OsmoTRX - Bug #4507
ubsan error in trxd
04/21/2020 03:34 AM - Hoernchen

Status: New
Priority: Normal
Assignee: pespin
Due date: 04/21/2020
% Done: 0%
Category: Target version: Spec Reference:

Description
pretty much upon startup, b210:

proto_trxd.c:65:18: runtime error: 128 is outside the range of representable values of type 'char'
 #0 0x4197c8 in trxd_fill_burst_normalized255 /foo/osmo-trx/Transceiver52M/proto_trxd.c:65:18
 #1 0x419e5e in trxd_send_burst_ind_v1 /foo/osmo-trx/Transceiver52M/proto_trxd.c:109:3
 #2 0x3b5ba1 in Transceiver::driveReceiveFIFO(unsigned long) /foo/osmo-trx/Transceiver52M/Transceiver.cpp:1103:14
 #3 0x39fc6c in RxUpperLoopAdapter(TrxChanThParams*) /foo/osmo-trx/Transceiver52M/Transceiver.cpp:1196:15
 #4 0x7ffff755a608 in start_thread /build/glibc-aevPTw/glibc-2.31/nptl/pthread_create.c:477:8
 #5 0x7ffff5dbd102 in clone /build/glibc-aevPTw/glibc-2.31/misc/../sysdeps/unix/sysv/linux/x86_64/clone.S:95
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior proto_trxd.c:65:18

68p *(bi)
>&"p *(bi)
~"p *(bi)

05/15/2020
- Assignee changed from fixeria to pespin

Assigning to Pau as he was working on osmo-trx side of the implementation.

Probable fix:

```c
diff --git a/Transceiver52M/proto_trxd.c b/Transceiver52M/proto_trxd.c
index 5a898b9..fbc0b14 100644
--- a/Transceiver52M/proto_trxd.c
+++ b/Transceiver52M/proto_trxd.c
@@ -62,7 +62,7 @@ static void trxd_fill_burst_normalized255(uint8_t* soft_bits, const struct trx_u
    
    unsigned i;
    for (i = 0; i < bi->nbits; i++)
-            soft_bits[i] = (char) round(bi->rx_burst[i] * 255.0);
+            soft_bits[i] = (uint8_t) round(bi->rx_burst[i] * 255.0);
   }
```

---

History

#1 - 04/21/2020 04:41 AM - fixeria

- Assignee changed from fixeria to pespin

Assigning to Pau as he was working on osmo-trx side of the implementation.

#2 - 04/21/2020 07:38 AM - pespin

Probable fix: