**【问题】工厂LTE综测时，设备Crash的问题**

|  |  |
| --- | --- |
| **创建时间：** | *2017/9/7 10:35* |
| **作者：** | *习凡* |

问题的现象：

     Device校准之后，进行综测；在进行LTE的综测过程中，设备Crash。其中，校准和综测过程中modem的工作模式的变化过程为：

          Online(Power-On)  -->  FTM(Calibration)  -->  Online(Finish Calibration)  -->  FTM(Test)  -->  Online(Finish Test)

Log及问题原因的分析：

     设备Crash后，抓取dump信息；通过Qualcomm的QCAP解出f3log，log信息如下：

Call Stacks:

-000|qurt\_exception\_shutdown\_fatal()

-001|err\_raise\_to\_kernel()

-002|err\_fatal\_handler()

-003|err\_fatal\_jettison\_core()

-004|err\_exception\_handler()

-005|main()

-006|lib\_qurt\_init()

-007|qurtos\_root\_entry()

----|end of frame

-000|memcpy()

-001|memscpy()

-002|ftm\_lte\_build\_msgr\_msg()

-003|ftm\_dispatch()

-004|FTM\_Sequencer\_Adaptation\_SendPacketToMobile()

-005|FTM\_Sequencer\_ProcessClientRequestPacket()

-006|ftm\_req()

-007|rf\_test\_task()

-008|TASK\_ENTRY()

-009|rex\_os\_thread\_entry\_func()

-010|\_pthread\_stub()

-011|qurt\_trampoline()

----|end of frame

F3 Software:

======================================================================

00:03:22.411:                   rf\_test\_task.c:2070     Start processing FTM packet: 75,11,30

00:03:22.411:                   rf\_test\_task.c:2425     Got LTE CMD 0x1e

00:03:22.411:   ftm\_lte\_common\_msgr\_helper\_functions.c:261      ftm\_lte\_build\_msgr\_msg: convert command 502

00:03:22.411:   ftm\_lte\_common\_msgr\_helper\_functions.c:458      ftm\_lte\_build\_msgr\_msg: Message built 0x5020204

00:03:22.413:                          udcif.c:1375     udci\_get\_instance\_for\_handle(): NULL instance pointer

     通过f3log，可以初步的分析是由于进行RF test的LTE测试时，NULL pointer导致的。

