of IC is not more 0,01 g.



Die thickness 0,460±0,022 mm.
Technological mark ”1991” has coordinates (mm): left bottom corner: x=2,230, y=0,150.

Contact pad number	Coordinates (left bottom corner), mm	
	X	Y
01	0,183	0,135
02	0,552	0,135
03	0,770	0,135
04	1,153	0,135
05	2,960	1,295
06	2,960	1,840
07	2,911	2,560
08	2,405	2,560
09	1,455	2,560
10	1,300	2,560
11	0,737	2,560
12	0,183	2,560
13	0,130	2,338
Note: Contact pad coordinates and dimensions 0,095 x 0,095 mm are indicated under «Passivation» layer		

Fig 13 – Chip and contact pad layout diagram