INTERNATIONAL MEASUREMENT CONFEDERATION

16th IMEKO TC4 International Symposium

Exploring New Frontiers of Instrumentation and Methods for Electrical and Electronic Measurements

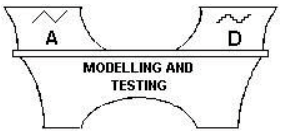
13th International Workshop on *ADC Modelling and Testing*

IMEKO TC4 - TC21 Joint Session

September 22 – 24, 2008

Florence, Italy

INTERNATIONAL MEASUREMENT CONFEDERATION



16th IMEKO TC4 International Symposium

Exploring New Frontiers of Instrumentation and Methods for Electrical and Electronic Measurements

13th International Workshop on *ADC Modelling and Testing*

IMEKO TC4 - TC21 Joint Session

PROCEEDINGS

September 22 - 24, 2008

Florence, Italy

Proceedings of the 16th IMEKO TC-4 International Symposium
"*Exploring New Frontiers of Instrumentation and Methods for Electrical and Electronic Measurements*" and
13th Workshop on ADC Modelling and Testing

IMEKO – International Measurement Confederation
University of Florence, Faculty of Engineering and Faculty of Economics
University of Siena, Faculty of Engineering

Printed with the financial support of:

ENTE
CASSA DI RISPARMIO
DI FIRENZE

Printed in September 2008 by Tipolitografia Contini s.r.l., Sesto Fiorentino, Italy
ISBN 978-88-903149-3-3

A&T Affidabilità & Tecnologia
Via Palmieri, 63 – 10138 TORINO
Tel. +39 011 5363440 – Fax +39 011 5363244
E- mail: info@affidabilita.com
WEB: www.affidabilita.com

Generic Environment for internet-enabled calibration services

Marko Jurčević, Hrvoje Hegeduš, Roman Malarić, Hrvoje Zeba

University of Zagreb, Faculty of Electrical Engineering and Computing, Zagreb, Croatia
(tel: +385 1 6129749; fax: +385 1 6129 616; e-mail: {marko.jurcevic; hrvoje.hegedus; roman.malaric}@fer.hr)

Abstract – Since many of the available digital instruments are provided with some communication interfaces and the internet-enabled metrology is rapidly developing in the recent years, it is possible to create an actual remote calibration system with remote control capabilities. This approach addresses a wide range of possible applications that allows driving many kinds of different devices and is easily upgradeable. This paper focuses on some of the solutions for security problems regarding remotely executed internet-enabled calibration processes.

Keywords: internet-enabled calibration, travelling standard, ISO/IEC 17799:2000, ISO/IEC 17025:2005

INTRODUCTION

The evolution of computer-based communications allows the development of new services that may partially replace human activities in the area of instrument calibration [1]. The capability of calibrating an instrument on-site instead of sending it to a calibration laboratory, allows saving time and money, provided the instrument itself have a standard communication bus interface (e.g. IEEE 488, IEEE 1394, PCI/PXI and USB). Such interface allows instruments to be connected to a PC and then a calibrating device can be sent to the instrument's location and operated remotely.

Remote calibration approach is especially efficient whenever the calibration of low-cost instruments is involved. The remote calibration of measuring instruments is an interesting application that has not yet been fully exploited, mainly due to the legal issues because of the possible lack of security, which is associated with the remote operations [2] [3]. The reliable remote control and monitoring of instruments is a crucial aspect of internet-enabled calibration procedure.

2. GENERAL DESCRIPTION AND DESIGN

In this paper we describe internet-enabled calibration system [4] that has the main goal to enable the control and supervision of the remote standard(s) and instrument(s) that are used in a calibration process under the conditions that are defined accordingly to the international standard ISO/IEC 17025:2005 [5].

This system consists of a PC-manageable high accuracy travelling calibration device or artefact standard (travelling unit, TU) and a CSP (Calibration Service Provider) server-side application system that controls and monitors the whole process of calibration (Fig. 1).

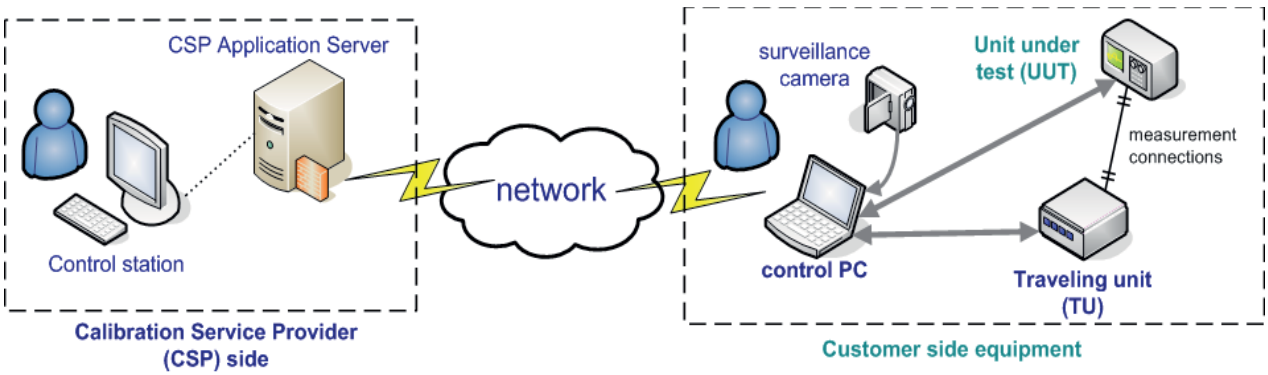


Figure 1. Remote calibration system architecture

Travelling standard and device/unit that are under test and/or calibration (UUT) must have a communication interface (e.g. USB, LAN or GPIB) in order to connect them to the customer PC that controls the calibration event. Application on the CSP side performs calibration procedure without any human assistance on the customer side. Also, customer-side equipment (CSE) has to self-recognize and make automatic configuration of available interfaces, connected instruments and standards.

Operator on the customer-side only has to make correct connections between the CSE and the UUT. This means that there is no need for a specialized engineer or technician in the customer side laboratory.

After the calibration procedure is completed, the travelling unit (TU) is returned to the CSP office for a test and verification. If the equipment passes this test, a calibration report is returned to the customer. This document should contain the date and time of calibration event, some information about calibrator output data, the minimum and maximum measurement uncertainty, the measurement results, the differences between measured data and calibrator outputs, and the calibration timing.

3. HARDWARE AND SOFTWARE ARCHITECTURE OF THE CALIBRATION SYSTEM

Model of the customer side equipment – the travelling unit (TU) is made up of two main components: communications and controller module (CCM) and one or more reference standard(s) or device(s) (REF). The CCM is a common name for a component that communicates with the customer -side control PC. For this purpose an IEEE 488 internal or external (USB, Ethernet, RS-232 or other type) interface card is usually used. The CCM sets all the parameters for REF and collects the measurement data during the verification and calibration process. A calibrated environmental probe can be used if necessary to acquire the customer -side temperature, pressure and humidity values.

The TU presented here allows performing basic calibration procedures that require the verification and calibration of few measured quantities and is not suitable for complex measurements and calibrations. The calibration procedure consists of: configuration of CCM and REF, identification and verification of UUT (using the IEEE 488 communications and visual control if necessary), testing the functionality of the remote calibration system and acquisition of the measurements carried by REF (reference device) and UUT.

Regarding the software part, the calibration system architecture consists of server and customer unit (Figure 2). The implementation code is divided in several main parts: a set of instrument-specific libraries (ILS) that allows to update or add new drivers for additional measurement equipment, a device-independent control and monitoring layer (DEICON), transport network control (TNC) layer, server and customer side application management layer (SECM) and database management system layer (DBMS). Customer-side software part is controlled using RPC (Remote Procedure Call) protocol from the server.

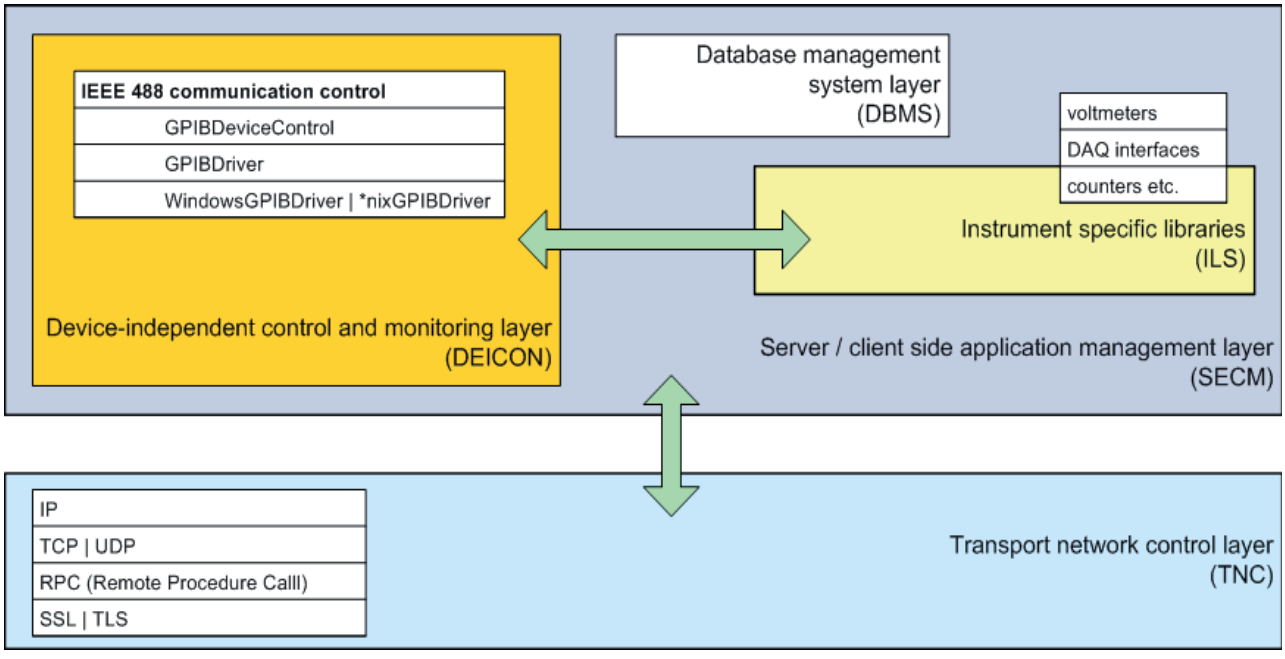


Figure 2. Software system architecture components

Architecture mentioned above assures several advantages: simplified management and control of the hardware resources, reliable and secure communication between customer and CSP side and foolproof software upgrades operations. Most of the system operations that are carried out within a test and calibration procedures are based on the abstract functional layer. This approach helps to simplify software control and monitoring of instruments, because it is independent of the instruments connected to the customer -side control computer.

Customer-side software components are divided into several main parts:

- platform dependent driver interface to the communications controller (e.g. GPIB interface card) manufacturers drivers (one DLL library under Windows or SO library under Linux),
- platform-independent Java interface to the platform-dependent driver interface (in a form of a JAR file),
- main application that provides GUI to the customer personnel and operates calibration procedure in a form of signed and authorized JAR (Java ARchive) applet or JNPL (Java Web Start) application.

Instrument libraries are created based on manufacturers programming manuals of each instrument and are dynamically loaded on the server-side according to the connected equipment and instruments on the customer side. These libraries are used to generate customer-side instrument commands and interpreting returned data. DEICON layer assures transport of commands, control messages and data to the connected measurement equipment.

The whole core of the software application (customer-side program component and instrument drivers) resides permanently on the server. In this way, there is no need to install any special software tool on a customer PC, except for a Java Virtual Machine runtime (JVM) and placing two files mentioned above into operating system directories (which can done automatically during the start-up of a customer-side application), providing thin-client application architecture safe for the whole calibration system. The calibration system as shown above assures the following: automatic management of the physical resources available on the server according to the type of calibration, integrity and access control between client and server side and optional upgrades with the newly added hardware components.

4. APPLICATION OF THE CALIBRATION SYSTEM

Figure 3. shows CSE part of a developed remote calibration system. An example system was implemented to provide the calibration of external USB DAQ card (in our case it is National Instruments 6020E model).
It is important to emphasize that this example was not designed to provide commercial calibration solution for DAQ cards. It is to show some of the obvious practical problems that occur when requirements from the ISO/IEC 17025 [5] are to be met in a case CSP wants its remote calibration system to be operated to this quality system.

In this case, the travelling unit is made of one 6 ½ digit DMM (with a valid, traceable calibration certificate) connected over the GPIB interface to the PC. The DMM measures the output signals from the DAQ during the verification of the board outputs. The similar calibration of DAQ inputs is done using a programmable voltage reference standard (e.g. 5700A calibrator, a case that is not discussed here). Accordingly to the manufacturers calibration instructions, DAQ analog output verification is done in a several steps: determine output channel, polarity and voltage to verify, configure the device and prepare it for verification process, write test point data (voltage values for verification purposes) to device registers, read the measured data from the DMM and repeat this procedure for every output channel and compare measured values from the samples taken to the limits specified by the DAQ card manufacturer.

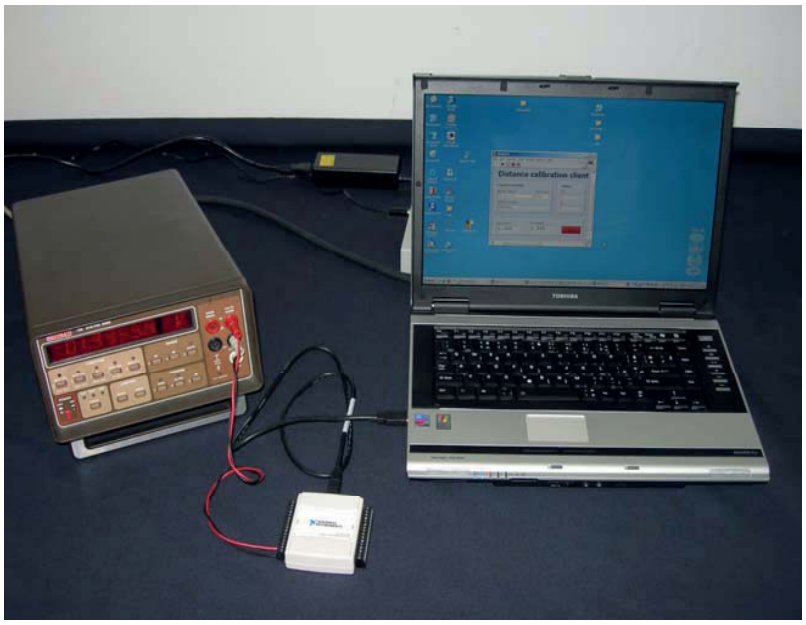


Figure 3. Sample customer-side equipment for described USB DAQ calibration

Measured information is also transferred and stored on the server side. As soon as the TU is returned to the calibration lab and passes specification tests, the laboratory can issue calibration certificate, or in this case, information that it is not possible to calibrate customers' device.

A. Information security issues of remote calibration

As mentioned earlier, an internet-enabled calibration session takes place between at least two parties – the CSP, the laboratory with the reference standards, and the customer laboratory with the equipment (standards and instruments) that needs to be calibrated. In this case the measurement data is constantly vulnerable, especially when it is transmitted over the communication media during the calibration process and when it is stored in a database as part of calibration data.

The special care is taken about the security of the system. The development of CSP security policy creation is to review all the requirements that both the CSP and remote customer need. Security policy provides a set of security objectives and tasks, as for example defined in the mostly used ISO/IEC 17799:2000 computer security standard [6] [7].

Auditing subsystem is used to store sufficient data about every relevant action in the calibration system. In this way, it can be confirmed that calibration took place and can be determined types of measurement, values and final result of the calibration process.

Data integrity protection over the communication network is obtained by using encryption. In our case, it is achieved using integrated IPSec security mechanisms that assure no data has been seen or altered during the transmission over the network. Integrity of the whole calibration system is achieved by combining the use of IPSec, authentication control on the client and CSP side and the storage of all (raw and processed) calibration data on the main CSP server. Currently, the CSP information system implements SSL protocol using Java Secure Socket Extension (JSSE) that implements SSL and TLS protocols and includes software parts for server and client authentication, data encryption and integrity.

When Java applets are used or JNPL application is delivered to the client PC to run client-side calibration procedure, security issues related to the connection between server and client are addressed directly to the secure web server (also using the SSL/TLS methods).

Unfortunately, network data transmission and storage security is only a part of a series of security aspects in this area that need to be considered.

B. Hardware security issues of remote calibration

Another potential problem, usually neglected or ignored because of not understanding, but requiring much consideration is the communication between customer-side PC and other instruments, for example over the often used IEEE 488 – GPIB interface. Since this protocol has no built-in security elements and was not designed to support integrity, encrypted and confident transmission, communication over this media is endangered.

The main risk points of unauthorized access and alteration of the calibration system are the data (e.g. GPIB) connection between the customer-side PC and CSE and UUT. For example, someone can use specially designed software components to listen and intercept GPIB commands and data transmissions, altering them, everything leading to forged calibration data.

For example, standard IEC 60488-2 [8] defines a set of commands that every measurement instrument should implement. One of the mandatory commands is "*IDN?" that implements identification query of every device over the GPIB system interface. Every instrument should respond to this command with the following information: full manufacturer name, instrument model, serial number and firmware version or equivalent data. With this information calibration software could get enough information to uniquely identify, to be able to self adopt and distinguish instruments and other connected equipment to the GPIB bus. In our case, a possible solution for this problem is specifically designed GPIB encryption module (implementing AES/DES crypto algorithms on ATMEL ATmega128 microcontroller) to serve as a communication protection for the instruments connected to the GPIB. Detailed discussion about this topic goes beyond the scope of this abstract, but more information can be found in [9] and [10].

In the future, the IEEE 488 and similar, future coming instrumentation interfaces and technologies should be upgraded for security services, providing the same protection level as used in the computer network surroundings.

5. APPLICATION AREAS OF REMOTE CALIBRATION

It is possible to imagine many different remotely enabled calibration procedure implementations, not every calibration is equally suited for remote operations. One of the leading prerequisites is that a calibration procedure is highly automated and

that only a minimum of human interaction is required. Usually it is needed to have, for example, a multifunctional calibrator for a calibration of electrical quantities, or extra hardware that will automate and facilitate measurement process, keeping human interaction at minimum level. Complex numerical analysis of measurement results and knowledge that stands behind are important part of calibration process. In a case of remote calibration process, all the expertise and knowledge that can be delivered to the client more easily compared to a classical calibration process.

6. CONCLUSION

This paper has shown a complete calibration system that is under process of constant development on the Faculty of Electrical Engineering and Computing, University of Zagreb. The key feature of the proposed distributed calibration system is its usability and extensibility. A client-server application manages the calibration process and implements all the necessary security solutions that minimize the possibility of fraud. It is important to consider that the data security methodology is relevant to the user of Internet-enabled calibration services. The system proposed could become the kernel of a future accredited certification service based on remote on-site calibrations.

References

[1] W. Anderson, N. Oldham, M. Parker, „SIMnet: an Internet-based video conferencing system supporting metrology“, Proceedings of the 2000 NCSL Workshop & Symposium, Washington, July 2000.
[2] R. A. Dudley, N. M. Ridler, "Traceability via the Internet for Microwave Measurements Using Vector Network Analyzers", IEEE Trans. Instrum. Meas., vol. 52, no. 1, pp. 130-134, February 2003
[3] F. Cicirelli, A. Furfaro, D. Grimaldi, L. Nigro, F. Pupo, “MADAMS: A software architecture for the management of networked measurement services”, Computer Standards & Interfaces 28 (2006), 396-411
[4] M. Jurčević, M. Boršić, D. Cmuk, “Design of an internet-enabled calibration system”, Proc. 19th Metrology Symposium, September 2005, pp 118-121.
[5] “ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories”, http://www.iso.org
[6] Stallings, W., “Cryptography and Network Security”, Prentice Hall, 2002
[7] “ISO/IEC 17799:2000 Information technology - Code of practice for information security management”, http://www.iso.org
[8] “International standard IEC 60488-2 – IEE 488 - Standard digital interface for programmable instrumentation – Part 2: codes, formats, protocols and common commands”, IEEE, 2004, http://www.iec.ch
[9] M. Jurčević, M. Boršić, R. Malarić, “Security issues of Internet-Enabled Calibration Services”, VI Sementro Anais Proceedings, Inmetro, Rio de Janeiro, Brazil 2005, pp 110 - 112
[10] M. Jurčević, R. Malarić, M. Boršić, “Designing a Public Key Infrastructure implementation for calibration laboratories”, Proc. of the 19th International Metrology Symposium, Zagreb, Croatia 2005, pp 113 - 118