life.augmented

Reminder of MOOC

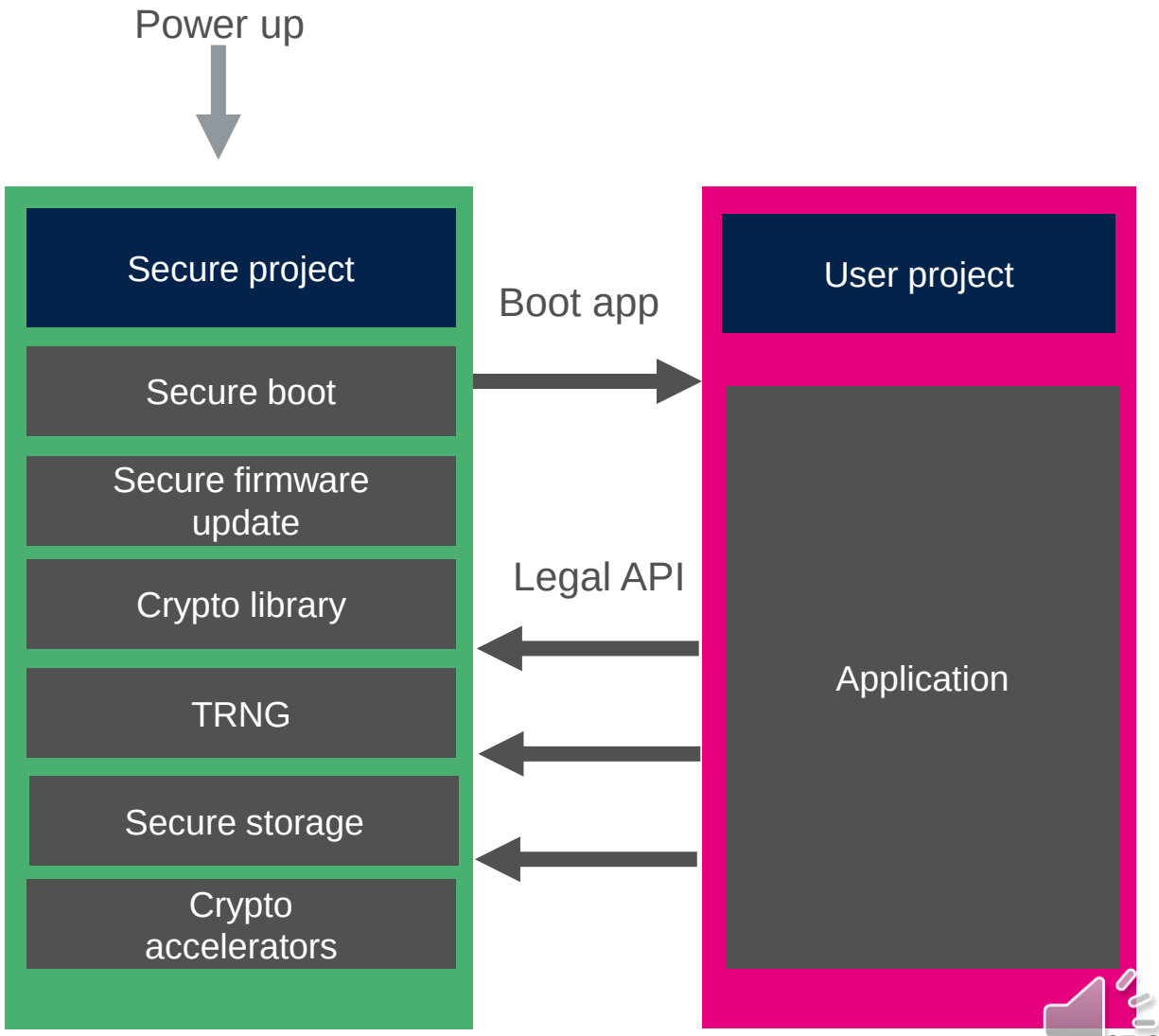
Software security based on Isolation

Agenda

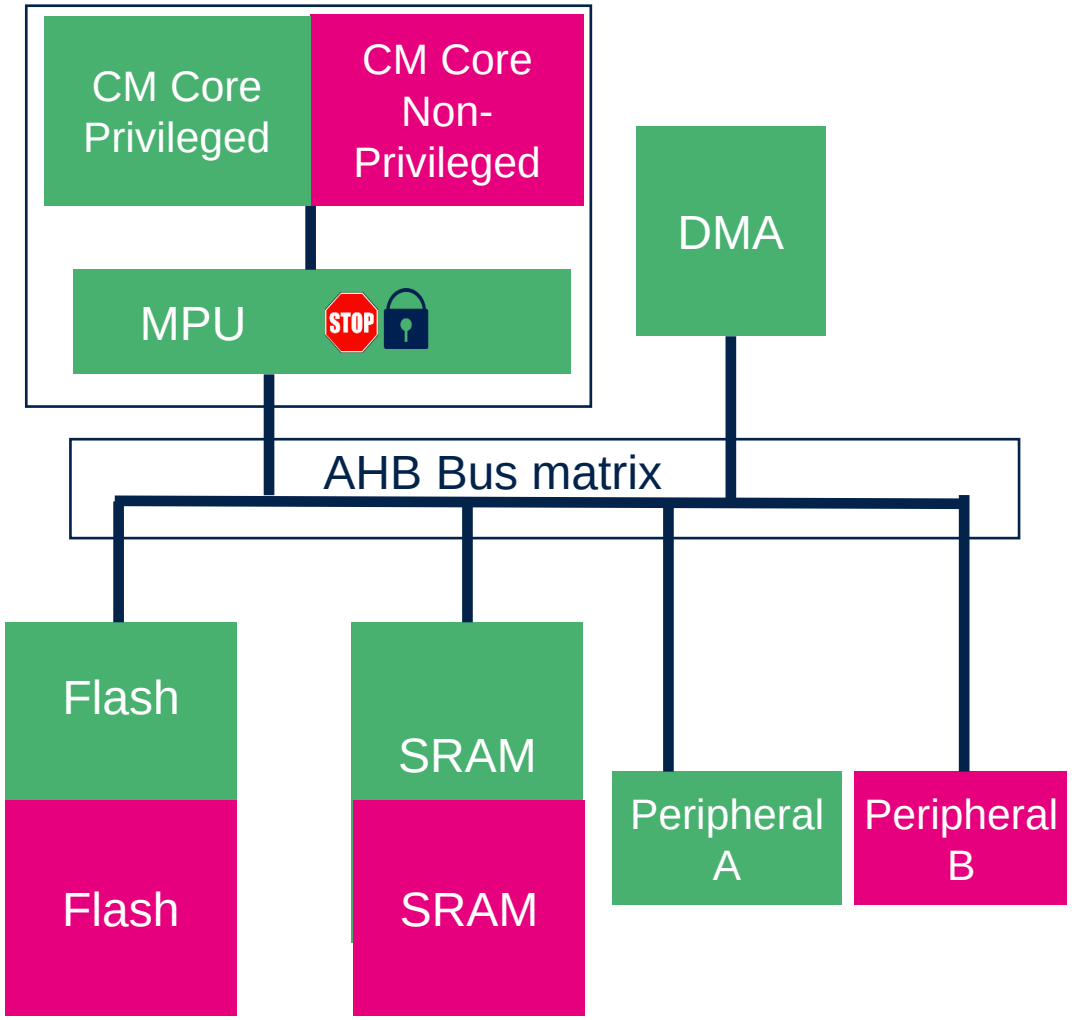
- What is isolation? Why is it important?
- What means of isolation we have today on STM32?
- What is Trustzone? How it works? What are the benefits over current solution?
- Show system integration of TrustZone on STM32L5
- Introduce development flow. CMSIS support of TrustZone

Isolate runtime environments

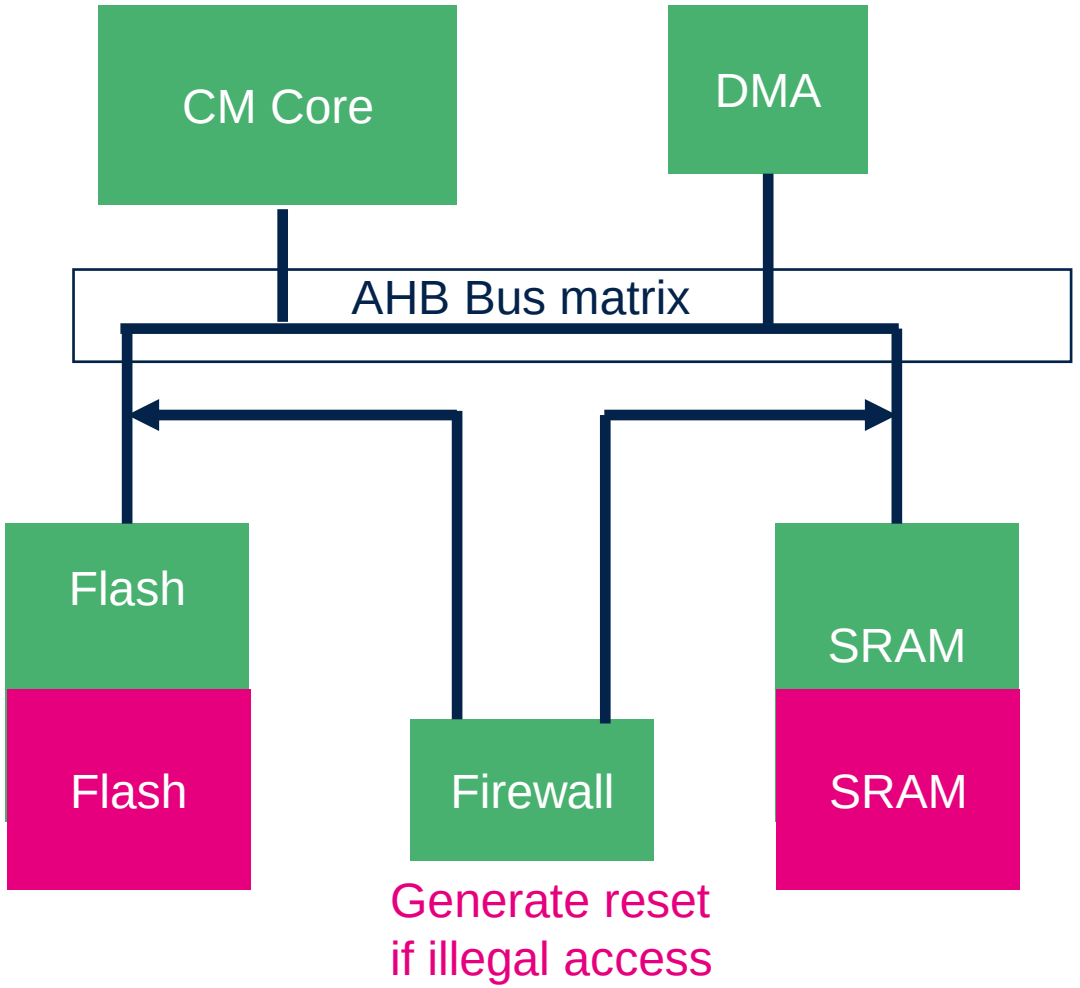
- Separate responsibilities
- Hardware based isolation
- Restrict access to code and data



Various means of isolation

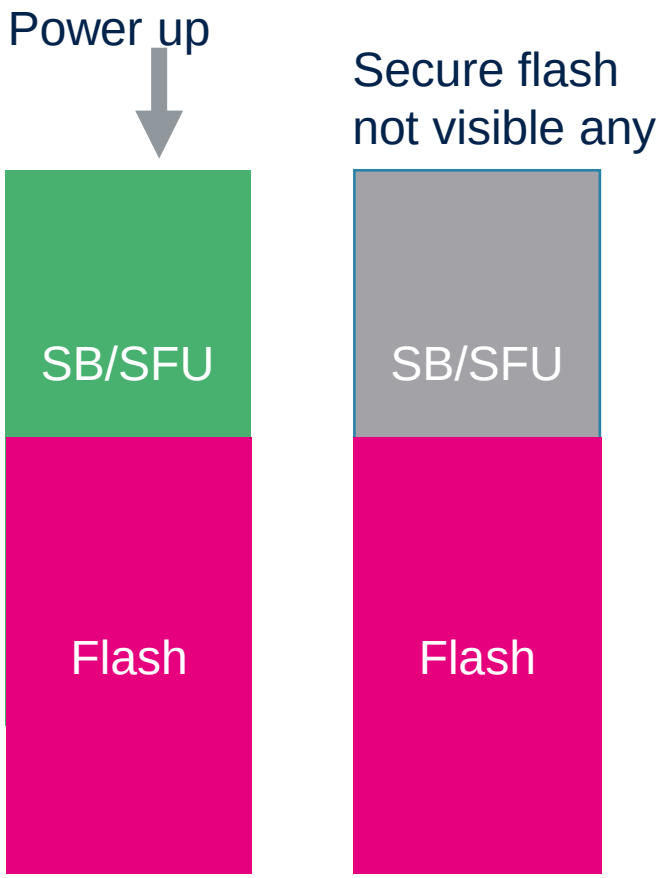


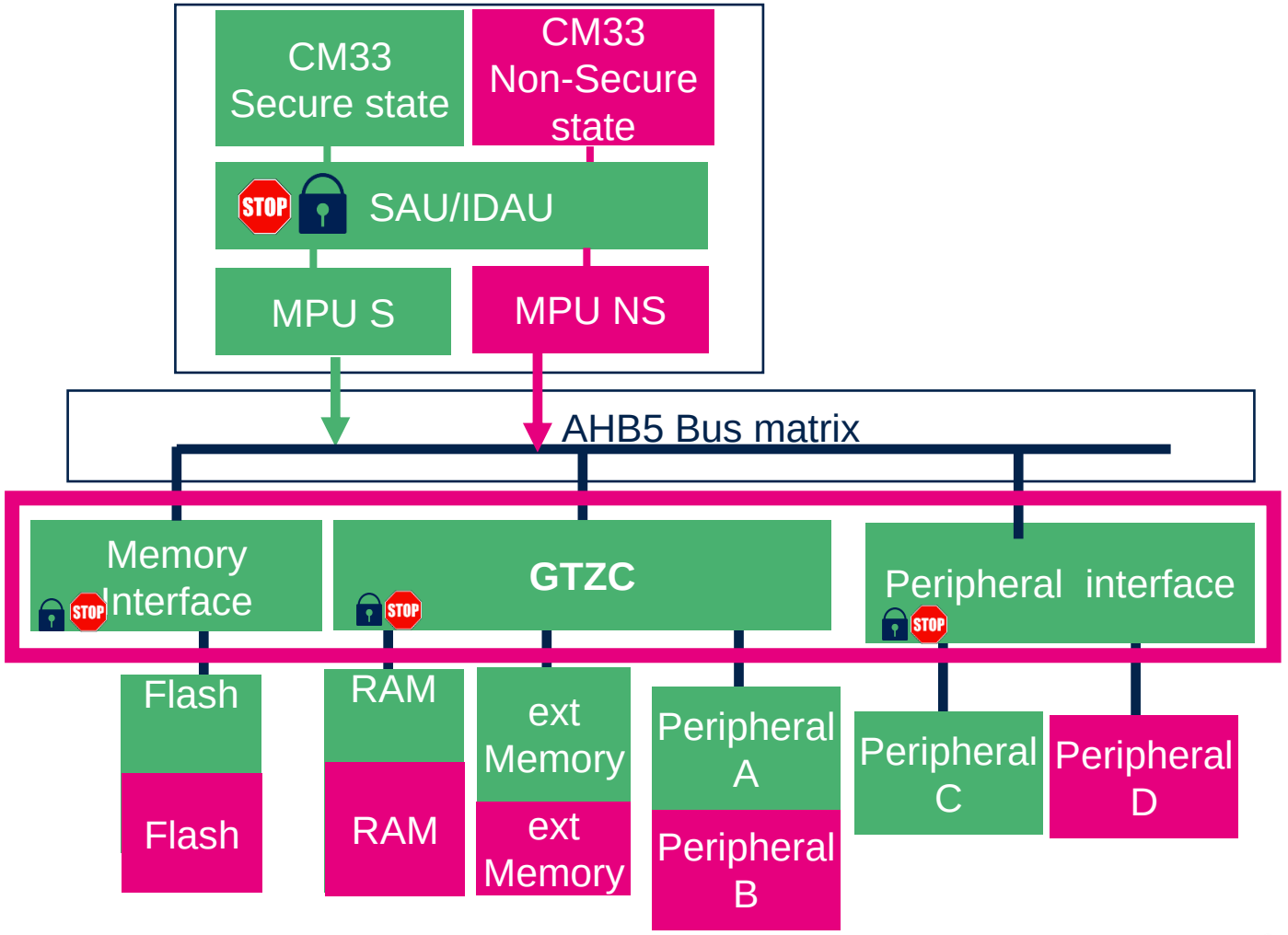
MPU



Firewall

Various means of isolation



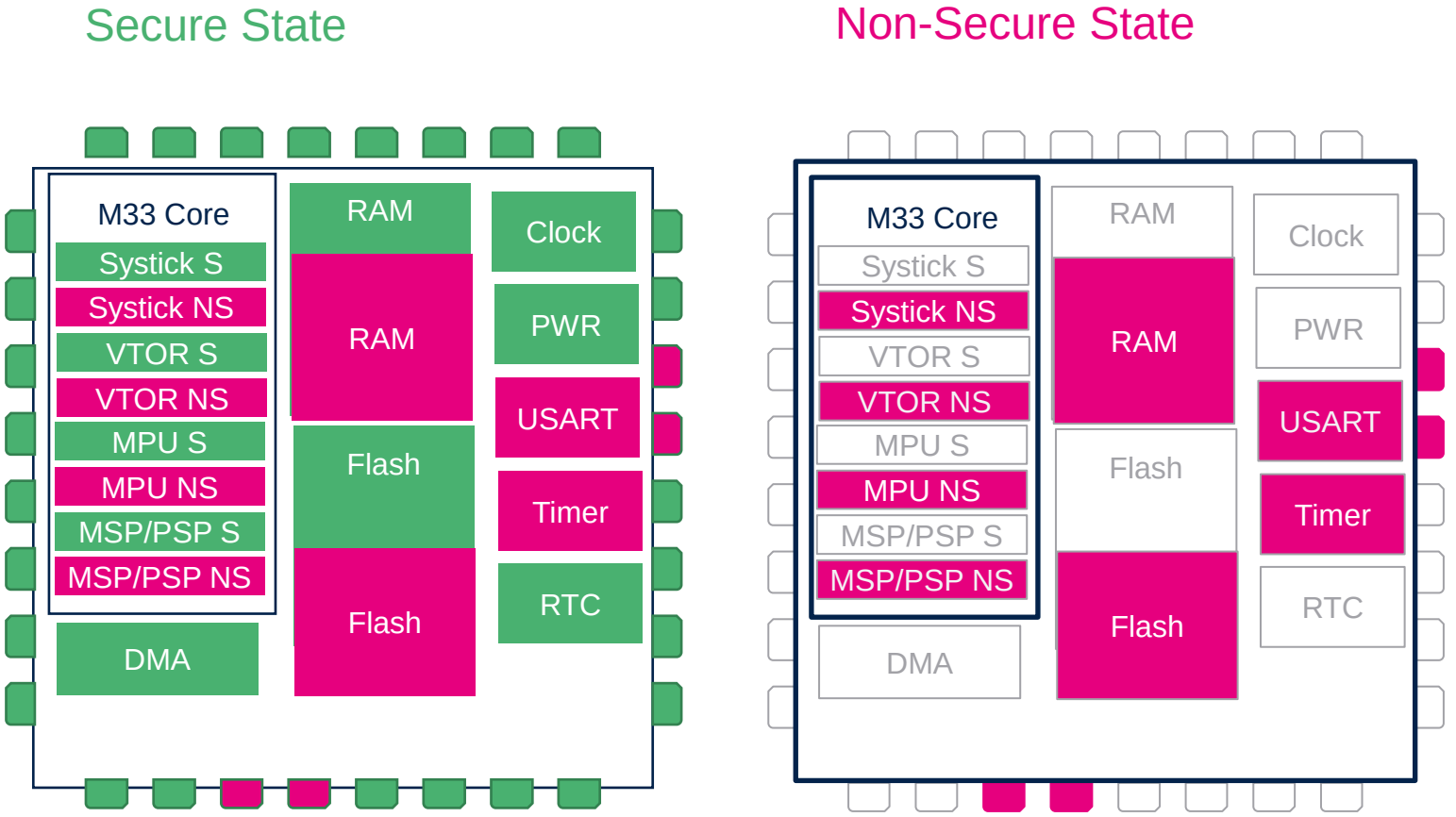


Secure flash

TrustZone

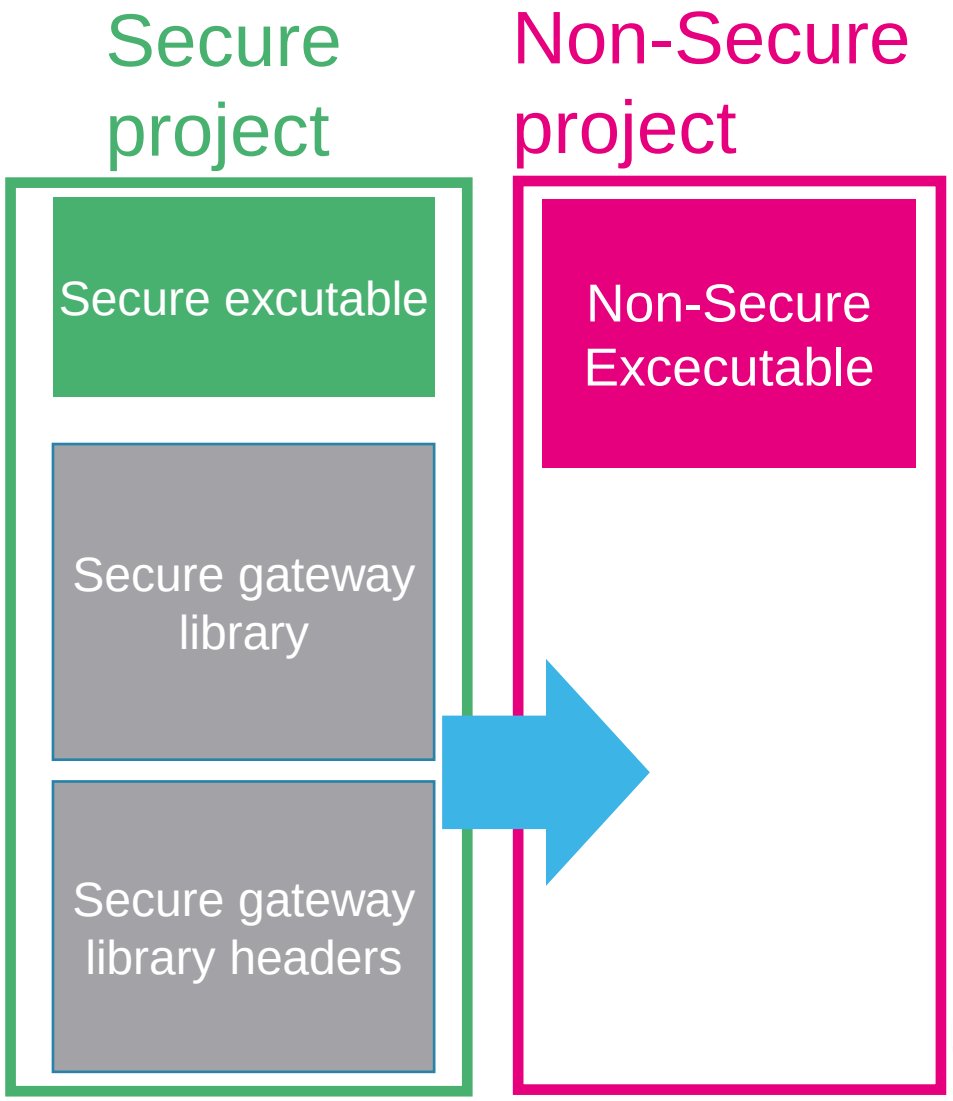
Cortex M33 and TrustZone Key features

- New processor state
- Real time
  - Low interrupt latency
  - Low state switching overhead
  - Deterministic



Development flow

- Independent development of Secure and Non-Secure
- Secure project exports legal API via Secure gateway library
- Non-Secure project is linked against Secure gateway library
- Rmk: Build order



Isolation Features by STM32 Series

STM32 Series	Isolation features				
	Secure mem/ HDP	MPU	Firewall	Trustzone	Arm Cortex®
STM32 **F0**					**M0**
STM32 **F1**		■			**M3**
STM32 **F2**		■			**M3**
STM32 **F3**		■			**M4**
STM32 **F4**		■			**M4**
STM32 **F7**		■			**M7**
STM32 **L0**		■	■		**M0+**
STM32 **L1**		■			**M3**
STM32 **L4**		■	■		**M4**
STM32 **L5**	■	■		■	**M33**
STM32 **H7**	▒	■			**M7/M4**
STM32 **G0**	▒	■			**M0+**
STM32 **G4**	▒	■			**M4**
STM32 **WB**		■			**M4/M0+**

■ Available on all devices

▒ Depends on device part number

life.augmented

Conclusion

- Isolation means on STM32 families
  - MPU
  - Firewall
  - Secure Memory
  - TrustZone

- Security Part 3: STM32 security features MOOC (link)
- How to enable TrustZone® and start a project with STM32L5 (Youtube link)

life.augmented