AN1432
APPLICATION NOTE

Write Protection and Code Storage on the M25Pxx Serial Flash Memory Family

Protection is one of the key features of a code storage memory. After all, the corruption of a single bit may cause an application to fail. Once programmed, the memory content must be secured against the stresses to which the system is exposed during its lifetime. These stresses include soldering, shipment, noisy environments, power-up and power-down.

In code storage based applications, the Flash memory is usually accessed on application start-up, and is inactive for the vast majority of the time. It is a highly attractive advantage, therefore, if the memory protection can be achieved using a mechanism that also leads to enormous reductions in power consumption while it is in operation. This is, indeed, the case with the M25Pxx family, as described later in this document.

In designing the new M25Pxx Serial Flash memory family, which is optimized for code storage, STMicroelectronics has thoroughly analysed these issues. The resulting design provides a comprehensive package of protection strategies, which are described here.

WRITE PROTECTION DURING POWER-UP/POWER-DOWN

The power-up/power-down phase is one of the most critical times for an application. Here the power supply is noisy and unstable, and, for much of the period, the voltage is below the minimum level for reliable operation of the components.

A Reset pin is provided by some memory suppliers to keep the memory in a Reset state during power-up. This relies on the Bus Master driving it appropriately. Unfortunately, though, the Bus Master is, itself, in an uncontrolled state at this time. We cannot, then, entrust memory protection during power-up and power-down to external components.

Where the Reset signal is managed by a Power Supervisor device, the Reset pin can be useful if the memory does not offer other protection features. Such protection is however redundant in the M25Pxx family from STMicroelectronics, where memory protection is enforced by the memory itself.

Dual Protection During Power-up

a) Reset State:

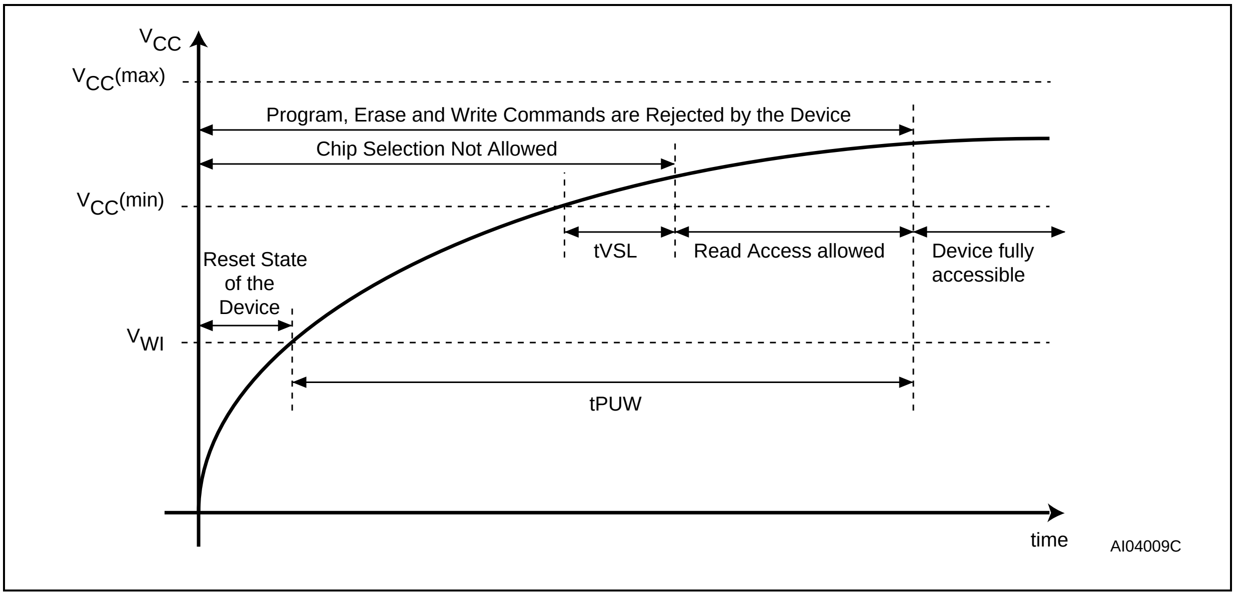
To avoid data corruption, an internal V_{CC} comparator inhibits all M25Pxx functions if the V_{CC} voltage is lower than the Write Inhibit threshold, V_{WI}. If so, the memory is remains in a Reset state.

The Write Inhibit feature is useful when the power supply is under the Power on Reset (POR) threshold. Another protection feature is however needed to protect the memory when the voltage supply is between V_{WI} and the minimum operating voltage. This is implemented using a delay, as described next.

b) Write protection during a delay (as specified in the datasheet) controlled by an internal timer:

Once the voltage passes above the V_{WI} threshold, Program, Erase and Write operations continue to be discarded during a further period, t_{PUW}. This period should be long enough for the voltage to stabiles. The memory content cannot be changed during this period. Note that if the power supply has reached the minimum operating level (2.7 V) before the end of this delay, the application can start to read the memory, thus saving time on the download. The Bus Master should, however, not access the memory during t_{VSL}, after V_{CC}(min) has been attained.

Figure 1. Power-up Timing



CHIP SELECT INPUT FEATURE

Usually the outputs of the Bus Master can be guaranteed to be at stable levels during the full power-up sequence. Furthermore, when a Power Supervisor Device maintains the Bus Master in a Reset state during power-up, its outputs are generally at a known level.

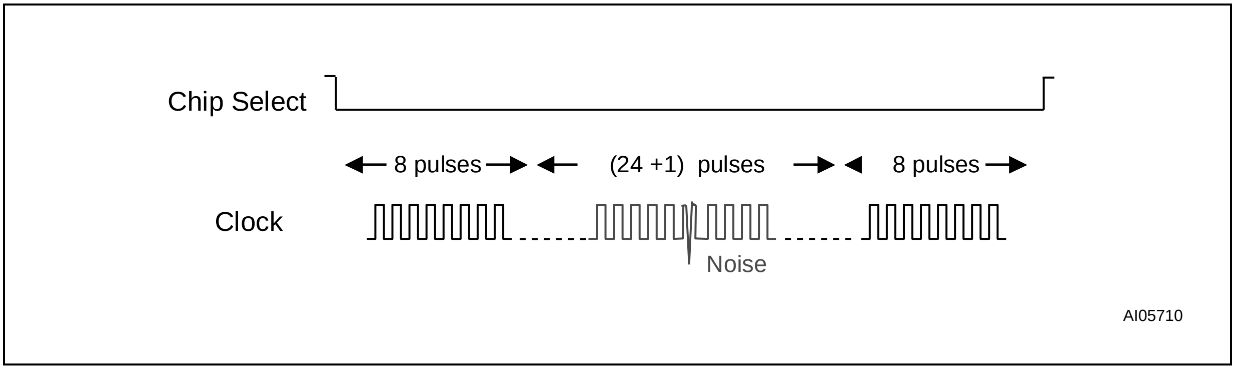
In both cases, the Bus Master can control the Chip Select pin to keep the memory deselected during this critical period. This is an additional protection, similar to the Reset pin feature. All communication with the memory in this state is impossible. Where the Bus Master’s output is high impedance during power-up, it is advised to connect the Chip Select pin of the Serial Flash memory to the power supply through a pull-up resistor. In this way, the Chip Select signal will follow the power supply ramp-up, and the device will be kept deselected during the entire power-up sequence.

CLOCK PULSE COUNTER FEATURE

Program, Erase or Write instructions are verified before being accepted for execution. They must consist of a multiple of eight clock pulses. Thus any commands that have been corrupted by noise are rejected, preventing the storage of corrupted data or overwriting at wrong addresses. The Write instruction shown in Figure 2 will not be executed, as the number of clock pulses is not a multiple of eight.

The Bus Master can send a Read Status Register instruction to check if its command has been correctly accepted. This reads the Write In Progress (WIP) bit which indicates if an internal operation is in progress. If the WIP bit has been set, it means a Program, Erase or Write instruction is executing.

Figure 2. Example of a Noisy Sequence Rejected by the Memory



WRITE ENABLE FEATURE

All instructions that modify data must be preceded by a Write Enable (WREN) instruction to set the Write Enable Latch (WEL) bit located in the Status Register. If the WEL bit has not been set, all Program, Write or Erase instructions are rejected.

The Write Enable Latch (WEL) bit is reset after:

– Power-up

– Write Disable (WRDI) instruction completion

– Write Status Register, Program or Erase instruction completion.

Thus the memory is routinely reset to a safe state, rejecting all data modifying instructions.

Table 1. Status Register Format

b7 … b0

SRWD	0	0	BP2[1]	BP1	BP0	WEL	WIP

SRWD: Status Register Write Disable

BP2, BP1, BP0: Block Protect Bits

WEL: Write Enable Latch Bit

WIP: Write In Progress Bit

Notes: 1. BP2 is not available on the M25P05-A, M25P10-A and M25P20 devices

SOFTWARE PROTECTION FEATURE

The non-volatile Block Protect bits (BP0, BP1 and, when available, BP2), located in the status register, allow parts of the memory to be configured as read-only. This can be extremely useful for applications that need to lift the write protection while updating a part of the memory, but do not need to lift the write protection on all of it (in the boot code region, for example).

Table 2. Protected Area Sizes for the M25P40

Status Register Content			Memory Content	
BP2 Bit	BP1 Bit	BP0 Bit	Protected Area	Unprotected Area
0	0	0	none	All sectors[1] (eight sectors: 0 to 7)
0	0	1	Upper eighth (Sector 7)	Lower seven-eighths (seven sectors: 0 to 6)
0	1	0	Upper quarter (two sectors: 6 and 7)	Lower three-quarters (six sectors: 0 to 5)
0	1	1	Upper half (four sectors: 4 to 7)	Lower half (four sectors: 0 to 3)
1	0	0	All sectors (eight sectors: 0 to 7)	none
1	0	1	All sectors (eight sectors: 0 to 7)	none
1	1	0	All sectors (eight sectors: 0 to 7)	none
1	1	1	All sectors (eight sectors: 0 to 7)	none

Note: 1. The device is ready to accept a Bulk Erase instruction if, and only if, all Block Protect (BP2, BP1, BP0) are 0.

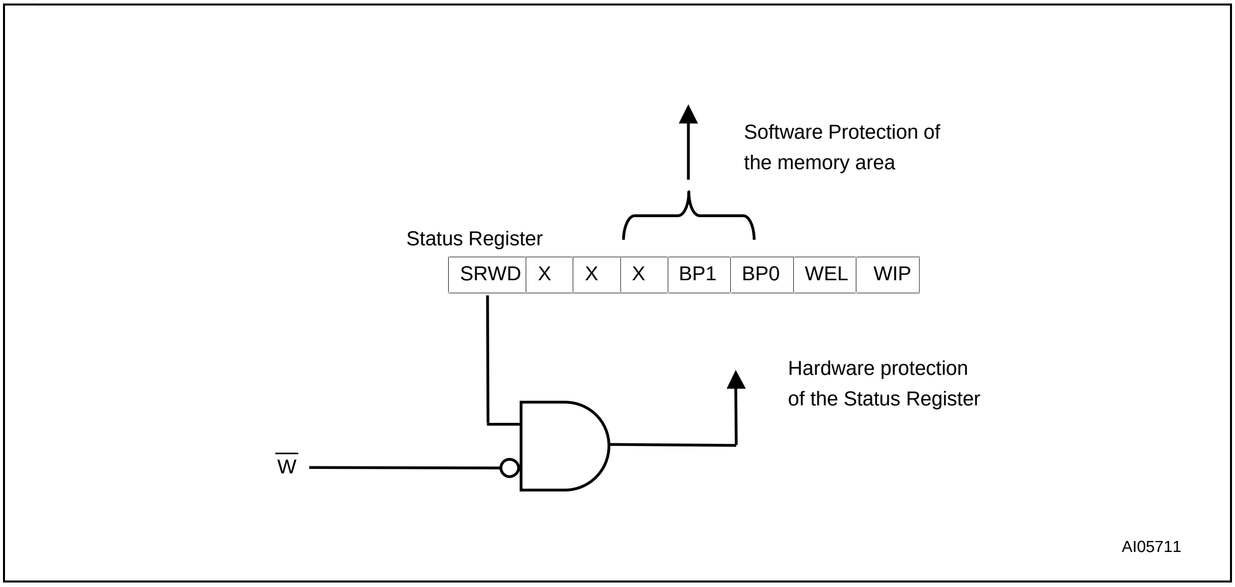
HARDWARE PROTECTION FEATURE

What is the Hardware Protection

The Write Protect ($\overline{W}$) pin allows the inhibiting of all write attempts in the Status Register, thereby keeping its content protected (the SRWD bit and the Block Protect bits). The memory area to be protected is defined by the Block Protect bits in the Status Register (software protection) and these bits are themselves protected from corruption by the hardware protection.

The Hardware Protection mode is entered only if the SRWD bit has been set and if the memory's Write Protect pin is driven Low, as shown in Figure 3.

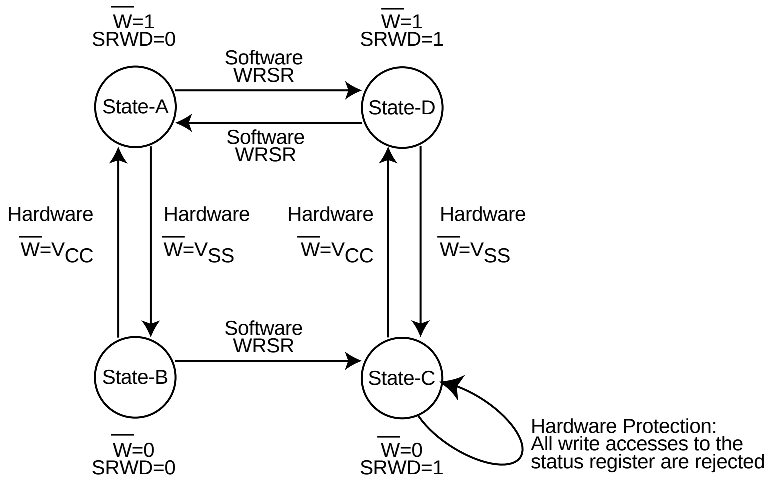
Figure 3. Architecture of the Software and Hardware Protection



Entering and Exiting Hardware protection

The device is delivered with the Status Register reset to 00h. This means the memory array is not software protected; the memory is ready for the first programming on production line. Since the SRWD bit is reset, the memory is not in Hardware Protection no matter what level is applied on the Write Protect pin. The Status Register is therefore unprotected, and the Block Protect bits can be written to define the read-only sections of memory.

Figure 4. State Diagram



AI05712

State A: Initial delivery state with the Write Protect pin connected to V_{CC} or driven High by a Bus Master output. Entering Hardware Protection from this state is a two-step process: the Master needs to set the SRWD bit by software (using a Write Status Register instruction), and then to drive the Write Protect pin Low by hardware, i.e. transition A → D, then D → C.

State B: Initial delivery state with the Write Protect pin connected to Ground or driven Low by a Bus Master output. Entering Hardware Protection from this state (B → C) is simpler: the Bus Master need only set the SRWD bit by software (using the Write Status Register instruction) after having programmed the memory and defined the read-only section using the Block Protect bits.

State C: The Hardware Protection rejects all write attempts to the Status Register. The Hardware protection is very secure, as the only way to exit from it is to apply V_{CC} on the Write Protect pin (transition C → D). Since the Status Register is write protected, it is not possible to exit Hardware Protection by resetting the SRWD bit i.e. it is impossible to switch from state C → B.

If the Write Protect pin is connected to Ground, it is impossible to bypass the protection.

State D: This state is useful for memory updates. For this, it is advised to connect the Write Protect pin to Ground via a pull-down resistor. This makes it possible to exit Hardware Protection (transition C → D) for updating by applying an external V_{CC} directly on the Write Protect pin. Hardware Protection can be reentered after the update (transition D → C) by removing this V_{CC} level.

Example of a Software and Hardware protection management:

Step 1: Programming the Serial Flash memory on the production line

1) Initial delivery state and hardware connection on the Write Protect pin

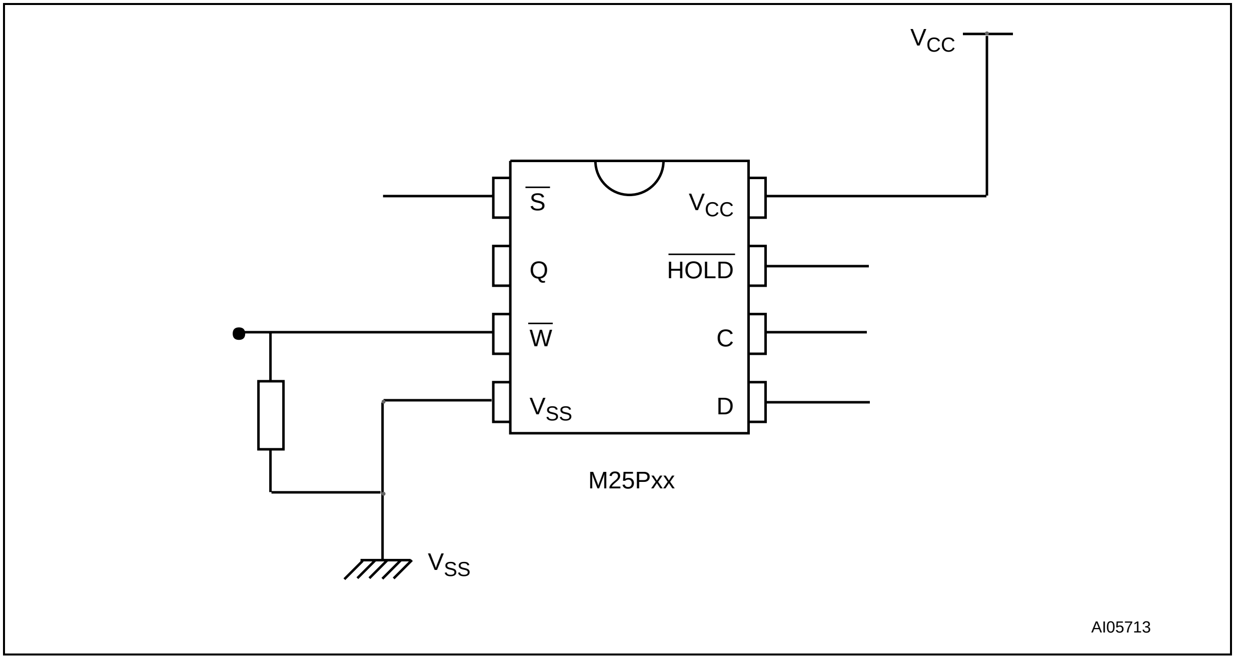
SRWD bit and Block Protect bits are all at 0 (initial delivery state)

=> All the memory area is available for programming (Block Protect bits at 0).

=> The Status Register can be written whatever the level applied on the Write Protect pin (SRWD bit = 0).

The Write Protect pin of the Serial Flash memory is connected to Ground (state B) through a resistor (to allow updating).

Figure 5. Connection on the Write Protect Pin



2) Programming of the Memory on the production line

The memory is delivered fully erased in preparation for initial programming. This saves time in production. The Status Register is delivered containing 00h, therefore programming in memory (no Software Protection, Block Protect bits = 0) and writing in the Status Register (no Hardware Protection SRWD=0) are both allowed.

3) Entering Software Protection

Once the memory is completely programmed, the application must protect its content by defining the read-only area. This is done by setting the Status Register's Block Protect bits.

4) Entering Hardware Protection

Once the read-only area has been defined in the Status Register, the Status Register must be protected. This is done by setting the SRWD bits of the Status Register (transition B → C).

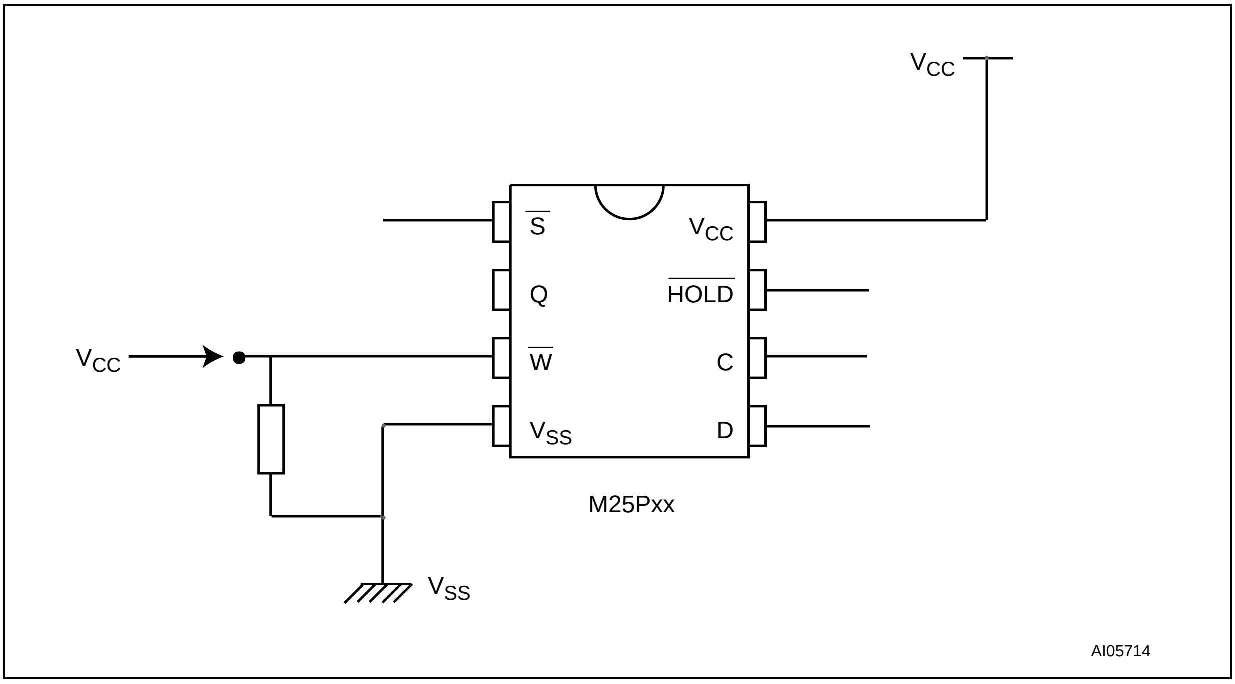
The memory content is now strongly protected for the lifetime of the application.

Step 2: Updating the memory content

1) Exiting Hardware Protection

The only way to exit Hardware Protection (transition C → D) is to apply V_{CC} on the Write Protect pin. This is possible when a pull-down resistor has been included.

Figure 6. Connection on the Write Protect Pin



2) Exiting Software Protection

It is now possible to write to the Status Register to exit Software Protection of the memory content. If the application needs to update all the code, the Block Protect bits must all be reset to 0. If the application needs to update only part of the memory (keeping, for example, the boot code protected), it can define the Block Protect bits to specify that section.

3) Updating the program

4) Reenter Software Protection:

The Block Protect bits of the Status Register define the read-only section.

5) Reenter Hardware Protection:

Remove the V_{CC} voltage applied on the Write Protect Pin (transition D → C).

THE DEEP POWER DOWN FEATURE

On downloading the code after Power-up, the Serial Flash memory is usually unused until the next Power-up. It is advisable to enter the Deep Power-down mode using the DP instruction. This lowers the consumption from the stand-by current to the deep power-down current. This also secures the memory against inadvertent overwrites.

As all instructions are rejected except Release from Deep Power-down, no Write, Program or Erase instructions can be executed when the Serial Flash is in Deep Power-down Mode.

CONCLUSION

The M25Pxx Serial Flash memory family from STMicroelectronics has been optimized for code storage, and is designed to offer maximum protection of non-volatile storage. An extensive set of Write Protection features is provided for this purpose, enabling the designer to fully safeguard any code storage application.

For current information on ST Flash Memory products, please consult our pages on the world wide web:

www.st.com/serialflash

If you have any questions or suggestions concerning the matters raised in this document, please send them to the following electronic mail addresses:

apps.serial-flash@st.com	(for application support)
ask.memory@st.com	(for general enquiries)

Please remember to include your name, company, location, telephone number and fax number.

Information furnished is believed to be accurate and reliable. However, STMicroelectronics assumes no responsibility for the consequence of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is grante by implication or otherwise under any patent or patent rights of STMicroelectronics. Specifications mentioned in this publication are subjec to change without notice. This publication supersedes and replaces all information previously supplied. STMicroelectronics products are nc authorized for use as critical components in life support devices or systems without express written approval of STMicroelectronics.

STMicroelectronics group of companies
Australia - Brazil - Canada - China - Finland - France - Germany - Hong Kong -
India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States.
www.st.com