

Team Project
“Software For Self-Testing Of The Telecommunication
Network Of University Of Freiburg”

Refik Hadžialić
Triatmoko

November 9, 2011



Albert-Ludwigs-Universität Freiburg
Lehrstuhl für Kommunikationssysteme
Prof. Dr. Gerhard Schneider

Supervisors:
Konrad Meier
Dennis Wehrle

Sommersemester 2011

Contents

1	Introduction and Motivation	4
2	Requirements	5
2.1	Logical and algorithmic requirements	5
2.2	Software requirements	6
2.3	Hardware requirements	8
3	Database design	9
4	Software design	12
4.1	Database access	15
4.2	Controlling the cell phones	15
4.3	Client and Server class	16
4.4	Ping class	17
4.5	Data logging	18
4.6	SSH Tunnel Class	18
4.7	USB Cell phone detection class	19
4.8	Truth table class	19
4.9	Init Test class	19
4.10	Controller class	20
5	Hardware design	21
5.1	BeagleBoard	21
5.2	Cell phones	21
5.3	Cables for the cell phones	22
5.4	Server	22
6	Communication protocol	23
6.1	Communication between the handler and controller	23
6.2	Verification of the protocol	26
7	Security and safety of the system	28
7.1	Encryption of the communication channels	28
7.2	Security on the web site	29
7.2.1	Configuring the http secure protocol https	29
7.2.2	Password protecting the web site using .htaccess	32
8	Web page	34
8.1	Communication between the web page and the test software	34
8.2	Results on the web page	34
9	Employing the test software system	36
9.1	Required software and libraries	36
9.1.1	Python installation	36
9.1.2	Apache Web server installation	36

9.1.3	SSH	36
9.1.4	MySQL database and MySQLdb library	37
9.1.5	Serial port library	37
9.1.6	PJSUA library	37
9.1.7	pChart library	38
9.1.8	proctitle library	38
9.2	Configuring hardware	38
9.2.1	Configuring the cell phones	40
9.3	Location of the files	41
9.4	Setting up the parameters	42
9.5	Test descriptions	42
9.5.1	Smart test	42
9.5.2	SIP test	43
9.5.3	GSM test	43
9.5.4	All test	43
9.5.5	Manual test	43
9.6	Result descriptions	44
9.7	Using the software	45
9.7.1	Web site guide	45
9.7.2	Terminal guide	47
10	Conclusion	49

1 Introduction and Motivation

In the following report, the authors will try to give you a brief insight into our team project. The goal of our project was to develop a mechanism for automatic testing of our University Telecommunication network. The Telecommunication network of University of Freiburg consists of: our own internal GSM and telephone network systems; GSM redirecting device (if one initiates a call to one of the four external GSM networks, it redirects the calls to: T-mobile, 02, Vodaphone or E-Plus); a SIP gateway for land-line calls inside of Germany (sipgate.de) and international calls. Since we did not have access to internal servers, our strategy was to exploit the existing systems from an external perspective and infer the results out of our findings. Before we had started working on our project, we had to analyze the overall network to come up with the test cases that contain the highest information content. The next step in our procedure was to implement our ideas into a working piece of software. Gradually we implemented a bit-by-bit of the final software. In the following chapters we will describe in more detail our approach to the problem and how each subsystem works. This particular report and our wiki page should be a sufficient guide and manual for understanding, running and continuing the development of our test software. Certainly, we had a lot of fun while working on the project due the fact that we lost one team member. We would like to thank the whole department for the free coffee and their support, especially Konrad Meier, Dennis Wehrle, Richard M. Zahoransky and Larissa Linz, without their support this project would not end up this way.

2 Requirements

At the start of the project the requirements were not completely known but as the time had passed we redefined our requirements and goals. The first and the most important part at the start was to identify the key goals of our team project. The basic goal of our team project was to build a test software system which could tell an operator user what part of the system is not properly working in our University telecommunication network. Konrad and Dennis suggested us to analyze figure 1 and depending on it to build our test software. Our first attempt was to see what could we test without having access to

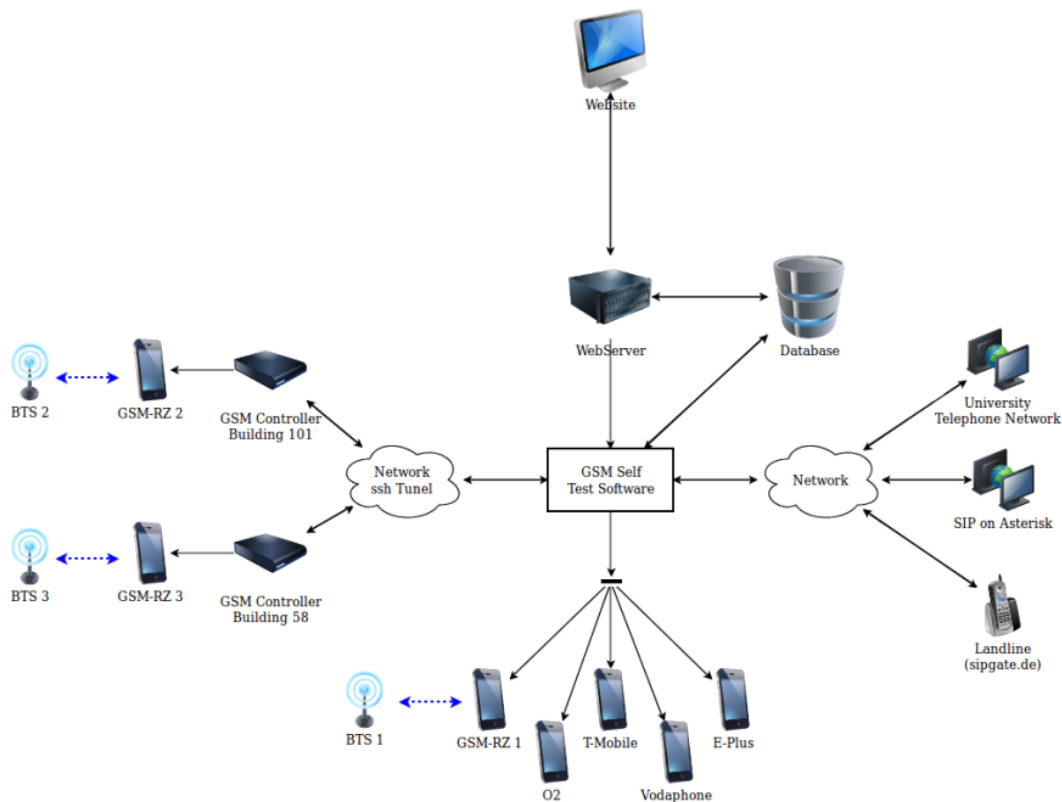


Figure 1: Overview of the Freiburg University telecommunication network [1]

the system. We installed numerous communication programs to see what others have done. After gaining access to the communication software, we had decided to build most of the test software ourselves. Libraries, which were used, were only the ones we could not develop ourselves because of the time-span of our team project.

2.1 Logical and algorithmic requirements

Despite the software and hardware requirements, the logic in our team project may be considered as the most important part. Controlling the software and hardware in a specific manner was one of the requirements in our team project. Moreover, we were required to draw a use case diagram and a simple test case diagram so that we could

better understand all the problems we had to deal with but also to easier follow the development of our test software.

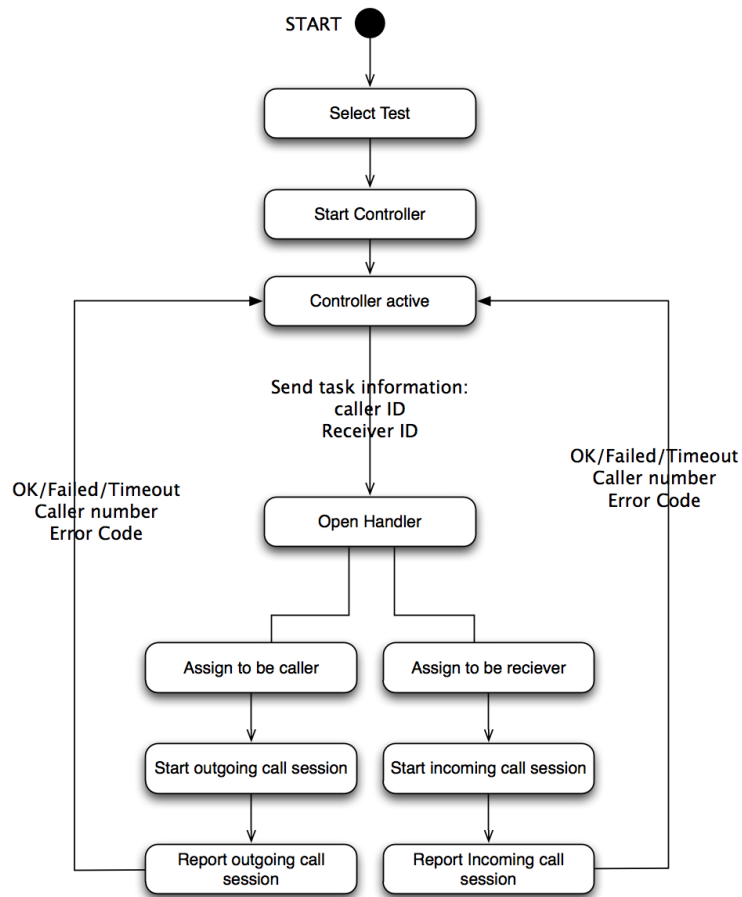


Figure 2: Simple algorithmic overview of a test case

2.2 Software requirements

Afterwards, as we had defined our logical approach to the problems, we had to choose the programming language to realize our ideas. Since we had the freedom of choice, between the three suggested programming languages Java, C++ and Python, we made a joint decision to use Python as the main programming language in our team project. One of the requirements was to finish the team project in time, therefore our decision to use Python is justified. Using Python we could work faster and integrate our subsystems more effectively [2]. Our programming language of choice is multi-platform, therefore our test software would be easy portable to other operating systems.

Likewise we had to decide how our test software will work. One of the requirements by Dennis and Konrad was to make the software capable of being run from the terminal. The

next requirement was to make an appealing GUI so that even an user without advanced Linux experience could handle the software and read out the results.

In addition it was required to log all the past tests. Later on a machine learning algorithm or some other intelligence could be applied to deduce some error behavior of the system (e.g. an intelligent algorithm could find that part of the system fail in a combined manner). To accomplish the logging of all the tests we had to use a database system. We decided to use MySQL since it is open source and well supported.

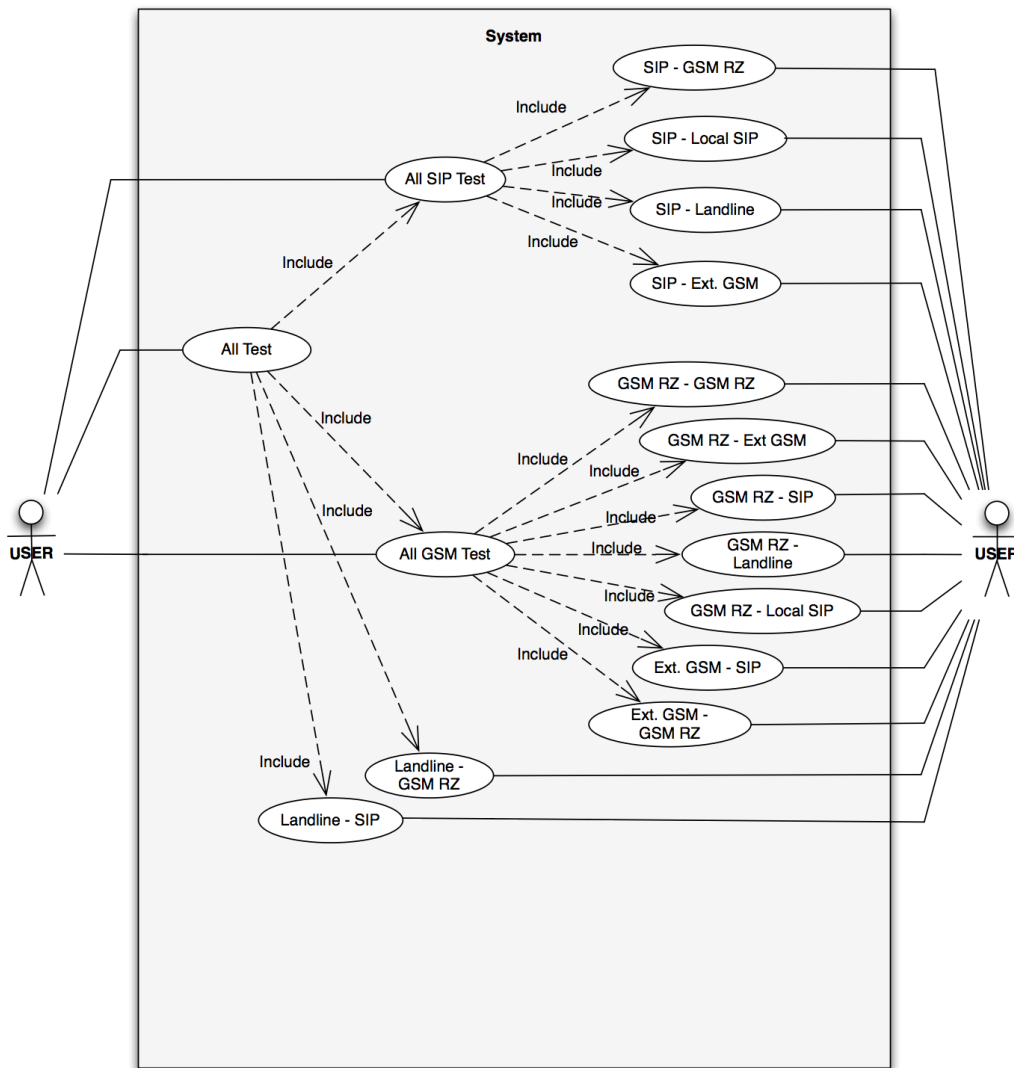


Figure 3: Test case diagram

2.3 Hardware requirements

Likewise the software requirements, we had hardware requirements as well. We were required to identify the hardware we will need to perform the tests. It was important to find old and cheap cell phones that could support *AT Modem* commands because our budget was limited.

A problem we had to deal with at the start was that the base stations are located at different geographical points which were not near to each other. No one should go everyday to the rooms where our cell phones are located only to change or charge the batteries. In the cable subsection we describe our approach to the charging battery problem. As we defined our requirements we continued with the process of developing the test software. During the development time we refined our requirements. In the next chapters we will explain our database, software and hardware design ideas.

3 Database design

As we mentioned in the software requirements section, we decided to use MySQL as our database system for storing the test information and results. It was not difficult to decide what database to use, since MySQL is one of the most supported database and one can find a library to use it with major programming languages. The key point in the design of our database was the simplicity and speed of accessing the data. We had decided to use seven tables. In the following paragraphs we will explain each table separately and its usage. The database design can be seen in figure 4.

The *PingResultTable* table has six attributes (*taskNo*, *sipServer*, *sipGate*, *unisip*, *gsmBox1*, *gsmBox2*), all of integer type. The *taskNo* attribute identifies the test number but not a single test (e.g. an operator user has selected three different tests to be executed, all of the three tests will have the same *taskNo* to identify them together as belonging to one test group and *taskId* identifies each single test and will be explained later). *sipServer* represents the Asterisk server ping result. *sipGate* is used to represent the SIP Gate server for the landline calls (<http://www.sipgate.de>). *uniSip* represents the ping results for our local University telephone network SIP server. *gsmBox1* and *gsmBox2* are the two single-chip Linux computers (BeagleBoard), that control two cell phones each one (i.e. they are also known under the name of *nanoBTSx controller*). *taskNo* is the primary and unique key in the table *PingResultTable*. Rest of the attributes (i.e. *sipServer*, *sipGate*, *uniSip*, *gsmBox1*, *gsmBox2*) are used to insert the ping results, if the assigned servers are reachable or not. Before any test attempt is made, our test software first tries to ping the servers. These results are then stored in the *PingResultTable*.

The *ErrorCodeTable* table defines all the possible test results in the system, in other words it represents a list with error codes with their appropriate descriptions and meanings. It consists of two attributes (*errorcode* and *description*), the first is of integer type and the second of varchar type (the description message is allowed to be only 100 characters long). The *ErrorCodeTable* table is used by the main test software (i.e. controller) to report the operator user what kind of error had appeared in the system.

The *DeviceAddressTable* is the table containing the location and identification data for each server and device. The table consists of seven attributes, *deviceName*, *portName*, *number*, *lastChange*, *username*, *password*, *server*. *deviceName* is the attribute with the name of the device or server (e.g. GSMRZ1 or landline), it is of varchar type. *portName* is the attribute field with the location address for a cell phone (e.g. */dev/ttyUSB1*) or 'localhost' instead of NULL value for a server, it is of the varchar type. *number* represents the number of the used service (i.e. number of the cell phone, SIP, etc.) and is of varchar type. *lastChange* is a time value and represents the date and time the given entry was modified (we had plans in future versions of our test software that if an device gets a new IP address assigned it automatically changes it in the database). *username* is the field with the username stored in for a server/service, like SIP and landline. *password* attribute stores the password information for the given service. The *server* attribute stores information about the location of the server, IP or DNS address of the server. All three fields, *username*, *password* and *server* are of varchar type. The information stored in the given table is used by the test software to obtain usernames, passwords and addresses of the used services for the tests.

The *ResultTable* table is used by the test system to store final results for the performed tests. Our given table consists of two fields, *taskID* and *result* and both are of integer type. For each test entry with unique *taskID* an error code is assigned in the *result* field, depending on the test results. Error codes found in the *ErrorCodeTable* table can be only assigned to this field.

The *TempTaskTable* table represents the table with the tasks the system has to execute next time the test software is started. The given table gets new data every time an operator user submits one or more test cases from the website to be executed. *TempTaskTable* includes four attributes, *taskID*, *taskNo*, *from*, *to*. Former two are of integer type and later two of varchar type. *taskID* and *taskNo* identify the test task to be executed, *taskID* is the unique primary key. *from* and *to* fields have to match the names given in *DeviceAddressTable.deviceName*, these two attributes specify the caller and callee devices/services. Consequently, after the tasks get executed, the test tasks are removed and the given table is empty again until next tests are added to it. However, all the test tasks even after deleting them from *TempTaskTable* are kept in the *TaskTable*. The reason why the authors of this project divided it into two tables was because of the database row selection speed. We had made the assumption that with time the database size will grow and therefore the database speed will not be the same as during the development period.

The *TaskTable* table, as mentioned before contains all the tests ever performed from the web site. It is made out of five attributes, *taskID*, *taskNo*, *from*, *to*, *timestamp*. The first four fields are the same as in *TempTaskTable*, however the last one, *timestamp*, is used to record the exact time when the test was performed.

The *GSMListPrefix* table contains the data about the GSM networks and their prefixes. It consists of two attributes, both of varchar type, *providerName* and *prefix*.

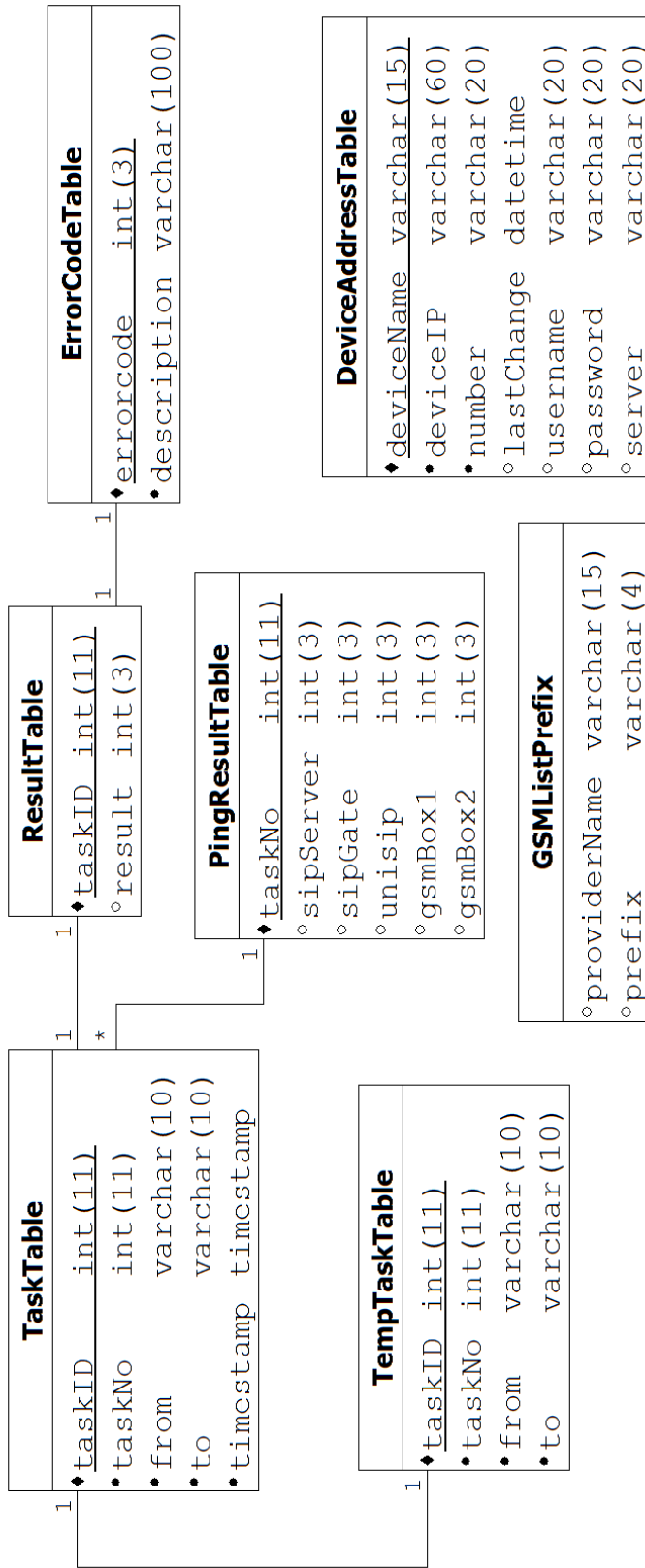


Figure 4: Database relationship diagram

4 Software design

Software design was the next step after we analyzed the problem and developed a plan how to proceed further. Good analysis and planning with poor algorithmic implementation is valueless. During the work on the project, we had spent most of our time for software design. We kept in mind that our software should satisfy major paradigms of software engineering, like compatibility, extensibility, modularity, reliability, security, fault-tolerance and usability. The software engineering design concepts were achieved following way:

- Compatibility - we used Python and MySQL which are multi-platform and work on major OS
- Extensibility - new parts of code can be easily added by just modifying the classes
- Mudalarty - the components are independent black boxes, they are tested and validated independently
- Reliability - we use mutex locks to perform tests and database transaction operations to insert data into the database
- Security - all communication channels, as well as the access to the web site, are encrypted with asymmetric key cryptography
- Fault-tolerance - the classes were designed to continue operating even if error events appear and handlers are logging all events
- Usability - we tried to create a simple user interface and easily to use for everyone

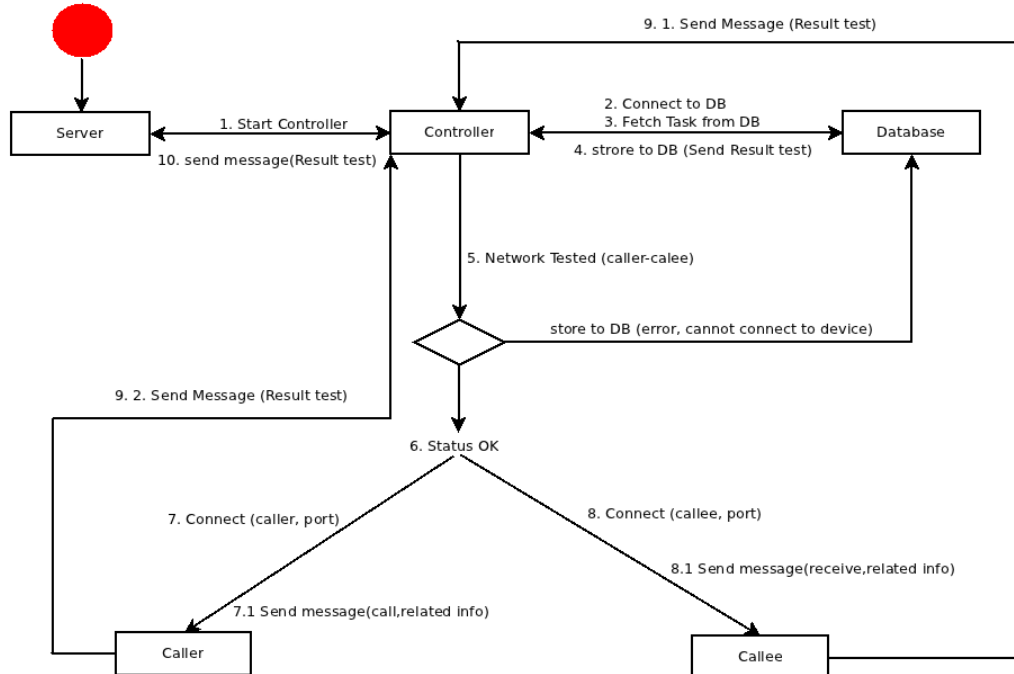


Figure 5: Working principle of the test software

The basic principle how the test software works can be seen in figure 5. The test software is started either manually from the terminal or using the web site. When the test software is started manually it is database dependent as well and therefore could not be used if the database is being maintained or not working. If it is started from the web site it connects to the database to get its tasks which have to be performed. After receiving the tasks it makes a simple network test by pinging all the servers. The ping results are stored in the database (in case the test was started from the web site). Then it proceeds with the tests by connecting itself to the handlers and sending them commands to perform the tests¹. At the higher level, these commands can be seen as requests for being the callee and caller. Meanwhile the handlers send their test results to the main test software which in return decides if the test result was successful or not. The result is written to the database (in case the software was started from the website), otherwise the results are displayed in the terminal window and the user who started it manually can see the test results. We will proceed with introducing the classes. The software class diagram can be seen in the following figure. More details for the classes, like the input/output can be found on our project's wiki page [4].

¹Before it connects to the handlers, it uses the ping results to see if the service/device is physically connected to the network.

4.1 Database access

Accessing the database is of critical value to our project, therefore we had developed our own class that limits the access to the database. In the process of developing our own class we used the MySQLdb library in Python [3]. The database class has two working modes, a normal working mode and a debugging mode. The difference between these two modes is in the output information. In case the error handling function raises an error and it is unknown, if the debug mode is set a complete back-trace of the error will be printed out. A developer can change the mode by setting the variable *debugMode=1*. The class diagram can be seen in the following figure. The method names are self-explanatory and

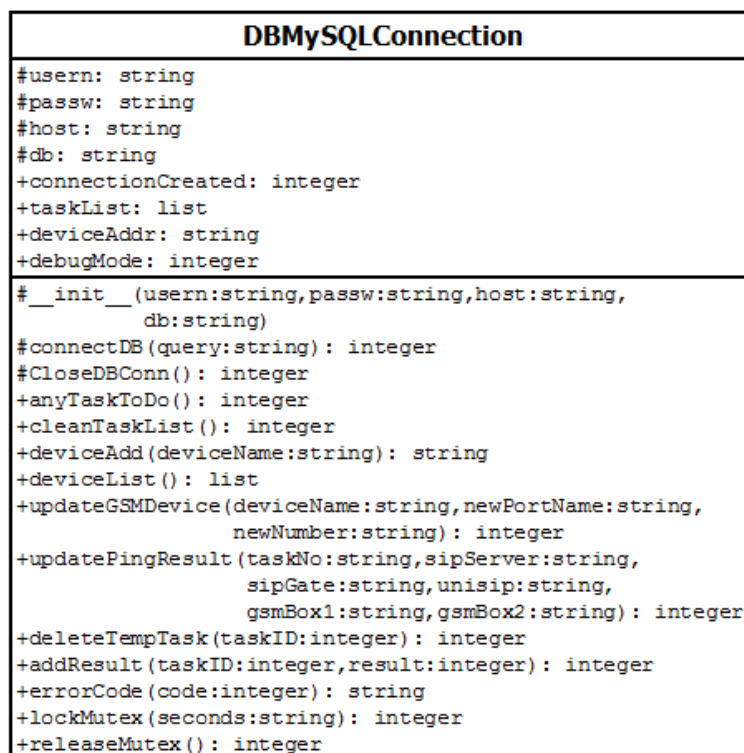


Figure 7: Class diagram for the dbClass

do not require extra explanations. All the outputs produced by the class can be found on the project wiki page [4].

4.2 Controlling the cell phones

Our first version of the developed program code for controlling the cell phones used predefined timed values to send commands instead of using a state controlled approach to confirm that every command was successfully received and executed by the cell phone. It meant we had to make an enormous number of assumptions. In comparison to our second approach, to build a state controlled cell phone control class, our first approach was inferior and slower. The state controlled method connected two cell phones, on the

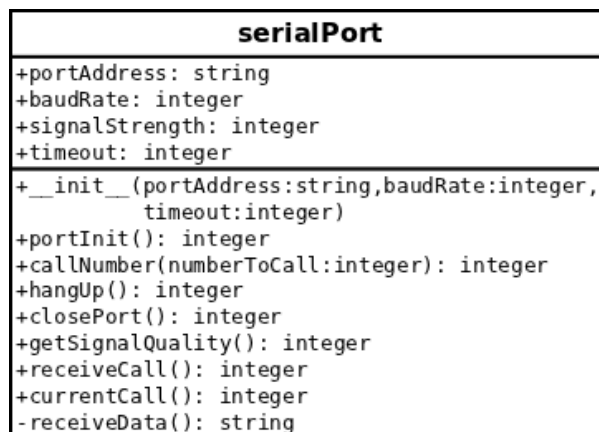


Figure 8: GSM class diagram for controlling the cell phones

same base station, up to 15 times faster than the timed approach. One can easily apply the class just by correctly defining the parameters: port address, baud rate and timeout. The former two are self-explanatory and the timeout parameter is used to define when the alarm function should raise a timeout exception. A timeout exception gets raised when the cell phone does not respond (i.e. when the cell phone enters a deadlock or delayed state). We had used the serial port library inside of Python although we use USB cables to connect to our cell phones. One should be aware that our USB cables create a virtual serial port. More details on class design and an example can be found on our project wiki [4].

4.3 Client and Server class

Our socket communication code is based on the example given in the Python socket manual [5]. We extended it into two classes, a client and a server class. We had used the TCP protocol to base our two classes on². The Server class can be seen in the following figure. The server class is implemented to accept only local connections³. First we determine our IP address and then create the socket to listen only for the same IP address (with a different IP address than the selected one a connection cannot be even established). One has to define the port on which the server object should listen. When receiving data one can easily define the timeout to be raised if data are not received in the timeout range or set it to 0 to infinitely wait for the buffer to be filled with received data. While testing the server class we had the problem to listen on the same port if the application was forcibly⁴ restarted in less than 60 seconds. We got the error message: *"Address already in use"*. This is not known as error behavior but rather an option to help the server to catch lost live packets (i.e. packets that are still in the network looking for it is goal destination). We solved the problem by changing the socket options with the

²TCP is reliable compared to UDP (i.e. transmitted packets get also delivered), packets are ordered when received and data are received in a stream (i.e. multiple packets can be read at once).

³More details are given in the section 7.1

⁴Manually closed using CTRL+C and run again.

`SO_REUSEADDR` parameter. This enabled us to get around the error when we tried to restart our server application. Before solving the problem without using the socket parameter, we had another solution to get around this problem by killing the application running the port, this old method is obsolete now. In the process of testing the client

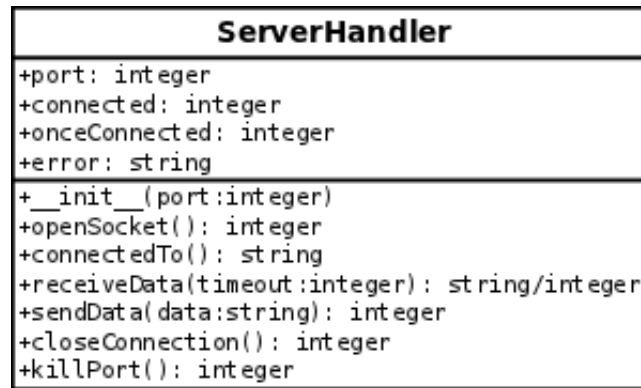


Figure 9: Server class, used by the server application

class we did not have any major problems. The only major flow we had to debug was when one of the sides disconnects that we get out of the waiting loop if the timeout variable was set to 0 (i.e. infinite waiting loop). The client class can be seen in the following figure. To initialize the client object one needs to define the IP address and the port of the server application listening on it. Once an instance of it is created and

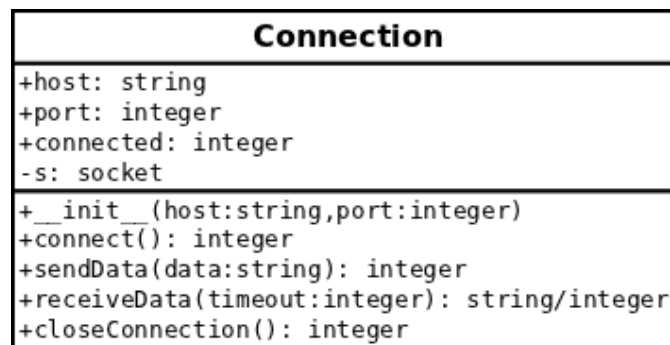


Figure 10: Client class, used by the client application

loaded with the IP address and the port, one needs to call the `connect()` method. The method will produce an integer based on its connection state. Output information and the programming code can be found on our project wiki page [4].

4.4 Ping class

Before making any test and establishing a connection we were required to ensure that the server is online. The best way to assess the liveness property was to ping the server computer running the required service. Once the class is properly defined, we could easily

set the number of ping tries. A ping timeout response was set up to 2 seconds. For more details and insights, one can read more about it on our wiki page [4].

Ping
+pingAddress: string
+ping(numberOfTries:integer): integer

Figure 11: Ping class, used by test software

4.5 Data logging

If errors appear it is important to reconstruct the events that led to the misbehavior of the software. One of the best ways to reconstruct the events was to log events for different blocks of programming code. We had used the logging class to follow our handler code run on the BeagleBoard. In case there is an error we could look inside of the log files and track the error. How the class works and what kind of outputs it produces can be found on our project wiki page [4].

Logging
+writeToFile: string
-justStarted: integer
+__init__(logFileName:string)
+logEvent(event:string)
+closeLogging()

Figure 12: Logging class

4.6 SSH Tunnel Class

Since security played an important role in our team project. We decided to encrypt all of our data that was not processed on our server computer. The simplest solution to this problem was to build an SSH Class that could open and close a local forwarding port. All data sent through the created port is encrypted until it gets to its destination location.

SSHTunneling
+lPort: integer
+rPort: integer
+rServer: string
+tunnelStarted: integer = 0
+init(localPort:integer,remotePort:integer, remoteServer:string): integer
+startTunneling(): integer
+killTunneling(): integer

Figure 13: SSH Tunnel class

4.7 USB Cell phone detection class

Since we had used cables to connect the cell phones with the computer, usually the devices got their own port addresses. They were automatically assigned by the operating system, either after the cables were plugged into the USB port or after a system reboot. One of the problems we had to deal with was assigning the right cell phone (i.e. with the appropriate GSM network) to the corresponding port address. The operating system

usbDetect
#portAddress: string
#initDB(): integer
#initUpdate(deviceName:string,newPortName:string, newNumber:string): integer
#portInit(): string
+isInteger(x:string): boolean
+findIMEI(): string
+findNumber(): string

Figure 14: USB cable detection class

randomly assigned the port names after every reboot. We were looking for a solution to prevent this misaddressing of the devices. Our solution was to recognize every device and update the port address in the database. The principle how we identify the cell phones is by their calling numbers in the database. More details can be found on our project wiki page [4].

4.8 Truth table class

The truth table class was built to identify the broken and working parts of the system. It requires the list with test results to be present to be operable. Then the class tries to

trueTable
#resultsList: list
#initDB(): integer
+lookingBTsname(btsname:string): boolean
+initTrueTable(): list

Figure 15: Truth table class

identify the broken parts of our telecommunication network. The class can easily identify how many nanoBTSs are installed in the network and derive a decision which part of the network is broken. All the test results are stored in a list and can be easily read by calling the *initTrueTable(x)* function. More details can be found on our project wiki page [4].

4.9 Init Test class

The main purpose of the class is to get device data from the database and to process it. The processed data get forwarded to the controller class and in the end the class fetches the results from the test. This class contains the *smart test* functionality. It selects automatically the important tests to perform. In the next step it tries to identify the problem in the network. More details can be found in the *smart test* description.

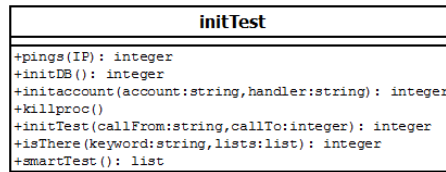


Figure 16: Init test class

4.10 Controller class

The controller class is used to assign jobs to handlers (in other words, which one is going to be the caller and callee). Simultaneously, it defines the port addresses for the communication between the handlers and the main test software (controller). If

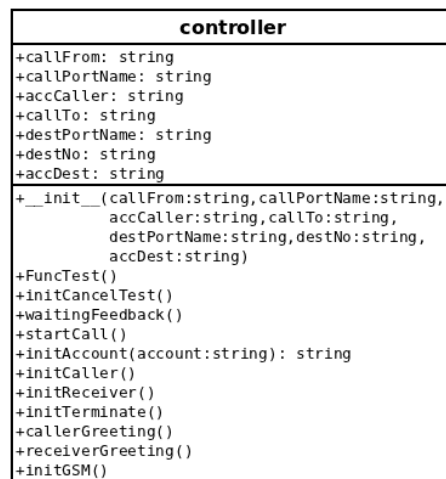


Figure 17: Controller class

the callee or the caller are nanoBTS controller boxes (i.e. BeagleBoards outside the Rechenzentrum), it will first create an SSH connection to make a tunnel before the local socket connection is created. Then the controller class sends all the required data regarding the test tasks to the handlers.

5 Hardware design

In our team project we had the option to choose all the required hardware ourself beside the two BeagleBoards, which we were supplied by Konrad and Dennis. Since one of the project goals was to reduce the costs as much as it was possible, we had tried to use some of the leftovers found in our lab.

5.1 BeagleBoard

“The BeagleBoard is an OMAP3530 platform designed specifically to address the Open Source Community. It has been equipped with a minimum set of features to allow the

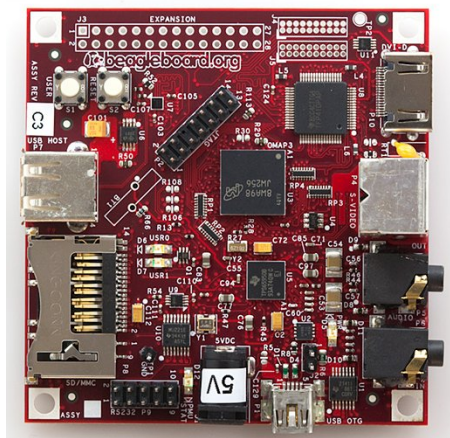


Figure 18: BeagleBoard, a Linux-on-chip board where our controller software runs the GSM device

user to experience the power of the OMAP3530 and is not intended as a full development platform as many of the features and interfaces supplied by the OMAP3530 are not accessible from the BeagleBoard” [11]. We run on it a special precompiled version of Ubuntu for the ARM processor type. The Linux system boots up from an SD Card. The board has an USB hub and network port attached to it. In our project it is connected to our internal university LAN network and to a cell phone. We positioned the two BeagleBoards in rooms where we had LAN access and GSM signal coverage of our two local base stations.

5.2 Cell phones

Our first attempt was to control a Nokia cell phone 3310 with the supplied USB connection cable. The protocols used by old versions of Nokia cell phones, as the 3310, use the F-Bus protocol. It was not easy to work with. After performing various experiments we succeeded to send and to read SMS messages. Later on we found out that it was not possible to send commands for receiving and making the calls. In the meantime we found two Siemens phones, one M45 and S55. The first one, Siemens M45, had a cable supplied with it and it was not difficult to control it with the standard set of AT modem

commands. At the start we did not have a cable supplied for the Siemens S55 phone. We controlled it over the Bluetooth port.

5.3 Cables for the cell phones

Due to the fact that we had used 5 cell phones on a single computer, the best solution was to order 5 USB cables. Konrad bought 5 cables for 5 Siemens S55 cell phones. All of the cables have an USB2Serial chip converter inside of them. Once they were plugged into the USB port, Ubuntu automatically recognized the cables and installed the drivers. The virtual serial ports were created and could be found on `/dev/ttyUSBx`, where `x` is the automatically assigned number for the port. Some of the cables had the capability to charge the Siemens S55 phones. Konrad had opened several cables to solder the power supplies to some contacts and the problem was solved for all of the cables.

5.4 Server

We were given an old Pentium 3 computer where we installed Ubuntu Linux. Configured the Apache web server and MySQL. Afterwards we installed the Python on it and all the required libraries⁵.

⁵Required libraries are mentioned in section 9.1.

6 Communication protocol

A communication protocol represents a set of well defined rules by whose help two or more computing systems exchange information in-between. When defining these rules, it is important to define a limited state space for every possible event, no matter did we get the appropriate response from the other side. Our approach to this problem was to build a simple synchronous protocol, where every expected message is confirmed or otherwise the connection between two sides is immediately terminated. Since designing protocols is a demanding and challenging topic which requires years of experience and verification, we do not expect that we had developed the best possible and an optimum protocol⁶. In the following paragraphs we will try to clarify how our protocol works. Before we start to go into detail how the protocol works, it is important to remember that we differentiate two sides, handler and the controller side. The handler side represent the device that physically handles the call (e.g. the BeagleBoard) whereas the controller (i.e. the main test software), is the test software controlling the handler side and assigning the task to it.

6.1 Communication between the handler and controller

The handler side is always in the waiting mode, by waiting we denote the mode where the socket is already created and it is waiting for a connection to be accepted at the defined port. The controller initiates a socket connection to the two handlers. Subsequently, after the connection has been established, it is waiting for a message to be received. The first message has to be 13 characters long and include the following content *HELLO HANDLER*. Thereupon, after the message has been validated, the handler side sends the controller side a response, *HELLO CONTROLLER*. We call this first message exchange the initialization. Now the controller side has to decide which of the two handler's will be the caller/callee whereas the other handler will be the opposite. Let's assume the controller sends to the first handler the message *RECEIVER* and to the second one the message *CALLER/#*, replace the callee number with the # sign. In the meantime, both handlers initialize the software required to make the call and to receive the call. Asynchronously they respond back to the controller their successful initialization. The successful initialization is reported by sending *RECEIVER READY* and *CALLER READY*. After receiving the mentioned messages, the controller first sends the callee handler the message *RECEIVE START* and then to the caller handler, the message *CALLER START*. As a result of these messages, the handlers enter the receiving, respectively calling state. In the given states two timeout timers gets activated. These timers are responsible for the case if the physical connection between the callee and the caller are not successfully established or terminated⁷. Afterwards, depending if the physical connection between the handlers (i.e. the callee and the caller) was successfully established or not, the handlers report their corresponding state with a message to the controller. The message is of the form *CALL OK*, meaning the handler successfully es-

⁶Design concepts and paradigms for the protocol design have been used from the "Network Protocol Design and Evaluation" course, lectured by Dr. Stefan Rührup

⁷The client and server classes responsible for the communication have timeout timers as well for the case if the connection between the controller and handlers are broken.

established a physical connection with the other handler, or of the form *CALL NOT OK*, meaning a physical connection was not successfully established on the given handler. The controller considers only a test successful if both handlers report with *CALL OK*. The test software ends the established connection with the handlers by sending them the *TERMINATE CONNECTION* command. After the handlers have terminated the connection, they enter the waiting for a new connection state and the process starts from beginning again. If the states are not entered in the specified order the connection is immediately terminated and the state machine is in the waiting for a new connection state⁸.

⁸It cannot be seen in the protocol flowchart but one should keep in mind it works like a well defined state machine.

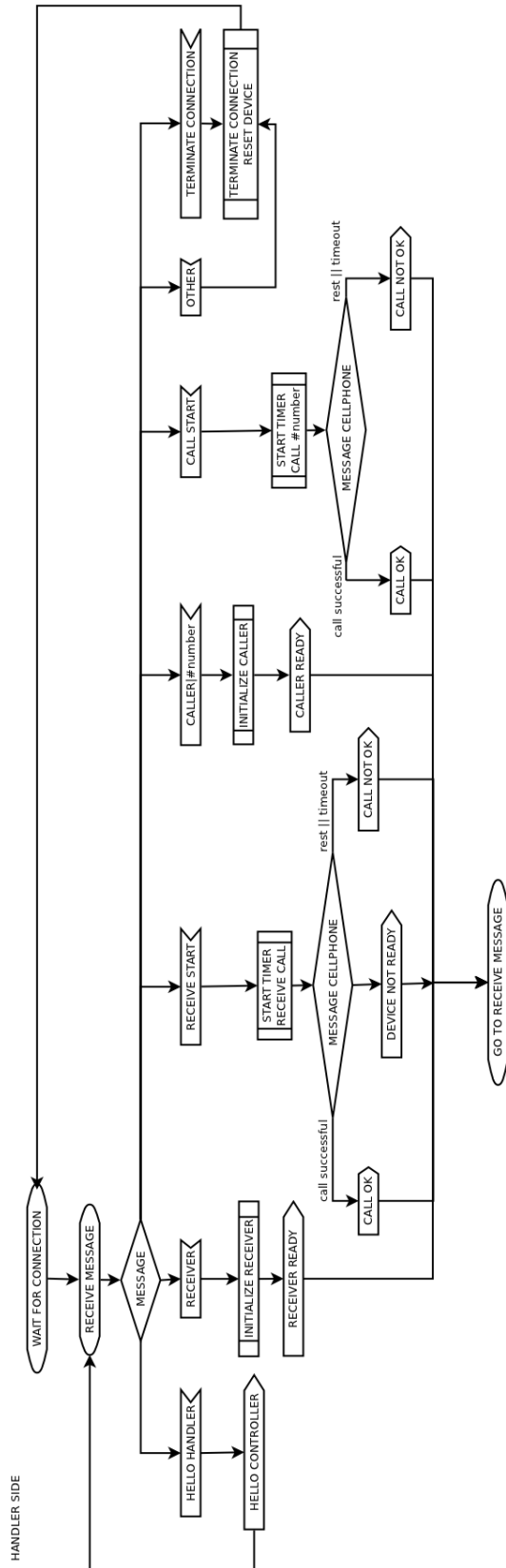


Figure 19: Flowchart of the protocol on the handler side without the state representation

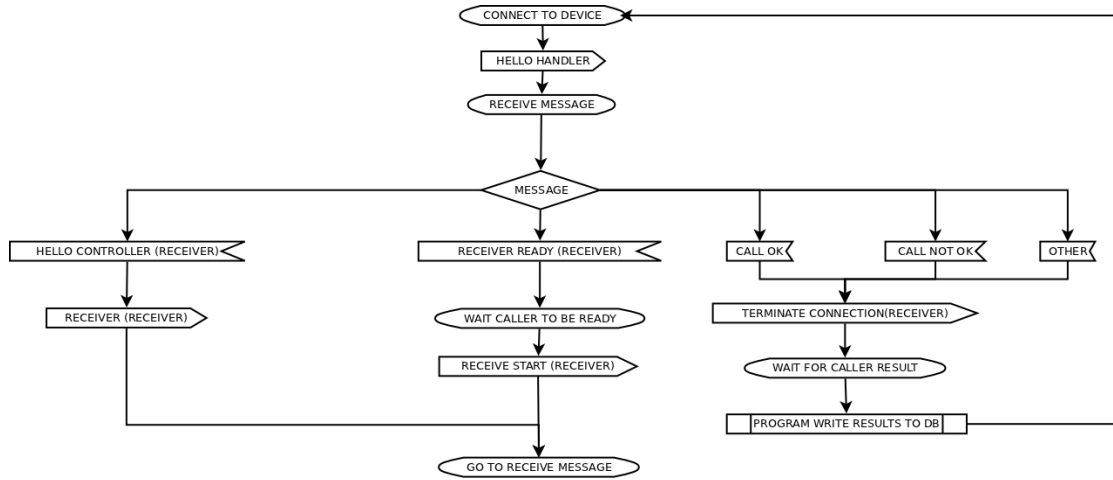


Figure 20: Flowchart of the protocol on the controller side for the caller without the state representation

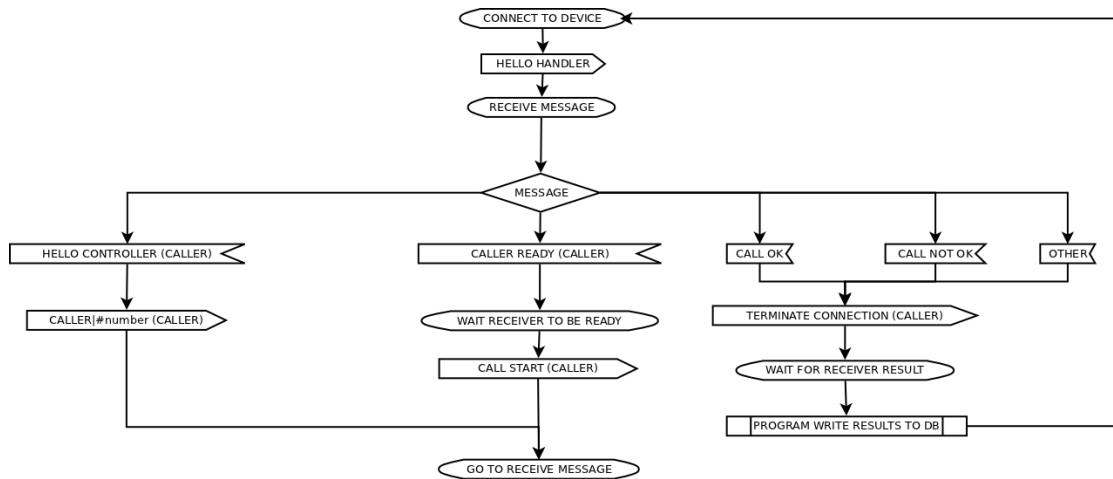


Figure 21: Flowchart of the protocol on the controller side for the receiver without the state representation

6.2 Verification of the protocol

“SPIN is a model checker - a software tool for verifying models of physical systems, in particular, computerized systems. First, a model is written that describes the behavior of the system; then, correctness properties that express requirements on the system’s behavior are specified; finally, the model checker is run to check if the correctness properties hold for the model, and, if not, to provide a counterexample: a computation that does not satisfy a correctness property.” [6]. We modeled our simple protocol in SPIN using the programming language PROMELA [6]. Since PROMELA is similar to C it was not possible to ensure 100% matching with Python but we had made the assumptions of it.

We modeled both sides, server and client side. As well as the server side being a caller and a callee. It was important to find out if our protocol is deadlock or delayed state free. For more details our model can be found on our wiki project page with the PROMELA source code [4]. We had built in a 50% random probability that the call test will not be successful, to make the model even more realistic. Our protocol idea was deadlock free and the verification results prove it. After we had modeled the basic idea we had written the code that implements our idea. The Python code resembles some kind of a state machine which remembers the last state and what the next state should be in case of receiving corresponding message. Otherwise it enters the exit state and then the start state.

```
(Spin Version 6.1.0 -- 2 May 2011)
+ Partial Order Reduction
Full statespace search for:
  never claim - (none specified)
  assertion violations +
  cycle checks - (disabled by -DSAFETY)
  invalid end states +
State-vector 44 byte, depth reached 65, errors: 0
  40 states, stored
  3 states, matched
  43 transitions (= stored+matched)
  90 atomic steps
hash conflicts: 0 (resolved)
  2.195 memory usage (Mbyte)
unreached in proctype Server1
  (0 of 36 states)
unreached in proctype Server2
  (0 of 36 states)
unreached in proctype Client
  (0 of 67 states)
pan: elapsed time 0 seconds
```

7 Security and safety of the system

Safety and security of the software plays a major role in our project. It is of vital importance that only as few as possible people have access to our test system since the resulting data could be exploited to plan an attack (e.g. assume the University alarm system uses the SIP gateway to connect to the outside world and to alarm the police, if one knows that the SIP gateway is not working properly, a burglar could plan to rob the University building just at that moment). Therefore the choice to go Open Source is justified due to the fact that one should know how every single detail of the system works. All the time, while we were working on the project, we were made aware of this issue by Dennis and Konrad. We decided to use asymmetric key cryptography, where each side has two keys (private and public). In the next sections we will explain in more details how we applied the methods.

7.1 Encryption of the communication channels

At first we thought to encrypt the data before sending them but since none of us was an expert on encryption standards the idea was rejected. Alongside the fact that none of us had been an expert in the field of cryptography, we were neither experts in the field of Internet programming. One could find maybe a way to disable our server software with various hacking methods (e.g. trying to open the port until the system runs out of memory and in our case the system which we used on the handler side was a BeagleBoard with ARM architecture running on a single chip TI OMAP processor, refer to the picture in figure). We had to eliminate even the slightest possible threat in return for spending more time for debugging the test software system. Despite we were aware of all these facts, we had to choose one of the plenty implemented encryption standards on Linux. Dennis and Konrad suggested using the SSH Tunneling method.

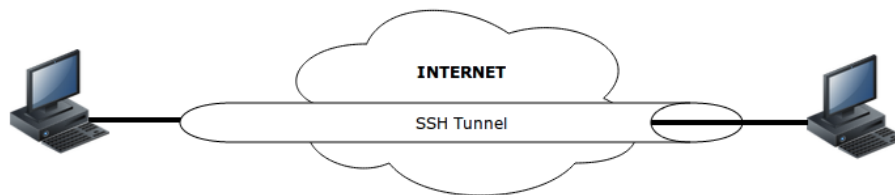


Figure 22: SSH Tunnel, all the communication inside the tunnel is encrypted

Using the SSH Tunnel port forwarding method we could hide the real port we had used for our socket connection. On the other hand we could force the socket to accept only local connections (i.e. from the machine where the handler software was running). The SSH Tunnel port forwarding method creates an encrypted tunnel between the two computers and then it creates two ports, one on the local and remote computer. All the data sent through the port on the local machine appear on the port at the remote machine.

The first problem we faced was that SSH required the username and password every time we tried to make an SSH connection. We could avoid this problem by copying the public key from our server (where our test software runs) to the BeagleBoard [7]. This can be

performed by executing the following commands in the terminal shell. One has to create first the private and public keys on the local machine (i.e. server computer, where the test software runs):

```
refik@ubuntu:~$ [Note: You are on local-host here]

refik@ubuntu:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/refik/.ssh/id_rsa): [Enter key]
Enter passphrase (empty for no passphrase): [Press enter key]
Enter same passphrase again: [Press enter key]
Your identification has been saved in /home/refik/.ssh/id_rsa.
Your public key has been saved in /home/refik/.ssh/id_rsa.pub.
The key fingerprint is:
33:b3:fe:af:95:95:18:11:31:d5:de:96:2f:f2:35:f9 refik@ubuntu
```

Then one needs to copy the public key to the remote machine (BeagleBoard) using `ssh-copy-id`:

```
refik@ubuntu:~$ ssh-copy-id -i ~/.ssh/id_rsa.pub remote-host
refik@remote-host's password:
Now try logging into the machine, with "ssh 'remote-host'", and check in:

.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.
```

After we have created the public and private keys, and copied the public key on the machine to which we want to connect, we can test if we can make an SSH connection to the remote machine:

```
refik@ubuntu:~$ ssh remote-host
[Note: SSH did not ask for password.]

refik@remote-host:~$ [Note: You are on remote-host here]
```

The test was successful. We tested it with our SSH Tunnel port forwarding class and it worked perfectly.

7.2 Security on the web site

Aside from having secured the data communication channels between various parts of our software (the handlers and the controller), it was crucial to ensure all the communication between test user's browser and our server. Therefore we had used the *https* protocol and the *.htaccess* file to password protect the web site so only the privileged users have access to our test system.

7.2.1 Configuring the http secure protocol https

Securing the communication channels without making certain the web site is safe would be worthless. We decided to use the *https* protocol instead of the *http* since a person in the middle could sniff our data (e.g. a person is connected with his/her smart-phone over an unprotected wireless network) [8]. At the same time the web site should be accessible

only by the authorized personnel. Our first approach to this problem was to build a PHP page with *MD5* hashed passwords, however we got a suggestion by Konrad and Dennis to use a safer encryption method implemented in the Apache web server software, *.htaccess*. By using these two techniques we protected the web site of some vulnerabilities known to us. If the web site will be only accessed from our local university network, we can additionally add an IP filter mask as well. In the following paragraph we will explain our procedure how to generate the keys and to enable the https protocol.

First we want to generate a server key by typing the following command:

```
openssl genrsa -des3 -out server.key 4096
```

This will generate a 4096 bit long private server key, one is asked to enter two times a password for the *server.key*. Using the generated private server key, we will create a certificate signing request, *server.csr*. We were prompted with a series of questions like country, state, organization name and etc which we had to enter to resume.

```
openssl req -new -key server.key -out server.csr
```

In the next step we had to sign the certificate signing request and enter the amount of days for how long it should be valid. In our case we entered the duration of one year, one can make it for longer periods as well (i.e. the amount of 365 has to be changed).

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

We were asked to enter the password again for *server.key*. After we have completed this step we had to make a version of the *server.key* which did not require a password, *server.key.insecure* and we will rename the files appropriately.

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

The generated files are very sensitive, since they are our keys. After these steps were completed, we had generated 4 files: *server.crt*, *server.csr*, *server.key* and *server.key.secure*. Now we need to enable the SSL engine on the Apache web server. We copied *server.key* and *server.crt* into */etc/apache2/ssl*.

```
refik@ubuntu:/etc/apache2$ sudo mkdir ssl
cp server.key /etc/apache2/ssl
cp server.crt /etc/apache2/ssl
```

Then we enabled SSL by typing in *a2enmod ssl*, “it is simply a general purpose utility to establish a symlink between a module in */etc/apache2/mods-available* to */etc/apache2/mods-enabled* (or give a message to the effect that a given module does not exist or that it is already symlink-ed for loading)” [8].

```
refik@ubuntu:/etc/apache2/ssl$ sudo a2enmod ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and create self
-signed certificates.
Run '/etc/init.d/apache2 restart' to activate new configuration!
```

In the next procedure we had to establish a symlink from the 'available' default-ssl file to the 'enabled' file [8]. Then we created a folder where our secured PHP files will be located (e.g. <https://some-domain-name.com/test-software>).

```
refik@ubuntu:/etc/apache2/ssl$ sudo ln -s /etc/apache2/sites-available/default-ssl /etc/apache2/sites-enabled/000-default-ssl
refik@ubuntu:/etc/apache2/ssl$ cd /var/
refik@ubuntu:/var$ sudo mkdir www-ssl
```

We had backed up our old configuration files for the virtual hosts, for the case if we damage the Apache configuration files. Then we edited the *default-ssl* file.

```
refik@ubuntu:/var$ cd /etc/apache2/sites-available
refik@ubuntu:/etc/apache2/sites-available$ sudo cp default default_original
refik@ubuntu:/etc/apache2/sites-available$ sudo cp default-ssl default-ssl_original
refik@ubuntu:/etc/apache2/sites-available$ sudo vim default-ssl
```

Only the beginning of the file is listed here and we have modified the line starting with *DocumentRoot* and `<Directory /var/www/>` from *DocumentRoot /var/www* to *DocumentRoot /var/www-ssl* and from `<Directory /var/www/>` to `<Directory /var/www-ssl/>` (i.e. we had to redefine the location of our SSL directory).

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www-ssl
    <Directory />
        Options FollowSymLinks
        AllowOverride None
    </Directory>
    <Directory /var/www-ssl/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
```

One should keep in mind that the port 443 should be free for Apache to use it. In the proceeding step we had to ensure that Apache listens on the given port for a *https* connection. One could test that by going into the */etc/apache2/ports.conf*.

```
<IfModule mod_ssl.c>
# If you add NameVirtualHost *:443 here, you will also have to change
# the VirtualHost statement in /etc/apache2/sites-available/default-ssl
# to <VirtualHost *:443>
# Server Name Indication for SSL named virtual hosts is currently not
# supported by MSIE on Windows XP.
Listen 443
</IfModule>
```

In our case it was set up correctly, since the command: *Listen 443* was present. In our last configuration step we had to edit *default-ssl* file to define the correct locations of our keys and to ensure the SSL engine was turned on.

```
refik@ubuntu:/etc/apache2/sites-available$ sudo vim default-ssl
```

The following part of the file had to be found and modified according to our locations:

```
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2.2-common/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/apache2/ssl/server.crt
SSLCertificateKeyFile /etc/apache2/ssl/server.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
```

Finally we had configured our server and can proceed with the restart of the apache web server. We created a test web site `/var/www-ssl/index.php` and navigated our browser to `https://localhost`. The test was successful!

```
refik@ubuntu:/etc/apache2/sites-available$ sudo /etc/init.d/apache2 restart
* Restarting web server apache2 [Sat Oct 08 21:52:51 2011] [warn] _default_ VirtualHost overlap on
port 443, the first has precedence
... waiting [Sat Oct 08 21:52:52 2011] [warn] _default_ VirtualHost overlap on port 443, the first has
precedence [ OK ]
refik@ubuntu:/etc/apache2/sites-available$
```

7.2.2 Password protecting the web site using `.htaccess`

Aside from using a secure communication protocol on the web, *https*, it is important to ensure that only permissioned users gain access to the web site. We had achieved it using the `.htaccess` file. However, to enable the use of Apache `.htaccess` files, we will have to reconfigure the Apache configuration files again. *root* access will be required. First we have to edit the `/etc/apache2/sites-available/default-ssl` file. Find the following lines and modify the *AllowOverride None* to *AllowOverride All* like in the given configuration segment:

```
<Directory /var/www-ssl/>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride All
    Order allow,deny
    allow from all
</Directory>
```

This will tell Apache web server that it is okay to allow `.htaccess` files to over-ride previous directives. We must reload the Apache web server before the changes can take effect. We can do it by typing:

```
sudo /etc/init.d/apache2 reload
```

The next step is to go to the directory where our test software web page is located (e.g. `/var/www-ssl/testsoftware`) and to create a file called `.htaccess`. Please insert the following code segment inside the created `.htaccess` file where `/var/www-ssl/testsoftware/.htpasswd` is your full path address to `.htpasswd`:


```
AuthUserFile /var/www-ssl/testsoftware/.htpasswd
AuthName "Authorization Required"
AuthType Basic
require valid-user
```

Then in the next step, create another file called *.htpasswd*. After you have created it, we will add the usernames that should have access to the web site. We do that by typing the following command, where you can replace *konrad* with any other combination of letters which will represent your username:

```
refik@ubuntu:/var/www-ssl/testsoftware$ sudo htpasswd -c .htpasswd konrad
```

Afterwards, you will be required to type twice the same password for the username you want to create, in this case *konrad*. “The *-c* flag is used only when you are creating a new file. After the first time, you will omit the *-c* flag, when you are adding new users to an already-existing password file. Otherwise you will overwrite the file!” [9]. You can add as many users as you wish, do not forget to remove the *-c* flag when you do it. In the last step, we have to modify the */etc/apache2/apache2.conf* file and to add at the end of it the following code segment where */var/www-ssl/testsoftware* is the full path to your web page directory where you put the *.htpasswd* file:

```
<Directory /var/www-ssl/testsoftware>
AllowOverride All
</Directory>
```

We are done with editing. All we have to do now is to restart the Apache web server. We can do that by typing:

```
sudo /etc/init.d/apache2 restart
```

You can test it now by opening a new browser tab and navigating to *https://localhost/testsoftware* (keep in mind to replace *testsoftware* with your name of the folder where the web page is located). If you configured everything properly, you should get a dialog where you can enter your created username and password and try to login.

8 Web page

One of the requests of our team project was to build a test system that could be started from the web site. Since we used the Open Source platform to base our project on, it was certain we will use it for the web site as well. The dynamic parts of the web site were programmed using PHP and JavaScript. The GUI was done using CSS. The web site opens TCP/IP sessions between itself and the Python test software. Due reasons explained in the section above, a test user needs first to enter his username and password to access the web site. Then a test user can manually select what type of tests he wants to perform or he can select already defined test, like the simple, smart or full test. (Describe here these three type of tests). Data about the performing tests are inserted into the database only in the case if the mutex lock for the web site can be obtained⁹. This way we can avoid inserting data about the test in case there is already a test user on the website performing some tests on the system.

8.1 Communication between the web page and the test software

Our first idea was that the PHP file starts the test software. However, parts of our test software open new terminal windows and since PHP has restrictions for starting GUI applications our approach was condemned for a failure at the start. We had to deal with this problem and our solution to it was to write a little Python script that will run in background and start our test software when required. Once a person starts the test over the web site, it automatically connects to the Python script over an TCP/IP socket. Before being able to start the test software one needs first to obtain the mutex lock on the web site and to check if there is a mutex lock for the test software running. Using this approach we can ensure that only one user at the time can be on the web site and run only one instance of the test software. In the next step we send the Python script a message to start the test software. The test software obtains a mutex lock as well. When the test software is started the web page checks if a software lock is obtained. Once it is obtained we can proceed with creating a new socket connection between the web site and the test software. Our TCP/IP communication between the web site and the test software is not encrypted since both the web page and the test software run on the same server computer. The mutex locks are freed after the tests are performed. Our test software has a timeout timer in case that the web site hangs or somehow the socket connection breaks where it automatically shuts down.

8.2 Results on the web page

All the performed test results are displayed on the web site. The results are displayed in real time after each selected test case is performed. After all the test cases have been performed a topological picture is generated which represents the current state of the system, this can be seen in the following figure. Afterwards, when the result picture is generated, the test user can easily see what is wrong in the system. Various icons represent different subsystems. Reading the test results is as simple as looking at the

⁹The mutex lock will be explained in the next subsection.

icons and identifying if they have: a green plus signs (i.e. working properly), a red minus sign (i.e. not working properly) and a yellow exclamation mark (i.e. it was not tested).

- Triangles represent BTS stations
- Cell phones represent the external networks (E-Plus, Vodafone, T-Mobile and O2)
- Telephone represents the landline and a telephone with a mortarboard the University telephone network
- Servers represent the OpenBSC and LsfKs-Asterisk
- Two monitors represent the SIP system

The inference mechanism works as following: if a test case works, we can conclude that the subsystems connected in-between the two ends are working properly as well. We use the pChart library¹⁰ to generate the topological picture of our telecommunication system [10].

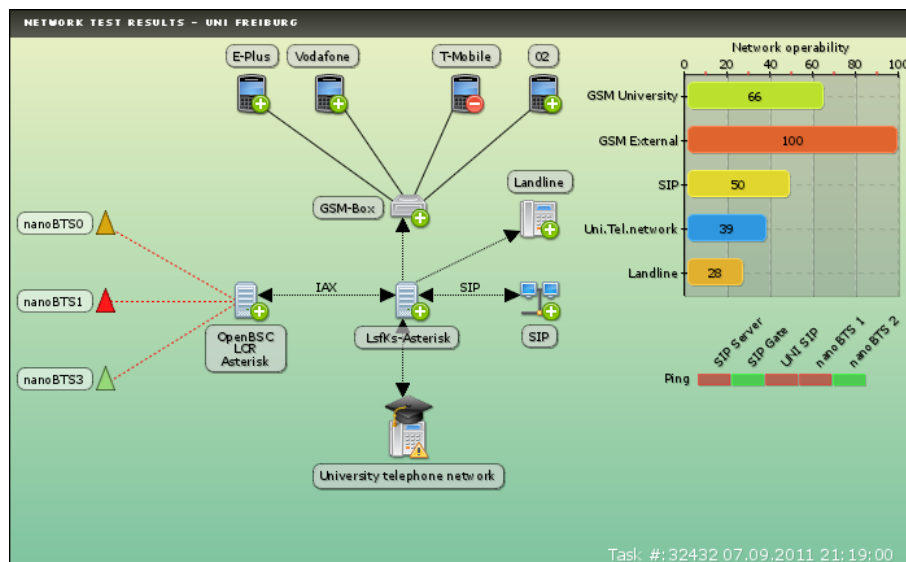


Figure 23: Result image showing working, defected and not tested subsystems

On the right side of the result picture the test user can immediately identify the network operability in percentage¹¹. Below the network operability statistics are the ping results statistics located. If one of the fields is red it means the subsystem is not online or cannot be seen by our server computer where the test software is located.

¹⁰It is under the GNU GPLv3 license and our project is nonprofit!

¹¹The test user has to take into account that this percentage is only valid if a full test is performed.

9 Employing the test software system

In this section the reader can find out how to install and how to use the test system. Our goal was to make a multi-platform test software, however we tested it only under Ubuntu 11.04 32 bit Linux OS and the given instruction manual is only tested under that OS. The test software performed well, both on PC and MAC computers. One should keep in mind that some of the libraries we had used do not work under the 64 bit version of Linux OS.

9.1 Required software and libraries

In the next subsections, we will guide you how to install all the required software and libraries to flawlessly run our test software on your employed server. You will be required to have *root* access privileges and to open a new terminal window where the commands will be typed in.

9.1.1 Python installation

Python was our programming language of choice¹². The required version of Python is 2.7. One can easily install python by typing the following commands:

```
sudo apt-get update
sudo apt-get install python2.7
```

It will take a short amount of time to be installed. You will be required to enter the *root* password.

9.1.2 Apache Web server installation

We had decided to use the Apache web server because of its wide support on the Internet and safety reasons. If there are any bugs or security flaws, the patches are easily installed with the Ubuntu update manager. The Apache web server can be easily installed by typing the following command:

```
sudo apt-get install apache2
```

You might be required to follow other installation instructions printed on the terminal screen. After the installation has completed successfully, one can test if it works by going to the following web address: *http://localhost*. For configuring the *https* please go to the section 7.2.

9.1.3 SSH

Secure Shell (SSH) is a network protocol for secure data communication between two computers inside of a network. All computers are required to have SSH installed on it. You can easily install it by typing the following command:

```
sudo apt-get install ssh
```

¹²We had explained earlier why we have decided to use Python.

9.1.4 MySQL database and MySQLdb library

The MySQLdb library is required to perform various operations on the MySQL database within Python. We used the MySQLdb library instead of the native MySQL C API `_mysql` library to make the code cleaner and more portable. We suggest you to install first the MySQL database on the server computer. If you have installed MySQL you can skip the next part. To start the installation process one can type the following commands:

```
sudo apt-get install mysql-server
```

You will be required to enter the Linux `root` password. At some point during the installation process, you will be required to enter the password for the MySQL database. After you have performed the above step, we can proceed with the MySQLdb library installation. By typing:

```
sudo apt-get install python-mysqldb
```

If the `python-mysqldb` name has changed, one can easily find the correct name of the file by issuing the following command:

```
apt-cache search MySQLdb
```

By typing in the commands given above, you should have successfully installed the MySQLdb library.

9.1.5 Serial port library

The serial port library is required for the cell phones to communicate with the server computer and the BeagleBoards. The required library for Python can be installed by typing the following command:

```
sudo apt-get install python-serial
```

The installation should not produce any errors or warnings.

9.1.6 PJSUA library

PJSUA is an open source command line SIP user agent (soft-phone). We use the library for the SIP handler. First, one needs to download the library from <http://www.pjsip.org/download.htm> [13]. Then extract it to some folder. Then we will build the library using `make`. This can be accomplished by typing the following commands:

```
cd your-pjsip-root-dir
./configure && make dep && make
cd pjsip-apps/src/python
sudo make
```

If you get an error similar to this one:

```
_pjsua.h:25:20: fatal error: Python.h: No such file or directory
compilation terminated.
error: command 'gcc' failed with exit status 1
```

Then you will be required to install `python-dev` as well, that matches your version of `python` (e.g. `python2.7-dev`). You can do it by typing:

```
sudo apt-get install python2.7-dev
```

After you have successfully installed `python2.7-dev`, repeat the the commands given above. Now you should have a properly installed PJSUA library. One can easily test if the installation was successful by compiling a simple python code, `python test.py`, with the following source code:

```
import pjsua
```

If you do not get any errors, you have successfully installed the library. More detail can be found on our project wiki page [4].

9.1.7 pChart library

The `pChart` library is within our installation files and does not require to be installed individually. The library is only required if one uses the web interface and requires the generated resulting image. The library is open source and does not require any licensing. However, if one needs to learn how the library works, information can be found on the `pChart` web page [10].

9.1.8 proctitle library

We had used this library to rename the currently executed process name. “The library allows a process to change its title (as displayed by system tools such as `ps` and `top`). Changing the title is mostly useful in multi-process systems, for example when a master process is forked: changing the children’s title allows to identify the task each process is busy with.” [12]. The library can be easily installed by typing:

```
sudo easy_install setproctitle
```

9.2 Configuring hardware

Before proceeding with the next steps, please connect all the cell phones to the USB hub using the suitable cables. Then make sure the cables are recognized by the operating system. This can be performed by typing the following command:

```
dmesg | grep ttyU
```

The given command should produce a result similar to:

```
[ 5178.753600] usb 1-1.2: p12303 converter now attached to ttyUSB0
```

We have two different ways to configure the cell phones, manually and automatic. Both options can be accessed either using the website or the terminal window. Using the manual configuration from the terminal, the user configures everything him/herself. The user will be presented with a few questions like the port address, cell phone number and IMEI. After the user enters all the required parameters, the software will check if the given port address is accessible and it will look for a response from the devices. Then

you will be asked to enter the IMEI and the cell phone number of the device. If the entered IMEI matches the device IMEI then the software will update the database with the entered information. You can run, both the manual and automatic configuration by typing:

```
python gsmselftest.py --devconf
```

In the automatic configuration, the software will automatically try to detect every cell phone that is connected to the USB hub. This configuration option can detect up to nine cell phones, that are connected to the server computer. We had set a limit to nine cell phones because we required only five (four for the external GSM networks and one for our internal GSM BST). The only limitation of the automatic cell phone configuration is that it only supports cell phones where we could read out the number using the *AT Modem* commands since some cell phone manufacturers do not use the standardized *AT Modem* commands.

9.2.1 Configuring the cell phones

It is important to write in the Siemens S55 cell phones their numbers if you want to use automatic device configuration. You can do that by following the next few steps:

Open the phone book on the S55 and choose *<Special books>* and press the select button.

In the second step, press select on *<OwnNumber>*.

In the third and last step, enter your cell phone number and save it!

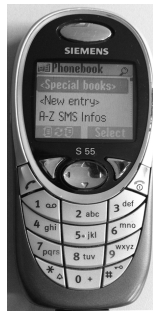


Figure 24: First step in configuring the phone

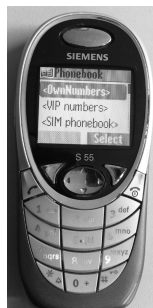


Figure 25: Second step in configuring the phone



Figure 26: Second step in configuring the phone

9.3 Location of the files

For proper operation of the software, it is important that each file is at its correct path located. In the given section you can find out the correct path locations. If you are not an expert, please do not change these locations. The following files have to be located in the `/var/www-ssl/testsoftware/` folder:

```
drwxr-xr-x 7 root root 4096 2011-10-28 12:45 .
drwxr-xr-x 3 root root 4096 2011-10-20 17:06 ..
-rw-r--r-- 1 root root 109 2011-10-26 16:55 .htaccess
-rw-r--r-- 1 root root 20 2011-10-26 17:11 .htpasswd
drwxr-xr-x 2 root root 4096 2011-10-20 17:06 class
drwxr-xr-x 2 root root 4096 2011-10-20 17:06 css
-rw-r--r-- 1 root root 7547 2011-10-20 17:06 delayedLoading.js
-rw-r--r-- 1 root root 3431 2011-10-25 14:38 devconf.html
-rw-r--r-- 1 root root 2024 2011-10-25 23:47 devconfigAuto.php
-rw-r--r-- 1 root root 1811 2011-10-26 13:44 devconfigManual.php
-rw-r--r-- 1 root root 2195 2011-10-25 23:45 devconfig.php
-rw-r--r-- 1 root root 3526 2011-10-27 14:51 devconf.php
-rwxr-xr-x 1 root root 725 2011-10-20 17:06 execute.php
drwxr-xr-x 2 root root 4096 2011-10-20 17:06 fonts
-rw-r--r-- 1 root root 2259 2011-10-28 12:43 index.html
drwxr-xr-x 2 root root 4096 2011-10-20 17:06 icons
drwxr-xr-x 2 root root 4096 2011-10-25 14:10 Images
-rw-r--r-- 1 root root 2038 2011-10-20 17:06 insertData.php
-rw-r--r-- 1 root root 636 2011-10-26 13:43 insertdevice.php
-rw-r--r-- 1 root root 10819 2011-10-20 17:06 loader.gif
-rw-r--r-- 1 root root 2268 2011-10-26 16:07 main.php
-rw-r--r-- 1 root root 5416 2011-10-20 17:06 moocheck.js
-rw-r--r-- 1 root root 75836 2011-10-20 17:06 mootools.js
-rw-r--r-- 1 root root 677 2011-10-20 17:06 mutexFunctions.php
-rw-r--r-- 1 root root 9063 2011-10-25 17:20 mutexSmartTest.php
-rwxr-xr-x 1 root root 9143 2011-10-28 12:45 mutexTry.php
-rw-r--r-- 1 root root 13304 2011-10-20 17:06 networkResult.php
-rw-r--r-- 1 root root 8294 2011-10-21 19:02 post.php
-rw-r--r-- 1 root root 19218 2011-10-21 17:36 startTest2.php
-rw-r--r-- 1 root root 18852 2011-10-20 17:06 startTest.php
-rw-r--r-- 1 root root 18787 2011-10-25 16:43 TaskTest.html
-rw-r--r-- 1 root root 3685 2011-10-20 17:06 testCase.php
-rw-r--r-- 1 root root 2545 2011-10-20 17:06 wait.gif
```

The `startSoftware.py` file is required to be in the `/etc/init.d/` folder, since it is required to be start with the computer boot however if that does not work, one should start it manually. This part of the software is responsible for starting the testing software from the web page¹³. The main test software python files should be located in `/home/gsm-selftest/SoftwareTesting/`.

```
drwxr-xr-x 2 gsmselftest gsmselftest 4096 2011-11-03 14:29 .
drwxr-xr-x 30 gsmselftest gsmselftest 4096 2011-11-02 18:28 ..
-rwxr--r-- 1 gsmselftest gsmselftest 2909 2011-10-20 17:54 ClientClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 3628 2011-10-20 17:54 ClientClass.pyc
-rwxr-xr-x 1 gsmselftest gsmselftest 9814 2011-11-02 16:19 ControllerClass.py
```

¹³The web page communicates with this script via a socket connection and sends a signal to start the main test software.

```
-rw-r--r-- 1 gsmselftest gsmselftest 9247 2011-11-02 16:20 ControllerClass.pyc
-rwxr-xr-x 1 gsmselftest gsmselftest 15129 2011-11-02 15:32 DbClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 11712 2011-11-02 15:32 DbClass.pyc
-rw-r--r-- 1 gsmselftest gsmselftest 8512 2011-11-02 13:30 GSMClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 7337 2011-11-02 13:42 GSMClass.pyc
-rw-r--r-- 1 gsmselftest gsmselftest 8063 2011-11-02 13:24 GSMHandler.py
-rwxr-xr-x 1 gsmselftest gsmselftest 20346 2011-11-02 18:32 gsmselftest.py
-rwxr--r-- 1 gsmselftest gsmselftest 698 2011-11-02 18:36 help.txt
-rwxr-xr-x 1 gsmselftest gsmselftest 8661 2011-11-02 16:35 initTestClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 7497 2011-11-02 16:37 initTestClass.pyc
-rwxr--r-- 1 gsmselftest gsmselftest 645 2011-10-20 17:54 LogFileClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 1509 2011-10-20 17:54 LogFileClass.pyc
-rwxr--r-- 1 gsmselftest gsmselftest 817 2011-10-20 17:54 PingClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 1263 2011-10-20 17:54 PingClass.pyc
-rwxr--r-- 1 gsmselftest gsmselftest 3982 2011-10-20 17:54 ServerClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 4596 2011-10-20 17:57 ServerClass.pyc
-rw-r--r-- 1 gsmselftest gsmselftest 4129 2011-10-20 23:17 WebsiteCommClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 4802 2011-10-20 23:17 WebsiteCommClass.pyc
-rwxr-xr-x 1 gsmselftest gsmselftest 5252 2011-10-22 03:58 SIPHandler.py
-rwxr--r-- 1 gsmselftest gsmselftest 1267 2011-11-02 14:07 SSHTunnelBoxClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 1852 2011-11-02 14:19 SSHTunnelBoxClass.pyc
-rw-r--r-- 1 gsmselftest gsmselftest 323 2011-11-02 18:44 startSoftware.py
-rwxr-xr-x 1 gsmselftest gsmselftest 6378 2011-11-02 16:13 truthTableClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 4583 2011-11-02 16:16 truthTableClass.pyc
-rwxr-xr-x 1 gsmselftest gsmselftest 2248 2011-10-28 14:04 usbDetectClass.py
-rw-r--r-- 1 gsmselftest gsmselftest 3590 2011-10-28 14:05 usbDetectClass.pyc
```

9.4 Setting up the parameters

After configuring the hardware, *https* and *.htaccess* on the web server, it is important to modify the files for proper operations. In the given section you can find out how to configure the rest of the files (e.g. database passwords, etc.). The following files you have to modify to have a working database access: *initTestClass.py*, *GsmSelfTest.py*, *UsbDetectClass.py* and *truthTableClass.py*.

9.5 Test descriptions

In the following section we will describe the tests that can be performed and what kind of problems they can identify. There are five types of tests:

- Smart test
- SIP test
- GSM test
- Everything test
- Manual test

Each test will be described in the next subsections.

9.5.1 Smart test

The *smart* test is not called smart without a reason. It tries automatically to identify problems inside of the telecommunication network. The user is not required to define

what kind of tests have to be performed. In the first part the test software communicates with the database to see what systems are available. In the next step it performs a call from the University telephone system to a random local cell phone¹⁴ inside of our University GSM network. While executing this task, automatically the Asterisk server, OpenBSC and a random nanoBTS (or the one cell phone in RZ) are tested. The next task to be performed in the smart test, a randomly selected cell phone inside of our local GSM network will try to call: a random cell phone within the external (O2, Vodaphone,E-Plus or T-Mobile) or local GSM network. This might test the external network and will test it with high probability, however the probability exists to make a local to local GSM test call. In the third task, we perform a test where we call from the landline a random cell phone inside of our local GSM network. In the fourth or last task, we call from SIP to the service we did not test yet (e.g. if we did not test the external GSM network using the second test task, then in this last task we will exploit it). After the smart test had been completed you will be presented with the results.

9.5.2 SIP test

The *SIP* test option will perform test in such a way that all the SIP subsystems are tested (SIP and University telephone network). It will try to identify if there are any problems on the Asterisk server and our University telephone network, including incoming and outgoing calls from the SIP side.

9.5.3 GSM test

In the *GSM* test both GSM networks get tested, the local and the external GSM network. We test the nanoBTS controller boxes (i.e. BeagleBoards) as well. Using this test, both incoming and outgoing calls are performed, we can detect possible errors on the OpenBSC and the nanoBTS.

9.5.4 All test

The *All* test selects all the given tests and executes them step-by-step. It is the test that takes the greatest amount of time. While the test are performed, results are immediately printed in the terminal window or on the web site.

9.5.5 Manual test

The *Manual* test as the name itself says, is the test where you can manually select what kind of tests you want to be performed.

¹⁴Local cell phone or local GSM network means our University GSM Network or RZ GSM.

9.6 Result descriptions

In the following table one can see the messages returned by the test software! These messages should guide the test user operator to debug the system.

Number	Code	Code number description
1	200	Call was OK
2	604	General Handler Error: Destination handler did not respond. Timeout
3	998	General Handler Error: Could not connect to the destination handler!
4	605	General Handler Error: Caller handler did not respond. Timeout
5	999	General Handler Error: Could not connect to the caller handler!
6	486	Call Failed
7	333	Could not establish a connection to the database!
8	100	Missing account detail
9	402	Payment Required (E-Plus Card)
10	801	Connection to caller established, but the device does not respond
11	802	Connection to destination established, but the device does not respond
12	501	Destination server Internal Error
13	502	Caller server Internal Error

The errors can be described the following way:

- *200*, Connection between the caller and callee was properly established
- *604*, Callee handler has a problem during executing the test, a connection error between caller and callee
- *998*, Controller cannot establish a connection and send messages to the callee handler but the callee handler is alive
- *605*, Caller handler has a problem during executing the test, a connection error between caller and callee
- *999*, Controller cannot establish a connection and send messages to the caller handler but the caller handler is alive
- *486*, Call test failed, the connection between the caller and callee could not be established
- *500*, Caller handler cannot be reached from the server
- *501*, Callee handler cannot be reached from the server
- *333*, Cannot login to the MySQL database
- *100*, Software cannot sign in to the SIP account(SIP at Asterisk, Landline at sip-gate.de, SIP at University telephone network), due to missing or incorrect information in the device address table
- *402*, Payment required for the E-Plus SIM card
- *801*, Caller device on the handler times out or is not properly connected
- *802*, Callee device on the handler times out or is not properly connected

9.7 Using the software

In this section, you will be taught step by step how to use our test software. There are two options to run our test software, from the web site or the terminal. The first is easier, but the second is easy as well however requires terminal skills.

9.7.1 Web site guide

Once you enter the address in the address bar of your browser (e.g. *https://localhost/testsoftware*). You will be required to enter your username and password for the web page¹⁵. If you entered the correct username and password you should see the same image as in the following figure. Here you can choose what kind of test you want to perform or

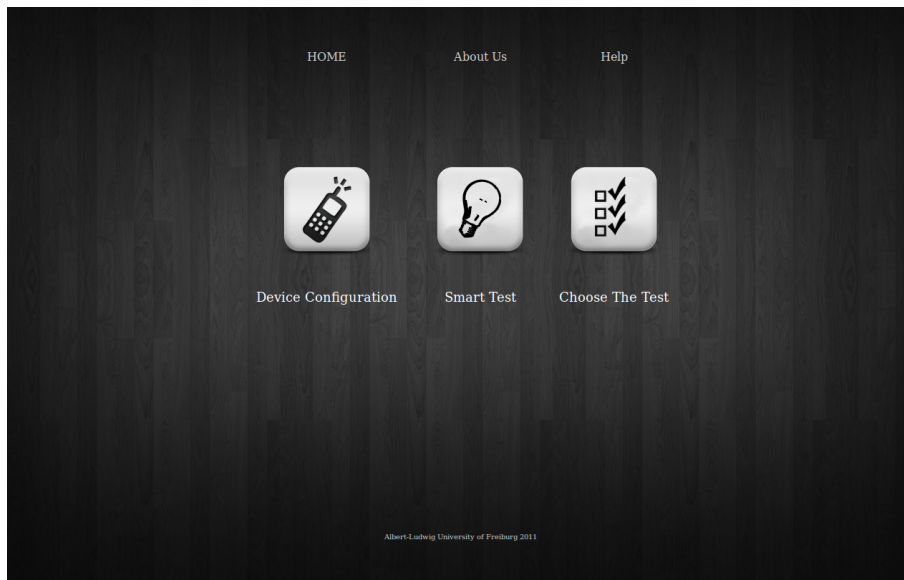


Figure 27: Web page of test software

maybe if you want to configure the devices (manually or automatically). If you press the “Smart test” button, you have to wait a few moments and the results should appear in a short amount of time. However, if you pressed the “Choose the test” button, you will be presented with a new page, given in figure 28. You will have to select the tests you want to perform manually or to press on the left side one of the given buttons for different tests. You can choose between “SIP Test”, “GSM Test”, “Check all” and “Uncheck all”. “Check all” will select all the possible tests, whereas “Uncheck all” will deselect all of them. After you finished the procedure of selecting the tests, you should press the “Submit” on the left side. Wait a few moments and the results will start to appear in real time. After the table on the left is filled (i.e. after all the tests have been completed) a result image will be generated on the right side, can be seen in figure 20. However, if your pressed the “Device configuration” button, then you will end up on a page as given in figure 30.

¹⁵The username and password creation process is explained in section 7.2.2.



Figure 28: Manually selecting the tests

If you press the “Automatic configuration” button, the test software will try automatically to match your cell phones with their port addresses and numbers. However, if the automatic matching does not work, you will have to manually configure it. You can do it by entering all the required information on the web site, as in figure 31. Once you correctly filled in the required information, you should press the “Submit” button.

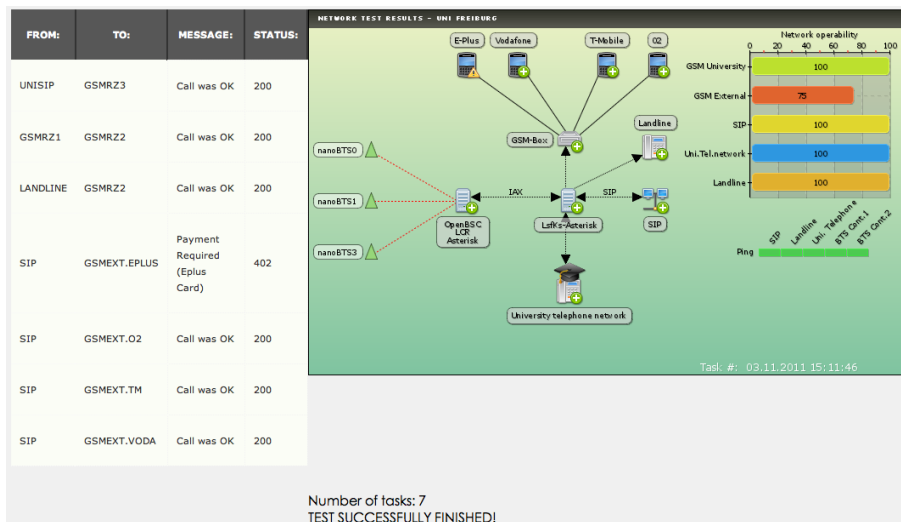


Figure 29: Result web page

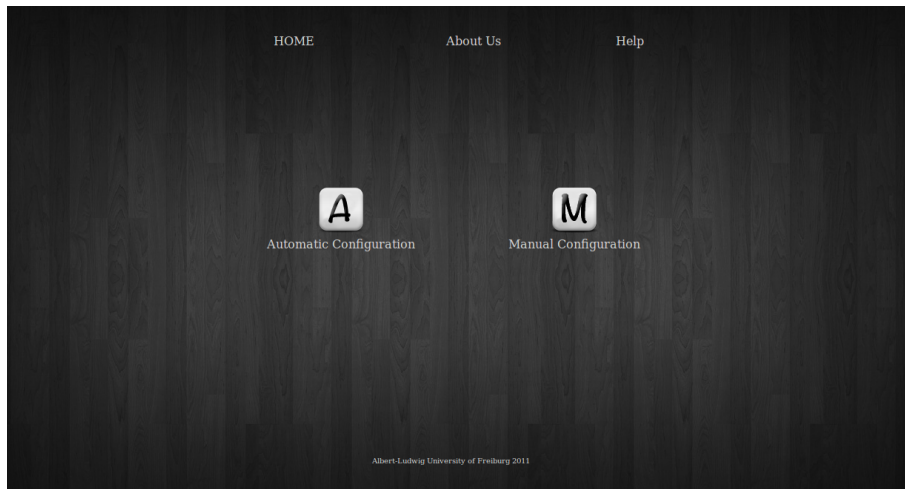


Figure 30: Device configuration web page

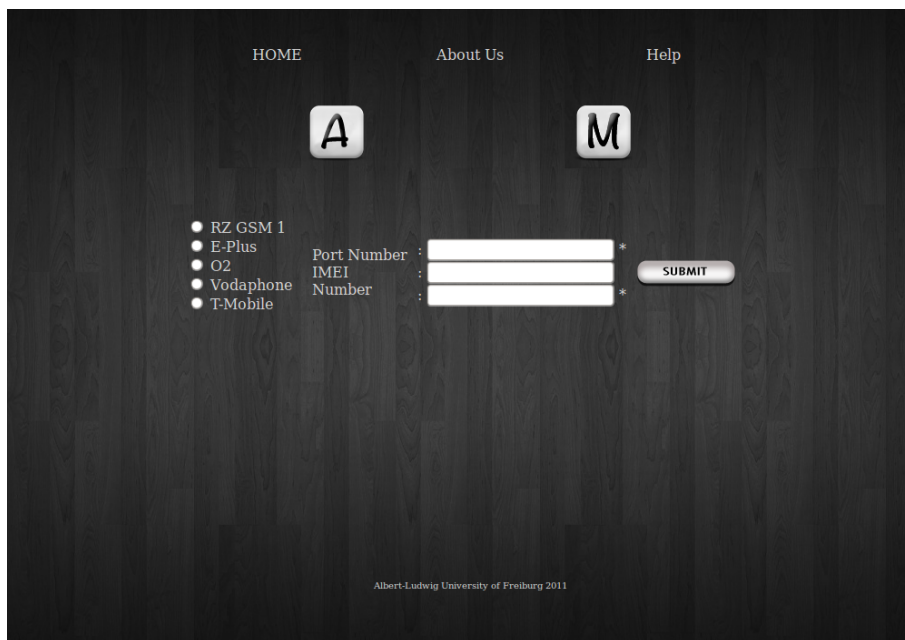


Figure 31: Manual device configuration page

9.7.2 Terminal guide

In the following text, we will guide you and show you step-by-step how to use the test software from the terminal. All you have to do is just type the command for starting the test software in the folder where it is located, `./gmsselftest.py --option` (keep in mind there are two dashes before *option*). You can perform the tests manually by typing what you want to test or by choosing one of the predefined tests. For example, you want to test manually does the SIP work with the University telephone network, you would type

```
gsmselftest@gsmselftest:~/SoftwareTesting$ ./gsmselftest.py --help
Usage: ./gsmselftest.py [option]
Options and arguments (and corresponding environment variables):
--db [caller] [callee] : To execute the test case given by defining the caller and callee
--all                   : To execute all test cases
--sip                   : To execute SIP test cases
--gsmrz                 : To check whether GSM RZ network has problems or not
--gsmext                : To check whether GSM BOX modem has problems or not
--incoming              : To check incoming calls from Landline
--smart                 : To test only important points in the network and to identify the problems
--devconf               : To configure the USB device on the server
example : ./gsmselftest.py --devconf
          ./gsmselftest.py --smart
          ./gsmselftest.py --db sip GSMRZ1
```

Figure 32: Test software terminal options

the following: `./gsmselftest.py -db sip unisip`. After the tests have been performed the

```
gsmselftest@gsmselftest:~/SoftwareTesting$ ./gsmselftest.py --db sip unisip
Lock the mutex: 1
Task ID      : 50
Calling From : sip
To           : unisip
Result      : 200 Call was OK
```

Figure 33: Example results from the terminal screen

results will be displayed. Green result text means the test was performed successfully and red result text means that something is not working properly.

If you need to configure the cell phones manually or automatically, you can do it by typing: `./gsmselftest.py -devconf` (keep in mind there are two dashes before `devconf`). Then you can press “a” on the keyboard for automatic configuration or “m” for manual configuration. One should keep in mind that the terminal test software can be started even through `ssh`, however with an additional command `-X`¹⁶.

```
gsmselftest@gsmselftest:~/SoftwareTesting$ ./gsmselftest.py --devconf
Mobile device configuration
Menu: a = automatic device configuration, m = Manual configuration, q = quit : a
Lock the mutex: 1
Device Name : GSMRZ1
IMEI        : 351083538066599
Phone Number : 07612034661449
Port Name   : /dev/ttyUSB0
Device Name : GSMExt.Tm
IMEI        : 351083512267833
Phone Number : 015128040906
Port Name   : /dev/ttyUSB1
```

Figure 34: Test software device configuration from terminal screen

¹⁶For example: `ssh -X username@address`

10 Conclusion

As a result of our successfully finished team project, we had felt how it is to work in a team. We had learnt how to confront various software and hardware issues. The problems were broken into smaller fragments and the solutions were derived in a step-by-step approach.

While designing the software, we kept in mind that every single step should be well thought-out, documented, tested and validated. At the end we joined all the “black-boxes” together into one big piece of software. We fulfilled our stated requirements and goals.

Despite the fact that our test software will be used by well educated engineers, we may conclude that all the way along we thought about the usage-simplicity, safety and security of our product. Our team members were enthusiastic about the idea that our team project will contribute to a better performance and quality of the overall telecommunication network, for all of the University staff and our colleagues, the students.

References

- [1] *Projects based on RZ-GSM*, accessed on 10.06.2011, available at <http://lab.ks.uni-freiburg.de/projects/gsm/wiki>.
- [2] *Python Programming Language - Official Website*, accessed on 10.06.2011, available at <http://www.python.org/>.
- [3] *MySQLdb User's Guide*, accessed on 05.06.2011, available at <http://mysql-python.sourceforge.net/MySQLdb.html>.
- [4] *[2011] GSM Selftest - Wiki - Lehrstuhl für Kommunikationssysteme*, accessed on 20.09.2011, available at <http://lab.ks.uni-freiburg.de/projects/gsm-selftest/wiki>.
- [5] *17.2. socket - Low-level networking interface*, accessed on 20.06.2011, available at <http://docs.python.org/library/socket.html>.
- [6] M. Ben-Ari *Principles of the Spin Model Checker*, Springer Verlag, Weizmann Institute of Science, Israel, ISBN: 978-1-84628-769-5, 2008.
- [7] R. Natarajan, *3 Steps to perform SSH login without password using ssh-keygen & ssh-copy-id*, accessed on 18.08.2011, available at <http://goo.gl/fX68N>.
- [8] P. Bramscher, *Creating Certificate Authorities and self-signed SSL certificates*, accessed on 05.09.2011, available at <http://www.tc.umn.edu/~brams006/selfsign.html>.
- [9] *EnablingUseOfApacheHtaccessFiles*, accessed on 18.08.2011, available at <https://help.ubuntu.com/community/EnablingUseOfApacheHtaccessFiles>.
- [10] *pChart*, accessed on 15.08.2011, available at <http://www.pchart.net/>.
- [11] *BeagleBoard System Reference Manual*, accessed on 20.06.2011, available at http://beagleboard.org/static/BBSRM_latest.pdf.
- [12] *setproctitle 1.1.2*, accessed on 20.10.2011, available at <http://pypi.python.org/pypi/setproctitle>.
- [13] *Open source SIP stack and media stack for presence, im/instant messaging, and multimedia communication*, accessed on 20.10.2011, available at <http://www.pjsip.org/>.