

## MAKE THE DIGITAL HOME A SAFER PLACE

**Integrating an off-the-shelf software safety solution can cut IEC610730 certification time and costs.**

Many things in life can present a risk to our well-being, from recreational activities to accidents in the workplace. However, the majority of accidents still occur in the home.

Our increasing reliance on domestic, labour-saving appliances, coupled with a commensurate need for their efficient operation, has created a scenario where safety at home is coming under threat.

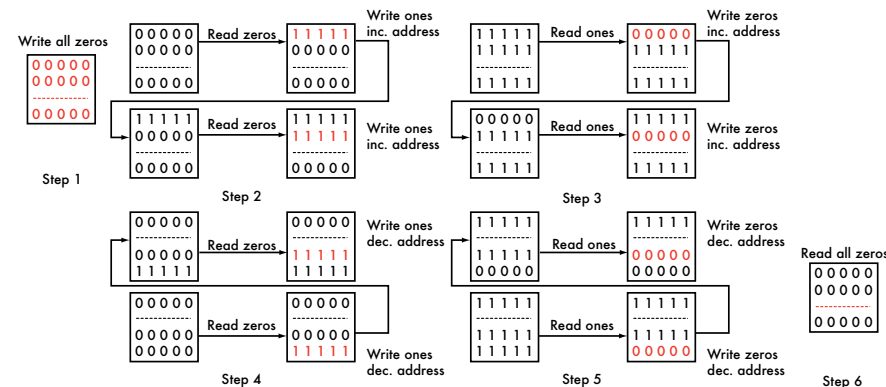
There's a bewildering number of microcontrollers (MCUs) deployed in white goods across the developed world. In Europe alone, some 90million MCUs are used in white goods every year. It's worth bearing in mind that these MCUs are often controlling devices that have large and heavy moving parts, or display the ability to

distribute kilowatts of power all around the home.

It is common nowadays for appliances to employ multiple MCUs. One controls functionality and another drives aesthetically pleasing user interfaces.

Through sophisticated algorithms, it's possible to apply real-time variability to power delivery, which when coupled with carefully monitored closed-loop feedback circuits, enable electric-motor control with much greater precision and efficiency. This reduces the power consumed and noise generated. The result is that the most widely deployed white goods now consume much less energy than those that, in the past, were controlled by simpler electromechanical switches.

An impact of this trend, however, is the increased potential for a fault in the closed-loop feedback to escalate to an open-loop catastrophe. It's a worst-case scenario that the European Union has foreseen and, through legislation, is determined to avoid.



As with so many other aspects of commerce throughout the EU, the use of MCUs—and associated embedded software—within white goods is now controlled through an International Standard as issued by the International Electrotechnical Commission (IEC). The Standard, IEC60730-1, passed into European law in October 2007, meaning all equipment coming under its remit must comply as of that date.

It extends beyond just washing machines, of course. It's intended to govern the operation of various electrical devices typically found in the home, including those that use solid or gaseous fuels, such as boilers. Perhaps because of the breadth of its application, the standard classifies these devices

**1. The RAM test uses the industry-recognised March C and March X algorithms.**

in terms of their potential to cause damage. It applies categories Class A, B, or C, depending on the device.

For instance, a washing machine would typically fall within Class B, which is defined as having control functions intended to prevent the unsafe operation of the equipment. In terms of a washing machine, this would include stopping the rotation of the drum if, for example, the door were inadvertently opened. Class C includes domestic boilers, where there's a higher inherent risk associated with the fuel used. In this case, an additional MCU is often required.

enlarge

cover

editorial

news

power design

technology

hot topics

design ideas

applications

pease porridge

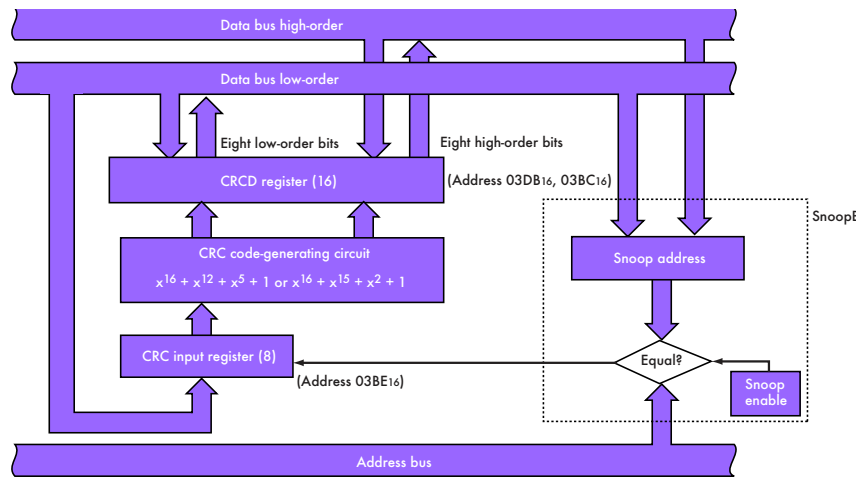
save

print

e-mail to a friend

close

enlarge



**2. A dedicated CRC calculation circuit can generate a CRC value for one byte of data in two machine cycles.**

If the “open door” scenario existed within a machine controlled solely by electromechanical operation, it would be exposed to a host of solutions. The most likely of those could be the use of a switch on the door to remove power to the electric motor, if it’s operated during an active period of the cycle.

The potential problem with this configuration is the multiple points of failure in the “reporting structure.” For instance, the door switch may fail to operate, while the connection between the door switch

and the electromechanical control mechanism has no inherent way of verifying its correct functionality in operation. Adding a hardware-based safety solution here would become cost-prohibitive when compared with a solution that’s implemented in software.

With control now passing to an MCU, the same solution might appear to be applicable. However, while the decision process is still based on a series of events, they all rely on the MCU executing its control sequence correctly. Through its embedded control sequence, the

MCU effectively becomes a single point of failure, which is much easier to monitor and cheaper to implement than a series of passive electrical switches.

Extending this image, the MCU also becomes perfectly placed to periodically check all features affecting the safe operation of the equipment. Such a benefit isn’t present in the traditional electromechanical solution.

While the implementation of IEC60730-1 may appear to be onerous on manufacturers, it can actually provide them with an opportunity to differentiate their products. This is the case with inferior products coming in to Europe, which can’t demonstrate compliance, as well as with competitor’s products that rely more heavily on a hardware solution in order to comply with the standard.

While equally compliant, a hardware-centric route may incur a higher bill of materials, a cost that may need to be passed on to the customer. For this reason, a solution that maximises the use of software to achieve compliance is proving to be a much more attractive option to the industry’s leading white-goods manufacturers.

In turn, these manufacturers are now turning toward leading MCU manufacturers to provide cost-effective measures to IEC60730-1 compliance that can be implemented predominantly in software alone.

**IMPLEMENTING THE TEST ROUTINES**

In order for its customers to achieve the level of demonstrable safety required to comply with Annex H of the standard, which deals with control systems using software, Renesas’ Engineering Division developed a series of low-level software routines. These routines can be implemented alongside existing software, enabling manufacturers to save on the bill of materials and accelerate the certification process.

Such low-level routines are applicable for all white goods affected by the IEC60730-1 Standard, including equipment classified as Class C (control functions that are intended to prevent special hazards), as well as those implicated in the UL1998 safety standard coming out of North America.

This process of “software checking software” may seem like a paradox. However, through a combi-

cover

editorial

news

power  
design

technology

hot  
topics

design  
ideas

applications

pease  
porridge

save

print

e-mail  
to a friend

close

## applications • digital home safety

nation of enhanced peripherals—in particular a more robust watchdog timer (WDT), as integrated in all Renesas MCUs—and the routines developed by Renesas engineers, the essential elements of the standard are covered.

Because the safe operation of the equipment now relies so heavily on the correct execution of the MCU's algorithm, the WDT plays an important role here. For Class B equipment, there are specific requirements made of the WDT: use of a separate time-based oscillator; the inability to disable the WDT register through software; the generation of a real hardware-based reset (and not a maskable interrupt), and the provision of a "safe" I/O state following initialisation and/or a hardware reset.

For Class C equipment, the standard calls for the mandatory use of an external WDT chip, as well as a second MCU to provide both hardware and software redundancy and the ability for one to check the other's operation.

Beyond the WDT requirements, the MCU must go through specific tests following startup and during normal operation to ensure correct operation is maintained. These

include ALU and CPU tests, RAM tests, ROM/flash tests, clock tests, and peripheral tests.

Renesas now provides low-level routines to achieve all of these tests for its R8C, H8, M16C, and SH families of MCUs, designed to provide the necessary test coverage for compliance. These routines are made available as source code and can be quickly integrated into existing software, as the routines' syntax has been fully checked against the Motor Industry Software Reliability Association (MISRA) coding standard. Once integrated, they can be called as, and when deemed, necessary during operation.

A typical example would be the RAM test, which uses the industry-recognised March C and March X algorithms. (Fig. 1). The March C test is used at startup, while the March X test may be executed at any time to detect RAM failures.

This may include testing for "stuck-at" faults (the logical value of a cell is always "1" or "0"), "transition" faults (a cell or line fail to change logical state), "coupling" faults (a logical transition in one cell affects the logical state of a neighbouring cell), and "address

decode" faults (any fault occurring in the address decoder).

The test itself is destructive, but the test function provides for the preservation of the data. This is achieved by copying the data to a buffer store before executing the test.

ROM/flash tests employ cyclic redundancy checking (CRC), which recognises all one-bit errors and a high percentage of multi-bit errors. The CRC values used as checksums can be calculated in software using either a lookup table or bit shifting. The former requires more code space than the latter, but requires fewer CPU cycles. However, for example, the Renesas M16C MCU has a dedicated CRC calculation circuit that can generate a CRC value for one byte of data in two machine cycles (Fig. 2).

The code for performing CPU tests needs to access specific registers, such as the general-purpose, flag/status, program-counter, and other specific registers. For this reason it is implemented in assembler code, written for each of the Renesas MCU architectures. However, they have been written to comply with any other C function call as specified in the Renesas tool-chain manual.

Therefore, they can be treated as any normal C function without the need for additional register preservation steps.

For some MCU manufacturers, including this functionality could add as much as 20kB of software and even require an upgraded MCU, which in turn drives demand for 16/32bit MCUs.

Renesas MCUs targeting this class of application already integrate the necessary hardware features. As a result, its low-level software routines can provide the majority of safety features necessary, without upgrading the MCU. In addition, the documentation provided can be used by manufacturers to speed up the certification process. It's already been certified in cold, wet, and hot appliances as certified by the likes of VDE, IMQ, BSI, LCIE, and LCOE.

In future MCUs targeting this class of application, Renesas intends to integrate even more hardware features. These features will add to the already extensive list of safety-centric peripherals. ■

**NEXT:** What's all this power LED stuff anyhow?

cover

editorial

news

power design

technology

hot topics

design ideas

applications

pease porridge

save

print

e-mail to a friend

close