1.9 SOFTWARE

General
Unless you are using a completely mechanical weighing instrument, it's almost certain that it is controlled by software in one form or another. It would also be fair to say that if your system uses a weight only instrument then there is software within the other areas that will also require consideration.

Apart from the obvious requirement that the software controls correctly, it is imperative that the software is secure. Security is required to ensure that changes to that software can either not be carried out, or, if changes are made then there is an indication. This security can also encompass both stored and transmitted data to provide confidence in its validity.

Once a weighing instrument or, say an EPOS device, has been type approved, certain aspects of the operating software is classified as legal metrology relevant and the approval restrictions will be applied to it. Changes to these areas are not permitted without authority and possible changes in the type approval certificate (weighing instruments) or the EC test certificate (EPOS software).

The software used in weighing instruments and other systems, for example an EPOS system, is often divided into two categories, legal metrology relevant and non-relevant to facilitate practical future development.

Legal metrology relevant software
The legal metrology relevant areas of the software will include those processes or routines that deal with the metrology data or the control of data to and from this area. For example, procedures that calculate weight data from raw A/D data, procedures that process and store calibration, and even the procedures that ensure that valid data comes from the A/D and valid weight data is passed on for processing. This classification would include procedures in an EPOS system, as well as a weighing instrument, which takes weight information and calculates prices.

It is important that these procedures are not accidentally altered. Equally as important is the need to prevent malicious alterations, but today's use of normal computers and high technology tools make this almost impossible, so it has become necessary to provide a means of tamper indication.

The most secure form of software is that which is contained in ROM or some other form of one-shot memory and is recognised as "embedded". Although secure, it is necessary that these components are either sealed in position or that some form of tamper indication is available.

Those instruments that use a PC for processing also use freely programmable software. This form of software is perceived as the most vulnerable to both accidental and malicious attack. A common security measure is to provide an indicator in the form of a checksum or CRC. This information is published in the certificate and the system provides a means of comparison.

Software submitted for approval must be produced in a controlled fashion, usually demonstrated by a form of issue version identification. Any alteration to the status of a software package should be reflected in a change to its version identification and submitted for any relevant changes to the certificate.

Non-relevant software

It would be unreasonable to require changes to a certificate if a software modification did not affect its legal metrology relevant area. For example, changes to move the position of an item on the screen or to alter a colour feature. This type of software is not relevant to the legal metrology; therefore, it need not be included within the security measures. It is still necessary to maintain some form of modification control and in these cases it might prove useful to use an issue identification system that clearly indicates the use of separated software. For example, the first issue of the software could be identified as **Issue 01.01** where the number to left of the point would relate to the legally relevant part of the software and the number to the right to the non-legally relevant part; the Type Approval Certificate would then say that any software with an issue number 01.xx. is acceptable. Thus when the non-legally relevant part of the software was updated, e.g. to alter the position of some information on the screen, the software issue identification would be updated to **Issue 01.02** but it would still be acceptable under the Type Approval Certificate.

Controlled updating

With today's technology, it is possible to carry out remote updates to software in the field. If this is to be carried out, updates either direct or remote must be authorised and controlled. Remote updating poses a number of questions, the most important of which are, has the update been completed successfully and does the instrument or system still operate correctly?

References

WELMEC 2.3 Guide for Examining Software
WELMEC 7 Guidelines for Examining and Testing Interfaces and Peripheral Equipment
WELMEC 7.2 Software Guide (Measuring Instrument Directive 2004/22/EC)
BS EN 45501