BLE Startup Failure Investigation Report

BLE Startup Failure Investigation Report

Project: DEU_V11_ENCRYPTED
Target: nRF52840 / ISP1807
Date: 2026-06-18
Debugger: J-Link, serial number 69651077

1. Problem Summary

The device freezes immediately after BLE initialization is executed in the application.

The relevant application code is:

```
ret = ble_init();
if (ret == 0) {
    ret = bt_ready();
    if (ret != 0) {
        LOG_ERR("BLE advertising start failed: %d", ret);
    }
} else {
    LOG_ERR("BLE init failed: %d", ret);
}
```

When debugging, execution repeatedly ends in Zephyr fatal halt:

```
arch_system_halt()
```

The call stack consistently includes the Nordic MPSL TIMER0 interrupt path:

```
MPSL_IRQ_TIMER0_Handler
mpsl_timer0_isr_wrapper
m_assert_handler
z_arm_fault
z_fatal_error
arch_system_halt
```

This indicates an internal MPSL/BLE controller assertion, not a normal application-level infinite loop.

2. Application-Level Debugging

The BLE startup sequence was debugged step by step:

1. Breakpoints were placed around `ble_init()`, `bt_ready()`, and `bt_le_adv_start()`.
2. The firmware reached the advertising start path.
3. An advertising TX power configuration call was identified as a possible trigger and removed.
4. After removing the advertising TX power call, the same MPSL fatal still occurred.
5. BLE privacy was disabled for testing.
6. Tickless kernel was disabled for testing.
7. MPSL/ECDH-related stack settings were increased for testing.
8. BLE was skipped in a debug build, and the rest of the application continued running.

These tests showed that the failure is triggered by BLE/MPSL startup, but is not explained by the application advertising code itself.

3. 32.768 kHz LFCLK Bypass Test

To check whether the low-frequency 32.768 kHz crystal was the cause, the firmware was rebuilt to use the internal LFRC instead of the external low-frequency crystal:

```
CONFIG_CLOCK_CONTROL_NRF_K32SRC_RC=y
CONFIG_CLOCK_CONTROL_NRF_K32SRC_500PPM=y
CONFIG_CLOCK_CONTROL_NRF_K32SRC_RC_CALIBRATION=y
```

The generated configuration confirmed that LFRC was selected:

```
CONFIG_CLOCK_CONTROL_NRF_K32SRC_RC=y
# CONFIG_CLOCK_CONTROL_NRF_K32SRC_XTAL is not set
CONFIG_CLOCK_CONTROL_NRF_K32SRC_RC_CALIBRATION=y
CONFIG_CLOCK_CONTROL_NRF_K32SRC_500PPM=y
```

Result: the same MPSL fatal still occurred.

Conclusion: the issue is not caused by the 32.768 kHz low-frequency crystal.

4. Official Zephyr BLE Sample Tests

To isolate the application code from the hardware and board configuration, official Zephyr BLE samples were built and flashed to the same board.

Samples tested:

```
zephyr/samples/bluetooth/peripheral
zephyr/samples/bluetooth/beacon
```

The `bluetooth/beacon` sample is a minimal BLE advertising sample and is useful for testing the BLE controller/radio path with minimal application logic.

The beacon sample was also built with LFRC selected for LFCLK, bypassing the 32.768 kHz crystal.

Result: the official `bluetooth/beacon` sample still entered the same MPSL fatal path:

```
MPSL_IRQ_TIMER0_Handler
m_assert_handler
arch_system_halt
```

Conclusion: the issue is not specific to the DEU_V11_ENCRYPTED application code.

5. Direct HFXO Hardware Clock Test

A direct hardware-level test was performed through J-Link/GDB by writing to the nRF52840 CLOCK peripheral registers.

The test sequence was:

1. Clear `EVENTS_HFCLKSTARTED`.
2. Trigger `TASKS_HFCLKSTART`.
3. Wait several seconds.
4. Read `EVENTS_HFCLKSTARTED` and `HFCLKSTAT`.

Register values after waiting:

```
EVENTS_HFCLKSTARTED = 0x00000000
HFCLKSTAT           = 0x00010000
```

Interpretation:

- `EVENTS_HFCLKSTARTED` remained `0`, so the external high-frequency crystal oscillator did not report a successful start.
- `HFCLKSTAT` indicated that HFCLK was running, but still sourced from the internal RC oscillator rather than the external crystal.

This strongly suggests that the 32 MHz HFXO did not start.

6. Important Distinction

The 32.768 kHz low-frequency crystal can be bypassed by using LFRC.

However, the BLE radio on nRF52840 requires the 32 MHz high-frequency crystal oscillator. BLE cannot reliably operate using only the internal high-frequency RC oscillator.

Therefore:

- The 32.768 kHz crystal was bypassed successfully during testing.

- The BLE failure persisted.
- The direct HFXO test showed that the 32 MHz crystal did not start.

7. Final Conclusion

The evidence strongly indicates that the 32 MHz HFXO on this specific ISP1807 module fails to start.

The failure is board-specific and is not caused primarily by the application BLE code.

Since the ISP1807 integrates the 32 MHz crystal, load capacitors, and XC1/XC2 connections internally, the most likely causes are an internal module defect or damage, although module power integrity and module-to-PCB soldering should also be verified.

Replacing the ISP1807 module is the most practical confirmation and corrective action.