TECHNOLOGICAL DEVELOPMENTS

Security of computerized instruments

JEAN-FRANÇOIS MAGANA, Sub-Directeur of Metrology, Ministry of the Economy, Treasury and Industry, France – CIML Member for France

Introduction

The objective of legal metrology is to ensure a sufficient level of confidence in measurement results. Measuring instruments must have well-suited metrological characteristics (i.e. accuracy, reliability, sensitivity and durability) such that they give exact measurement results during their life-cycle. In addition, they must either not be affected by external influences which may distort these results, or be protected against such influences, or even clearly indicate those factors which might alter the measurements.

The influences to be considered may depend on:

- the instrument's conditions of installation (horizontality of a weighing machine or of a water meter, straight lengths of pipes, etc.);
- the instrument's environment (very few factors were actually found to influence the correct operation of mechanical instruments, though these factors did tend to affect durability);
- the actions of the user (bad handling or attempts to engage in fraudulent use: mechanical instruments only allowed very simple operations to be performed. Handling errors also needed to be reduced).

When instruments were purely mechanical, the risk factors (and the consequences thereof) were simple, there were not very many of them and they could virtually all be analyzed.

Fraudulent handling was rendered impossible by simple methods:

- either such attempts were subsequently clearly visible,
- or fraudulent handling was made impossible by physical access protection (sealing) of the instrument's critical elements.

At this time and up until the middle of the 1970's, the legal metrology profession called for competence mainly in the fields of mechanics and fluid mechanics, and perhaps also to a certain extent in thermodynamics. Since then, the general and constant trend within the civil service has been to reduce staff, which has put the brakes on staff renewal and the recruitment of new skills.

Meanwhile, the use not only of electronics but especially of computer technology in measuring instruments has acutely disrupted the "state of the art".

The technological electronic evolution

Electronics has considerably developed instruments' performance, though at the expense of increased sensitivity to their external environment (temperature, humidity, electrical and electromagnetic disturbances, etc.). The reliability and durability of these instruments have become critical subjects, which Document OIML D 11 goes some way to addressing. Techniques have developed, but in a way which has allowed legal metrology staff to adequately keep pace with these new technologies.

A difficulty nevertheless began to appear: the extreme rapidity with which electronic components have developed, which raised the problem of conformity of the instruments to the approved pattern. This problem was not completely new, since even for mechanical instruments, the quality of the steel used and the quality of the processing of the surface of certain metallic parts,

La version originale française de cet article ("Sécurité des instruments informatisés") a été publiée dans le Bulletin d'avril 1999

the composition of plastics, or even the packaging of plastic granules before injection were all essential criteria, though of course difficult (if not impossible) to check on the finished product. Conformity assurance of electronic instruments was therefore dealt with in the same way as that of mechanical instruments, which has in fact given satisfactory results. Conformity falls under the responsibility of the manufacturer and is presumed to exist unless the contrary is proved. On the initiative of the manufacturer or of the checking authorities, instruments or parts of instruments selected at random from a production batch can be submitted to some or all pattern approval tests. This "black box" type examination provides sufficient confidence as to the conformity of electronic instruments.

Computerization

Computerization, on the other hand, has radically changed the legal metrology profession. Whilst a computerized instrument can on the surface look like an electronic instrument and may seem to be only a development of it, this is in fact misleading. What beneficial effect does computerization actually have on instruments?

- It does not inherently improve rough measurement results. The key element for the metrological performance of an instrument is the sensor. Whilst the reliability and reproducibility of sensors have increased, this progress owes nothing to computerization. Computerization allows the behavior of a sensor to be modeled and allows complex procedures (that could be applied at calibration laboratory level) to automatically be applied to the processing of its output.
- It allows more complex calculation and processing operations to be carried out. This power of calculation allows pressure, temperature and density corrections to be made to a flow measurement with a high sampling rate. It allows the non-linear sensor response curves to be rectified, and permits analog-digital conversions to be traced to a sole standard component instead of several.
- It allows for considerably more functions, which are more complex and sometimes outside the scope of legal metrology. For example, a gasoline service station terminal manages not only the fuel pumps, but also handles the accounting side of credit card transactions, calculates the remaining stock volume of fuel in the tanks, and also takes care of the shop sales transactions.
- It allows different instruments to function in a network: for example in a sugar beet warehouse, computers link together in a network the identification badge readers, the "in" and "out" weighbridges, the various sample-weighing machines, and the analysis laboratory saccharimeters.
- But it also introduces new vulnerability, much more complex and this time invisible. Computerization offers the possibility for instruments to communicate with their users and to receive orders, even basic ones. However, any possibility of giving orders to a computerized system or to provide it with parameters or data may also provide an ideal opportunity to hack its normal operation.

The techniques of legal metrology are consequently much more fundamentally modified by the introduction of computerization than by electronics. Whereas electronics simply required a parallel development of personnel skills which could be accomplished by providing ongoing training, computerization introduces a radical break from this concept. The required techniques now relate to the security of computerized systems and can only be acquired by in-depth training.

The study carried out in France

The *Sous-direction de la Métrologie* conducted a study by security experts in computerized systems of:

- current requirements of regulations (transcribed from the most recent OIML Recommendations);
- methods and procedures for type/pattern approval (harmonized in Europe by the various WELMEC Guides and Draft Guides);
- the instruction of certain pattern approval dossiers; and
- the state of the art as regards computer security

among a number of French measuring instrument manufacturers. This study, of which some extracts are given in the annex to this article, shows how questions of legal metrology are tackled by computer security professionals and what the necessary skills are, respectively, for:

- specifying the statutory requirements as regards the computer security of measuring instruments;
- approving instrument models with a view to their security certification being delivered by a specialized body; and
- dealing entirely with an approval dossier, including computer security.

This study also addresses the problem of modifications to models of instruments after their approval and the taking into account of these modifications in the

regulations. This extremely important question is not, however, the subject of the present article.

Instruments and fraudulent use

One of the main questions brought up in this report on the security of measuring instrument software is whether there is a risk of fraudulent use: this has always been possible in the case of mechanical instruments, even by merely removing the seal and replacing it with a counterfeit or stolen seal. The difference brought about by computer technology is that fraud now tends to be more widespread: whilst fraud on mechanical instruments remained localized and was limited by the availability of tools and the necessary know-how (for example a false stamp), a means of defrauding a computerized instrument may instantly be communicated to numerous potential defrauders, or even broadcast on the Internet. Furthermore, defrauding a computerized instrument may be subtle and not visible when the instrument is checked.

Another characteristic of fraud is that it depends on the confidentiality of information held by the manufacturers and by repair engineers. The codes authorizing access to protected parameters and zones of an instrument are intangible (e.g. password, coded message, etc.). Even if the instrument knows how to "defend itself" against intrusion attempts, a certain vulnerability remains if there is a risk that certain staff of the manufacturer or of the repairer are likely to disclose these keys. If such disclosure by a dishonest employee does not necessarily harm the manufacturer, limited legal means are available to repress such deeds and the penal sanctions of legal metrology regulations are not adapted to these new crimes. Complicity of fraud can be put forward, but the fraud will for its major part be potential and not actually witnessed.

The temptation to defraud

All categories of instruments do not, however, suffer from the same degree of risk: certain users are reliable (the police force for example), and certain frauds are not profitable. One recommendation of the study should be rapidly followed: to define a risk scale for various categories of instruments as regards the temptation to defraud, which can be evaluated by counterbalancing two types of considerations:

- the gains anticipated by the fraudsters, depending on the number of instruments being used, on the cost of products or the services measured by the instruments;
- the risk that the fraud is discovered without any particular anti-fraud measures being incorporated in instruments (denunciation, cross-checking between several independent measurements, risks of leaks due to the number of people involved, etc.).

One can therefore define a scale of initial risk of fraud (before this risk is reduced by the security measures required by the regulations). The level of resistance of the security mechanisms in the instruments will then be determined in view of this initial risk.

Taking into account the risk of fraud

Another question raised by this study is to decide what measures to take if an inherent weakness in the system becomes known to the public (a password for example). Three cases are possible:

- either the risk of fraud is accepted as such;
- or it is possible to reconfigure the security mechanisms or to bring into operation counter-measures which reduce this vulnerability (reconfiguration or reprogramming) on instruments in service; or
- the instrument must be withdrawn from service.

This problem arose for a scrambled TV channel when the circuit diagrams for its first decoder were published in a magazine. The TV channel set about designing a new generation of decoders, which completely replaced the previous generation. In this case their decision was made on economic and business grounds, but in legal metrology if such a decision has to be made by the statutory authorities then various complex problems arise, notably as regards the onus of responsibility.

No computer system is completely risk-free as far as its vulnerability is concerned: a certain degree of inherent risk is acceptable during pattern approval, but can become unacceptable when this risk element becomes a real threat, even though the instrument is strictly identical. This raises the difficult problem of the onus of responsibility. A manufacturer takes responsibility for any defects that arise in the instruments he produces, however when a residual risk has been identified and accepted (even implicitly) by the pattern approval authority, if this risk subsequently becomes a reality then only the authority's responsibility should be questioned. Can a known risk be legally considered as a hidden defect once it appears? Can the pattern approval body be held responsible for the consequences of this risk? These questions are legally complex, but must be dealt with.

The skills of legal metrology experts

The study report also suggests a description of the skills required to carry out the activity of regulation and pattern approval, as well as a training plan to this end. Three levels are defined, in line with the following objectives:

Level 1:

To know how to set out statutory requirements (in the electronics and computerization fields);

Level 2:

To know how to read and understand an assessment report of the computerized security aspects of an instrument;

Level 3:

To know how to evaluate the computerized security of an instrument.

One only needs to read this part of the report, which describes the basic pre-requisites and the training plans corresponding to these three levels, to realize that legal metrology is really a new profession.

Each person in charge of a legal metrology technical unit will be able to judge what proportion of its personnel meets the necessary requirements and is therefore capable of following the training described. This report will often be worrying for those bodies that did not experience a rapid and recent turnover of their personnel with a recruitment profile such as that proposed in the report.

Some may feel that the author of the report has voluntarily set very demanding objectives in his recommendations in order to increase the value of those organisms specializing in computer security. But this is not the perception of the experts at the *Sous-direction de la Métrologie*, who have worked together with that expert on the practical analysis of approval files, and who are convinced that these recommendations are indeed relevant.

Experts at the *Sous-direction de la Métrologie* regularly carry out pattern approval of computerized instruments and apply the "state of the art" as accepted in Europe, which represents some of the methods presented in this report. The recommended in-depth analysis does therefore appear necessary to the specialists of the *Sous-direction de la Métrologie* in order to better master the subject, and provides both an approach and tools which are more complete and more coherent.

Conclusion

A final piece of advice for those in charge of legal metrology bodies who perhaps are not convinced of the need to radically update skills would be that they compare the evolution of the age-structure (and types of training) between:

- the designers of measuring instruments in the majority of companies; and
- specialists in legal metrology services.

Without detracting from any of the credit that is due to our elders, and whose experience and judgment is still of great value, the above comparison is self-explanatory. ■

Excerpts of the CR2A-DI report on the security of computerized instruments

2.3 Fraudulent use of measuring instruments

The level of examination of the security of computer programs that are subject to legal control can be adapted in line with the degree of risk of fraud that is associated with the category of measuring instruments of which such programs are an integral part. This risk factor can be determined according to various parameters, for example:

- the potential gain of tampering with a computer program, which is to be compared with that which might result from the instrument itself being fraudulently manipulated whilst actually in use: in some cases it is perhaps neither necessary nor justified to excessively protect the software components of a measuring instrument that can in fact easily be manipulated during use;
- the penalty incurred, which is to be weighed up against the potential gain;
- the probability of whether the fraud might be detected within a reasonable time period;
- the number of people who must be involved in the fraud;
- the number of measuring instruments manufactured, since no criminal will ever invest more time and money in trying to cheat an instrument than the amount he hopes to gain from such an activity. The development of anti-fraud mechanisms (for example, "clocking" taximeters) may require several months

of study, design and development. It is more profitable for the criminal who is looking for a return on his investment to concentrate on measuring instruments manufactured by the thousand rather than in small quantities, and so consequently the size of the criminal's potential market is directly proportional to the number of measuring instruments on the market;
- the type of customers using the measuring instruments in question to make transactions: industrials have more means at their disposal to cross-check and verify information than retail sellers, for example. One is therefore more likely to see dishonest practices in the retail sector rather than in the industrial sector;
- the category of users (such as police officers, postal workers, bailiffs, experts, garage owners, truck drivers, retailers, etc.).

When the stakes are particularly important, it can be necessary to require that the metrological part of the measuring instrument be the subject of an assessment according to ITSEC criteria, in which case the level of assessment must be determined as early on as possible, since taking into account certain assessment criteria has an influence on the development process and on manufacturers' internal organization. For an assessment according to ITSEC criteria to be successful, these criteria must be respected before development even begins. The case of pattern approval of a measuring instrument that is the subject of an assessment according to ITSEC criteria is dealt with in more detail later on in this document.

2.4 Security objectives

The security objectives stated below are of a generic nature so that they may be adapted to any category of measuring instrument. They are expressed independently of any notion of assessment according to ITSEC criteria:

- to give advance warning of attempts to defraud using commercially available tools (such as text editors);
- to prevent unintentional misuse;
- to guarantee that the measuring instrument does not comprise any hidden functions which would allow its metrological behavior to be modified. Such hidden functions may either exist without the knowledge of the manufacturer (design defect or vulnerability of one of the instrument's components), or be voluntarily added to the metrological program by the development team, in order to negotiate their illicit use;
- to guarantee the exactness (i.e. the integrity) of the metrological data throughout the measurement operation, during their transmission, printing and/or display and possibly even throughout the duration of their storage. Anyone in possession of a measuring instrument must not be able to modify such data;
- to guarantee the availability of the metrological data throughout the whole measurement, and possibly throughout the duration of their storage;
- to guarantee the origin of the metrological data during their transmission;
- to guarantee the inviolability of the critical security mechanisms;
- to guarantee that no design, implementation or applicational defect is present;
- to guarantee that each category of user (owner, repair engineer, etc.) only has access to those functions that are authorized for him;
- to guarantee that the various user modes allow the user's identity to be confirmed (ID check);
- to guarantee that any malfunction of the metrological part of the program is detected and that the measurement is not able to be carried out;
- to guarantee the exactness of the identification of the program (version and serial numbers, etc.);
- to guarantee the permanent operation of the security functions and mechanisms;
- to guarantee the presence of certain mandatory devices, where appropriate;
- to guarantee the preservation of security in the case where the instrument malfunctions or in the event of a power failure;
- to guarantee, if necessary, the protection of the confidentiality, integrity and availability of secret elements (codes, passwords, etc.), including cases of malfunctioning;
- in the case where this option is applicable, to ensure the imputability of any actions executed on the instrument that have a bearing on the metrological part (calibration, tariff entry, etc.) by keeping a log of these actions.

Measuring instruments undergo laboratory tests which serve to ensure their continuity of operation despite any electrical, electromagnetic or atmospheric (hygrometry, temperature) disturbances. Any malfunction that occurs due to this type of disturbance is therefore outside the scope of this study and does not call for any security objectives to be detailed.

3.1 Determination of the level of assessment for a category of measuring instruments

The cost of an ITSEC assessment depends on the size of the assessment target and on the level of assessment. The ITSEC criteria lay down the requirements for conformity and efficiency assurance.

The requirements for conformity assurance can be summed up as follows:

- *level E1:* at this level, a security target and an informal description of the general conception of the assessment target must exist. The functional tests must indicate that the assessment target complies with its security target;
- *level E2:* apart from the requirements of level E1, an informal description of the detailed conception must exist and elements of proof of the functional tests must be evaluated. There must also be a configuration management system and an approved distribution process;
- *level E3:* in addition to the requirements of level E2, the source code and/or the descriptive diagrams of the equipment corresponding to the security mechanisms must be evaluated. The elements of proof of the mechanism tests must be evaluated;
- *level E4:* in addition to the requirements of level E3, a "formal underlying pattern of security policy supporting the assess-

ment target" must exist. This formal pattern is an abstract presentation of the important security principles that an assessment target should cause to be respected. It is a model of security requirements which absolutely has to be realized in a formal language and accompanied by an informal interpretation from the angle of the security target. The functions dedicated to security, plus the general and detailed conception must be specified in a semi-formal style;

- *level E5:* in addition to the requirements of level E4, a close conformity must exist between the detailed conception and the source code and/or the descriptive diagrams of the equipment;
- *level E6:* in addition to the requirements of level E5, the functions dedicated to security as well as the general conception must be specified in a formal style and in a coherent way with the underlying formal pattern of security policy.

The meaning of the quotation of the resistance of the mechanisms is as follows:

- in order for the minimum resistance of a critical mechanism to be quoted as being "elementary", it must be evident that it provides sufficient protection against random accidental subversion, even though it is likely to be overridden by competent criminals;
- in order for the minimum resistance of a critical mechanism to be quoted as being "average", it must be evident that it provides sufficient protection against criminals who only have limited opportunities or competence;
- in order for the minimum resistance of a critical mechanism to be quoted as being "high", it must be evident that it can only be overridden by criminals who are highly competent, and who have the necessary skills and resources - however a successful attack is normally deemed as not being feasible.

Within the framework of programs, criminals can use means of attack such as password dictionaries (available on the Internet) which allow them to discover passwords and thus gain access to privileged modes of use such as system administrator access rights. Criminals may also make use of retro-engineering tools which allow them to piece together the source code from the executable code. It then becomes easy to modify the code in order to introduce complementary functions or modify its existing functions.

The level of assessment must mainly be chosen both in line with the risk of fraud for the category of measuring instrument and in line with the stakes associated with the fraud. For example, if it is really necessary to ensure that there are no hidden functions in the metrological program, then it is preferable that the source code be examined by the assessors. In this case, only assessment from level E3 up caters for this.

Likewise, if the stakes associated with the fraud are so potentially high that there is a quasi-certain risk of large-scale attempts being made to bypass the security mechanisms protecting the metrological parts of programs, possibly even at international level (as is already the case on the Internet where whole sites are devoted to hacking), then it will be necessary to increase these mechanisms as much as possible.

Note: The preceding statement about Internet leads to a first recommendation: it is becoming increasingly necessary for legal metrology authorities to monitor and regularly search for sites or forums on the Internet whose intent is to propagate piracy of measuring instruments that are subject to legal control. In order to remain anonymous during these searches, it is preferable to set up a separate Internet access and to use a pseudonym. It is clear that for example an address like X.Y@industry.gov.country is too conspicuous and might cause the surveillance to fail.

4.1 Typical elements of the pattern approval program

One of the objectives of this study is to determine the typical elements of the program to be requested of manufacturers with a view to pattern approval. These typical elements are those which allow all or part of the following to be ensured:

- the integrity of the metrological part of the program is regularly checked, at time-intervals to be defined according to the category of the measuring instrument (e.g. before each measurement, on each power-up, every hour, etc.);
- a measurement cannot be made if the result of the integrity check of the metrological part of the program reveals the existence of a problem, in which case a specific error message must be displayed;
- the integrity of the main indications (i.e. quantities whose values are subject to state control) is maintained and regularly checked;
- during the measurement operation it is impossible to modify those main indications that are not intended to be measured during that operation (e.g. the unit price);
- if the measuring instrument comprises a programming/consulting mode which allows the user to enter data (e.g. unit price, nature of the marketed products, etc.) or to consult management data stored in the memory (e.g. total sales, total mileage covered, etc.) then it must be impossible to make a measurement when the measuring instrument is in programming/consulting mode;
- access to programming, repair and calibration functions intended for use only by approved bodies is protected by a security mechanism (e.g. by a password), the resistance of which is sufficient to counter the risk of fraud of the measuring instrument;
- the integrity of the metrological data is checked throughout the measurement by a security mechanism whose resistance is proportional to the risk of fraud of the category of measuring instrument (CRC, encryption, etc.). A specific error message is displayed if a problem arises and if possible the measurement is stopped;
- the integrity of the data stored in the memory is preserved and regularly checked;
- the data are stored in the memory together with the date of the transaction in order to allow them to be kept over a predefined period;
- data stored in the memory cannot be erased before the end of this predefined period;
- if the data storage media become saturated, transactions are blocked or a special process of data deletion is activated. In both cases, a specific error message must be displayed. The special process of memorized data deletion must only take place after explicit agreement has been obtained and in accordance with an exceptional procedure;

- the interfaces of the metrological part of the program protect it with regard to the outside;
- the communication protocols used guarantee that the integrity of information flow is checked;
- the program does not comprise any hidden functions, i.e. the set of visible commands is exhaustive;
- the data display times and the transition from user mode to data programming/consulting mode are compatible with the type of measuring instrument. These display times serve to avoid any confusion between the amount due and (for example) a totaling up of the management data memorized;
- the confidentiality of non-transferable information, if it exists, is maintained;
- it is possible to identify the version number of the program and to prove that it is really the version number which is displayed;
- it is possible to ensure that the same program that actually underwent pattern approval is in fact installed in the measuring instrument;
- the metrological part of the program has been the subject of functional tests according to a scenario of predefined tests. The scope of the tests leads to a reasonable assurance that the security of the program is determined in line with the resistance it must put up to attempts to defraud.

The elements of proof which enable the officer to carry out the necessary checks can take the form of a descriptive documentation of the instrument's functioning, conception documents (specification of needs, general conception, detailed conception, analysis file, logic diagram, source code, etc.), technical specifications of components, tests reports, etc. These elements of proof currently vary in content.

5.1 Core syllabus training

5.1.1 Pre-requisites

The examination of the security of programs or of electronic transmissions requires certain knowledge both of computerization/electronics and of information systems security. The latter is dealt with in section 5.1.2 *Security awareness*.

The objective of this section is to list the skills required in the fields of computerization and electronics. Given the wide scope of the subjects in question, it will doubtless prove necessary to divide up the skills amongst several individuals who will act in a complementary manner.

Note: Dividing the skills up in this manner may have an influence on the future organization of the pattern approval body. In the future it might perhaps be necessary to share out the examination of pattern approval files between the recorders by fields of competence, in line with the internal structure of the measuring instrument rather than by categories of measuring instruments, as is the case now.

The required knowledge in the field of computerization is as follows:

- good general knowledge of microcomputing: knowledge of the internal structure and of the functioning of PC's and of different peripheral devices;
- good practical knowledge of standard operating systems (Windows 3.X/95/98/NT, Unix, etc.);
- good general knowledge of basic computerization skills including knowing what an operating system is and what programming languages, compilers, linkers, communication protocols and so on are;
- good knowledge of standard protocols (TCP/IP, etc.) and OSI layers;
- practical knowledge of Internet.

The required knowledge in the field of electronics is as follows:

- good knowledge of cabling (twisted pairs, coaxial cables, optical fibers) and of different types of network mapping and of their consequences;
- good general knowledge of components likely to be incorporated in measuring instruments (RAM, ROM, EPROM, network cards, microprocessors, etc.) and of their use;
- necessary knowledge for the examination of the appropriateness of an electronic circuit diagram;
- good general knowledge of electricity.

5.1.2 Security awareness

Recorders' awareness of the security of information systems is a necessary prerequisite to more advanced training on security. The organization of the awareness session may comprise two parts:

- general security aspects;
- personalized aspects.

The general security aspects may follow the following plan:

- generic description of an information system, which consists of physical resources (computers, networks, peripherals, etc.) and logical resources (software packages, applications, data);
- definition of the main concepts used in security (security objectives, threats, parries, availability, integrity, privacy, authentication, identification, access control, attack, vulnerability, etc.) and explanations on vocabulary that is specific to the security of information systems;
- illustration of some cases of damage caused to computers due to piracy, for example unauthorized changes made to Internet sites, etc.);
- general description of the tools which could be used to carry out such piracy (password dictionaries, etc.);
- general description of some known weaknesses (usurpation of administrator rights);
- description of the main security functions used (access control, audit, etc.) and of their implementation (use of the functionalities of the operating system, presentation of the main sets of tools used in the trade such as firewalls, etc.);
- introduction to network security;
- succinct presentation of the ITSEC assessment criteria and of the actors and roles associated with these (SCSSI, CESTI, assessor, manufacturer, etc.);
- succinct presentation of the documents produced in association with the ITSEC assessment criteria (security target,

efficiency and conformity, RTE, etc.), as well as notions of the assessment target, security function, etc.;
- summary of the regulations associated with the security of information systems (legal protection of confidential information, encoding, etc.);
- presentation of the main French methods of assessing the security of information systems: MELISA, MARION, MASSIA.

Note: MELISA, MARION and MASSIA are methods which allow on-site audits to be carried out in order to estimate the degree of vulnerability of an information system. Although these methods are not directly exploitable within the framework of legal metrology, consulting them may prove fruitful since they provide useful information as to the global vulnerabilities and threats that can exist, as well as the countermeasures to be implemented to efficiently combat them.

5.2 Level 1 training

The objective of level 1 training is to be in a position to formulate statutory requirements in terms of program and electronic transmissions security. The aim is to use these requirements as specifications when drawing up security targets for those measuring instruments that must be assessed according to ITSEC criteria. They must be adapted to the applicational context of the measuring instruments, to the risk of fraud which is associated with them as well as to the technologies used. It is advisable to gain an in-depth knowledge of information systems security in order to have a global overview of the subject.

The degree of skill aimed at must be equivalent to that of a computer/electronics engineer with 2–5 years' experience, including significant experience in security.

The aspects to be examined are:

- good knowledge of regulations relating to the security of information systems;
- good knowledge of ITSEC assessment criteria;
- good general knowledge of security solutions: this knowledge must allow the requirements to be dimensioned in accordance with the category of measuring instrument concerned;
- good knowledge of network security;
- practical knowledge of the EBIOS method.

Note: The EBIOS method aims to express needs and identify security objectives. Although this method is not directly exploitable within the framework of legal metrology, it does give rise to a methodological framework which is appreciable when determining security objectives and which proves to be particularly useful when it is necessary to draw up a security target.

5.3 Level 2 training

The objective of level 2 training is to be in a position to understand the documents available when a product has been assessed according to ITSEC criteria and which are accessible to the pattern approval authority. These documents are: the security target, the certificate, the certification report and the product documentation. Actually, the assessment supplies are confidential, as are the assessors' end of task reports, as well as the RTE. The level 2 training complements the level 1 training.

The degree of skill aimed at must be equivalent to that of a computer/electronics engineer with 2–5 years' experience, including significant experience in security.

The aspects to be examined are:

- practical knowledge of the ITSEC assessment criteria and of the ITSEM manual;
- good knowledge of security solutions: this knowledge must be adequate to determine whether a security function is sufficient to ensure that security objectives are achieved;
- notions of encoding.

5.4 Level 3 training

The objective of level 3 training is to be in a position to carry out the equivalent of the profession of assessor. The level 3 training complements the level 2 training.

The degree of skill aimed at must be equivalent to that of a computer/electronics engineer with 5–10 years' experience, specialized in security. As stated before, the necessary skills should be spread out between several individuals.

The skills to be acquired are as follows:

- technological monitoring, in particular on the Internet, to stay informed of technological evolutions and to watch out for potential weaknesses and means of attack;
- in-depth knowledge of the ITSEC assessment criteria and of the ITSEM manual;
- in-depth knowledge of programming and assembler languages;
- in-depth knowledge of operating systems;
- in-depth knowledge of network architecture;
- in-depth knowledge of communication protocols (to know how to interpret data packets circulating on a network);
- in-depth knowledge of technologies such as micro chips, firewalls, encoding, etc.;
- in-depth knowledge of development platforms (workshops for program engineering and for computer-assisted design, etc.);
- in-depth knowledge of test techniques (data flow analysis, static and dynamic tests, analysis of test coverage, etc.);
- practical knowledge of attack tools (oscilloscopes, spectrum analyzers, deciphering machines, protocol analyzers, sniffers, password dictionaries, retro-engineering tools, source code analysis tools, etc.);
- if necessary, training in formal methods (in the event of assessment from level E4 upwards).
- knowledge of on-site audit techniques.