Globale Sicherheit

Peripheriefunktionen in den STM32-Mikrocontrollern

Die auf dem Cortex-M3-Core beruhenden Mikrocontroller STM32F10x von STMicroelectronics und ihre globalen Sicherheits-Features zeigen auf, wie sich eine elektronische Applikation mit Hilfe spezifischer Peripheriefunktionen besser denn je absichern lässt.

Die Sicherheit hat heutzutage in vielen Applikationen einen äußerst hohen Stellenwert. Für viele Entwickler ist dies der Anlass, viel Zeit in die Absicherung ihrer Anwendungen zu investieren. Damit einer Applikation ‚globale Sicherheit' bescheinigt werden kann, müssen sowohl die Daten als auch die Anwendung selbst sicher sein. Für eine elektronische Applikation und insbesondere für ein Embedded-System resultiert dies in der Forderung, Störungen, Unstimmigkeiten und Eindringversuche in den Griff zu bekommen, damit die Verfügbarkeit, Integrität und Vertraulichkeit gewährleistet ist (**Bild 1**):

- Wahrung der Verfügbarkeit. Hierzu gehört der Schutz vor Ausfällen, die durch ungünstige Umgebungsbedingungen verursacht werden, also z. B. durch Schwankungen der Versorgungsspannung, der Temperatur oder der externen Taktfrequenz. Eine geordnete Verschlechterung der Werte kann einem System zu mehr Toleranz gegenüber Einflüssen der Außenwelt verhelfen.
- Wahrung der Integrität. Hierbei geht es um das Management von Unstimmigkeiten, die bei einem Durchgehen der Software auftreten können. Unter anderem kann eine zu hohe CPU-Auslastung die Integrität der Software beeinträchtigen.
- Wahrung der Vertraulichkeit. In diese Sparte fällt der Schutz vor Piraterie sowohl auf der Programm als auch auf der Daten-Ebene. So kann z. B. der Designer die Software so absichern, dass die Vertraulichkeit der Resultate gewahrt bleibt, nachdem die Applikation abgearbeitet ist.

AUTOR

David Bellegarde ist Mitarbeiter von STMicroeletronics

In einem Embedded-System kommt dem Mikrocontroller, der immerhin so etwas wie das Gehirn des Systems darstellt, entscheidende Bedeutung für die Wahrung der globalen Sicherheit zu. Der Mikrocontroller

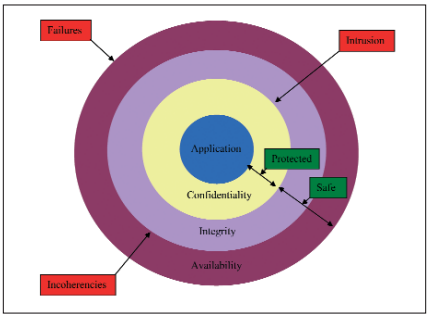

Bild 1: Globale Sicherheit für eine elektronisches Applikation.

muss deshalb die Forderungen nach Verfügbarkeit, Integrität und Vertraulichkeit erfüllen, was allerdings nicht einfach ist und neben intelligenter Peripherie auch ein durchdachtes Mikrocontroller-Design erfordert. Der Mikrocontroller STM32 von STMicroelectronics gehört in dieser Hinsicht zu den fortschrittlichsten Produkten. Im Folgenden werden die globalen Sicherheits-Features des STM32F10x näher beleuchtet. Der Wahrung der Verfügbarkeit dienen die folgenden Features: Programmierbarer Spannungswächter (Bestandteil des Power Voltage Supervisors), Taktsicherheits-System und Notabschaltung (um ein Ausbreiten der Störung zu verhindern).
Zur Wahrung der Integrität werden herangezogen: Power-On-Reset und Power-Down-Reset (Bestandteil des Power Voltage Supervisors), Write-Once-Register,

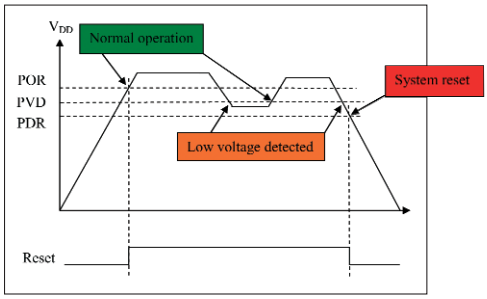

Bild 2: Funktionsweise des Power Voltage Supervisors. Reset-Zeitablauf und Spannungshysterese sind in diesem Diagramm nicht berücksichtigt.

verriegelbare I/Os, Exception-Behandlung und zwei Watchdogs.
Zur Aufrechterhaltung der Vertraulichkeit kommen zum Einsatz: Schreib-/Leseschutz für den Flash-Speicher sowie Backup-Register und Manipulationsschutz.

Power Voltage Supervisor

Bestandteil der Schaltung ist ein Spannungswächter, der sich in drei Abschnitte gliedert: Der Funktionsabschnitt Power-On-Reset (POR) hält beim Einschalten den Reset-Status des Bausteins so lange aufrecht, bis die nominelle Versorgungsspannung erreicht ist. Die Funktion Programmable Voltage Detector (PVD) generiert einen Interrupt, sobald die Spannung auf einen zwischen 2,2 und 2,9 V programmierbaren Grenzwert absinkt. Der Firmware obliegt es daraufhin, ein geordnetes Herunterfahren zu veranlassen, bevor es zu einem Reset kommt. Die dritte Funktion, Power-Down-Reset (PDR), löst ein System-Reset aus, wenn die Versorgungsspannung auf 2 V absinkt (**Bild 2**) Die solcherart erzielte Absicherung der Stromversorgung sorgt für Ausfalltoleranz und bewirkt außerdem, dass das System für eine bestimmte Phase in einen sicheren Betriebszustand wechselt, bevor es zu einem völligen Reset kommt. Dieses Reset wiederum erfolgt bevor das System vollständig ausfällt.

Taktsicherheits-System

Dieses Feature beruht auf der Erkennung eines Taktausfalls. Das System löst einen Interrupt aus, sobald der externe Haupt-Quarz nicht mehr angeschlossen ist oder defekt wird. Der Mikrocontroller wird daraufhin automatisch mit einem intern erzeugten sicheren Takt angesteuert. Das System kann sich dann selbst herunterfahren

oder ein Reset auslösen (durch Ausführung eines nicht maskierbaren Interrupts – NMI).

Notabschaltung, Write-Once-Register und verriegelbare I/Os

Der Control-Timer des STM32F10x bietet einen Notabschalt-Modus, in dem die Signale dieses Timers auf sichere, vom Anwender vorgegebene Werte gesetzt werden. Diese Break-Funktion wird entweder bei einem Taktausfall oder durch Setzen des Break-Input-Pins (BKIN) aktiviert. Da sich die PWM-Funktion des Timers zur Ansteuerung von Motoren eignet, ist es sinnvoll, bei einem Ausfall für einen sicheren Betriebszustand der Motoren zu sorgen, damit eine Beschädigung vermieden wird.

Wird der beschriebene Timer zur Ansteuerung eines Motors verwendet, kann eine unzulässige Modifikation von Parametern bei laufendem Motor zu einer Zerstörung der Leistungsstufe und in der Folge zu einer ernsten Beschädigung des Motors führen. Aus diesem Grund lässt sich die Konfiguration der Ausgänge schützen, indem die Konfigurationsregister verriegelt werden. Eine solche Konfigurations-Verriegelung lässt sich nur durch ein Reset wieder aufheben. Ziel dieser Maßnahme ist es, das Setzen fehlerhafter Werte durch außer Kontrolle geratene Software zu verhindern.

Einen ähnlichen Mechanismus hat eine Funktion, die das Verriegeln von I/O-Ports und ihrer Konfigurationen ermöglicht. Wird ein Bit-Port mittels einer ‚Lock'-Sequenz verriegelt, kann die Konfiguration erst nach einem Reset wieder verändert werden (**Bild 3**). Dies unterbindet ein ungewolltes Modifizieren der I/O-Konfiguration. Ein Eingang kann folglich nicht in einen Ausgang verwandelt werden, sodass das unabsichtliche Herbeiführen eines Kurzschlusses verhindert wird.

Exception-Behandlung

Der Cortex-M3-Core unterstützt mehrere Arten von Exception-Behandlungen, mit denen sich feststellen lässt, wann der Mikrocontroller ein fehlerhaftes Verhalten an den Tag legt. Eine Störung ist eine Exception, die aus einem fehlerhaften Zustand infolge einer Befehlsausführung resultiert. Exceptions dieser Art gliedern sich in drei Gruppen:

- Speichermanagement-Fehler entstehen durch einen Sprung in einen Speicherbereich, in dem sich kein ausführbarer Code befindet.
- Busfehler werden ausgelöst, wenn das Programm das Abspeichern von Daten in einem Bereich versucht, in dem sich kein Speicher befindet.
- Nutzungsfehler werden generiert, wenn ein nicht definierter Befehl ausgeführt wird.

Bei diesen Exceptions kann eine Softwareprozedur für ein sicheres Anhalten und/oder einen Reset sorgen. Die CPU kann deshalb ein fehlerhaftes Verhalten stets erkennen und in einen definierten Zustand zurückkehren.

Zwei Watchdogs

Sollte sich die Software trotz aller eben genannten Schutzmaßnahmen aus irgendwelchen Gründen (z. B. durch fehlerhaften Code) aufhängen, sind Watchdog-Timer die ultimative Rettung. In den STM32F10x sind zwei Watchdogs integriert, von denen einer unabhängig arbeiten und der andere im Windowed-Modus operieren kann. Die endgültige Applikation gewinnt hierdurch ein hohes Maß an Sicherheit, Genauigkeit und Flexibilität. Beide Watchdogs können zur Aufdeckung und Behebung von Firmware-Fehlfunktionen verwendet werden, indem sie einen Interrupt oder einen System-Reset auslösen, sobald ihr Timer einen gewissen Grenzwert erreicht, wenn das bei ordnungsgemäßer Funktion der Software erfolgende periodische Zurücksetzen ausbleibt.

Der unabhängiger Watchdog ist für Anwendungen geeignet, die einen von der Programmverarbeitung vollkommen unabhängigen Watchdog-Timer benötigen, der automatisch gesetzt werden kann und bei einem Taktausfall von einem unabhängigen Takt angesteuert wird, um der Applikation eine zusätzliche Taktsicherheits-Ebene zu verleihen. Der Windowed Watchdog eignet sich für Applikationen, die einen Watchdog benötigen, der innerhalb einer präzise vorgegebenen Zeitfensters neu geladen werden kann. Er kann per Software gesetzt und so konfiguriert werden, dass er einen Interrupt auslöst, sofern er nicht innerhalb eines vorgegebenen Zeitfensters aufgefrischt wird. Das System muss somit schnell reagieren.

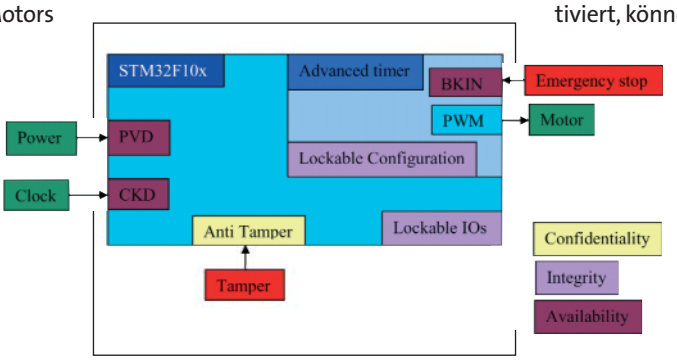

Bild 3: Timer-Sicherheits-Features und mehr.

Schreib-/Leseschutz für Flash-Speicher

Der Flash-Speicher lässt sich vor Programmen schützen, die ihn auszulesen versuchen. Darüber hinaus lassen sich die Seiten dieses Speichers vor unerwünschten Schreibzugriffen bewahren. Einmal aktiviert, können diese Features durch ein im RAM ausgeführtes Programm deaktiviert werden. Der Flash-Speicher wird nach dieser Operation gelöscht. So ist sichergestellt, dass ein vertrauenswürdiges Programm nicht auf die im Flash-Speicher enthaltene vertrauliche Firmware zugreifen kann.

Backup-Register und Manipulationsschutz

Im STM32F10x sind zehn 16-Bit-Register vorhanden, die zum Ablegen von Chiffrierschlüsseln verwendet werden können. Die Daten sind geschützt, da diese Register durch eine Stützbatterie gespeist werden (Verfügbarkeits-Feature). Allerdings werden sie automatisch gelöscht, sobald über den Anti-Tamper-Pin eine Manipulation signalisiert wird. Eine Applikation kann z.B. mit einem gesicherten Gehäuse versehen werden, bei dessen Öffnung die Anti-Tamper-Funktion aktiviert wird, um das Löschen kritischer Daten zu veranlassen. (jj)

infoDIRECT 510*ei*0208

www.elektronik-industrie.de
► Link zu **STMicroelectronics**