2025 IMEKO TC-6 International Conference on
Metrology and Digital Transformation - **M4DConf 2025**
Benevento, Italy, September 3-5, 2025

Single-Device Integration of Legal Metrology and Third-Party Software via Virtualization

Nicola Zingirian[1], Marco Profeti[2], Federico Botti[3]

[1] *Dept. of Information Engineering, University of Padova, Italy, nicola.zingirian@unipd.it*
[2] *Sampi S.p.A, Altopascio (LU), Italy, mprofeti@idexcorp.com*
[3] *Click & Find s.r.l, Genova (GE), Italy, f.botti@clickandfind.it*

***Abstract* – Integrating process-support functionalities within legal for trade-certified metering heads is a significant challenge in the digital transformation of industrial metering. In this context, we present a virtualized software architecture successfully implemented on the TEX® electronic metering head by IDEX/Sampi S.p.A., a commercially available, legally certified metrological device. The resulting system includes a host machine running legal metrology software and a virtualized guest machine managing auxiliary functions, which may be developed by third-party integrators. The guest handles the display, keypad, and I/O ports when no measurement is in progress. During measurement, the legal metrology software takes preemptive control to ensure legally relevant pulse counting, visualization of metrological data, printouts via sealed printers, and data storage in a database with read-only access for the guest system. This approach enables software extensibility without requiring frequent re-certifications while maintaining regulatory compliance, data integrity, and system flexibility. The proposed solution advances modern industrial metering, as demonstrated in a real-world use case.**

Keywords – Industry 4.0, Measurement Data Protection

I. INTRODUCTION

In modern industrial processes, the precise measurement and control of volumes and weights are essential to ensuring efficiency, safety, and regulatory compliance. Sectors such as petrochemical, food and beverage, and pharmaceuticals rely on metering devices to deliver accurate and legal for trade measurements. However, rising demands for automation, digital integration, and cloud connectivity introduce significant challenges, particularly in integrating metrological systems with enterprise resource planning (ERP) platforms [1]. Achieving this integration while remaining compliant with metrological regulations calls for innovative software and hardware architectures [2].

Metrology software that is certified as legal for trade—hereinafter simply referred to as "certified"— must guarantee that measurement data remain unaltered and protected from unauthorized changes. At the same time, industrial operators increasingly require flexible integration with automation systems, control platforms, and quality assurance tools to record, process, and analyze data automatically. This boosts efficiency and reduces errors common in manual reporting [3],[4]. It also enables automation of procedures like loading, unloading, and digital authorization, improving real-time inventory tracking and overall process optimization [5]. Security requirements further complicate integration. As industrial devices grow more connected and cloud-based solutions become widespread, robust cybersecurity measures are needed to safeguard measurement data integrity and compliance. Software must enable secure interactions between control systems and external applications without undermining metrological standards [6],[7].

This paper addresses these challenges by presenting an innovative hybrid architecture that combines a certified metrology system with a virtualized environment for process-support applications. Virtualization allows non-certified auxiliary software to share the same hardware platform, ensuring compliance with regulatory and technical standards while enabling automation and digital integration. Key benefits include software segregation and data protection within a single device. Unlike traditional systems requiring separate hardware for compliance, often rigid and costly, this solution uses virtualization to logically isolate metrological and non-metrological functions, offering greater scalability and flexibility. Support applications can thus be integrated without additional hardware, overcoming major limitations of conventional approaches and enhancing operational efficiency, adaptability, and security in line with Industry 4.0 goals.

The remainder of this paper reviews the state of the art (Sect. II), defines the design goals (Sect. III), describes the implementation (Sect. IV), and presents a real-world use case (Sect. IV), followed by discussion and conclusions (Sect. V).

II. STATE OF THE ART

Modern metrological systems increasingly adopt digital architectures that allow integration with external applications. Some of the most relevant trends include:

- *Embedded Software in Certified Devices:* Many metrological instruments now include embedded software functions capable of executing certified measurement operations while providing controlled data access to external applications [8].
- *Cloud Connectivity and IoT Integration*: Industrial metrology is progressively adopting cloud-based architecture, allowing measurement data to be securely transmitted to cloud platforms for analysis, storage, and remote monitoring [9].
- *Edge Computing for Metrology:* Edge processing enables real-time data analysis and decision-making at the device level, reducing latency and enhancing system autonomy [10].

The virtualization approach presented in this paper offers an effective alternative for integrating ancillary functionalities, while maintaining compliance with key software certification requirements, according to the international guidelines issued by organizations such as OIML and WELMEC, taking care of:

- *Separation of Certified and Non-Certified Software*: Regulations mandate that certified metrology software must operate independently from any auxiliary software to prevent unauthorized influence on measurements [11][12].
- *Data Integrity and Security*: Measurement results must be securely stored, tamper-proof, and only accessible through controlled interfaces that do not allow modifications [13].
- *Software Update and Certification Compliance*: Any software updates affecting the measurement process must undergo a new certification process to ensure compliance with legal metrology requirements [13][14].
- *Interfaces and Interoperability*: Regulatory frameworks specify how metrological devices can expose data to external applications, ensuring that data integrity is maintained while allowing industrial interoperability [13][15].

III. DESIGN GOALS

Table I summarizes the key design goals of the virtualized metrology system, highlighting its architecture, security mechanisms, and operational safeguards. At its core, the system should support a multi-layered structure responsible for running the certified metrology software, and a virtualized execution environment, which safely hosts third-party applications without interfering with legally compliant operations. Metrological task preemption should ensure that certified functions always take precedence over auxiliary processes, with hardware resource locking preventing unauthorized access during measurements. To maintain security and regulatory compliance, the system should enforce certified firmware execution, using checksum validation, OTP authentication, and MD5 hashing.

Table 1. Design Goals

Design Goal	Description
Multi-Layered System Architecture	Host Layer, Virtualized Guest Environment, and Metrological Software & Data Handling.
Metrological Host Layer	Runs certified metrological software, manages low-level hardware, and ensures isolation of RS232, CAN, RS485, keyboard, display, and printer. Implements checksum validation and OTP authentication.
Virtualized Execution Environment	Provides an independent execution space for non-certified applications, ensuring fast boot and supporting UI, logging, and automation tasks.
Metrological Data Processing	Handles pulse counting, digital flow measurement, and secure read-only storage. Communicates via RS232 interface to metrological printer and exposes structured API.
Secure External Integration	Facilitates safe communication and execution of third-party software without compromising metrological processes.
Access-Controlled Display Management	Requires third-party applications to provide Application ID, Security Key, and Shared Memory ID for accessing shared display memory.
Secure Connectivity & Authentication	Supports LAN, Wi-Fi, and USB connectivity with strict access control policies.
Controlled Third-Party Application Execution	Regulates execution of auxiliary applications with CPU and memory allocation policies to ensure no interference with metrology.
Metrological Task Preemption	Ensures that metrological operations always take priority over auxiliary software.
Hardware Resource Locking	During active metrology operations, critical hardware is locked, suspending all auxiliary processes until completion.
State-Based Process Management	Defines operational states: Startup & Initialization, Idle Mode, Measurement Mode, Post-Measurement Processing.
Regulatory Compliance Enforcement	Security mechanisms to ensure firmware validation and legally compliant execution policies.
Read-Only Data Protection	Stores metrology data in a read-only database to prevent modification, with all interactions logged and audited.

Additionally, secure software update mechanisms guarantee that all updates follow encrypted and signed protocols, mitigating risks of unauthorized modifications. The combination of strict access control policies, secure connectivity, and state-based process management makes this architecture scalable, compliant, and future-ready for industrial metrology applications.

IV. IMPLEMENTATION

The diagram in Fig. 1 illustrates how virtualized architecture has been implemented on the TEX electronic metering head, through a host-guest virtualization model.

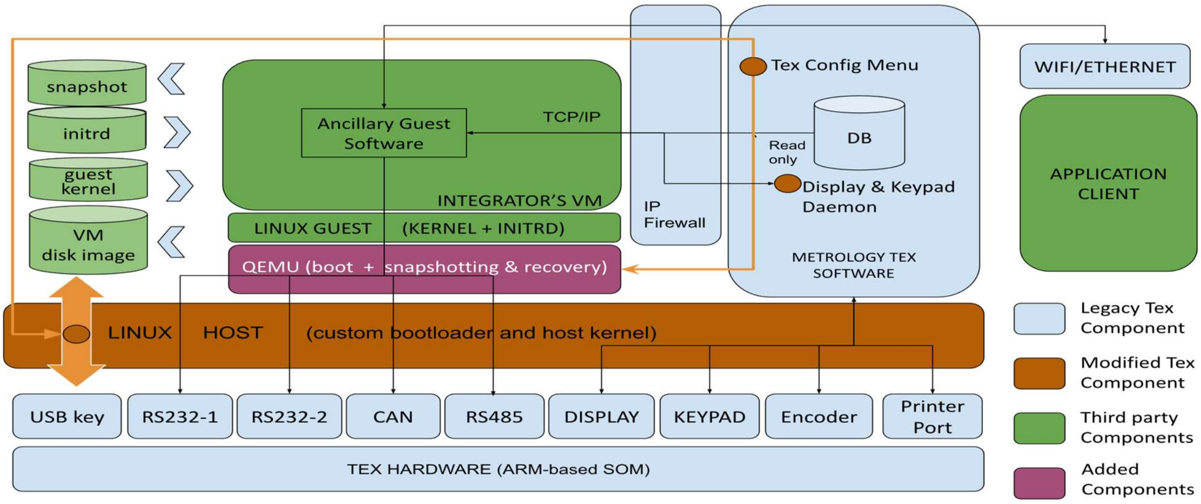

Fig.-1. System modules

A. Host Layer

The Host Layer runs a customized Linux-based operating system, modified to support efficient host-guest virtualization on ARM CPU. Some of the device drivers may be selectively shared with the Guest Layer through virtualized channels or controlled passthrough mechanisms, allowing the guest environment to access specific resources under tightly regulated conditions.

B. Virtualization Layer

The Virtualization Layer utilizes QEMU (Quick Emulator) [16], an open-source hypervisor capable of hardware emulation and Virtual Machine (VM) management. QEMU also manages VM snapshots, enabling quick, safe and reproducible initialization of third-party environments. Leveraging QEMU with KVM (Kernel-based Virtual Machine) [17] ported to the ARM CPU, this layer efficiently isolates the guest virtual machine, managing hardware resources and ensuring effective virtualization.

C. Guest Layer

The Guest Virtual Machine operates as an isolated environment within the QEMU/KVM infrastructure. It relies on a lightweight custom kernel, designed for rapid initialization and efficient resource management. The guest VM specifically handles non-metrological software applications, providing essential support services without affecting certified metrological operations. It has read-only access to metrological data, ensuring compliance with regulatory standards. During system installation, a USB key is used to load the third-party guest kernel and *initrd* (initialization RAM disk) through a configuration procedure integrated within the metrological software, for the secure and consistent guest VM bootstrapping.

D. Certified Metrological software

The certified metrological software runs directly on the Host Layer and relies on a secure database specifically customized for storing metrological data. To ensure data integrity, the Guest VM is granted read-only access, preventing any unauthorized modifications. Compliance with metrological regulations is further reinforced by restricting access to critical metrically relevant interfaces, such as the dedicated I/O port for the measuring encoder and the serial port for the fiscal printer.

E. Ancillary Guest Software

Non-certified applications, possibly developed by third-party integrators, run as Ancillary Guest Software exclusively within the VM, isolated from certified operations to ensure regulatory compliance, operational security, and data integrity. The software interacts with the TEX display and keypad through an internal LAN-based communication channel. This communication is handled by a dedicated daemon on the host system, which mediates access to the display and keypad. When permitted, the guest can read keypad input and write to the display without compromising metrological compliance.

F. Application Clients via Wi-Fi

The Application Client operates externally to the TEX system and connects Wi-Fi (or Ethernet) to interact with internal software components. Communication can be established through secure RESTful web services exposed by the Guest VM.

V. USE CASE: INTO-PLANE DELIVERY

The Dyna-Bus aviation refueling system, developed by Click & Find integrator, is the first real application based on the virtualized development environment within the TEX electronic metering head. This system demonstrates how third-party software can leverage virtualization to extend the functionality of metrological systems without compromising regulatory compliance.

A. Segregation of Metrological and Non-Metrological Processes

Virtualization architecture ensures strict separation between certified metrological functions and auxiliary process control applications. In the Dyna-Bus system, the metrological software exclusively manages:

- legal-for-trade fuel measurement and dispensing operations,
- pulse counting and calibration procedures
- data logging and communication with metrological storage

Meanwhile, the virtual machine (VM) executes all non-certified functions, including:

- supervision and control of interlock sensors (e.g., valves, hatches, handrails, overfill, etc.),
- automated pre-dispensing checks and actuation
- real-time visualization and user interface

This ensures that auxiliary software enhances automation without affecting legal metrology compliance.

B. Preemptive Hardware Control and Process Automation

The virtualization layer enables dynamic hardware resource allocation, ensuring that the metrological system always has priority access. The Dyna-Bus application benefits from this by:

- Taking over the user's interface during measurement execution
- Allowing automated actuation of fueling system components without interfering with legal metrology functions
- Implementing a multi-step interlock verification process, ensuring that all safety and compliance conditions are met before and during refueling

This preemptive control mechanism prevents unauthorized software interactions while allowing seamless process automation.

Fig. 2 – Application Screenshot: The yellow top bar, managed by the metrology software, indicates that the displayed data are not valid for legal metrology purposes.

C. Secure Data Handling and Interoperability

To prevent unauthorized modifications, the virtualized environment enforces strict data protection policies:

- Metrological data remains locked within the host environment, ensuring compliance
- Dyna-Bus applications access operational data in read-only mode, preventing tampering
- Remote diagnostics and configuration updates can be performed without altering legally certified measurement records

This ensures that real-time monitoring and process control functionalities can be integrated securely and efficiently.

D. Remote Supervision and Cloud Integration

The Dyna-Bus system also utilizes the virtualization architecture to support:

- Cloud-based telemetry and remote diagnostics via the Click & Find telecontrol platform
- Firmware updates and system adjustments over secure communication channels
- Data-driven decision-making through real-time fuel level monitoring and predictive maintenance

By running these functionalities within the virtualized guest environment, the system maintains compliance, security, and extensibility while minimizing hardware costs.

E. Performance

To ensure optimal resource isolation and compliance with the certified metrological execution environment, the virtualized architecture was deployed on a dual-core ARM platform, explicitly assigning a single core as a resource limit to the guest virtual machine. This constraint was introduced to guarantee that the metrology host layer always retains exclusive access to not less than one core, avoiding contention during legally relevant operations. Despite this limitation, both the certified metrological software and the auxiliary guest applications performed flawlessly under real-world workloads. The virtual machine boot time, often a critical factor in embedded deployments, was minimized by leveraging QEMU snapshot mechanisms. This approach enabled near-instantaneous startup of the guest environment without introducing latency or delays during system initialization.

VI. DISCUSSION AND CONCLUSIONS

The implementation of the proposed architecture required addressing several non-trivial technical challenges, notably the adaptation of the QEMU/KVM virtualization stack to operate on ARM-based metering hardware. This involved low-level engineering tasks such as kernel modification, driver integration, and the development of secure guest initialization procedures—none of which are provided by standard toolchains. These efforts went beyond standard hypervisor deployment and were necessary to meet the stringent operational and regulatory requirements of legal-for-trade systems.

The results demonstrate that this technical investment is fully justified by the benefits achieved in the target domain. The novel system-level approach to separating certified metrological functions from non-certified auxiliary processes, supports automated hardware resource arbitration and allows certified software to preemptively control critical interfaces during measurements. This reduces the risk of interference and enhances robustness compared to manual access control in non-virtualized systems. The modular separation also simplifies maintenance: updates to auxiliary components can be performed within the guest environment without re-certification of the metrological core. Table 2 summarizes the advantages of this virtualization-based approach, including improved software isolation, data integrity, hardware control, and regulatory compliance. These characteristics make the solution suitable for scalable and compliant industrial metrology systems.

Table 2. Virtualization added value

Aspect	Traditional Approach	Virtualized Architecture
Software Segregation	Dedicated hardware partitions or separate physical devices.	Hypervisor-based VM isolation for non-metrological software.
Data Protection	Read-only storage with OS-level access control.	Read-only database accessible only by the host.
Hardware Access Control	Manual restrictions; API-based access for non-certified software.	Preemptive hardware control by metrology software.
Security Enforcement	Firmware-level restrictions and predefined OS policies.	Hypervisor isolation, VM sandboxing, and controlled data exchange.
Flexibility for Third-Party Applications	Limited: separate execution environments or dedicated devices needed.	High; third-party apps run in VM without interfering with metrology processes.
Regulatory Compliance	Physical isolation and certified firmware; difficult modifications.	Host software remains untouched; VM enables software extensions.
Physical Protection of Wired Commun.	Shielded cables, dedicated wired links, tamper protection.	Virtualization-based isolation and cryptographic protocols.

REFERENCES

[1] C. R. H. Barbosa, M. C. Sousa, M. F. L. Almeida, and R. F. Calili, "Smart manufacturing and digitalization of metrology: a systematic literature review and a research agenda," Sensors, vol. 22, no. 7, 2022.

[2] J. Sousa, J. P. Mendonça, and J. Machado, "A generic interface and a framework designed for industrial metrology integration for the Internet of Things," Computers in Industry, vol. 142, 2022.

[3] P. A. Dreyfus, F. Psarommatis, and G. May, "Virtual metrology as an approach for product quality estimation in Industry 4.0: a systematic review and integrative conceptual framework," International Journal of Production Research, vol. 60, no. 21, pp. 6620-6642, 2022.

[4] P. Tambare, C. Meshram, C. C. Lee, R. J. Ramteke, and Y. T. Chang, "Performance measurement system and quality management in data-driven Industry 4.0: A review," Sensors, vol. 21, no. 20, 2021.

[5] A. Varshney, N. Garg, K. S. Nagla, et al. "Challenges in sensors echnology for industry 4.0 for futuristic metrological applications," Mapan, vol. 36, no. 2, pp. 215-226, 2021.

[6] S. Catalucci, A. Thompson, and S. Piano, "Optical metrology for digital manufacturing: a review," The International Journal of Advanced Manufacturing Technology, vol. 120, pp. 597-616, 2022.

[7] E. V. Dudukalov, V. D. Munister, A. L. Zolkin, et al., "The use of artificial intelligence and information technology for measurements in mechanical engineering and in process automation systems in Industry 4.0," Journal of Physics: Conference Series, vol. 1889, no. 3, 2021.

[8] L. De Santis, "Blockchain: the distributed paradigm for secure metrology digitalization," Elea, University of Salerno, 2022.

[9] K. Soni, N. Kumar, A. S. Nair, P. Chourey, and N. J. Singh, "Artificial Intelligence: Implementation and obstacles in industry 4.0," Handbook of Metrology and Applications, 2021.

[10] E. G. Machado, R. T. R. Gomes, E. V. A. Martins, and I. L. Vieira, "Blockchain network to conformity assessment bodies," Metrologia 2023.

[11] International Organization of Legal Metrology (OIML). (2019). General requirements for software-controlled measuring instruments (OIML D 31:2019).

[12] Physikalisch-Tech Bundesanstalt, “Requirements for software separation in measuring instruments and ancillary equipment in legal metrology”, 2020, PTB-8.51-MB07-SWtrennung-EN-V04

[13] European Cooperation in Legal Metrology e.V., WELMEC Guide 7.2:2021, 2021.

[14] B.Wichmann, G. Parkin, R. Barker, “Software Support for Metrology Best Practice Guide No. 1: Validation of Software in Measurement Systems”, NPL Report DEM-ES 014, 2007.

[15] J. Horst, S. McSpadden, “A roadmap for metrology interoperability.” NIST Interagency/Internal Report (NISTIR) – 7381

[16] F. Bellard, "QEMU, a fast and portable dynamic translator," in USENIX Annual Technical Conference, FREENIX Track, 2005.

[17] Y. Kamay, D. Laor, U. Lublin, and A. Liguori, "KVM: the Linux virtual machine monitor," in Proc. Linux Symposium, vol. 1, pp. 225–230, 2007.