how differes on Cortex-M cores the security through TrustZone and something different, mfg. specific, say on the stm32 MCUs?

TrustZone is a security technology developed by ARM for its Cortex-M cores, specifically the Cortex-M23 and Cortex-M33 processors. TrustZone creates two separate execution environments on a single core, one for secure tasks and another for non-secure tasks. The secure environment has access to all system resources, while the non-secure environment only has limited access, as dictated by the secure environment. This separation helps protect sensitive data and code from being accessed or tampered with by non-secure tasks.

On the other hand, manufacturers like STMicroelectronics, who produce STM32 MCUs, may offer their own security features specific to their devices. For STM32 MCUs, one such feature is the Hardware Security Module (HSM), which is designed to enhance the security of embedded systems.

Some differences between TrustZone and manufacturer-specific security features like HSM on STM32 MCUs are:

1. Architecture: TrustZone is a security feature provided by ARM and is tightly integrated with the Cortex-M processor's architecture. In contrast, manufacturer-specific security features are designed and implemented by the MCU manufacturer and are not necessarily tied to the processor's architecture.
2. Availability: TrustZone is available only on specific ARM Cortex-M cores (Cortex-M23 and Cortex-M33), while manufacturer-specific security features may be available on various MCU models, regardless of the specific ARM core they are built on.
3. Functionality: TrustZone focuses on creating secure and non-secure execution environments, while manufacturer-specific security features may include a broader range of functionalities, such as cryptographic accelerators, secure key storage, tamper detection, and secure boot mechanisms.
4. Customizability: Manufacturer-specific security features may be tailored to the specific needs of the target application or industry, whereas TrustZone is a more general-purpose security solution provided by ARM.

5. Compatibility: TrustZone is designed to work seamlessly with the ARM ecosystem, including development tools and software libraries. Manufacturer-specific security features may require custom tools or software components to be fully utilized.

In summary, ARM TrustZone and manufacturer-specific security features like HSM on STM32 MCUs can provide different levels of security and functionality. TrustZone is a more general-purpose solution that focuses on separating secure and non-secure tasks, while manufacturer-specific features can offer a more customized approach to securing embedded systems. In some cases, both TrustZone and manufacturer-specific features can be used together to create a more comprehensive security solution for an embedded system.