

0J66D MC68HC08AZ32 MICROCONTROLLER RESEARCH REPORT

Theory:

A security feature discourages unauthorized reading of ROM locations while in monitor (MON 08) mode. The host can bypass the security feature at monitor mode entry by sending eight security bytes that match the byte locations \$FFF6–\$FFFD. Locations \$FFF6–\$FFFD contain user-defined data.

During monitor mode entry, the MCU waits after the power-on reset for the host to send the eight security bytes on pin PA0. If the received bytes match those at locations \$FFF6–\$FFFD, the host bypasses the security feature and can read all ROM locations and execute code from ROM.

Security remains bypassed until a power-on reset occurs. After the host bypasses security, any reset other than a power-on reset requires the host to send another eight bytes. If the reset was not a power-on reset, security remains bypassed regardless of the data that the host sends. If the received bytes do not match the data at locations \$FFF6–\$FFFD, the host fails to bypass the security feature.

The MCU remains in monitor mode, but reading ROM locations returns undefined data (for example \$AD), and trying to execute code from ROM causes an illegal address reset. After the host fails to bypass security, any reset other than a power-on reset causes an endless loop of illegal address resets. After receiving the eight security bytes from the host, the MCU transmits a break character signaling that it is ready to receive a command.

0J66D, 1H56A MASK SETS

The ROM security feature is not offered on the 68HC08AZ ROM devices, because the operation of security in monitor mode does not match that of other HC08 family members. MCU does not wait after the power-on reset for the host to send the eight security bytes on PIN PA0. There is no sense to send any combinations of the SS sequences, because MCU do not accept it.

Conclusions:

There is no way read ROM code of 0J66D MASK based MCU !?

Practice:

THE ROMSCOUT

The ROMSCOUT (ROM reader) designed to gain access of 0J66D MCU ROM code. The ROMSCOUT help to replace broken 0J66D devices to FLASH based microcontrollers with similar features and same amount of memory.

Target MCU: 0J66D XC527253 / 509020720000

Target cluster: MAGNETI MARELLI / O1 550411810005

Target IC MC68HC08AZ32

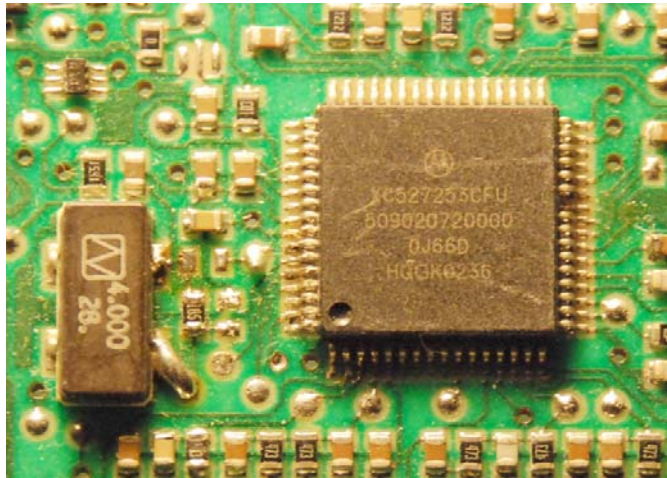


Figure 1.

Target cluster MAGNETI MARELLI



Figure 2.

The ROMSCOUT (Rom reader) hardware

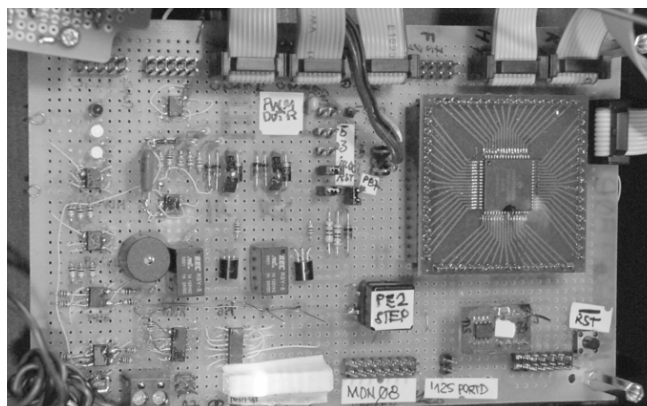


Figure 3.

Results:

Time to access ROM code:.....1 – 6 min
Operate mode:..... MON 08
Vcc:..... 5.0V
Vtst:..... 8.8V
External Clock-In (if applied):..... 8.0 MHz

The ROM data (ROMSCOUT extracted):

For example:

```
~~~~~  
$FFE0: $83 $83 $F9 $D3 $F9 $D6 $F9 $F9 $F9 $DC $D9 $DF $F9 $E2 $F9 $E5  
$FFF0: $F9 $E8 $F9 $EB $F9 $EE $F9 $F1 $F9 $F4 $F9 $F7 $F9 $FA $FD $75
```

Reset vector: \$FD75

```
~~~~~  
$FD75: $45 $04 $4F $94 $C6 $F9 $FF $26 $03 $CE $F9 $FE $27 ~~~~~~  
~~~~~
```

Appendix:

Feature:

Few of 0J66D mask set derivatives do not turn off COP during entering to MON 08 and it is seems no able to execute code into the RAM, because IRQ reminds normal operate voltage level instead of TST level. In this case, disable COP by software before definite the stack, for example:

```
BSET 0,$1F ; COP disable  
LDHX #RAMEnd-1 ; initialize the stack  
TXS  
.....  
.....
```