The Benefits of Global Security Peripherals in STM32-based Applications

Author:
David Bellegarde, Engineer, STMicroelectronics

Synopsis:
The Cortex™-M3 based STM32 from STMicroelectronics includes a set of peripherals, which make applications more secure and significantly extend the chip capabilities. These include anti-tamper and flash protection features alongside advanced security features such as clock detection, lockable IOs, backup registers, dual watchdogs, power voltage supervisor, exception handling, and write once registers.
In this article, we will illustrate for the first time how a Cortex-M3 based MCU with these enhanced peripherals can manage secure applications which are outside of the capabilities of a standard microcontroller.

Nowadays, security and safety are crucial challenges in a wide array of applications and many developers spend a significant amount of time enhancing systems to take into account these issues.

Global security is the condition of being protected (data security) and safe. For an electronic application and furthermore for an embedded system, this consists of managing a) failures (availability), b) incoherencies (integrity) and c) intrusion (confidentiality).

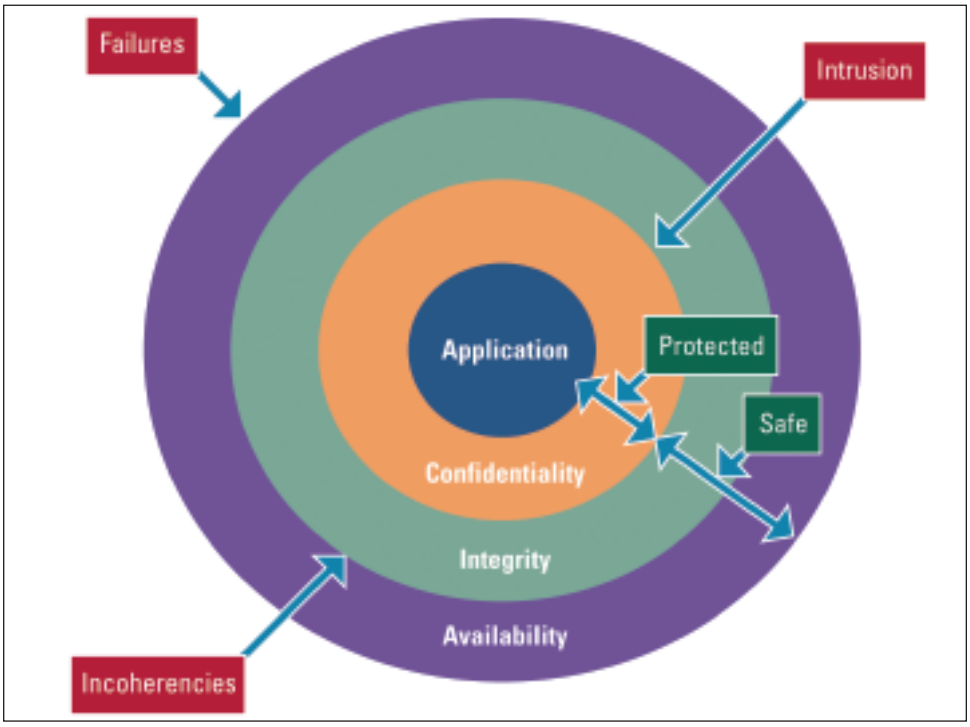


Figure 1: Global security for an electronic application

a) Maintaining Availability (part of safety features)

Maintaining the availability of a system requires protection against any failure, which could happen in hostile environment. For instance, the power supply, the temperature or external clock could fluctuate consequently. A graduated degradation could make a system more fault tolerant against the external world.

b) Maintain Integrity (part of safety features)

Maintenance of integrity requires management of the incoherencies, which could happen if software overflow occurs. For instance, when the CPU load becomes too high the integrity of the software could be reduced.

c) Maintain Confidentiality (data security features)

Data confidentiality requires robust protection against piracy at a program and/or data level. For instance, when the application is complete, the designer should ensure data is completely eradicated to protect the user and maintain a high level of confidentiality.

In an embedded system, the microcontroller is critical in ensuring a high level of global security. It must thus meet these three criteria of availability, integrity and

WE'RE WITHIN

THE THINGS YOU CAN'T DO WITHOUT.

Deep within, in fact. Because we provide the software that enables designers to create the electronics inside your PDA and mobile phone. And laptop. And MP3 player. And just about every other gizmo that's an indispensable part of your life today. For more information, visit **www.cadence.com/within.**

CDNS
NASDAQ-100
LISTED

cadence™

confidentiality. This is not simple to achieve and requires some smart peripherals and microcontroller design. The STM32 microcontroller by STM, introduced in June 2007, is one of the most advanced MCU in this field, and has a number of integrated security features.

To maintain the availability, the following features are used:
- Programmable voltage detector (part of power voltage supervisor)
- Clock security system
- Emergency stop state (to ensure the failure does not spread)

To maintain the integrity, the following features are used:
- Power-on reset and power down reset (part of power voltage supervisor)
- Write once registers
- Lockable IOs
- Exception fault handling
- Dual watchdog

To maintain the confidentiality the following features are used:
- Flash memory protections (write and read)
- Backup registers and anti-tamper feature

So, let's investigate some of these features in more depth:

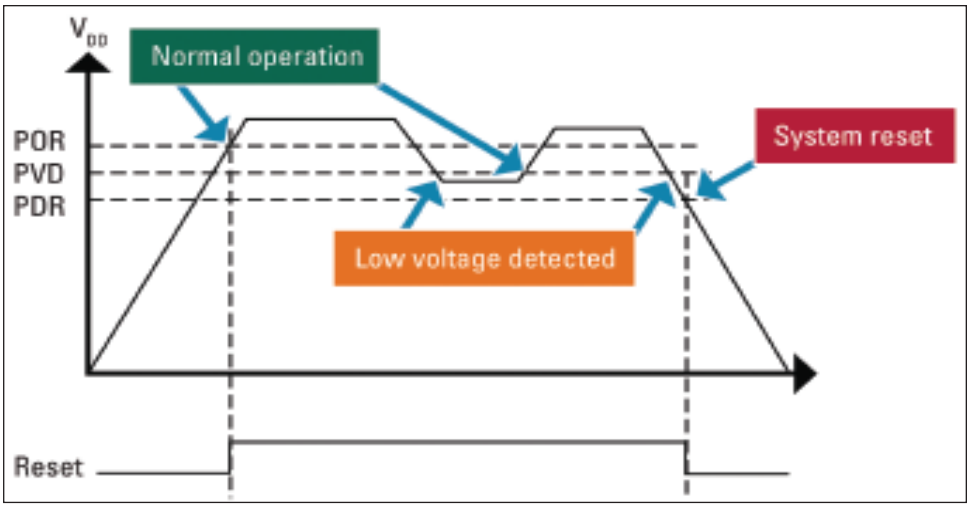
Power Voltage Supervisor

Inside the circuit, there is a voltage supervisor which can be separated into 3 elements:
- POR (power-on reset) which maintains the component under reset until the nominal voltage is reached.
- PVD (programmable voltage detector) which generates an interruption if a predetermined voltage (between 2.2V and 2.9V, settable by software) is reached. In this case, it is up to the firmware to introduce a safe shutdown before an eventual reset.
- PDR (power down reset) which generates a system reset if the voltage drops down to 2V.

This power system ensures a fault-tolerant property and furthermore introduces a phase in which the system will be kept in a safe mode before a complete reset. Additionally, this reset occurs before a complete system failure can occur.

Clock security system

The clock security system is based on the detection of a clock failure. The system generates an interrupt if the main external clock is disconnected or broken. If this occurs, the microcontroller is automatically clocked with an internal safe clock so the system can perform shutdown or reset operation by executing an NMI (non-maskable interrupt).



Note: this diagram does not introduce reset temporization and voltage hysteresis

Figure 2: Power voltage supervisor overview

Emergency Stop

The advanced control timer of the STM32F10x provides an emergency stop mode, which allows the safe mode of signals generated by this timer (level configured by user). This is called the break function, and this can be triggered either on a clock failure or a break input pin (BKIN) event.

For example, the PWM of the timer is designed to perform a set of motor control tasks, where if the failure happens it is useful to maintain the motor in a safe state in order to avoid damage.

Write Once Registers

The same timer outlined above could be used to perform motor control task. When it is running, the inopportune modification of this parameter can destroy the power stage and then seriously damage the motor. To prevent this, the configuration of these outputs as well as the configuration registers can be locked with changes only permissible following a system reset.

Lockable IOs

In a similar way, there is a mechanism which can lock the I/O ports and also freeze their configurations. When a lock sequence is applied on a bit port, it is not possible to change its configuration until the next reset. (see next page)

This prevents the on-the-fly modification of the IOs and therefore the input can not become the output ensuring a short circuit can not happen accidentally.

Exception Fault Handling

The Cortex-M3 processor supports several exception fault handlers that allow detection of faults that result from an error conditions in instruction execution. These kinds of exceptions are grouped in 3 types:
- Memory management fault, generated when a branch to memory area where there is no executable code,
- Bus fault, generated when the program tries to store data where there is no memory,
- Usage fault, generated when an undefined instruction is executed.

In these exceptions, a software procedure can be implemented to perform safe halt and/or reset.

This means, the CPU will be always able to detect wrong behaviors of the firmware and so to get back to a known state.

Dual watchdog

If despite all the above protection, the software becomes deadlocked (for example due to bad code), the ultimate backup protection is the watchdog timers.

The STM32F10x has 2 embedded watchdogs, one which can be independent and another one which can windowed. This

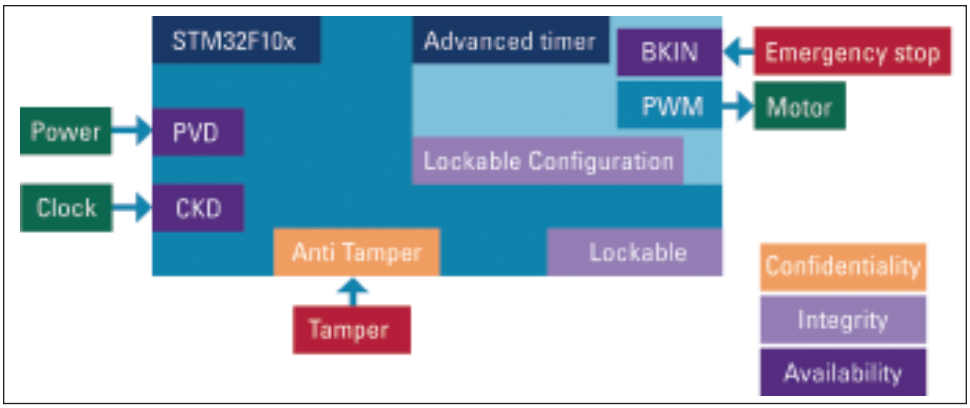


Figure 3: Advanced timer security features and others

provides the final application a high level of safety, accuracy and flexibility. Both watchdogs can be used to detect and solve firmware malfunctions by either generating an interrupt or a system reset (when their timer reaches a value which corresponds to a limit time value) without being refreshed.

- Independent watchdog: this watchdog is suitable for applications which need a watchdog which is completely independent from the program execution because it can be automatically set. Furthermore, in case of clock failure, this watchdog will be clocked by an independent clock and this offers the application a second level of clock protection

- Window watchdog: this watchdog is suitable to an application which needs a watchdog which can be reloaded inside an accurate time window. It can be set by software and configured to generate an interruption if the refresh didn't occur in a settable window. This means the system has to provide a quick response.

Flash memory protections (write and read)

The Flash memory can be protected against a program which attempts to read it. The pages of this memory can also be protected against unauthorized write. Once activated, these features can be deactivated by a program executed in RAM. The Flash memory will be erased after this operation.

This ensures an entrusted program can not access the confidential firmware loaded in the Flash memory.

Backup Registers and Anti-tamper Feature

The STM32 F10x provides 10 16-bit registers which can be used to store key data. This data will be saved in the registers via the optional backup battery, but it will be erased automatically if a tamper is detected via the anti-tamper pin.

For instance, the application could be put in a sealed box and when opened, the tamper feature will be switched on and crucial data erased.

All these features can be experienced with the STM32 evaluation board.

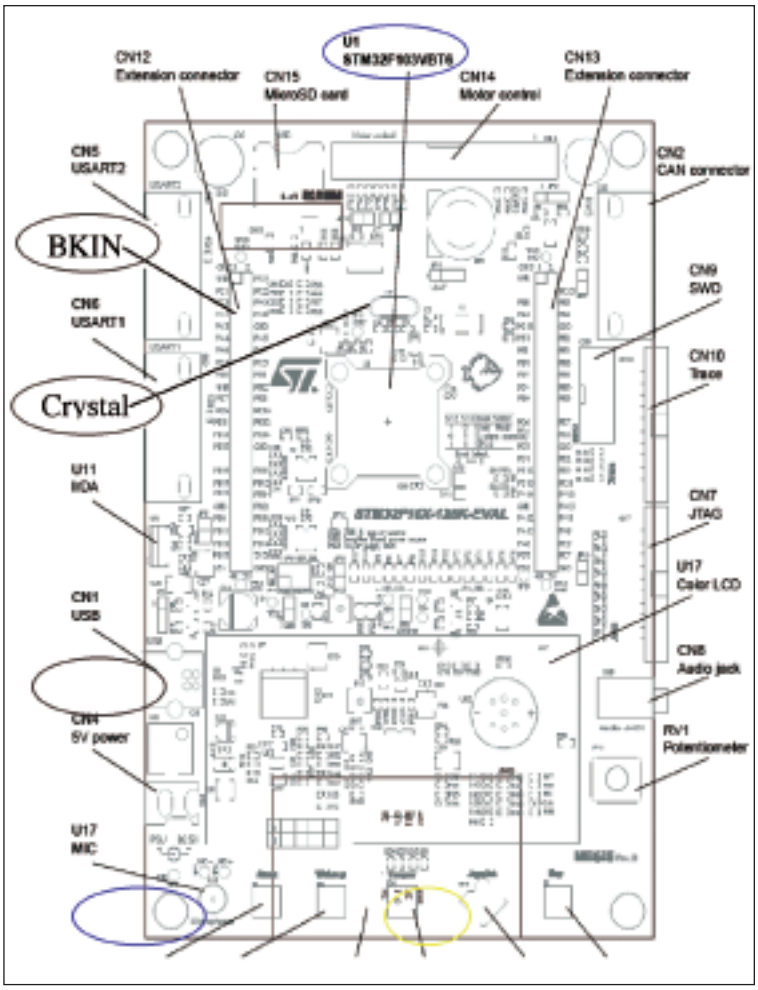


Figure 4: Board features used

The Firmware library provided by STMicroelectronics implements all of these features. The interrupts relating to the appropriate features such the exception faults, anti-tamper, window watchdog, clock detection and programmable power detection can be used.

Board description

- STM32F103: used microcontroller
- BKIN: pin to test the emergency stop
- Crystal: this can be easily removed to test the clock detection
- Power supply: variable to test the power voltage detector
- Reset button: to restart the application
- Tamper button: to simulate the anti-tamper feature

The STM32F10x and the global security features illustrate how an electronic application can be protected by implementing distinct peripherals. Furthermore, it can be said a standard microcontroller with more and more peripherals inside and fast execution enables us to see that future embedded system in a wide array of applications including home automation, cybernetic and transportation will be able to provide both high performance and security.