OsmocomBB - Bug #5202

[Assert failed rc >= 0 l1ctl.c:83] cell_log crashes (mostly) when monitoring specific ARFCN

07/25/2021 01:38 PM - antfarmer

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
<th>Start date:</th>
<th>07/25/2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
<td>Due date:</td>
<td></td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
<td>% Done:</td>
<td>0%</td>
</tr>
<tr>
<td>Category:</td>
<td></td>
<td>Spec Reference:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resolution:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description
Upon execution of ./cell_log -A 117 -i 127.0.0.1, the program crashes after a while with:

```
Assert failed rc >= 0 l1ctl.c:83
backtrace() returned 13 addresses
/usr/local/lib/libosmocore.so.17(osmo_generate_backtrace+0x18) [0x7f10d726684f]
/usr/local/lib/libosmocore.so.17(+0x24557) [0x7f10d7266557]
/usr/local/lib/libosmocore.so.17(osmo_panic+0xdc) [0x7f10d7266638]
./cell_log() [0x407f4a]
./cell_log() [0x40821d]
/usr/local/lib/libosmocore.so.17(osmo_wqueue_bfd_cb+0x3a) [0x7f10d7259e3d]
/usr/local/lib/libosmocore.so.17(+0xf2c4) [0x7f10d72512c4]
/usr/local/lib/libosmocore.so.17(+0xf3ba) [0x7f10d72513ba]
/usr/local/lib/libosmocore.so.17(osmo_select_main+0x15) [0x7f10d72513d8]
./cell_log() [0x40402f2c]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf0) [0x7f10d66db840]
./cell_log() [0x4030b9]
Aborted
```

Line 83 in l1ctl.c:

```
/* if FN is negative, we were called for something that's not CCCH! */
OSMO_ASSERT(rc >= 0);
```

The problem exists mostly when specifying an ARFCN manually, although I have seen the same type of crash even when no ARFCN is specified and an active scan is in place, but it is a very rare occasion and takes much more time to occur.

I have tried with different cells of different network carriers, so this is very unlikely to be a network issue.

Using the latest revision to date of master branch.