Common Criteria Applications on Software Assessment Infrastructure for Legal Metrology in Brazil

Flávia Paiva Agostini
Researcher-Technologist in Metrology and Quality
Brazilian National Institute of Metrology, Quality and Technology - Inmetro

Agenda

- Inmetro
- Motivation
- Measurement System
- Conformity Assessment
- Legal Metrology
- History
- Guidance Documents
- Software Requirements for Legal Metrology
- Security Level
- Common Criteria and Legal Metrology
- New Opportunities
- CCRA

Inmetro Activities

- Scientific and Industrial Metrology
- Legal Metrology
- Accreditation
- Conformity Assessment
- Authority to issue Mandatory Technical Regulations

Legal control of measuring instruments

- **Type Approval:** Systematic examination and testing of one or more specimens of an identified type (pattern) of measuring instruments against documented requirements
  - *Performance tests (accuracy, repetition)*
  - *Durability*
  - *Disturbing tests (temperature, humidity, EMS*
  - *Protection*
  - *Software*
- **Verifications:** Examination for conformity with approved type, Initial, Subsequent (periodic, after repair, etc)

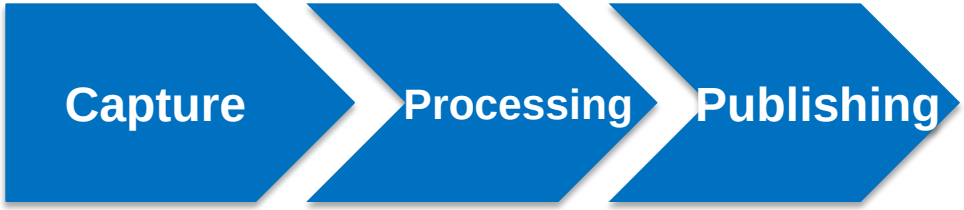
Motivation

Nowadays, software plays an important role on metrology, as most measuring instruments are mainly determined by embedded software.

Hence, software certification becomes part of the process to be performed in order to have a secure system.

Measurement Systems

- **A measurement system consists of all the elements involved in the capture, processing and publication of the measurement data.**



Legally relevant chain

Conformity Assessment

Time attendance clock employee recorder

PKI equipments

Legal Metrology

Vehicle Speed Meters

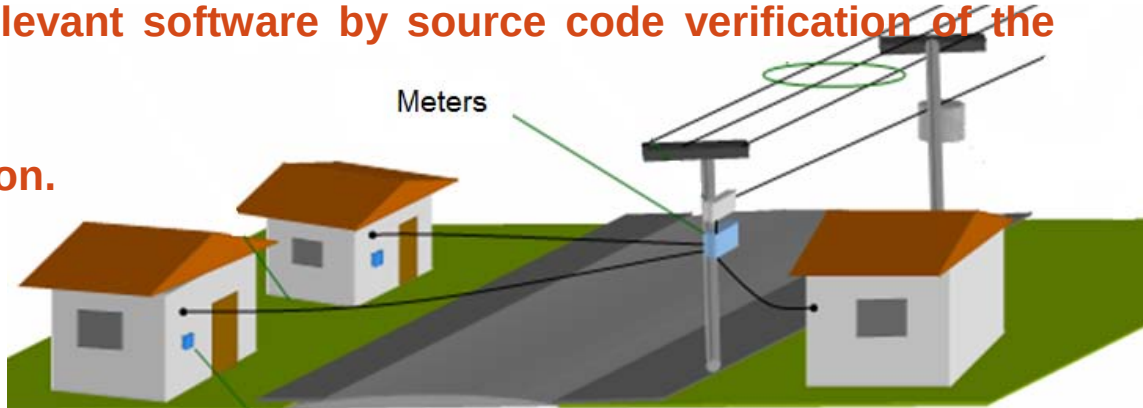
Fuel Dispensers

Weighting Instruments

Electrical Energy Meters

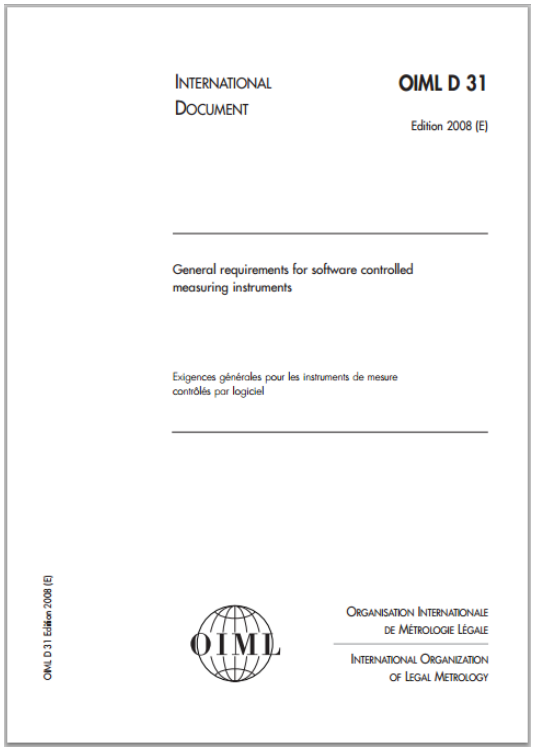
History

- In 2007, a first specific regulation for the Electric Energy Distributed Measurement System (SDMEE) was developed by Inmetro, requiring the existence of a consumer display.
- A specific regulation for the Centralized Measurement System (SMC) describing software requirements was first published by Inmetro in 2009.
- Based on this regulation, an assessment methodology was developed to the Electric Energy Distributed Measurement System (SDMEE), including three main steps:
  - Evaluation of the architecture and its operation based in the documentation analysis
  - Validation of the legally relevant software by source code verification of the embedded software, and
  - Software integrity verification.



Guidance Documents

- **WELMEC 7.2 [10] and OIML D-31 are some of the main sources of requirements and validation recommendations for software-controlled measuring instruments subject to legal control.**



Software Requirements for Legal Metrology

- Basic requirements
  - Software identification, user and communication interfaces security
  - Data transmission
    - Completeness, integrity, authenticity, confidentiality of keys, handling of corrupted data, delay and availability
    - Software Separation
      - Distinction of legally relevant software and not relevant, protective software interface
      - Download of legally relevant software
        - Authentication, integrity, software traceability, download consent
        - Fault recovery

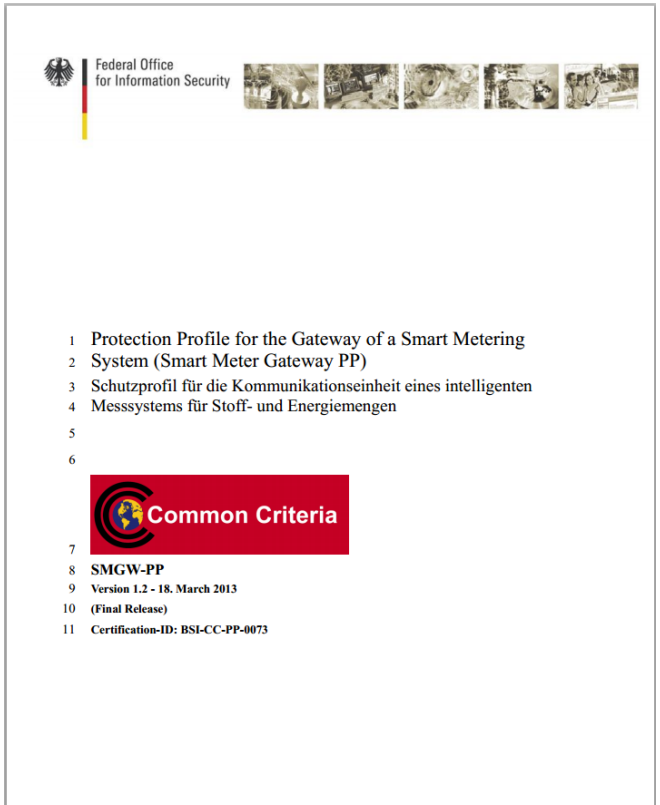
Security Level

- Welmec has defined 3 software examination levels:
  - Low: Standard type approval functional testing of the instrument performed.
  - Middle: In addition to the low level, the software is examined on the basis of its documentation.
  - High: In addition to the middle level, an in-depth test of the software is carried out, usually based on the source code.
- The requirement of opening the legally relevant software (source code) to Inmetro was a decision resulting from a broad discussion with internal and foreign manufactures, influenced by the architectural complexity of the system.

Common Criteria and Legal Metrology

- **In Germany, the BSI took the initiative to define a Common Criteria Protection Profile for the Gateway of a Smart Metering System.**

Clear security requirements for Smart Metering Gateways.



Federal Office for Information Security

Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)

Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen

Common Criteria

SMGW-PP

Version 1.2 - 18. March 2013

(Final Release)

Certification-ID: BSI-CC-PP-0073

New Opportunities

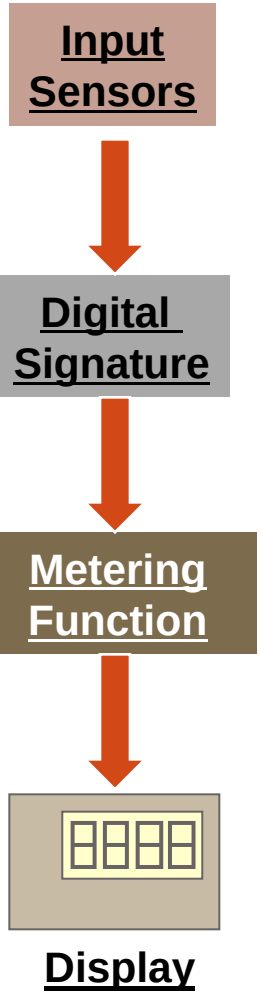
- **Digital Signature:**

The use of digital signature in measurement systems with embedded software not only as a tool to reduce or eliminate potential flaws/fraud in the type approval process, but also to enable the construction of a more efficient and reliable software validation process.

- **Common Criteria:**

Conduct the software evaluation process more efficiently, besides considering that it can also open the way to worldwide mutual recognition of evaluation results.

Unburden authorities of Legal Metrology.



CCRA

- **Brazil is encouraged to participate in the Common Criteria Recognition Agreement (CCRA), having already given rise to the first steps in that direction.**

Thank you!

Flávia Paiva Agostini
fpagostini@inmetro.gov.br