General Hospital Secure Heart Information Transmitter

This document is meant to give a basic overview of the Secure Heart Information Transmitter system. The Secure Heart Information Transmitter a device undergoing medical trials here at General Hospital and is designed to help improve patient outcomes by alerting doctors whenever it detects a change in the condition of a patient's heart. As the device is currently undergoing medical trials frequent testing of the device may be performed by staff to ensure it is functioning properly.

The Secure Heart Information Transmitter is broken up into three main components. These are the Hardware Action Reporting Device, the reporting database, and the Alarm Database Interface Connector. The specific function of each component is detailed below.

The executeable files for the Secure Heart Information Transmitter are located in /home/pi/MADSHIT/MADSHIT.

Hardware Action Reporting Device for the Secure Heart Information Transmitter

The Hardware Action Reporting Device is used to detect changes in the patent, user interaction with the device and trigger audio/visual alerts. It has several command line parameters which can be set below to help customize it for the environment.

```
usage: ./HARDSHIT.py [-h] [-N DATABASENAME] [-H DATABASEHOST] [-U
DATABASEUSERNAME]
        [-P DATABASEPASSWORD] [-a LASTALARMNUMBER] [-p PINMAP]

Hardware Action Reporting Device for the Secure Heart Information Transmitter.

optional arguments:
  -h, --help            show this help message and exit
  -N DATABASENAME, --databaseName DATABASENAME
                        Name of the database used by the Secure Heart
                        Information Transmitter. Default is doshit
  -H DATABASEHOST, --databaseHost DATABASEHOST
                        The host the database is running on. Default is
                        127.0.0.1
  -U DATABASEUSERNAME, --databaseUsername DATABASEUSERNAME
                        Username to be used for the database connection.
                        Default is dashit
  -P DATABASEPASSWORD, --databasePassword DATABASEPASSWORD
                        Password to be used for the database connection.
                        Default is Password1!
  -a LASTALARMNUMBER, --lastAlarmNumber LASTALARMNUMBER
                        The set the inital value for the last alarm
  -p PINMAP, --pinMap PINMAP
```

```
                        Specify the pin mapping file for pin to alarm
                        mapping. Default filename is pinMap.json
```

Secure Heart Information Transmitter Alarm Database Interface Connector

The Alarm Database Interface Connector acts as an interface to the database allowing changes to be made. A web interface to help manage this can be accessed on port 5000.

```
usage: ./SHITADIC.py [-h] [-N DATABASENAME] [-H DATABASEHOST] [-U
DATABASEUSERNAME]
       [-P DATABASEPASSWORD] [-L LOGFILE] [-S LOGSIZE] [-B LOGBACKUPS]
       [-s SECRETKEY]

Secure Heart Information Transmitter Alarm Database Interface Connector

optional arguments:
  -h, --help            show this help message and exit
  -N DATABASENAME, --databaseName DATABASENAME
                        Name of the database used by the Secure Heart
                        Information Transmitter. Default is 'doshit'.
  -H DATABASEHOST, --databaseHost DATABASEHOST
                        The host the database is running on. Default is
                        127.0.0.1
  -U DATABASEUSERNAME, --databaseUsername DATABASEUSERNAME
                        Username to be used for the database connection.
                        Default is dashit
  -P DATABASEPASSWORD, --databasePassword DATABASEPASSWORD
                        Password to be used for the database connection.
                        Default is blank
  -L LOGFILE, --logFile LOGFILE
                        The path to a file where you would like output logged.
                        By default, a new log file will be created once the
                        first reaches 100kB. Default is SHITADIC.log
  -S LOGSIZE, --logSize LOGSIZE
                        The maximum size of the log file in bytes. If this is
                        set to 0 all data will be logged to the same file
                        Default is 100000
  -B LOGBACKUPS, --logBackups LOGBACKUPS
                        The maximum number of old log files to keep.
                        Default is 5
  -s SECRETKEY, --secretKey SECRETKEY
                        Path to file containing 24 random bytes to be used as
                        the secret key
```

Database

For speed and storage reasons the Secure Heart Information Transmitter database is currently running on mysql.general.local