RL78 Safety Features

Renesas Electronics Corporation
Introduction

- **Purpose**
  - This course provides an introduction to the RL78 safety features. The capabilities and function of each feature will be explained.

- **Objective**
  - Learn about the RL78 security features and its capabilities.

- **Content**
  - 34 pages (including this page)

- **Learning Time**
  - 20 minutes
Safety features overview
Safety Features overview

Two types of CRC Hardware
• Type1: Fast checking (512us for 64KB) for test on initialize routine
• Type2: Part of Flash check for test during operation

Parity / Write Protection
• Parity: Internal reset when parity error generated on “write”, checked on “read”
• Write Protection: Protect area can be selected Lowest address ~ 128B/~256B/~512B

Illegal memory access
• Illegal memory access: generate “internal reset”
• Trap instruction: “FF” instruction generate “internal reset”

Stop Detection / Frequency check
• Stop detection by WWDT
• Frequency check by special Timer function

Ideal support to comply with IEC60730 Safety Standards & Class B SW requirements
VDE Approval already done

More Relief for your system by H/W Safety functions

ADC measurement sources:
• ANIx (external signal)
• AVref+ (external / internal)
• AVref- (external / internal)
• Internal Vref (1.4V typ)
• Temperature sensor

Libraries available

© 2011 Renesas Electronics Corporation. All rights reserved.
VDE certification

- VDE certification already done
- No need to re-certify* safety s/w block (Savings ~ €10K)
- Reduce development time (Savings ~ 3 Man Months)

Following modules are available
  - CPU register test
  - Variable memory test
  - Invariable memory test
  - System clock test
Safety features on Flash

Flash
(Invariable Memory)
CRC functionality

- High speed CRC
  - Able to calculate the CRC over the whole code flash area
  - Intend to use directly after reset.
  - CPU is stopped during calculation (512us for 64 K)
  - CRC0CTL control register
    - Sets range (blocks of 16k)
    - Start operation
  - PGCRCL result register
    - Store the result after completion

---

Start

Setup high speed CRC

Execute HALT

Process result

512us for 64K

Stop
CRC functionality

- General purpose CRC
  - Able to calculate the CRC for single bytes
    - Partly cyclic check of code flash
    - CRC check for other data (e.g. transmit data)
  - Conform to CCITT algorithm \((x^{16} + x^{12} + x^5 + 1)\)
  - Result within one clock cycle
  - CRCIN 8-bit input register
  - CRCD 16-bit result register
ECC functionality

- A 6-bit ECC is implemented in the code flash area

During the Flash Write the data are encrypted in the ECC Encryption Logic and the resulting bits are stored in the ECC part of the flash.

During Flash Read these bits are used by the ECC Decryption Logic to correct single bit failures on the fly.

Flash cells with maximum 1 bit failure over lifetime
Safety features on RAM

RAM
(Variable Memory)
RAM write protection

- A write protection shield can be used to protect a part of the RAM
- Size could be controlled with GRAM1,2 bits
  - 0 bytes
  - 128 byte
  - 256 byte
  - 512 byte
- Can be used for
  - Function pointers
  - Code in RAM
RAM parity check

- Adds 1 parity bit to each 8 bit data
- Able to generate a reset or just a flag in case of parity error

During RAM Write the parity is calculated and stored as an additional bit.

During RAM read the parity is checked and in case of an error a reset will be generated.

Reset
Safety features on SFR

SFR
(Variable Memory)
SFR write protection

- A SFR write protection can be used to secure sensitive hardware configurations

- Following three guard bits are available
  - GPORT (Port control registers)
    - Guard PMxx, PUxx, PIMxx, POMxx, PMCxx, ADPC and PIOR registers
  - GINT (Interrupt control registers)
    - Guard IFxx, MKxx, PRxx, EGPx and EGNx registers
  - GCSC (chip state control registers)
    - Guard CMC, CSC, OSTS, CKC, PERx, OSMC, LVIM, LVIS and RPECTL registers

- After reset all guards are inactive
Safety features on ADC
AD converter Diagnostics

- Test of the sample and hold circuit by switching the internal references against Vdd and GND.
- Controlled by the ADTES register
Safety features on Clock
Window Watchdog Timer

- Function
  - Detection of an inadvertent program loop (runaway)
  - RESET generation

- Watchdog functionality is set by option byte
  - Watchdog timer interval interrupt
  - Enable/Disable Window Watchdog Timer operation
  - Select overflow time
  - Select window size
  - Window Watchdog timer operation in HALT/STOP mode

- Watchdog Timer Enable Register (WDTE)
  - Writing ACH to WDTE clears the watchdog timer and starts counting again
Window Watchdog Timer

Block Diagram

- WDTINT of option byte (000C0H)
- INTERVAL of option byte (000C0H)
- WINDOW0 and WINDOW1 of option byte (000C0H)
- WDTON of option byte (000C0H)

[Diagram showing the block diagram of the Window Watchdog Timer with various components and their connections, including an interval time controller, a 17-bit counter, a selector, a window size check, and a watchdog timer enable register (WDTE).]
The watchdog timer triggers a hard reset,

- if the watchdog timer counter overflows
- if, the magic word is written into WDTE register when window is closed
- if a wrong value is written into WDTE
- if the WDTE register is accessed by a 1-bit manipulation instruction

*: example shown for 50% window opening
Internal main system clock can be checked based on an ext. or internal reference signal

- Reference signals
  - 32kHz \( f_{\text{SUB}} \) signal
  - 15kHz int. low speed osc.
  - T105 timer input

- The reference signal will be captured based on the main system clock

Count clock from main osc (\( f_{\text{mck}} \))

\[
\text{fil} \quad n \times f_{\text{mck}} \quad \text{TIS0}
\]
Safety functions for CPU

(CPU
(PIC / Interrupt)
Trap function

- TRAP function
  - Supervise the executed instruction code
  - Generate Reset if invalid instruction (0xFF) is fetched as 1st opcode

<table>
<thead>
<tr>
<th>opcode</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap (RESET)</td>
<td>FF</td>
<td>xx</td>
<td>xx</td>
<td>xx</td>
<td>xx</td>
</tr>
</tbody>
</table>

- "FF" is erased state of flash memory. If program-counter jumps to erased area, CPU execute trap instruction at soon.
Invalid Memory access

- Invalid memory access (IAWEN register)
  - Supervise the valid address range
  - Generate Reset in case fetch, read or write is outside the valid area.
  - Covers complete addressable range

<table>
<thead>
<tr>
<th></th>
<th>Fetch</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Flash</td>
<td>Normal</td>
<td>Normal</td>
<td><strong>Illegal access</strong></td>
</tr>
<tr>
<td>Data Flash</td>
<td><strong>Illegal access</strong></td>
<td>Normal</td>
<td><strong>Illegal access</strong></td>
</tr>
<tr>
<td>RAM</td>
<td>Normal</td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>General Register</td>
<td><strong>Illegal access</strong></td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>SFR</td>
<td><strong>Illegal access</strong></td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>2nd SFR</td>
<td><strong>Illegal access</strong></td>
<td>Normal</td>
<td>Normal</td>
</tr>
<tr>
<td>Mirror Area</td>
<td><strong>Illegal access</strong></td>
<td>Normal</td>
<td><strong>Illegal access</strong></td>
</tr>
<tr>
<td>Other Area</td>
<td><strong>Illegal access</strong></td>
<td><strong>Illegal access</strong></td>
<td><strong>Illegal access</strong></td>
</tr>
</tbody>
</table>
Reset functionality
Reset

- The RESF register allows to detect the Reset-source

- Block Diagram

Caution: An LVI circuit internal reset does not reset the LVI circuit.
Option byte
Option Byte

- Option byte is used to set different system settings
- Option byte area is located from 000C0H to 000C3H (010C0H to 010C3H in boot cluster 1, only necessary if boot swap is used)
  - 000C0H/010C0H:
    - Enable/Disable watchdog timer operation
    - Enable/Disable watchdog timer operation in HALT/STOP mode
    - Interval time setting
    - Select window time
    - Use of watchdog timer interval interrupt
  - 000C1H/010C1H:
    - LVI voltage setting
    - Enable LVI operation for power-up
  - 000C2H/010C2H:
    - Flash operation mode
    - Oscillator speed selection
  - 000C3H:
    - Enable/Disable on-chip debug function
    - Flash memory handling in case of failure in on-chip debug security ID authentication
## Option Byte

### User option area 000C0H/010C0H

<table>
<thead>
<tr>
<th>WDTINIT</th>
<th>WINDOW1</th>
<th>WINDOW0</th>
<th>WDTON</th>
<th>WDCS2</th>
<th>WDCS1</th>
<th>WDCS0</th>
<th>WDTSTBYON</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| WDTINIT | Use of interval interrupt of watchdog timer  
0 | Interval interrupt is not used.  
1 | Interval interrupt is generated when 75% of the overflow time is reached. |

| WINDOW1 | WINDOW0 | Watchdog timer window open period*2  
0 | Setting prohibited  
0 | 50%  
1 | 75%  
1 | 100% |

| WDTON | Operation control of watchdog timer counter  
0 | Counter operation disabled (counting stopped after reset)  
1 | Counter operation enabled (counting started after reset) |

| WDCS2 | WDCS1 | WDCS0 | Watchdog timer overflow time (f₀ = 17.25 kHz (MAX.))  
0 | 0 | 0 | 2⁻⁴f₀ (3.71 ms)  
0 | 0 | 1 | 2⁻⁴f₀ (7.42 ms)  
0 | 1 | 0 | 2⁻³f₀ (14.84 ms)  
0 | 1 | 1 | 2⁻²f₀ (29.68 ms)  
1 | 0 | 0 | 2⁻¹f₀ (116.72 ms)  
1 | 0 | 1 | 2⁰f₀ (474.90 ms)  
1 | 1 | 0 | 2¹f₀ (949.80 ms)  
1 | 1 | 1 | 2²f₀ (3799.19 ms) |

| WDTSTBYON | Operation control of watchdog timer counter (HALT/STOP mode)  
0 | Counter operation stopped in HALT/STOP mode*2  
1 | Counter operation enabled in HALT/STOP mode |

- WDT interval interrupt setting
- WDT window open period setting
- WDT operation setting
- WDT overflow time setting
- WDT operation setting in HALT/STOP mode
Option Byte - User option area 000C1H/010C1H

LVD voltage setting

<table>
<thead>
<tr>
<th>Detection voltage of the falling edge</th>
<th>VPOC2</th>
<th>VPOC1</th>
<th>VPOC0</th>
<th>LVIS1</th>
<th>LVIS0</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.63V</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>...</td>
<td>0</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>...</td>
<td>0</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>4.06V</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.53V (LVD is OFF)</td>
<td>1</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

LVD mode setting

<table>
<thead>
<tr>
<th>mode</th>
<th>LVIMDS1</th>
<th>LVIMDS0</th>
</tr>
</thead>
<tbody>
<tr>
<td>interrupt mode</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>interrupt &amp; reset mode</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>reset mode</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Option Byte - User option area 000C2H/010C2H

Table of Flash operation mode settings:

<table>
<thead>
<tr>
<th>CMODE1</th>
<th>CMODE0</th>
<th>Setting of flash operation mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>LV (low voltage main) mode</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>LS (low speed main) mode</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>HS (high speed main) mode</td>
</tr>
<tr>
<td>Other than above</td>
<td>Setting prohibited</td>
<td></td>
</tr>
</tbody>
</table>

Table of Frequency setting:

<table>
<thead>
<tr>
<th>FRQSEL3</th>
<th>FRQSEL2</th>
<th>FRQSEL1</th>
<th>FRQSEL0</th>
<th>Frequency of the internal high-speed oscillator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32 MHz</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>24 MHz</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>16 MHz</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>12 MHz</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>8 MHz</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>4 MHz</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1 MHz</td>
</tr>
<tr>
<td>Other than above</td>
<td>Setting prohibited</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Option Byte

- User option byte area 000C3H/010C3H

<table>
<thead>
<tr>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCDENSET</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>OCDERSD</td>
</tr>
</tbody>
</table>

- On-chip debug operation setting
- Erasure operation setting

<table>
<thead>
<tr>
<th>OCDENSET</th>
<th>OCDERSD</th>
<th>Control of on-chip debug operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>Disables on-chip debug operation.</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>Setting prohibited</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>Enables on-chip debugging.  Erases data of flash memory in case of failures in authenticating on-chip debug security ID.</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>Enables on-chip debugging.  Does not erase data of flash memory in case of failures in authenticating on-chip debug security ID.</td>
</tr>
</tbody>
</table>
Summary

■ RL78 Safety Features
  ● Flash
  ● RAM
  ● SFR
  ● ADC
  ● Clock
  ● CPU

■ For more information, visit:

www.renesas.com