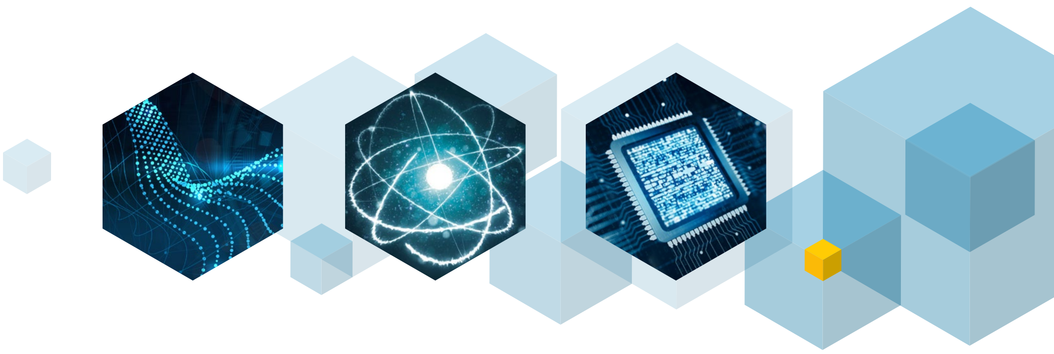
TECHNICAL STANDARDIZATION

TECHNICAL STANDARDIZATION

QUANTUM TECHNOLOGIES

Version 1.0 · November 2023
ISBN 978-99987-869-8-1



ANEC

TECHNICAL STANDARDIZATION

QUANTUM TECHNOLOGIES

Version 1.0 · November 2023

ILNAS

Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services

ANEC

Agence pour la Normalisation et l'Economie de la Connaissance

Foreword

Technical standardization plays an important role in the support of economic development. Nowadays, almost every sector relies on standards to provide services in an efficient manner. Standards are therefore considered as a major source of benefits, and this is particularly true for Information and Communication Technology (ICT), which supports all other economic developments.

The Grand Duchy of Luxembourg has understood the importance of the digital economy and has engaged since several years in an ambitious innovation strategy for the ICT sector. The "Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services" (ILNAS) supports this development through the "Luxembourg Standardization Strategy 2020-2030", signed by the Minister of the Economy, which identifies the ICT sector as one of the most relevant to support, specifically in terms of technical standardization, along with the Construction and Aerospace sectors.

In addition to the strategy, ILNAS has also developed the "Luxembourg's policy on ICT technical standardization 2022-2025", which it carries out with the support of the Economic Interest Group "Agence pour la Normalisation et l'économie de la Connaissance" (ANEC GIE – Standardization Department). The policy aims to promote and strengthen the use of technical standards by the national market, to reinforce the positioning of Luxembourg in the global ICT standardization landscape, particularly through a stronger involvement of national stakeholders in the relevant standardization technical committees, and to pursue the development of research and education programs. In the frame of this policy, ILNAS has notably launched different activities in the ICT domain.

As a result, a series of White Papers and reports, that aim to inform the market about technical standardization developments in certain ICT subtopics have been published. Moreover, a Standards Analysis of the ICT Sector - Luxembourg consisting in a practical tool to discover the latest standardization developments in the overall landscape of ICT related technologies, is published twice a year by ILNAS, with the support of the ANEC GIE.

Within this global framework, this document is intended to present current standardization developments in the area of quantum technologies, with a view towards informing the national stakeholders and encouraging their involvement in the standards development process, for the benefit of Luxembourg's economy.

Jean-Marie REIFF
Director
ILNAS

Jean-Philippe HUMBERT
Deputy Director
ILNAS

Abstract

According to Gartner, “[...] q*uantum solutions could revolutionize the entire IT industry with major economic, industrial, academic, and societal impacts* [...]”. Quantum solutions are also transforming other industries. Numerous initiatives have been launched to accelerate their development and subsequent adoption.

This report aims to support the national stakeholders by describing the field of quantum technologies (QT) and relevant standardization activities that can contribute to its development and acceptance.

In this frame, this document starts by providing an overview of QT and its subfields, highlighting their potential impact on various industries.

The report then addresses the economic implications of QT and introduces some challenges associated with their development. It explores the concept of technical standardization and underscores its critical role in advancing QT. Additionally, it sheds the light on key standards developing organizations activities related to QT on a global scale, along with existing standards and ongoing projects in the field.

Finally, the document outlines standardization opportunities specific to Luxembourg and explains how individuals and organizations can actively participate in standards development to drive innovation and technological advancement.

Table of contents

1

Quantum technologies overview

1. Quantum technologies overview

Quantum technologies is a rapidly growing field that explores the fundamental principles of quantum mechanics. Due to the specificity and complexity of quantum systems, this interdisciplinary domain brings together experts from various fields such as physics, computer science, mathematics and engineering to develop new technologies exploiting the unique properties of quantum systems. Together, they innovate technologies by harnessing the unique properties of quantum systems, including superposition and entanglement. These distinct characteristics enable the creation of powerful tools for computation, communication, and sensing.

Superposition represents one of the fundamental characteristics of quantum systems. It allows these systems to exist in a combination of multiple states simultaneously. For example, a photon can occupy multiple states, each corresponding to different potential outcomes. Until we interact with or measure the photon, it exists in a state that encompasses all possible states at once. However, once an interaction or measurement is performed, the superposition collapses, and the photon settles into one specific, well-defined state [1]. Another significant concept is the concept of entanglement, famously referred by Einstein as “spooky action at a distance” [2]. Quantum entanglement is the state in which two systems are strongly correlated so that obtaining information about one system will give immediate information about the other, no matter how far these systems are [3].

QT, leveraging the principles of quantum mechanics, hold the potential to revolutionize numerous domains, including healthcare, supply chain management, data processing, cryptography, and more. They offer unprecedented capabilities beyond the limits of classical systems. QT are not yet widely used for commercial purposes but the research is ongoing to progress towards widespread adoption.

QT is typically categorized into the areas of quantum computing, quantum communications, quantum sensing, and quantum simulation [4].

Opinion of standardization experts

“The QT for quantum networking is at early development stages and specific technologies are in the process of being developed, such as quantum key distribution (QKD), quantum memory, wide range efficient entangled quantum state distribution, space-based laser communication. Many of these techniques are not ready for any commercial operation today, but we expect the Quantum networking specific services to become an integral part of future network infrastructure. Especially for securing end-to-end communications, the QT should become an essential element for reliable future communications.”

Dr. Joel Grotz
SES Engineering

“Quantum computers are actively being developed and the research is continuously progressing. However, quantum computers that have been developed in the past few years [...] are not powerful enough. We can only speculate when or even if “powerful enough” quantum computers will be built. Currently the scientific consensus is that in the next 20 years it is likely that such computers will be built.”

Mr. Jan Oupicky
SnT

1.1. Quantum computing

As defined by ISO/IEC DIS 4879, quantum computing is a computation that can be carried out on a fully programmable quantum processor that can implement or approximate any unitary dynamics defined within its full Hilbert space[1].

Quantum computing aims to perform computations exponentially faster than classical computers. Instead of using classical bits, which can only be a “0” or a “1”, quantum computers utilize quantum bits, or qubits, which can represent multiple states simultaneously. The primary objective of quantum computing is to solve highly complex problems that are currently inaccessible to classical computers. For instance, quantum computing can revolutionize machine learning for pattern recognition tasks. In fields like artificial intelligence, identifying intricate patterns within vast datasets is a fundamental challenge. Quantum algorithms, such as the Quantum Support Vector Machine (QSVM), enable quantum computers to analyze and recognize complex patterns in data exponentially faster than classical counterparts. This capability enhances the efficiency and accuracy of machine learning tasks, promising significant advancements in fields such as image recognition, language processing and data mining [5].

Quantum computing aims to provide a solution that allows to significantly reduce the computation time. Figure 1, represents a simplified view of the theoretical promise of quantum computing. It illustrates a future scenario where, as the problem size increases, classical computing time might grow exponentially. In contrast, quantum computing could potentially demonstrate a substantial difference. Even with larger problems, quantum systems could process computations significantly faster, highlighting their efficiency and potential for handling intricate tasks. However, it is important to note that while the promise of quantum computing is important, it is still a work in progress. The current efforts are still a long way from fully realizing quantum computing potential and delivering practical applications. It is crucial to approach quantum computing with cautious optimism, recognizing that there are significant challenges to overcome before it becomes a widely accessible technology [6].

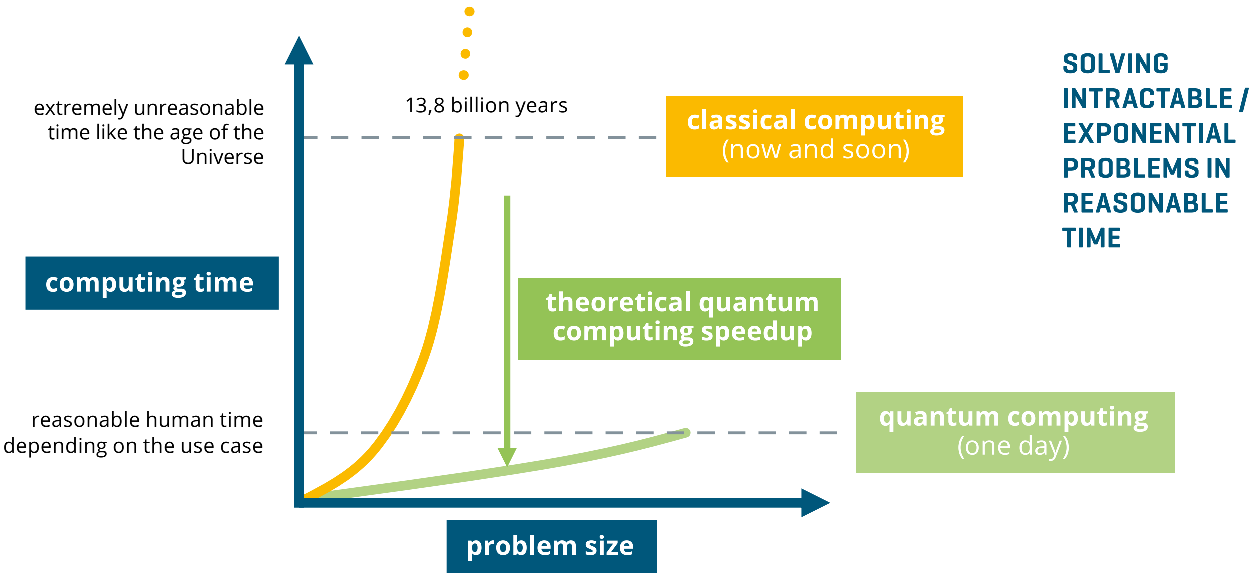


Figure 1: simplified view of the quantum computing theoretical promise. (adapted from [6])

1 *“Hilbert space is a complete, complex vector space equipped with an inner product operation which allows distances and angles to be defined”* - ISO/IEC DIS 4879

1.2. Quantum communication

Quantum communication focuses on securing the transmission of information using the principles of quantum mechanics. It aims to ensure the confidentiality and integrity of the exchanged data based on quantum properties such as superposition and entanglement. It uses the quantum bits to encode and transmit the information. One of the key applications of quantum communication is quantum key distribution (QKD) [7]. QKD allows two parties to establish a secret encryption key in a way that is immune to eavesdropping. The operational concept of a QKD system is relatively simple: two parties ("A" and "B"), employ single photons that are randomly polarized to represent ones and zeros. These photons are used to transmit sequences of random numbers, which serve as cryptographic keys for secure communications. These two stations are linked by both a quantum channel and a classical channel. "A" generates a random sequence of qubits, transmitting them over the quantum channel. Upon receiving this sequence, "A" and "B", through the classical channel, perform standard procedures to check for any attempts by eavesdroppers to extract information from the qubit stream. Detecting eavesdropping relies on observing an imperfect correlation between the two sets of bits obtained after transmitting the qubits between the sender and receiver [7].

The development of practical quantum communication systems is an active area of research, and various technologies, such as photons and superconducting circuits, are being explored for implementing quantum communication protocols. Quantum communication has the potential to significantly enhance the security and privacy of information exchange, making it a crucial component in the future of secure communication networks.

Opinion of standardization experts

"Maturing of the QKD and Quantum Memory technology development from the current technology readiness to a prototype state would be a major step in building a quantum internet."

Dr. Joel Grotz
SES Engineering

1.3. Quantum sensing

Quantum sensing is an emerging field that exploits the special properties of quantum mechanics to create highly sensitive measurement devices [8]. These sensors operate on the principles of quantum superposition, entanglement, and others, allowing them to detect and quantify with a high accuracy even the faintest signals and changes in physical quantities such as magnetic fields, temperature, and time [9]. Thus, they can achieve unprecedented levels of precision and accuracy. Quantum sensors have diverse applications, from revolutionizing timekeeping with atomic clocks to enhancing medical diagnostics through ultra-sensitive magnetometers. As QT continues to advance, quantum sensing promises to open up new frontiers in scientific research and various industries, providing solutions for a wide range of measurement challenges.

1.4. Quantum simulation

Simulating the behavior of the physical world is crucial for advancing science and developing innovative technologies. Quantum simulations utilize quantum principles to construct physical models that help us understand real systems. In recent years, the field of quantum simulation has experienced rapid development. Experimental advancements have led to the emergence of various platforms that employ large arrays of single quantum systems, such as atoms or ions, to solve complex problems. The objective of quantum simulators is to understand and solve some important physics challenges which will be key to the design of chemicals, such as new drugs or fertilizers for medicine and agriculture, the creation of new materials, such as high temperature superconductors for energy distribution without any losses, or even the improvement of mathematical algorithms for traffic flow optimization [10].

In classical simulation, researchers use classical computers to model and study the behavior of physical systems. However, as the complexity of the system increases, classical computers become inefficient as the processing time increases exponentially, as explained in section 1.1.

Quantum simulation offers an alternative approach. Instead of using classical computers, quantum systems, such as quantum computers or other quantum devices, are utilized to simulate the behavior of other quantum systems. Thanks to the unique properties, such as superposition and entanglement, quantum systems can represent multiple states of a physical phenomenon at the same time. This ability allows them to perform certain simulations much more efficiently than classical computers.

Quantum simulation and quantum computing are related fields within QT, but they have different objectives and applications. On the one hand quantum simulation focuses on understanding complex physical systems by simulating their behavior using other quantum systems. Quantum computing, on the other hand, is about solving computational problems more efficiently using quantum algorithms and principles.

2

2

Economic overview of quantum technologies

2. Economic overview of quantum technologies

2.1. Global overview

Over the last two decades, quantum science has experienced remarkable advancements, leading to the emergence of QT that stand on the brink of revolutionizing our daily lives. As shown on Figure 2, governments and organizations worldwide are making substantial investments, nearing a total of $36 billion, with the aim of fully harnessing the potential of these technologies. Collectively, the global QT market is anticipated to attain a value of $106 billion by the year 2040 [11].

This chapter summarizes the major international investments and initiatives that have been realized in the fields of QT.

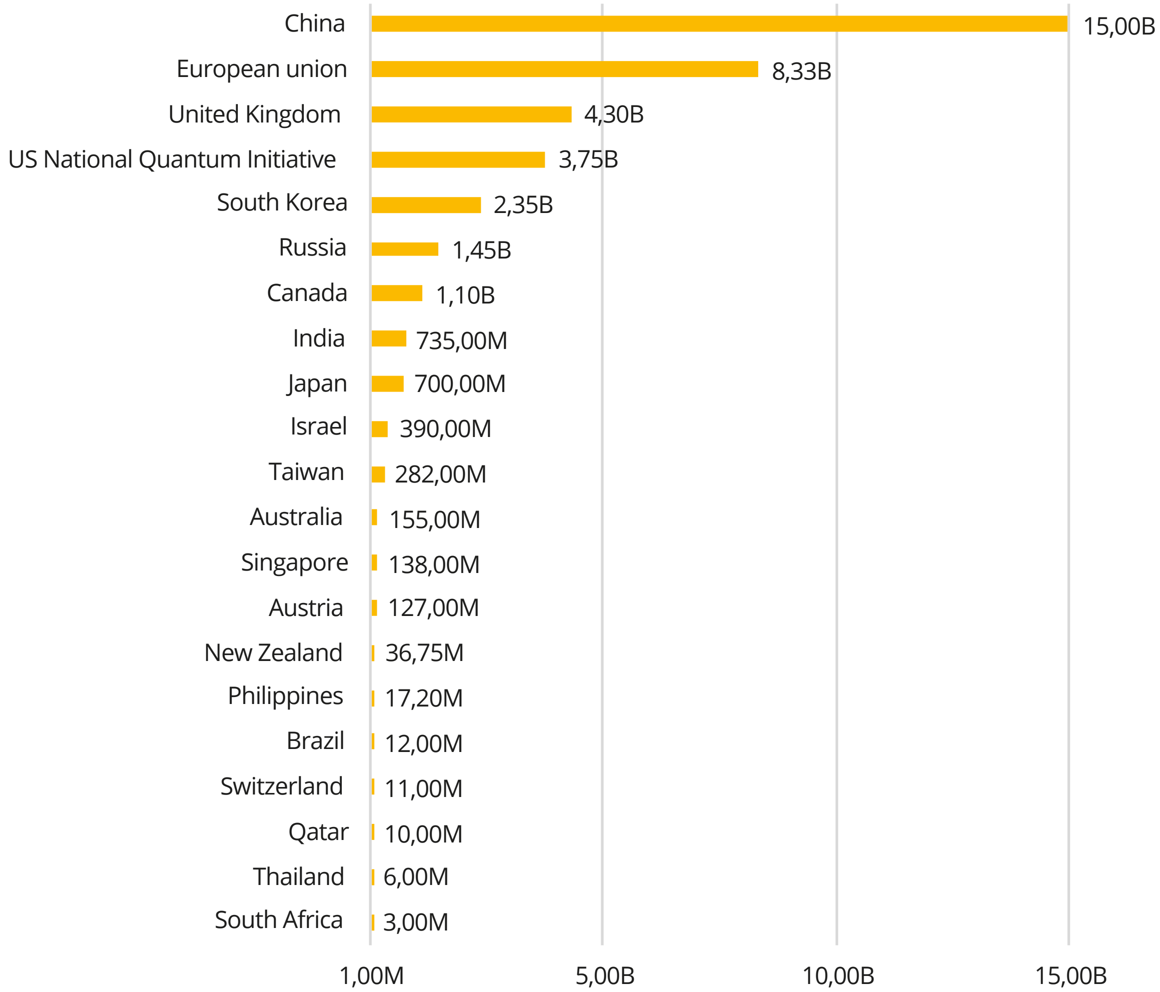


Figure 2: Investment in Quantum research and innovation worldwide ($US) [11]

Asia, North America, Europe, Africa and Australia showcase diverse innovation ecosystems, leading to each nation's government charting distinct pathways in the development of QT.

Asia has shown a persistent and expanding commitment in QT. Singapore initiated its focus on quantum information back in the early 2000s. In similar vein, China has engaged in a significant endeavor, initially concentrating on quantum communications and later shifting its focus towards quantum computing.

China's five-year plan, launched in 2016, made quantum computing a top priority to ensure national technological autonomy. Over the past decade, China has invested more than $1 billion in QT and has also established a startup fund of an additional $150 million. Looking forward, China has aspirations for public investments that could potentially reach up to $15 billion. By 2030, China aims to achieve several key milestones, including the nationwide expansion of its quantum communications infrastructure, the successful development of a prototype for a general quantum computer, and the realization of a practical quantum simulator [11].

Starting in 2019, both Japan and South Korea adopted formal quantum strategies. Their initiatives involve constructing quantum computers and accessing such systems remotely through cloud-based platforms developed by other companies [12]. In 2020, Taiwan revealed a substantial commitment of $282 million towards advancing QT over the next five years. This investment reflects Taiwan's aspiration to evolve into a prominent technology hub, aiming to establish a reputation beyond its existing strength in semiconductor manufacturing [11].

In early 2022, India joined the quantum journey by unveiling plans to allocate more than $1 billion over the next five years to foster QT development. Part of their plan is to create a prototype quantum computer by 2026 [12].

In the United States, a comprehensive effort known as the National Quantum Initiative Act has been launched in 2018. It is designed to support the progress of diverse QT. As part of this initiative, the Quantum Economic Development Consortium (QED-C) was established. This consortium aims to support quantum supply chain, strategically designed to support the future quantum industry [12].

Canada is actively developing its strategies in QT. It's recognized as a top global player in quantum research. In the last ten years, Canada has invested over $1 billion in quantum research. A review conducted in 2015 on global quantum research spending ranked Canada the fifth in the world for the amount of money dedicated to quantum science each year [11].

Australia has committed substantial funding to advance QT, with $83.76 million already invested through federal funding. In their Budget 2023 announcement, Australia is poised to invest an additional $65.482 million over the next five years from the government's $1 billion critical technology fund to bolster a new national quantum strategy [11].

2.2. Focus on the European Union

In the European Union (EU), many national and regional initiatives have been launched to support the development of QT with a total public support of over $7 billion. The European Commission has also established a separate $1.1 billion research and innovation initiative known as the EU Quantum Flagship, which is devoted to develop and commercialize QT in the European Union. The goal of this initiative is to enhance Europe's scientific leadership in this research field, to stimulate the growth of a competitive European QT industry, and to make Europe an attractive and dynamic region for innovative research, business and investments in this field [13].

The investments allocated by the Member States of the European Union vary from one country to another. Figure 3 shows examples of these investments.

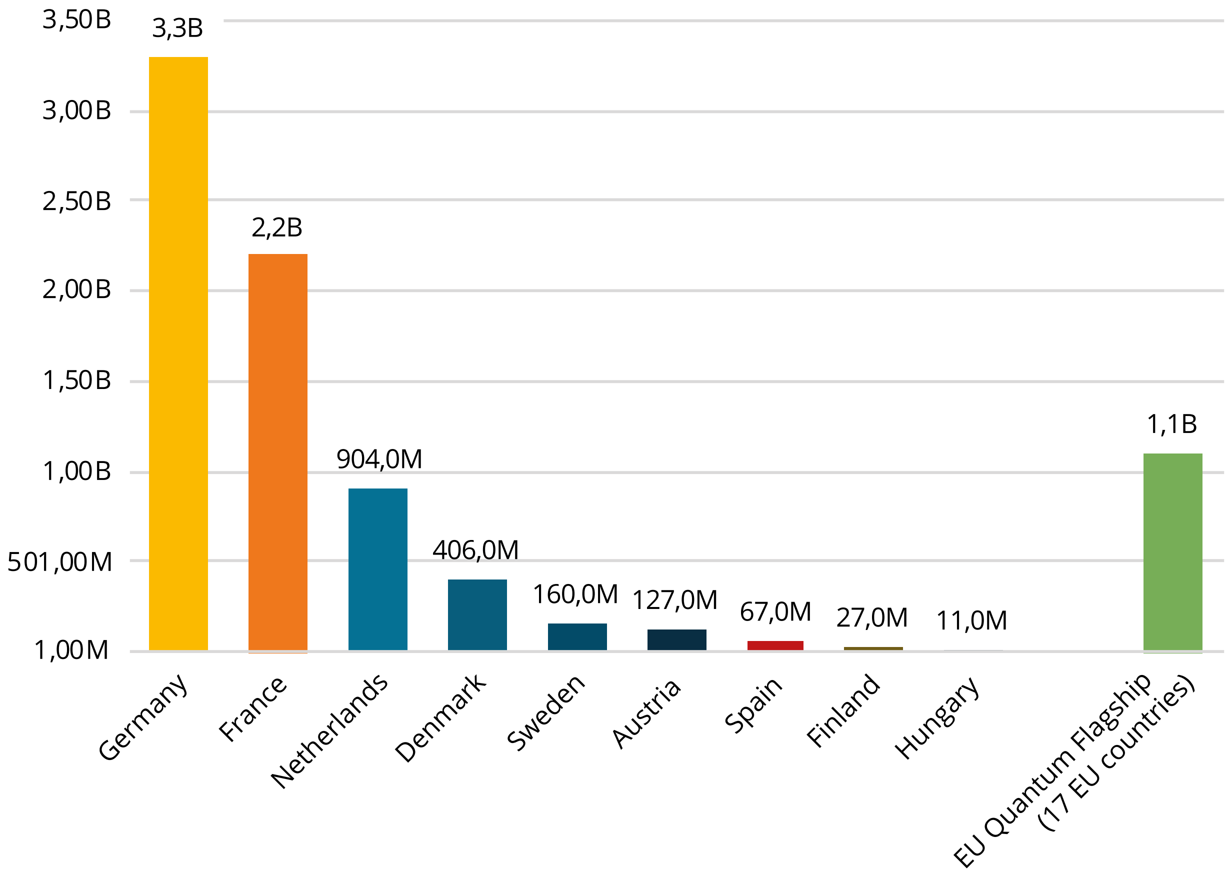


Figure 3: Investment in Quantum research and innovation in the EU ($US) [11].

Within the EU, quantum computing is prominent and its development goes hand in hand with the European efforts on high-performance computing. For example, in addition to the existing research centers and clusters of excellence in QT, there are other national initiatives, such as Quantum Delta NL in the Netherlands, a dedicated legal entity that governs all related public investments in technology.

In line with these investments, the European industry has also started to collaborate in order to accelerate the development of commercial quantum solutions. One example is the European Quantum Industry Consortium (QuIC). This consortium functions as a collaborative hub across Europe, fostering a robust and dynamic ecosystem that connects various business entities, including SMEs, large corporations, investors, and leading research and technology organizations [14].

At the national levels, several other industry associations have been established, including Le *Lab Quantique* in France and the Danish Quantum Community in Denmark, the Finnish Institute Q and UK Quantum in United Kingdom.

Luxembourg, recognizing the significant importance of QT, actively participates in various European initiatives like the European Quantum Communication Infrastructure (EuroQCI) initiative[2]. It has significant expertise in both satellite-based and quantum communications. In addition, Luxembourg has recently taken an important step by signing a Memorandum of Understanding (MoU) with South Korea, demonstrating its commitment to strengthening expertise in diverse aspects of quantum communications. This collaboration aims to draw from South Korea's pioneering national strategy on QT and foster a mutually beneficial partnership [15].

2 https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

3

3

Challenges of quantum technologies

3. Challenges of quantum technologies

QT are poised to bring significant changes in several areas, promising substantial advancements. However, the development and adoption of these technologies can represent significant challenges. Some of them are shown in Figure 4:

Figure 4: Some challenges of QT

As the field of QT continues to advance, the importance of standards in guiding the development of these technologies becomes increasingly crucial and participates in tackling some of the QT challenges. Normative efforts vary depending on the subfield of QT. The following section of this report provides an overview of technical standardization, its role in promoting the development of new technologies, and some normative efforts carried out by standards bodies.

4

Quantum technologies and technical standardization

4. Quantum technologies and technical standardization

4.1. Definition of a standard

As defined by CEN, CENELEC and ETSI [17], a standard is *"A document, established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Standards should be based on consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits."*

4.2. Benefits of standardization

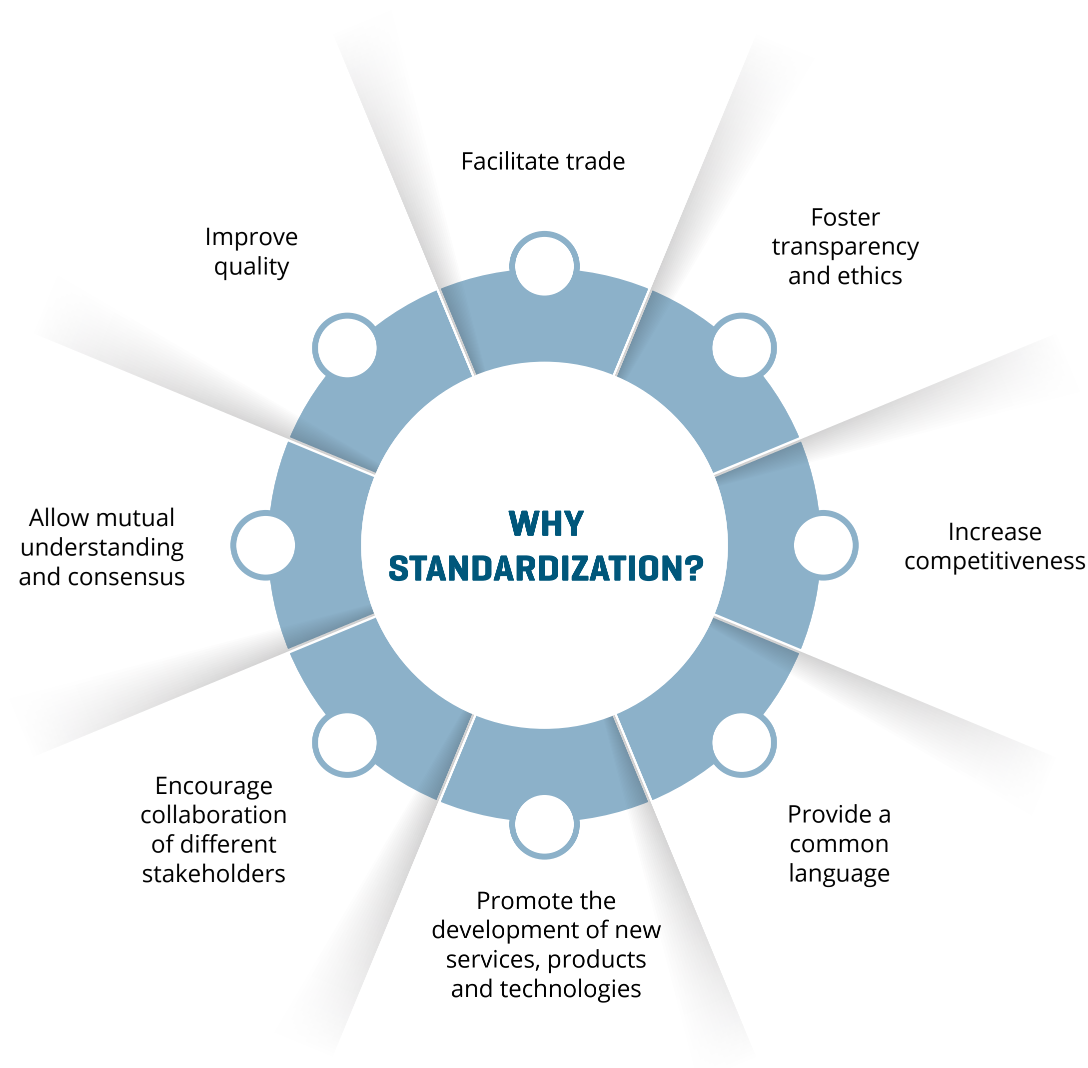


Figure 5: Benefits of standardization

4.3. Standards development organizations

Technical standards are developed by organizations that bring all interested stakeholders together and follow well-accepted principles (e.g., defined by the World Trade Organization[3]). In the European Union, Regulation (EU) No 1025/2012[4] recognized the following standardization organizations:

At the international level, the three recognized standardization organizations are the:

- International Organization for Standardization (ISO).
- International Electrotechnical Commission (IEC).
- International Telecommunication Union's Telecommunication Standardization Sector (ITU-T).

At the EU level, the three recognized standardization organizations are the:

- European Committee for Standardization (CEN).
- European Committee for Electrotechnical Standardization (CENELEC).
- European Telecommunications Standards Institute (ETSI).

Finally, at **national level**, the *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services* (ILNAS) is the national standards body representing Luxembourg in international and European standardization organizations. As such, ILNAS is a member of the six recognized standardization organizations.

4.4. Standards fostering the development of new technologies and innovation

In the past, standardization has often been seen as being at odds with innovation. However, this view is changing rapidly. Standardization does not hold back the innovation. Instead, it is recognized as one of the most effective and powerful tools to rapidly capitalize on knowledge and disseminate it throughout industries [18].

QT are advancing toward technological maturity and wider adoption. One of the measures identified by the EU Quantum Technologies Flagship[5] in its strategic research program to accelerate development and adoption of QT, is the promotion of coordinated and dedicated efforts in standardization and certification.

Standardization initiatives are not restricted solely to technologies that have already reached a high level of maturity. On the contrary, they are equally relevant and valuable for emerging technologies. These initiatives play an important role in developing a roadmap for new technologies, offering several significant advantages:

- **Terminology and Vocabulary:** Defining a common set of terms and vocabulary specific to QT can facilitate communication and knowledge sharing between researchers, developers, and other stakeholders. Establishing a shared language is a foundational step.

3 https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm

4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025

5 https://qt.eu/

- **Benchmarking:** Creating benchmark tests and performance metrics can enable researchers and engineers to assess and compare the capabilities and limitations of different quantum systems objectively. This can help identify areas for improvement.
- **Quality Control:** Standardization can help ensure the quality and reliability of quantum devices and systems. This is important to build trust among users and investors and prevent the unsafe quantum systems from entering the market.
- **Security Guidelines:** Even in early stages, it is important to establish guidelines to secure the communications in quantum systems. This includes protocols for handling quantum hardware and data encryption.
- **Education and Training:** Standardized curricula and training materials for QT can be created to ensure that individuals entering this field have a fundamental understanding of the technology.
- **Interoperability:** As QT advance, it will become increasingly necessary to integrate various quantum components, systems, and software from different manufacturers and research groups. Standardized interfaces and protocols will facilitate this integration and enable more transparent development and deployment of quantum applications.
- **International Collaboration:** International collaboration in standardization is essential for the development of QT, as it brings together knowledge and expertise from experts around the world.
- **Long-term Planning:** Standardization efforts can provide a roadmap for long-term planning, investment, and development in various quantum industries.

Although standards have already been developed for some areas of QT while others are under development or investigation, it is also essential to recognize that QT are still evolving and standards may need to be adapted over time. Collaboration between researchers, industry stakeholders and standards bodies is essential to ensure that the standards developed are both practical and effective.

Opinion of standardization experts

"Standardization (at the right time and with the right approach) can help build a global Quantum internet."

Dr. Joel Grotz
SES Engineering

"Technical standardization is already playing an important role in the post-quantum cryptography development. For example, the National Institute of Standards and Technology (NIST) - in the United States - is leading the development of post-quantum algorithms."

Mr. Jan Oupicky
SnT

4.5. Standardization activities related to quantum technologies

Despite QT are in the early stages of technological maturity, the industry has begun considering future standardization needs to support a robust global market. Many efforts have been established and others are currently underway through various prominent standardization organizations, with a focus on quantum communication as one of the most mature sub-field. Significant efforts are also underway to develop terminology and expand existing classical standards to accommodate QT.

4.5.1. ETSI

Groups active in quantum standardization

Groups	Description
ETSI ISG-QKD	Industry Specification Group[6] (ISG) on Quantum Key Distribution was established in 2008. It aims to connect stakeholders from commerce, industry and science to develop ETSI Group Specifications (GSs) describing quantum cryptography for ICT [18]. QKD is the essential credential in order to use quantum cryptography on a broad basis. It is the main task of the QKD ISG to specify a system for QKD and its environment.
ETSI TC CYBER WG QSC	ETSI TC CYBER WG QSC is a working group for Quantum-Safe Cryptography. The primary responsibilities of this working group are to make assessments and recommendations on the various proposals from industry and academia regarding real-world deployments of quantum-safe cryptography, including practical properties, (such as efficiency, functionality, agility, etc.), security properties, appropriateness of certain quantum-safe cryptographic primitives to various application domains (Internet protocols, wireless systems, resource constrained environments, cloud deployments, big data, etc.). Note: before operating as a WG in TC CYBER, QSC was initially created as an ISG in ETSI. In order to produce normative ETSI deliverables, such as technical reports or technical specifications, it was necessary to promote the ISG as a WG within an ETSI Technical Committee.

6 Industry Specification Groups operate alongside traditional standards-making committees in a specific technology area. They are designed to be quick and easy to set up. They provide an effective alternative to the creation of industry fora. (source ETSI)

Relevant documents developed by ETSI

Committees	Document reference	Title	Date of publication
ETSI ISG-QKD	ETSI GS QKD 002	Quantum Key Distribution; Use Cases	06/2010
	ETSI GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces	03/2018
	ETSI GS QKD 004	Quantum Key Distribution (QKD); Application Interface	08/2020 *(under revision)*
	ETSI GS QKD 005	Quantum Key Distribution (QKD); Security Proofs	12/2010 *(under revision)*
	ETSI GR QKD 007	Quantum Key Distribution (QKD); Vocabulary	12/2018 *(under revision)*
	ETSI GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification	12/2010
	ETSI GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems	05/2016
	ETSI GS QKD 012	Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment	02/2019
	ETSI GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API	02/2019
	ETSI GS QKD 015	Quantum Key Distribution (QKD); Control Interface for Software Defined Networks	04/2022 *(under revision)*
	ETSI GS QKD 016	Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules	04/2023 *(under revision)*
	ETSI GS QKD 018	Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks	04/2022
ETSI TC CYBER WG QSC	ETSI GR QSC 001	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework	07/2016
	ETSI GR QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios	02/2017
	ETSI GR QSC 004	Quantum-Safe Cryptography; Quantum-Safe threat assessment	03/2017
	ETSI GR QSC 006	Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes	02/2017
	ETSI TR 103 570	CYBER; Quantum-Safe Key Exchanges	10/2017
	ETSI TR 103 616	CYBER; Quantum-Safe Signatures	09/2021
	ETSI TR 103 617	Quantum-Safe Virtual Private Networks	09/2018
	ETSI TR 103 618	CYBER; Quantum-Safe Identity-Based Encryption	12/2019
	ETSI TR 103 619	CYBER; Migration strategies and recommendations to Quantum Safe schemes	07/2020
	ETSI TR 103 692	CYBER; State management for stateful authentication mechanisms	11/2021
	ETSI TS 103 744	CYBER; Quantum-safe Hybrid Key Exchanges	12/2020 *(under revision)*
	ETSI TR 103 823	CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation	10/2021
	ETSI TR 103 949	Quantum-Safe Cryptography (QSC) Migration; ITS and C-ITS migration study	05/2023

Example of projects under development

Committees	Document reference	Title
ETSI ISG-QKD	ETSI GS QKD 010	Quantum Key Distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems
	ETSI GS QKD 013	Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules
	ETSI GR QKD 017	Quantum Key Distribution (QKD); Network architectures
	ETSI GR QKD 019	Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication
	ETSI GS QKD 020	Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API
	ETSI GS QKD 021	Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Nsetworks for Interoperable key management system
ETSI TC CYBER WG QSC	ETSI TR 103 965	Quantum-Safe Cryptography; Impact of Quantum Computing on Cryptographic Security Proofs
	ETSI TR 103 966	Quantum-Safe Cryptography; Deployment Considerations for Hybrid Schemes
	ETSI TR 103 967	Quantum-Safe Cryptography (CYBER); Impact of Quantum Computing on Symmetric Cryptography
	ETSI TS 104 015	Quantum-Safe Cryptography (CYBER); Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies
	ETSI TR 104 016	Quantum-Safe Cryptography (CYBER); A Repeatable Framework for Quantum-safe Migrations
	ETSI TR 104 017	Quantum-Safe Cryptography (CYBER); QSC Protocol Inventory

4.5.2. ITU-T

Groups active in quantum standardization

Groups	Description
ITU-T Study Group 13	The Study Group 13, 'Future networks,' focuses on general functional requirements for QKD networks. Their ongoing work involves the exploration of a functional framework, the development of a generic functional architecture, and a specific emphasis on key management functions.
ITU-T Study Group 17	The activities of the Study Group 17 'Security' focuses on cybersecurity, security management, service and application security, fundamental security technologies, and security strategy and coordination which include quantum-based security.
ITU-T FG-QIT4N	The ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N) was established in September 2019 to provide a collaborative platform for pre-standardization aspects of QIT for networks.

Relevant documents developed by ITU-T

Committees	Document reference	Title	Date of publication
ITU-T Study Group 13	Y.3800	Overview on networks supporting quantum key distribution	10/2019
	Y.3801	Functional requirements for quantum key distribution networks	04/2020
	Y.3802	Quantum key distribution networks – Functional architecture	12/2020 *(amendment under development)*
	Y.3803	Quantum key distribution networks – Key management	12/2020 *(amendment under development)*
	Y.3804	Quantum key distribution networks – Control and management	09/2020 *(amendment under development)*
	Y.3805	Quantum key distribution networks – Software-defined networking control	12/2021 *(amendment under development)*
	Y.3806	Quantum key distribution networks – Requirements for quality of service assurance	09/2021
	Y.3807	Quantum key distribution networks – Quality of service parameters	02/2022
	Y.3808	Framework for integration of quantum key distribution network and secure storage network	02/2022
	Y.3809	A role-based model in quantum key distribution networks deployment	02/2022
	Y.3810	Quantum key distribution network interworking – Framework	09/2022
	Y.3811	Quantum key distribution networks – Functional architecture for quality of service assurance	09/2022 *(amendment under development)*
	Y.3812	Quantum key distribution networks – Requirements for machine learning based quality of service assurance	09/2022
	Y.3813	Quantum key distribution networks – Functional requirements	01/2023
	Y.3814	Quantum key distribution networks – Functional requirements and architecture for machine learning enablement	01/2023 *(amendment under development)*
	Y.3815	Quantum key distribution networks – Overview of resilience	09/2023
	Y.3816	Quantum key distribution networks – Functional architecture enhancement of machine learning based quality of service assurance	09/2023
	Y.3817	Quantum key distribution networks interworking – Requirements of quality of service assurance	09/2023
	Y.3818	Quantum key distribution networks interworking – Architecture	09/2023
	Y Suppl. 70	ITU-T Y.3800-series – Quantum key distribution networks - Applications of machine learning	07/2021
	Y Suppl. 74	ITU-T Y.3800-series – Standardization roadmap on quantum key distribution networks	03/2023
	Y Suppl. 75	ITU-T Y.3000 series – Quantum key distribution networks – Quantum-enabled future networks	03/2023

ITU-T Study Group 17	X.1702	Quantum noise random number generator architecture	11/2019
	X.1710	Security framework for quantum key distribution networks	10/2020
	X.1712	Security requirements and measures for quantum key distribution networks – key management	10/2021
	X.1714	Key combination and confidential key supply for quantum key distribution networks	10/2020
	X.1715	Security requirements and measures for integration of quantum key distribution network and secure storage network	07/2022 *(amendment under development)*
	X.1811	Security guidelines for applying quantum-safe algorithms in IMT-2020 systems	04/2021

Example of projects under development

Committees	Document reference	Title
ITU-T Study Group 13	Y.QKDN-qos-auto-rq	Quantum key distribution networks – Requirements for autonomic quality of service assurance
	Y.QKDN-qos-mmq	Quantum key distribution Networks – Measurement methodology for QoS parameters
	TR.QKDN-nq	Overview for integration of quantum key distribution network with non-quantum cryptographies
	Y.QKDN_SSNarch	Functional architecture for integration of quantum key distribution network and secure storage network
	Y.QKDN_SSNreq	Functional requirements for integration of quantum key distribution network and secure storage network
	Y.QKDN-amc	Quantum key distribution networks – Requirements and architectural model for autonomic management and control enablement
	Y.QKDNf-fr	Framework of Quantum Key Distribution Network Federation
	Y.QKDNi-SDNC	Quantum Key Distribution Network Interworking – Software Defined Networking Control
	Y.QKDN-rsrq	Requirements for quantum key distribution network resilience
	Y.QKDN-TSNfr	Framework for integration of quantum key distribution network and time sensitive network
	Y.supp.QKDN_sync	Analysis of Time Synchronization in quantum key distribution networks
	Y.Supp.QKDN-UC	Use cases of quantum key distribution networks
	Y.TR-QK-UC	Use cases of quantum networks beyond QKDN
ITU-T Study Group 17	TR.hyb_qsafe	Overview of key management of hybrid approaches for quantum-safe communications
	X.1715Amd1	Security requirements and measures for integration of quantum key distribution network and secure storage network
	X.sec_QKD_profr	Framework of quantum key distribution (QKD) protocols in QKD network
	X.sec_QKDN_AA	Authentication and authorization in QKDN using quantum safe cryptography
	X.sec_QKDN_CM	Security requirements and measures for quantum key distribution networks – control and management
	X.sec_QKDNi	Security requirements for Quantum Key Distribution Network interworking (QKDNi)
	X.sec-QKDN-tn	Security requirements and designs for quantum key distribution networks – trusted node

4.5.3. IEC and ISO/IEC

Groups active in quantum standardization

Groups	Description
ISO/IEC JTC 1/WG 14	ISO/IEC JTC 1/WG 14 “Quantum information technology”, serves as a systems integration entity to focus on JTC 1’s standardization program on quantum computing and maintain relationships with other related ISO and IEC/TCs and other organizations.
ISO/IEC JTC 1/SC 27	ISO/IEC JTC 1/SC 27 “Information security, cybersecurity and privacy protection”, has started to develop standards related to the security requirements, test and evaluation methods for QKD products, through its working group 3 “Security evaluation, testing and specification”.
IEC SEG 14	The Standardization Evaluation Group IEC SEG 14 dedicated to QT was established in October 2022 and is focusing on the following tasks: • Investigate needs for standardization in the area of QT. • Evaluate technical capabilities and applications in this field. • Propose a roadmap for standardization in the area of QT. • Engage with TC/SC/SyCs, including JTC 1, as well as with ISO and other market and policy relevant organizations. • Make recommendations to SMB as appropriate.

Note: Based on a recommendation from IEC SEG 14, a proposal for the creation of an ISO/IEC joint technical committee for quantum technologies has recently been submitted to ISO and IEC member bodies for voting and commenting. This first step resulted in the approval of the proposal by the member bodies. In a second step, Management Boards of ISO and IEC are now reviewing the votes and comments in order to decide whether a new JTC will be created or if the proposed work will be assigned to one or several existing technical committees.

Proposers initially intended to cover different areas in the field of quantum technologies with this new JTC, including:

- Quantum computing;
- Fundamental quantum technologies;
- Quantum simulation;
- Quantum sources;
- Quantum metrology;
- Quantum detectors;
- Quantum communications;
- Low-loss photonics;
- Radio-frequency electronics for cryogenic temperatures.

Relevant documents developed by ISO/IEC

Committees	Document reference	Title	Date of publication
ISO/IEC JTC 1/ SC 27	ISO/IEC 23837-1	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements	08/2023
	ISO/IEC 23837-2	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 2: Evaluation and testing methods	09/2023

Example of projects under development

Committees	Document reference	Title
ISO/IEC JTC 1/ WG 14	ISO/IEC DIS 4879	Quantum computing – Terminology and vocabulary
	ISO/IEC AWI TR 18157	Information technology – Introduction to quantum computing

In addition, ISO/IEC JTC 1/WG 14 is exploring the possibility to develop new projects in different QT areas, including:

- General requirements for quantum resource simulation platform;
- Quantum machine learning datasets;
- Taxonomy of quantum simulator architectures and quantum simulation programming.

4.5.4. CEN/CENELEC

Groups active in quantum standardization

Groups	Description
CEN/CLC FGQT (2020-2023)	CEN and CENELEC established the Focus Group on Quantum Technologies (FGQT) in 2020 with a duration of activities for 3 years. The goal was to create connections among the relevant European stakeholders across various domains of QT and promote their collaboration. FGQT was not in charge of developing standardization deliverables but aimed to consolidate the ongoing QT initiatives, assess existing requirements, define needs and opportunities and recommend further action to ensure that standards support the deployment of QT in industry.
CEN/CLC JTC 13	CEN/CLC JTC 13 "Cybersecurity and Data Protection", is a joint technical committee between CEN and CENELEC dedicated to the development of standards for cybersecurity and data protection covering all aspects of the evolving information society. The JTC 13 has recently approved the creation of a new WG 10 "Cryptography", which includes post-quantum cryptography in its scope.
CEN/CLC JTC 22	CEN/CLC JTC 22 "Quantum Technologies", is a joint technical committee between CEN and CENELEC dedicated to QT standardization. It has been created based on the work performed by the CEN/CLC FGQT. CEN/CLC JTC 22 shall produce standardization deliverables in the field of QT. This field includes quantum enabling technologies, quantum sub-systems, quantum platforms & systems, quantum composite systems and applications. CEN/CLC JTC 22 is composed of 4 WGs: WG 1 "Strategic Advisory Group"; WG 2 "Quantum Metrology, Sensing and Enhanced Imaging, and Quantum Enabling Technologies"; WG 3 "Quantum Computing and Simulation"; WG 4 "Quantum Communication and Quantum Cryptography".

Relevant documents developed by CEN/CENELEC

Committees	Document reference	Title	Date of publication
CEN/CENELEC FGQT	FGQT Q04	Standardization Roadmap on quantum technologies	03/2023
CEN/CENELEC FGQT	FGQT Q05	Quantum technologies Use Cases	03/2023

Example of projects under development

Currently, there is no officially registered ongoing project. However, the CEN/CLC JTC 22 is discussing the possibility to develop several projects in the QT area:

- Characterization of quantum technologies – Metrics and terminology;
- Layer model of quantum computing;
- Performance benchmarks of quantum computing applications;
- Quantum network best practices;
- QKD and PQC – An equitable analysis and comparison of both technologies;
- Gap analysis of current quantum communication and quantum cryptography standards;
- Hybridization of quantum computing;
- Cryogenic Solid-State quantum computing - Descriptions and functional requirements of modules.

5

Standardization opportunities in Luxembourg

5. Standardization opportunities in Luxembourg

A proper understanding of the stakes associated with technical standardization, including QT, is key to adopting the appropriate position across the standardization landscape and benefit from all the related opportunities. In this frame, ILNAS aims at facilitating the appropriation of technical standards by the national stakeholders and their participation in the standardization process, for the benefit of the national economy.

5.1. How to access the standards?

The application and uptake of standards is a key opportunity that the market can take advantage of. In order to encourage this, ILNAS allows the consultation of published standards for free and their purchase for further use.

The ILNAS e-Shop is a catalog of more than 210,000 normative documents. It offers the possibility to purchase national (ILNAS and DIN), European (CEN and CENELEC) and international (ISO and IEC) standards in electronic format at competitive prices. In addition, the ILNAS e-Shop provides access to ETSI standards, which are generally accessible to the public for free, except in specific cases where fees may apply. These standards can also be found on the ETSI website.

In addition, ILNAS offers the possibility to consult its entire standards' catalog free of charge through dedicated reading stations located in different places in Luxembourg. This service allows, for example, interested organizations or individuals to consult a standard before its purchase on the ILNAS e-Shop.

5.2. Who can participate in standards development in Luxembourg?

ILNAS, with the support of ANEC GIE, encourages companies, institutions, researchers, etc. to participate in the standardization ecosystem. For the technical committees of ISO, IEC, CEN and CENELEC, such as ISO/IEC JTC 1/WG 14, "Quantum information technology" or CEN/CLC JTC 22 "Quantum Technologies", any interested stakeholder can get involved through ILNAS by becoming an active national standardization delegate free-of-charge. Interested experts can request to ILNAS their registration using a dedicated form.

5.3. Good reasons to participate in standards development

- Access drafts standards and influence their content based on your know-how;
- Increase your knowledge regarding the state of the art in standardization of your core business;
- Propose new standards projects;
- Anticipate the evolution of your activity sector's good practices;
- Integrate strategic network of national, European or international experts;
- Collaborate to defend common interests;
- Learn about your competitors and their positions in meetings;
- Promote your organization and your skills at national, European and international levels.

Conclusion

This report has the objective to inform the national market of the opportunities to seize in terms of using technical standards and participating in the standards development process of the recent, and very promising field of quantum technologies. The document provides a comprehensive overview of QT and their subfields, highlighting their significant implications across various industries. It also discusses the economic impact of QT, acknowledging the substantial investments made by governments and organizations worldwide to fully harness the potential of these technologies.

Moreover, the report sheds light on the challenges associated with the development of QT, emphasizing the critical need for technical standardization in this rapidly evolving field. In this frame, the document defines the role of standards and explains the benefits of standardization, especially in fostering innovation and the development of new technologies. In addition, it provides to national stakeholders, an overview of the main standardization organizations active in developing standards related to QT, both at European and international levels, while detailing the published standards along with ongoing projects and initiatives for the standardization of these technologies.

Indeed, one of ILNAS' missions, as stated in the Luxembourg Standardization Strategy 2020-2030, is to actively promote the use of standards as they are published, to benefit from these effects as early as possible. To this end, ILNAS communicates regularly on standardization updates, disseminating the information of the publication of new standards and technical committee activities. This is done through different channels, such as news items available on the Portail-Qualite.lu, reports and white papers, or national standards analyses (such as the Standards Analysis of the ICT sector), developed with the support of ANEC GIE.

Finally, the report details valuable insights into the standardization landscape specific to Luxembourg, outlining the opportunities for individuals and organizations to actively participate in standards development. ILNAS can indeed register national delegates in standardization, in the technical committees of ISO, IEC, CEN, and CENELEC free of charge, so that they may make their voices heard and their ideas accepted in upcoming normative documents. In addition, ILNAS, as the National Standards Body representing Luxembourg in ETSI, strongly encourages any interested national organization to become a member of ETSI in order to take part in the development of important ICT standards that will participate in designing the future of new technologies. Since QT are still at an early stage, notably in terms of standardization, now is the best time to take part in these opportunities.

References

[1] "Quantum Computing." Accessed: Jul. 12, 2023. [Online]. Available: https://universe-review.ca/R13-11-QuantumComputing.htm

[2] A. Muller, "What is quantum entanglement? A physicist explains Einstein's 'spooky action at a distance,'" Astronomy Magazine. Accessed: Jul. 12, 2023. [Online]. Available: https://www.astronomy.com/science/what-is-quantum-entanglement-a-physicist-explains-einsteins-spooky-action-at-a-distance/

[3] "Quantum Entanglement: What is it & Why is it Important in 2023?" Accessed: Aug. 25, 2023. [Online]. Available: https://research.aimultiple.com/quantum-computing-entanglement/

[4] Written by the CEN-CENELEC Focus Group and on Quantum Technologies (FGQT), "Quantum Technologies Use Cases." [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q05_quantumtechnologiesusecases_release1.pdf

[5] B. Martin, "Quantum Computing: Revolutionizing the Future of AI," Medium. Accessed: Oct. 12, 2023. [Online]. Available: https://medium.com/@BobMartin89/quantum-computing-revolutionizing-the-future-of-ai-13f6a9cbf254

[6] O. Ezratty, "Understanding Quantum Technologies 2022".

[7] "Quantum Communication | PicoQuant." Accessed: Aug. 25, 2023. [Online]. Available: https://www.picoquant.com/applications/category/quantum-optics/quantum-communication

[8] S. D. Bass and M. Doser, "Quantum sensing for particle physics." arXiv, May 19, 2023. Accessed: Sep. 22, 2023. [Online]. Available: http://arxiv.org/abs/2305.11518

[9] "Quantum Sensors in '23: Best 8 Use Cases & Case Studies." Accessed: Sep. 22, 2023. [Online]. Available: https://research.aimultiple.com/quantum-sensors/

[10] "The future is Quantum," Quantum Flagship. Accessed: Oct. 13, 2023. [Online]. Available: https://qt.eu/

[11] Maninder, "Overview of Quantum Initiatives Worldwide 2023," Qureca. Accessed: Aug. 10, 2023. [Online]. Available: https://qureca.com/overview-of-quantum-initiatives-worldwide-2023/

[12] "State of Quantum Computing: Building a Quantum Economy," World Economic Forum. Accessed: Aug. 16, 2023. [Online]. Available: https://www.weforum.org/reports/state-of-quantum-computing-building-a-quantum-economy/

[13] "Introduction to the Quantum Flagship," Quantum Flagship. Accessed: Aug. 24, 2023. [Online]. Available: https://qt.eu/about-quantum-flagship/

[14] "QuIC members," QuIC. Accessed: Aug. 21, 2023. [Online]. Available: https://www.euroquic.org/members/

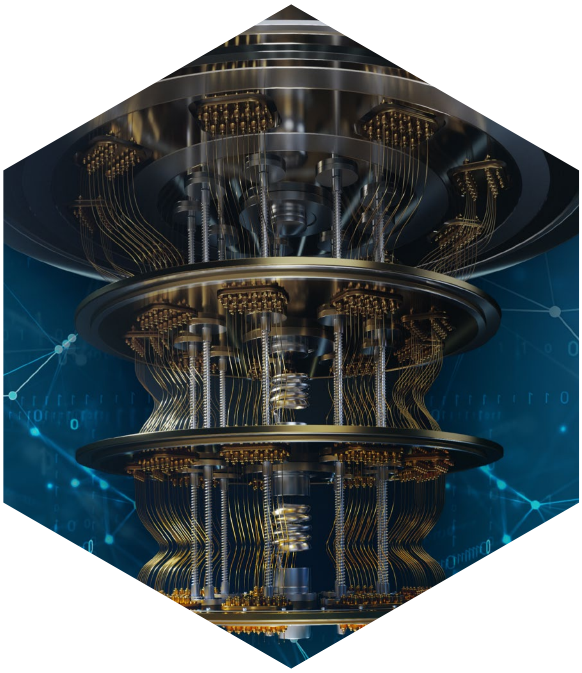
[15] "Luxembourg and SK Telecom deepen relationship on quantum expertise." Accessed: Oct. 18, 2023. [Online]. Available: https://gouvernement.lu/en/actualites/toutes_actualites/communiques/2023/10-octobre/05-bettel-fayot-sk.html.

[16] "What Are The Remaining Challenges of Quantum Computing?" Accessed: Oct. 30, 2023. [Online]. Available: https://thequantuminsider.com/2023/03/24/quantum-computing-challenges/

[17] "European Standards," CEN-CENELEC. Accessed: Oct. 18, 2023. [Online]. Available: https://www.cencenelec.eu/european-standardization/european-standards/

[18] "Quantum Technologies (RP2023) | Joinup." Accessed: Sep. 14, 2023. [Online]. Available: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/quantum-technologies-rp2023

[19] CEN-CENELEC Focus Group and on Quantum Technologies (FGQT), "Standardization Roadmap on Quantum Technologies." CEN-CENELEC Focus Group on Quantum Technologies (FGQT), 2023. [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf



Please fill out the satisfaction survey

https://gd.lu/46rnJ3

November 2023 · TECHNICAL STANDARDIZATION · QUANTUM TECHNOLOGIES · Version 1.0 · · ISBN 978-99987-869-8-1

ILNAS
Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services

ANEC
Agence pour la Normalisation et l'Economie de la Connaissance

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -70 · Fax : (+352) 24 79 43 -70 · E-mail : normalisation@ilnas.etat.lu

www.portail-qualite.lu