Device Failure Recovery with EmSPARK™ Security Suite

High availability is a key component of any IoT device design. A device can stop functioning properly due to a variety of hardware, software or security issues. The device's software application typically maintains a set of conditions that are used to determine that it has failed; for example, a number of attempts to access it without a response. When a device fails, it needs to be able to come back online quickly with known and trusted software. This is typically a reboot with a backup firmware image. Similar to the boot and update processes, the recovery process is a time when the device is vulnerable. The failure recovery process must be secure in order to get the device up and running quickly and safely.

Typically, a device will signal a failure when the software is no longer responding or behaving as it should. This can occur during 1.) normal operation, when tamper events are detected, indicating improper behavior, or 2.) during the boot process, when the device fails to successfully complete a boot sequence. After one of these events, the device re-boots and loads a new, trusted software image that follows a secondary boot path. This image is often a backup, or previous version, loaded into the same flash memory. Similar to firmware updates, the device's failover application—sometimes the update application—checks for a new image and retrieves the package.

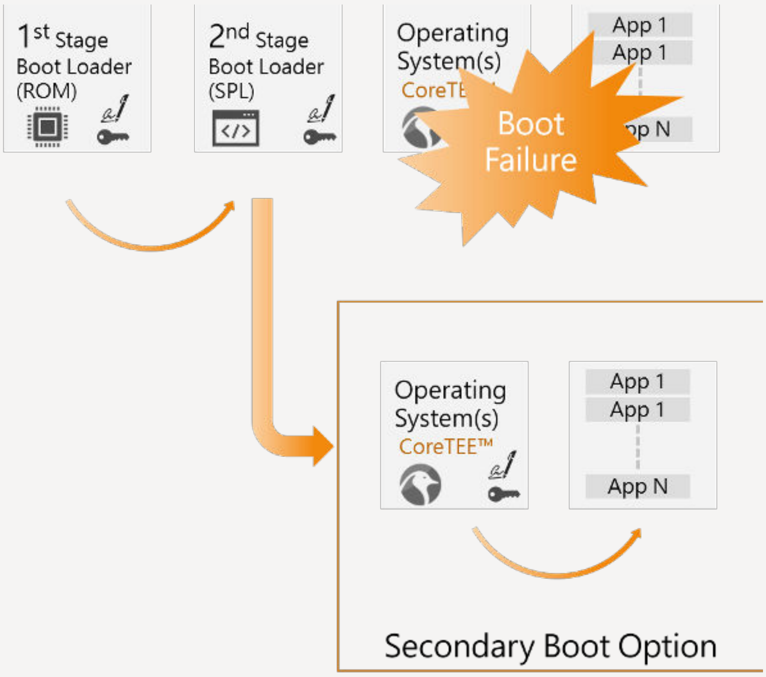
To determine a failure and what steps are needed to recover, the device uses the processor's state variables and registers to detect anomalous behavior. Examples of state variables are below:

- Primary Boot Image (A or B)
- Boot Image A is Valid
- Boot Image B is Valid
- Update Non-Primary Image
- Activate Updated Image

These state variables tell the device which image to validate and activate during the boot process. (See the Secure Boot Solutions Brief for details on the entire boot process.) In this example, memory is set at failure to Validate Image B (the backup software Image) during re-boot to deliver the proper firmware.

After the correct image is determined for re-boot, a process similar to the **Secure Firmware Update** process is followed:

1. The Read-Only Memory (ROM) then loads the Secondary Boot Loader (SPL), unencrypted but signed.
2. The device determines—by reading boot state variable— that the boot process is in failure recovery.
3. The device locates and reads the backup firmware location.
4. The backup package is loaded, and verified by checking its signature.
5. Following the secure boot process, the shared memory and Sequitur CoreTEE™ is established, and Rich Environment functions such as U-Boot and Linux Kernels are loaded.
6. The backup firmware is re-encrypted using a diversified key.


1st Stage Boot Loader (ROM)
2nd Stage Boot Loader (SPL)
Operating System(s) CoreTE
App 1
App 1
pp N
Boot Failure
Operating System(s) CoreTEE™
App 1
App 1
App N
Secondary Boot Option

Sequitur Labs' EmSPARK™ Security Suite provides the following for secure failure recovery:

1. Response to a detected fault in the operation
2. Creation of a secondary boot path for recovery
3. Coordination with backup firmware images
4. Backup Firmware authentication and encryption

Learn More

EVAL KIT Download the free evaluation kits and user's guide for more details and code examples

Download "Surviving The IoT Wave: EmSPARK™ Security Suite" Whitepaper

A **FREE** EmSPARK™ Security Suite Evaluation Kit is available at:
https://www.sequiturlabs.com/iot-security-suite/free-iss-eval-kit.

SEQUITUR LABS

Sequitur Labs is developing seminal technologies to improve trust in a connected world, reducing the cost and complexity to build secure embedded and IoT devices. Sequitur's products span a range of disciplines required for trusted computing, from boot through the full device lifecycle. Sequitur's security solutions provide real business value to device makers, such as reducing BoM costs, protecting revenue by thwarting IP theft, improving product reliability and reducing liability, and improving device lifecycle management processes. To learn more about Sequitur's security platform, visit us at www.sequiturlabs.com.

PO Box 1127
Issaquah, WA 98027

+1 425 654 2048
+44 20 3318 1171

info@sequiturlabs.com
www.sequiturlabs.com

Photo by Daniele Levis Pelusi on Unsplash.
MSBEm-0005-Rev A. Printed in the U.S.A.