XVII IMEKO World Congress
Metrology in the 3rd Millennium
June 22–27, 2003, Dubrovnik, Croatia

SOFTWARE VALIDATION OF SERIAL LINE COMMUNICATION

Roman Flegar, Tanasko Tasić

Metrology Institute of the Republic of Slovenia (MIRS), Ljubljana, Slovenia

Abstract – The software validation of measuring instruments is a complex procedure, which can be divided into the validation of separate software functions. The paper deals with the software validation of functions for serial line communication. It describes methods for preparation and validation. Methods are based on demands and facts, which are important for measuring instruments under legal control. They were developed during type approval process of an automated liquid level measuring instrument, but they can be easily adopted and used with other measuring instruments or communication interfaces. At the end of validation procedure, results of methods are gathered together and evaluated.

Keywords: software validation, communication security, legal metrology.

1. INTRODUCTION

In the last decade there was significant development in the measurement instruments technology. Measurement instruments became a microcomputer based systems. Software is taking nowadays the most significant part in those systems. A lot of functions of measurement systems are now implemented with software rather than with hardware. The main advantage of software implementation is faster and more flexible development and easier maintenance.

Software in the measurement system covers usually the following main functions: data collection from the sensors, data processing, data storage, data transfer over communication line and configuration control and work flow control. The main question about software is, how reliable software is? The quality and reliability of the software directly effects measurement results. There is also the another question about the software reliability, how to prevent unauthorized access and interference with the software? The possibility of unauthorized access and interference significantly increase the fraud risk.

Measurement instruments are used and present in several different areas: industry, laboratories, science, commerce, health care, etc. Some of those measurement instruments are directly involved in: human and animal health and life preservation, commercial transactions, state taxation, monitoring and preventing environmental risk and dangerous situations. The goal of every state is to provide accurate and repayable measurement in those cases. To achieve that, some measurement instruments are under legal control of the state. State provides legislation to control measurement instruments under legal control. This legislation deals with introduction of new type of measuring instrument, minimal technical requirements and how to perform verification. Before a new type measuring instrument is introduced, it has to go through a process of type approval. This process is performed by notify body. They check if the measurement system is in accordance with the legislation and fulfils all the necessary technical requirements. If measurement system meets all requirements, the type approval certificate is produced. This certificate is also accompanied with a document guideline for future verification process of the measurement system.

As we have mentioned, there was development of the technology. Nowadays a majority of measurement instruments under legal control are computer based. These results, that some new reconsideration about the quality and reliability of the software during the type approval process should be taken into account. If the fraud risk is the biggest reconsideration, the focus of examiner should be the communication interface. It is usually the weakest point of the measuring instrument.

The main question is how to approach software validation of communication interface. Possible methods and the procedures were developed in the case of type approval process of an automated liquid level measuring instrument in MIRS Laboratory for Information Technology in Metrology. This measuring instrument uses serial communication line, but methods can be easily adopt and use also with another type of communication interface.

2. COMMUNICATION INTERFACE

Communication interface can be part of the measuring instrument. Standalone measuring instrument does not have it, so the possibility of fraud is low. The possibility of fraud or misuse is significantly higher, if measuring instrument is equipped with communication interface. Communication interface can be connected to another device under legal control or any other devices. In the last case, there is even higher possibility of risk. So the communication interface should be protected. The level of the protection depends on the type of the measurement instrument. For higher levels of risk the communication interface has to be more protected. Communication interface can be protected with encryption, passwords to provide different access levels, identification of both communication nodes etc.

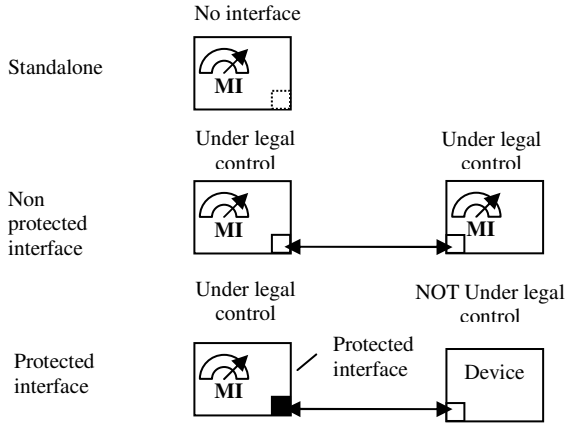

Fig. 1. Communication interface possibilities

3. SERIAL COMMUNICATION LINE

Serial communication interface is the most widely used interface in measuring instruments. It is implemented, because it is inexpensive and easy to integrate.

It is used for controlling, monitoring and reading measurements from measurement instrument by other devices. In major cases, the other device is personal computer with special terminal software to operate measuring instrument. Terminal software in provided by manufacturer of the measuring instrument.

Serial communication interface has not any additional security features to increase reliability or decrease the risk of the fraud. Manufacturer is responsible for the protection of the measuring system and terminal software. Protection can be built within communication protocol. Those facts and the facts of wide spread and simple implementation just increase the possibility of the fraud.

4. METHODES

Methods are divided into two groups. The first group is dealing with the methods to analyze the protocol on the communication interface. The goal of these methods is to provide communication protocol. It happens in several cases that it is not available from the manufacturer. The communication protocol is the most important input for the second group methods. The first group includes following methods: Monitoring and Reverse Engineering.

The second group covers the methods for validation and testing the communication interface. It was necessary to develop a special hardware and software monitoring to tool to support methods from the both group. The second group includes following methods: Encryption implementation, Identification, Login testing, Password recognition, Illegal commands.

4.1. Hardware monitor tool

The idea of the hardware monitor tool is to connect directly to the serial communication line and start to listen the communication. This connection should be made transparent to the both end nodes.

The hardware monitor is build in the following way. It is connected to the data line and control lines like a piggy back. It makes a copy of characters which is send in both direction without any interferences.

The hardware monitor tool can be operated by terminal software. This software is usually built in operating system such as VT-100, telnet, Hyper Terminal, etc. In our case we have specially developed more handy terminal simulator, which can be also used for logging the communication line activities.

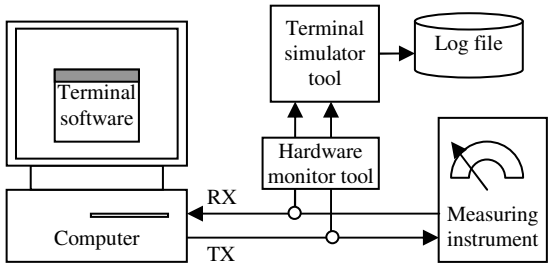

Fig. 2. Serial line communication with monitor

4.2. Terminal simulator tool

Terminal simulator tool was basically developed to simulate operating terminal for the measuring instrument. The idea was to swap between the original terminal software produced by manufacturer with our own terminal simulator. Our terminal simulator allows more control over the communication line. The communication protocol can be loaded or manually programmed in the terminal simulator. It allows to execute a complete or partial communication lines step by step and separately log a responses from measuring instruments. It is also possible to program some communication patterns and control loops. This is used for automatization of some testing and validation methods.

Another function of terminal simulator is also support for hardware monitor tool. It allows logging all activities on the communication interface. It can log data and control signals. Logs can be later used for analyses.

4.3. Monitoring method

Monitoring method belongs to the first group. The main goal of this method is to gather all necessary information about the communication interface. Measuring instrument and original terminal software are connected with special Hardware monitoring tool. The usual way of communication with measuring instrument is started: initialization, setting parameters and reading data. All activities are logged by Software monitoring tool in text files. If we want to implement Protocol reverse engineering method, it is important that all known possible ways of communication with measurement instrument are covered.

4.4. Protocol reverse engineering method

This method is used, when communication protocol is not provided by manufacturer. The input for this method are log files provided by Monitoring method. By visual inspection or by word processing tools a patterns of commands and parameters are trying to be recognized. Basically all communication activities can be fitted in following building blocks: commands, parameters, results

and acknowledgments. Each of this building blocks can be recognized and determined with special approach within the log files.

Commands can be determined with following approach. We can send a specific command several times with the different parameters. By visual examination of the log file, we can establish that some patterns stay the same all the time. This static pattern represents a command. A part of pattern which differs in each step of communication is parameter of the command.

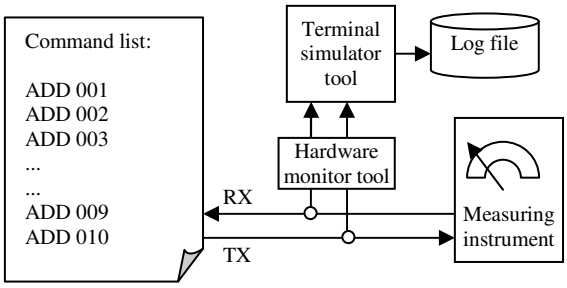

Fig. 3. Sending specific command with different parameters

After the pattern is found which represent a command, it is possible to try to find out pattern for parameters. We can use several approaches. The most common are increasing the value each time by 1 or increasing the value by power of number 2: 2, 4, 8, 16, 32, etc. With first approach, it is possible to found out if parameter is implemented with decimal values, with second approach we can found out if parameter is implemented in binary or hexadecimal number format.

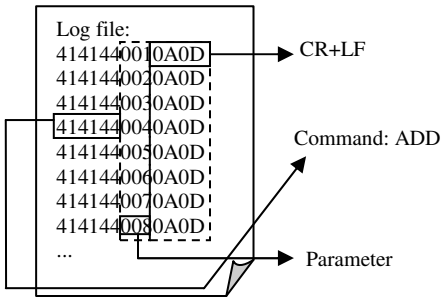

Fig. 4. Example of reverse engineering

The same approach is used to determine all results and acknowledgments. The final result of this method is a communication protocol list which provides an input for methods in the second group.

4.5. Encryption implementation method

This method is used to determine if the communication interface is encrypted. There is no software tool to find out this, so the visual inspection of the log files should be made. If it is impossible to reconstruct the protocol from the log file or if the same command with the same parameter is always represented with different pattern, than it is possible to conclude that communication interface is encrypted. In this case it is necessary to use the original terminal software provided by manufacturer for further testing and validation. Implemented encryption of communication interface decraese the risk of fraud.

4.6. Identification method

One of the possibility to decrease the risk of the fraud and increase the reliability of measuring instrument is identification of the both communication nodes. With this method is checked, if the terminal software is able to identify the measuring instrument and if measuring instrument is aware who is sending commands. Three testing sets have to be prepared: terminal software with measuring instrument, terminal software with simulator and simulator with measuring instrument. The beginning of communication is monitored for each set separately. Usually measuring system or terminal software does not want to start the communication, if there is not correct identification of both communication nodes. A communication node can be faked with simulator.

4.7. Login testing method

Measurement system is protetced also with different sets of passwords. Passwords are used to identify security and authority level. Passwords are sent during the login procedure. The login procedure can be implemented on different ways. The simple login procedure are not effected by invalid passwords. The more advance login procedures has different response on continuous invalid password for example: increasing the time to next possible login in, blocking to login rights for current security level, log of unsuccessful login attempts, sending alerts to operators. More advanced login procedures reduces the risk of fraud.
Method is performed with sending several legal and illegal passwords to measuring instruments and observing the results.

4.8. Password recongition method

This method is recommended to use if more advanced login procedure is not implemented. There are several different methods for password recognition. Terminal simulator tool allows to use brutal force algorithm combined with dictionary of most common words in certain languages. Simulator is sending in loop different passwords and observing the response of the measurement instrument to find out the correct password.

4.9. Illegal commands method

Fraud can be made also with intentional or unintentional sending of illegal commands. Illegal commands can have invalid command or parameter. It can affect the complete measurement system by blocking it or cause invalid computation or representation of the measured values. The measurement system shall be protected against this possibility. This method is implemented by sending set of illegal commands to the measurement system and observing its response.

5. TESTING AND VALIDATION PROCEDURE

5.1. Type approval procedure

For the purpose of the type approval procedure in MIRS for measuring instrument with serial communication interface was made a special flow chart with check list table.

Every measuring instrument with serial communication interface is tested according to this flow chart and checklist table. Based on the result the type approval process is continued or stopped and interaction from customer is required.

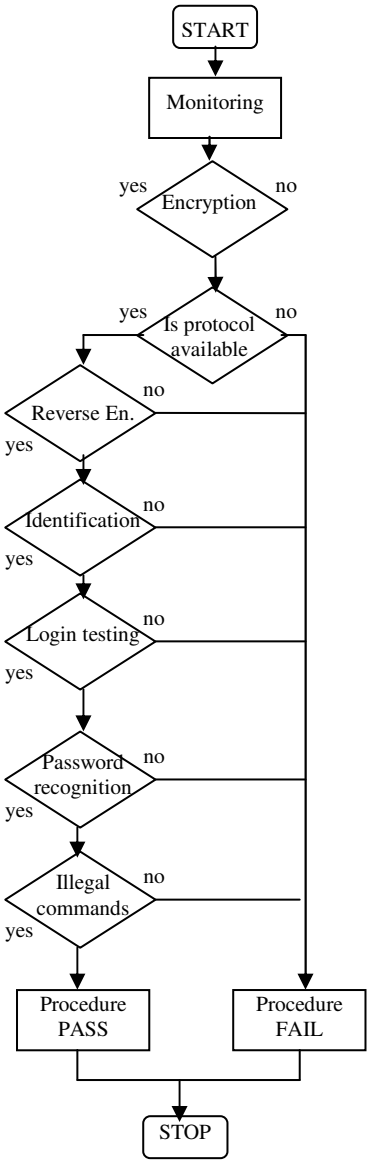

Fig. 4. Example of reverse engineering

5.2. Example

All methodes were tested for the first time during the process of type approval of automated liquid level measuring instrument. Manufacturer has not provided the communication protocol. This measuring system has two main parts: sensor head with control unit and personal computer with special terminal software provided by manufacturer to operate control unit and represent measured values. Control unit is connected to the personal computer with serial communication interface. Sensor head provides only the information about the level of the liquid in the reservoirs. This information is compiled and computed by control unit. Control unit is set and operated by terminal software. It returns on demand liquid level and stored volume in the reservoir. The legal relevant parameters, for example: the terminal software can set reservoir geometry and the waste level. Because of this fact, the testing and validation checklist was done with following results:

TABLE 1. Check list table results

Method	Results
Monitoring	- no encryption
Protocol reverse engineering	- found complete set of commands
Identification	- no terminal identification
Login testing	- no delay for next login, - no logging, if invalid password is used
Password recognition	- manufacturer password found
Illegal commands	- illegal commands can't be used - illegal value parameter can be used

Based on this result the type approval for this measurement instrument was rejected. Manufacturer was advised to increase the security of communication to fulfill the fundamental requirements of legal metrology – decrease the risk of fraud and increase the reliability of complete system. The suggestions were: implementation of communication encryption, implementation of the identification of the both sides in the communication and improvement of the login procedure.

6. CONCLUSION

Above-mentioned testing and validation procedure was found out to be enough sufficient to test the capability of serial communication interface to fulfill the requirements of legal metrology for protective communication interface. This procedure can be also easily adapted also to the other types of the communication interfaces such us Ethernet, USB, RS448, I^2C, etc. The only necessary thing to change in this case is *hardware monitoring tool*.

REFERENCES

[1] European Commission, "Measuring Instruments directive (MID) – III.D.2", Working Document MID/2, November 1997

[2] WELMEC - WG7, "Software Requirements on the Basis of the Measuring Instruments Directive (MID), WELMEC 7.1 (Issue 1), October 1999

[3] Debra S. Herrmann, "Software Safety and Reliability", IEEE Computer Society, 1999

AUTHORS:
Roman Flegar, Metrology Institute of the Republic of Slovenia, Grudnovo nabrežje 17, 1000 Ljubljana, Slovenia, tel: +386 1 244 27 26, fax: +386 1 244 27 14, e-mail: roman.flegar@gov.si;
Tanasko Tasić, Metrology Institute of the Republic of Slovenia, Grudnovo nabrežje 17, 1000 Ljubljana, Slovenia, tel: +386 1 244 27 10, fax: +386 1 244 27 14, e-mail: tanasko.tasic@gov.si.