Why SESIP™ Certification for FreeRTOS Matters

Richard Elberger
Head of IoT Ecosystem Services

About your speaker

- With Amazon for > 5 years
- Technology professional for > 20 years
- Leads the IoT Ecosystem Services team at Amazon Web Services in the AWS IoT service team
- Evangelizes the art of the possible
- Passion for embedded hardware and software and how the AWS Cloud accelerates customer outcomes
- linkedin.com/in/richardelberger

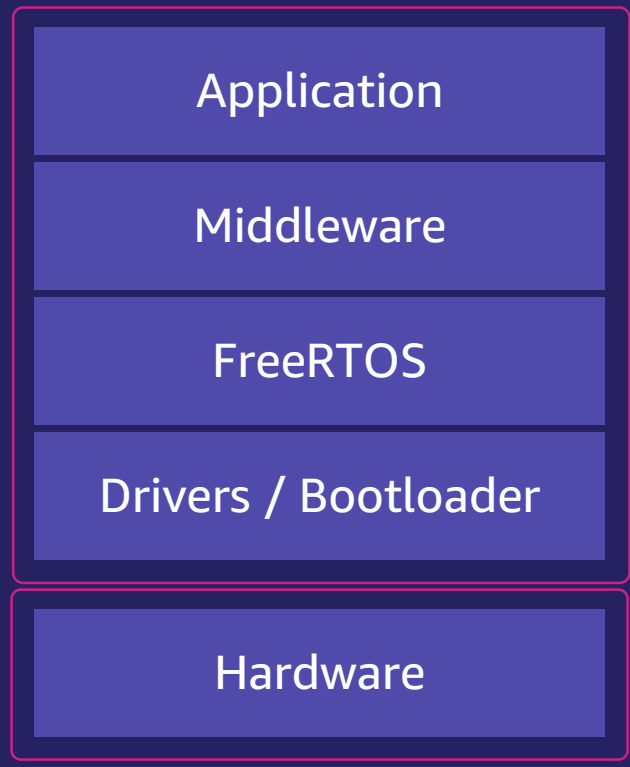
Agenda

- Why SESIP™ excites the FreeRTOS project
- Target of Evaluation (TOE) assumptions
- Considerations for your future SESIP certified product
- Call to action

Why SESIP™ Certification excites the FreeRTOS project

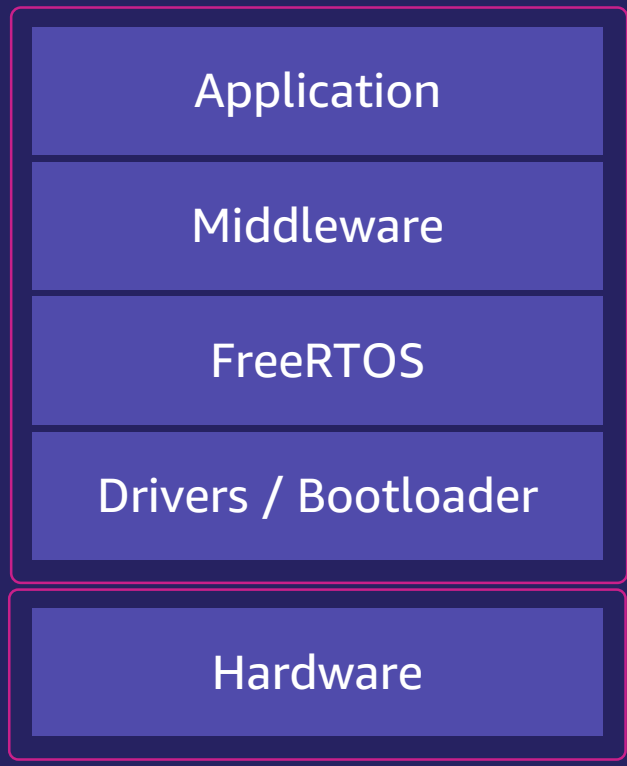
Certification prior to the SESIP™ model

- ↓ Certification of all layers occur at the end of development
- ↓ Certification duration is uncertain due to breadth of potential issues
- ↓ Certification process resets in whole if any layer is modified
- ↓ IoT product delivery risk is always high



Certification using the SESIP™ model

- Certification of individual layers occur outside of IoT product developer's cycle
- Certification duration is more certain due to focus on application
- Certification process discretely reset if any layer is modified
- IoT product delivery risk is greatly reduced



FreeRTOS test areas and Target of Evaluation (TOE) assumptions

Basic assumptions

- Physical attacks not in scope
- The TOE must have a Memory Protection Unit (MPU)
- Tests do not add any hostile code to the TOE
  - Development teams need to be trusted and must implement development team rules that constrain FreeRTOS source code modification
- Firmware Over-the-Air (FOTA) function uses AWS IoT OTA Update Manager

Users can verify that they have a secure product only if they can obtain the identifications of the product parts (application and Connected Platform).

Security Evaluation Standard for IoT Platforms (SESIP)

Public Release v1.1

Section 3.1.1

Test: Identity verification

- Implementers can verify software versions included in their products by the LTS manifest file
- Environment condition: the implementer is trusted and would not modify any SESIP™ certified FreeRTOS source code
- Identity verification for the connected platform relates to the runtime identification under device operation
- The MQTTConnectInfo structure is coded to use unique client ID according to application requirements

Addressing security flaws, functional bugs, or improvements may require an update of the platform in the field. Composite developers and evaluators can be assured that the update mechanism itself will not enable an attack.

Security Evaluation Standard for IoT Platforms (SESIP)

Public Release v1.1

Section 3.2.3

Test: system update via Over-the-Air update (OTA)

- An Over-the-Air update makes it possible to update device firmware without an expensive recall or technician visit
- Quick response to security vulnerabilities and software bugs that are discovered after the devices are deployed in field
- FreeRTOS OTA client library enables update notifications, downloads, and cryptographic verification
- The OTA library is continuously verified using formal methods. See Using Formal Methods to validate OTA Protocol for more

https://freertos.org/2020/12/using-formal-methods-to-validate-ota-protocol.html

The platform developer can separate the critical assets in different parts of the platform, and thus safeguard them from compromises of other parts of the platform.

Security Evaluation Standard for IoT Platforms (SESIP)

Public Release v1.1

Section 3.4.4

Test: software isolation

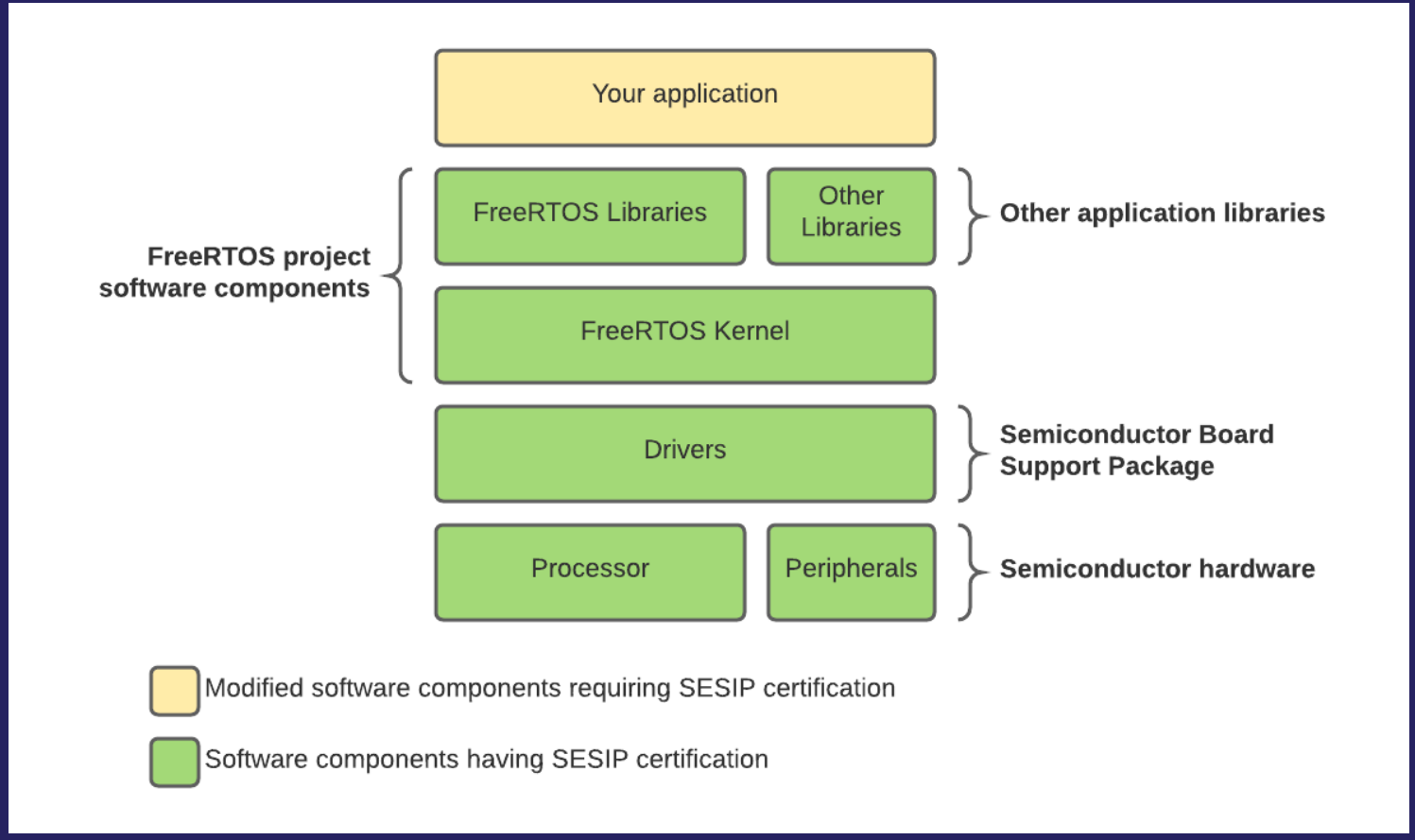
- Software isolation helps protect against attackers modifying memory
- Two parts: hardware and software.
  - Hardware requires a Memory Management Unit (MMU) or a Memory Protection Unit (MPU)
  - Software: kernel port implements capabilities to work with the MMU and MPU.
- For more information on this topic, see Gaurav Aggarwal's blog section relating to ARMv8-M features.

https://freertos.org/2020/04/using-freertos-on-armv8-m-microcontrollers.html#FREERTOS_WITH_MPU

Considerations for your future SESIP™ certified product

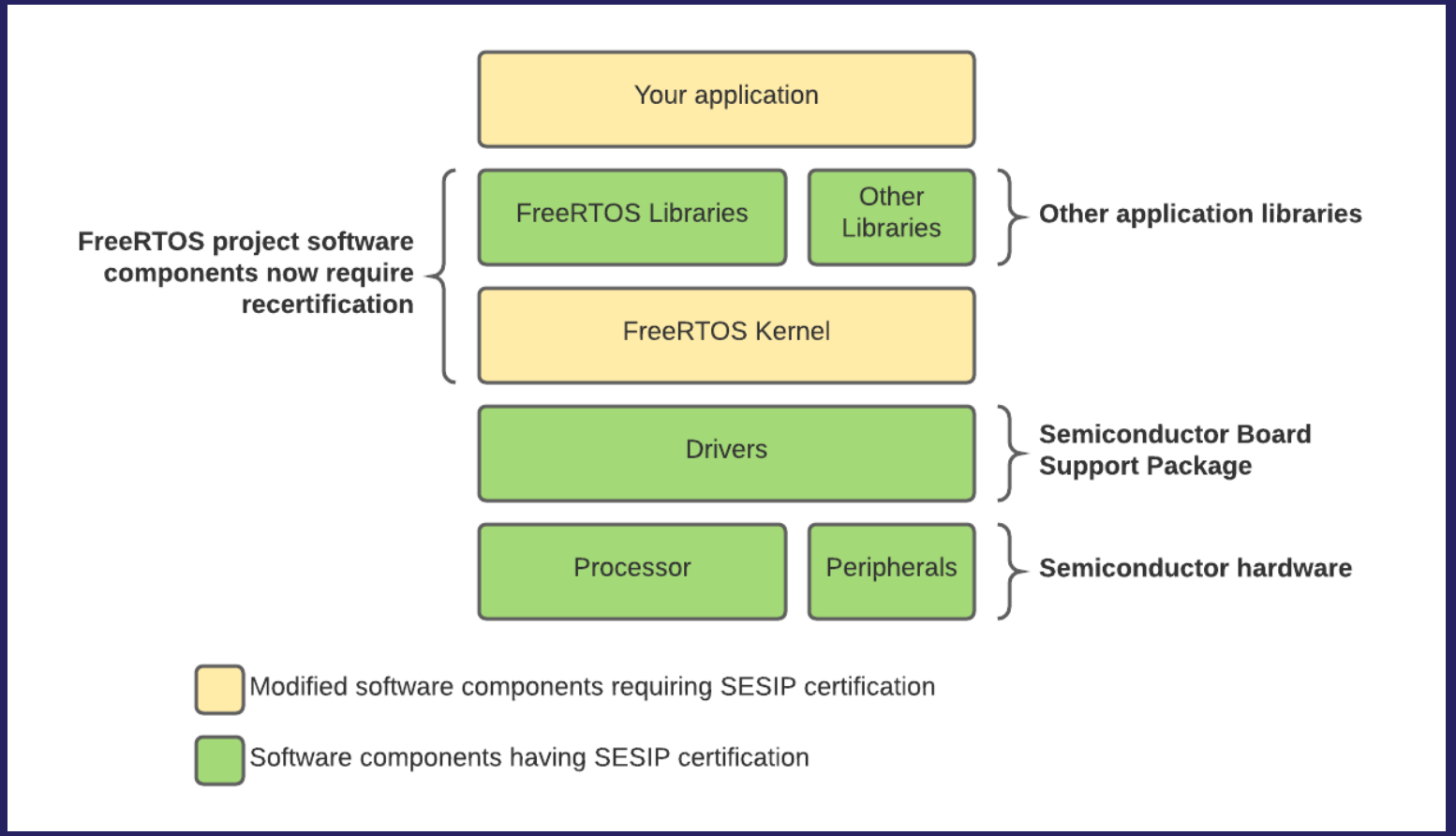
Application with no modified layers

Everything is fine, nothing to see here, results in expected benefits



Application with modified layers

“Let me tweak the kernel just a little bit”



WHY SESIP™ CERTIFICATION FOR FREERTOS MATTERS

FreeRTOS long-term support

Device software

Get predictability and feature stability for two years with FreeRTOS LTS libraries

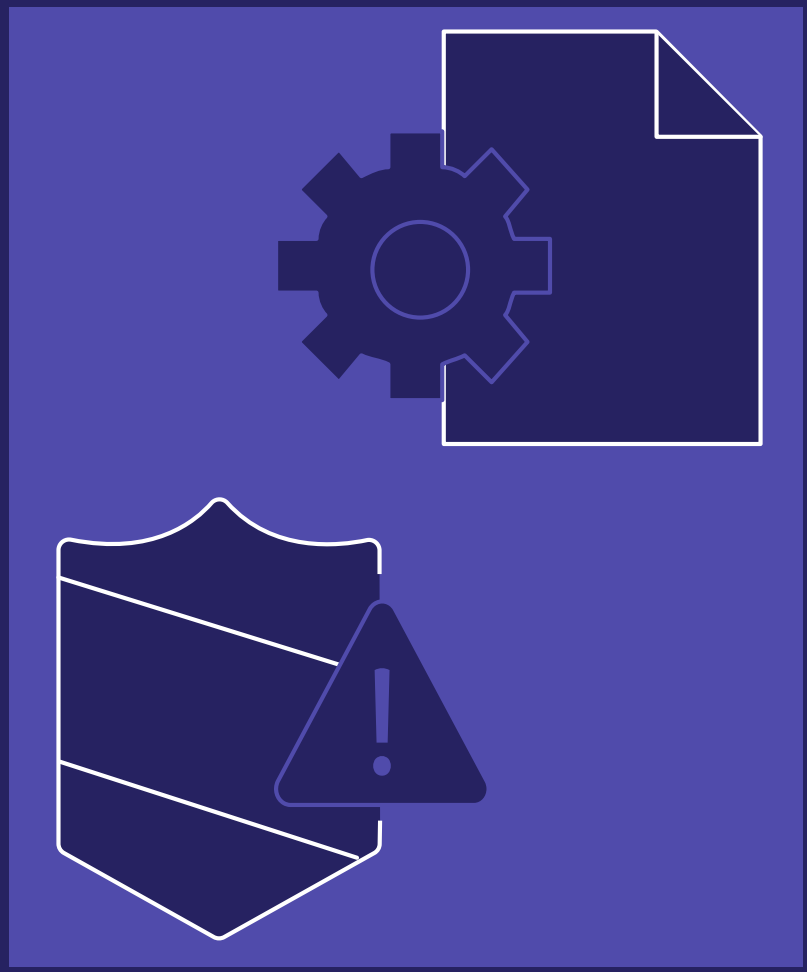
Covers:

- FreeRTOS kernel
- Connectivity/other libraries: FreeRTOS+TCP, coreMQTT, coreHTTP, coreJSON
- Security library: corePKCS11
- AWS library: AWS IoT Device Shadow, AWS IoT Jobs, AWS IoT OTA, AWS IoT Device Defender

Libraries receive security updates and critical bug fixes but no new features for at least two years

Maintained by AWS

Free and open source under the MIT license



FreeRTOS extended maintenance plan

Device software

Receive security patches and critical bug fixes on your chosen LTS version for up to 10 years beyond the expiry of the initial LTS period

Reduce product liability risks

Save operating system upgrade costs

Improve device security for the long term

Reduce the risk of delayed updates by receiving timely notification of upcoming patches

Annual subscription plan per FreeRTOS LTS version and use on single/multiple products

Continue to renew subscriptions annually for a duration up to 10 years

Call to action

Call to action

- Where is your business on the stack?
- What layers do you depend on? Are they certified?
- Learn which SESIP specification areas are important to you
- Do a gap analysis on your layer
- Get certified ☺

Thank you!

Richard Elberger

Head of IoT Ecosystem Services

Amazon Web Services

linkedin.com/in/richardelberger