OsmoTRX - Bug #3141

Refactor / clean up TRX CTRL / DATA interfaces implementation

04/05/2018 05:46 PM - fixeria

Status:	New	**Start date:**	04/05/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

Some code parts of the Transceiver::driveControl() were already cleaned up,
but some parts are still require the refactoring, for example:

```
int maxDelay;
sscanf(params, "%d", &maxDelay);
mMaxExpectedDelayAB = maxDelay; // 1 GSM symbol is approx. 1 km
sprintf(response,"RSP SETMAXDLY 0 %d",maxDelay);
```

Here the sscanf may fail, which would result in an uninitialized stack-memory access.
This is related to the following commands: SETMAXDLY, SETMAXDLYNB, SETRXGAIN,
SETPOWER, ADJPOWER, RXTUNE, TXTUNE, SETTSC, SETSLOT, _SETBURSTTODISKMASK.

Both RXTUNE and TXTUNE commands are using integer to parse the
freq. value. What if a negative number would arrive?

Also, have a look at the Transceiver::driveTxPriorityQueue():

```
// ...
int timeSlot = (int) buffer[0];
// ...
GSM::Time currTime = GSM::Time(frameNum,timeSlot);
// ...
```

There is no range check.

Feel free to use the TRX Toolkit to fuzz the TRX interface:

https://git.osmocom.org/osmocom-bb/tree/src/target/trx_toolkit?h=fixeria/trx