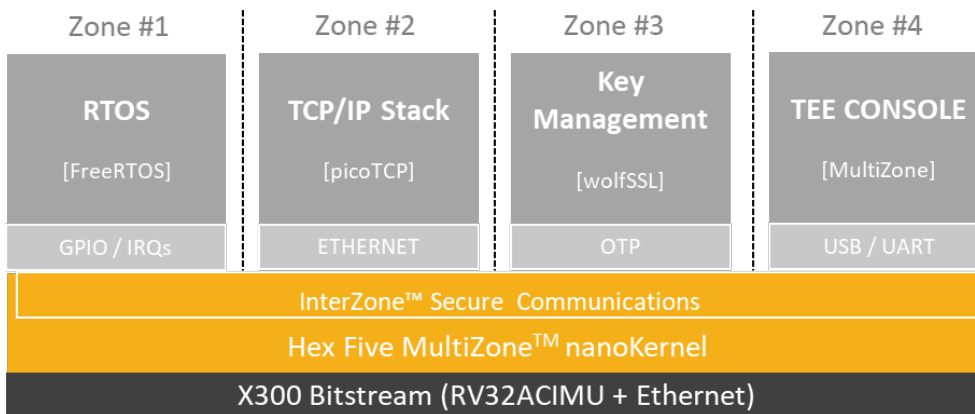




# wolfSSL + Hex Five Multizone™ Security on RISC-V

Secure implementation of FreeRTOS with wolfSSL TLS 1.3 and hardware-enforced separation between OS, TCP/IP stack and root of trust.

The wolfSSL embedded SSL/TLS 1.3 library now has a secure implementation on MultiZone™ Security, the first Trusted Execution Environment for RISC-V. The traditionally monolithic firmware is decomposed in multiple security domains with hardware enforced separation between OS, TCP/IP stack and root of trust. The resulting light-weight stack provides a zero-trust framework for secure Internet of Things applications.



HEX-Five™



## MultiZone™ Secure Secure IoT Stack

- FreeRTOS kernel with three tasks:
  - Command Line Interface (CLI)
  - Realtime LED Fade Task
  - Realtime Robot Control
- TCP/IP Stack in its own Zone with hardware-enforced separation preventing exploit propagation
- wolfSSL TLS 1.3 library in its own Zone
  - 256 bit Elliptic Curve Cryptography (ECC) using wolfSSL's libraries without any special hardware
  - Cipher TLS\_AES\_128\_GCM\_SHA256
- Root of Trust (RoT) keys and certificates are held in a further Zone with hardware-enforced separation
- Communication across zones based on InterZone™ Secure messages with no shared memory
- MultiZone™ Security overhead of only 1kB of SRAM, 4kB of Flash and 0.01% of cycles

## Learn More

For more information about using wolfSSL with the Hex Five Multizone™ Security as a platform, please contact us at [info@wolfssl.com](mailto:info@wolfssl.com), or visit our website [www.wolfssl.com](http://www.wolfssl.com). The X300 bitstream and code base is open source and available at <https://github.com/hex-five/multizone-secure-iot-stack>

[wolfssl.com](http://wolfssl.com)  
[github.com/wolfssl](https://github.com/wolfssl)

Copyright © 2019 wolfSSL Inc. All Rights Reserved