FGQT Q04

Standardization Roadmap on Quantum Technologies

written by the CEN-CENELEC Focus Group on Quantum Technologies (FGQT)

Release 1 – March 2023

Table of Contents

Abstract

In 2018, the European Commission launched its long term and large scale Quantum Technology FET Flagship Program. The European Commission is also very interested in boosting standards for quantum technologies (QT). The Quantum Flagship has its own cooperation and coordination activities to "coordinate national strategies and activities" and in its "Quantum Manifesto" [1] explicitly advises to form "advisory boards" to promote collaboration in standardization. The CEN/CENELEC Focus Group for Quantum Technologies (FGQT) was formed in June 2020 with the goal to support the plans of the Commission.

Currently, a multitude of standardization activities in QT are ongoing worldwide. While there is overlap in certain areas, other areas of this wide technological field are not being addressed at all. A coordinated approach will be highly beneficial to unleash the full potential of standardization for speeding up progress—also because the pool of standardization experts available for quantum technologies is still very limited. Furthermore, not all areas are yet "ready for standardization", i.e., while in some fields early standardization is capable of boosting progress, it may be a problem in other areas. Thus, an assessment of standardization readiness of the different areas is required, too.

The FGQT was established to identify standardization needs and opportunities for the entire field of QT with the final goal to boost the establishment of new industries in Europe and consequently the development and engineering of unprecedented novel devices and infrastructures for the benefit of European citizens.

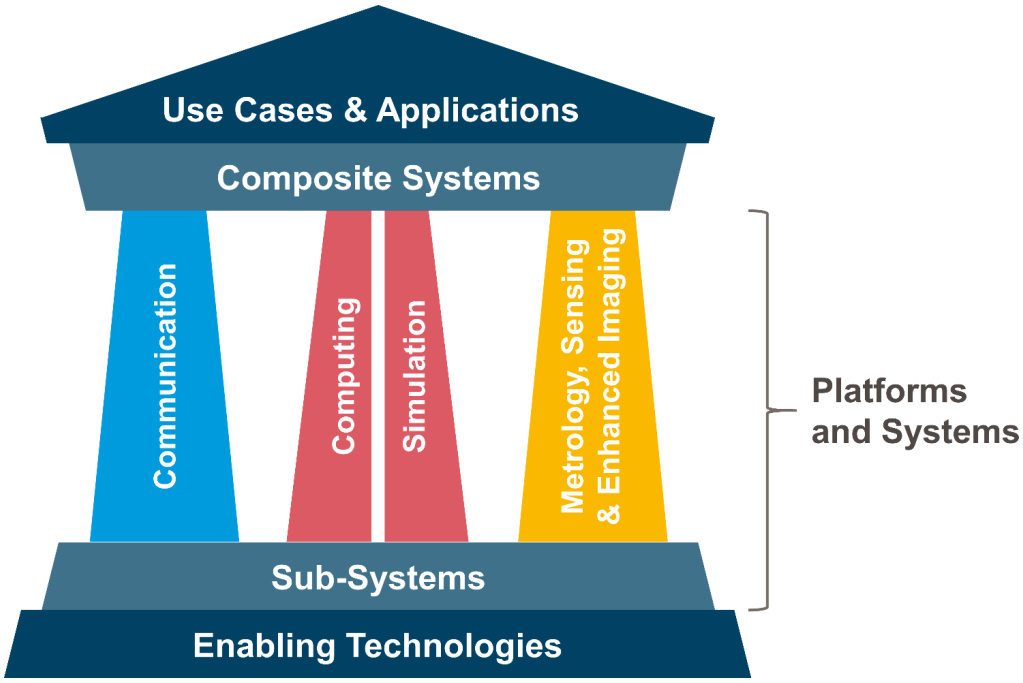


Figure 1 "Greek Temple" design of the quantum technologies standardization roadmap

The QT standardization roadmap follows a constructive approach, starting with basic enabling technologies, from which QT components and subsystems are constructed, which again are assembled into QT systems that in turn form composite systems, constituting the building blocks for use cases (see Figure 1). Thus, the roadmap is structured approximating very closely the categories of the EC quantum technology FET Flagship Program: quantum communication, quantum computing and simulation, quantum metrology, sensing, and enhanced imaging, while the basic enabling technologies and sub-systems are organized in two pools —thus supporting re-use in the different system categories. The separate types of QT unit systems are then foundations of general QT infrastructures or composite systems. On the level of use cases, the QT standardization roadmap describes basic domains of applicability, so-called "meta use

cases", while the detailed use cases are listed in a separate document of the FGQT: "FGQT Q05 Use Cases". Finally, the QT standardization roadmap presents an outlook and conclusions, including an actual prioritization of the single identified standardization needs in the form of sequence diagrams (Gantt charts).

This approach differs slightly from the QT "Pillar design" of the EU Quantum Flagship but, in our opinion, it extends it and is better adapted to standardization purposes, while the former is optimally suited as a research program design (see Figure 2).

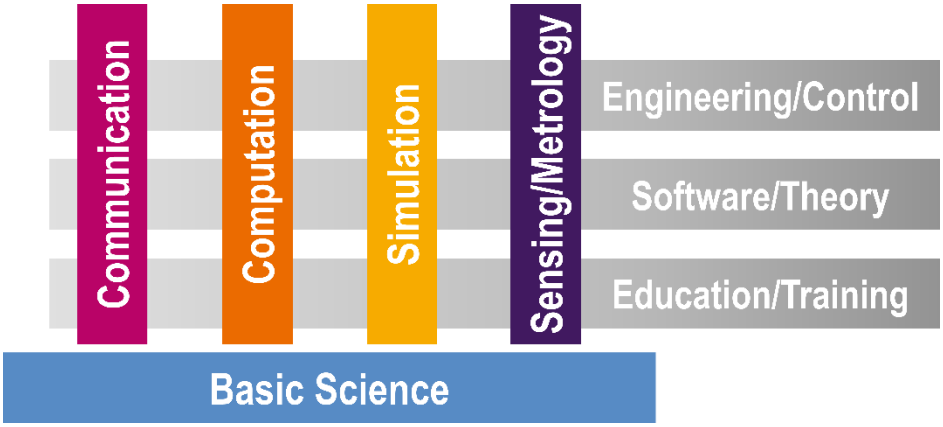


Figure 2 "Pillar design" of the EU Quantum Technologies Flagship research program

The FGQT is an open group of European-based experts, working in QT research areas or enabling technologies, and of developers of components, products, or services related to QT. If you are based in Europe, and interested in guidelines and standards to help setting up a research infrastructure, or structuring and boosting your market relevance; if you want to improve coordination with your stakeholders and are interested in coordination and exchange with other experts in the field of QT—please consider to join the CEN/CENELEC FGQT.

NOTE 1 European QT standards development in CEN/CENELEC will take place in the new JTC 22 QT (Joint Technical Committee 22 on Quantum Technologies). The work in JTC 22 QT will be guided by the present roadmap document, and it is expected that the FGQT roadmap-development activity will be absorbed/continued by JTC 22 QT.

Contact:

Secretariat: Marius Loeffler, DIN, Germany, E-mail: marius.loeffler@din.de

Online: https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologes/

NOTE 2 An excerpt of the present roadmap document was published in of EPJ Quantum Technology [2] in the Special Issue on Quantum Standardization [3]. This except also includes the motivations from the 20+ co-authors why they are actively contributing to European standardization for quantum technologies.

Foreword

This document was composed by the CEN/CENELEC Focus Group on Quantum Technologies (FGQT) between mid-2020 and end 2022 in a series of 30 online meetings (due to COVID-19), as well as two physical meetings. Over 200 European experts have participated in these meetings and contributed to discussions to achieve a common view and consensus about drafted texts.

CEN/CENELEC acknowledges written contributions from the following people and organizations (alphabetical on family name):

— Nooshin Amirifar (CEN/CENELEC)
— Michele Amoretti (CINI)
— Georgy Astakhov (HZDR)
— Thomas Attema (TNO)
— Jonathan J. Attia (Feynman Foundation)
— Amado Bautista Salvador (PTB)
— Andreas Barthel (PTB)
— Ettore Bernardi (INRIM)
— Jean-François Boissou (Pasqual)
— Rob van den Brink (Delft Circuits)
— Natalia Bruno (CNR-INO)
— Niels Bultink (Qblox)
— Fabio Cavaliere (Ericsson)
— Chris Chunnilall (NPL)
— Mario Castaneda (Single Quantum)
— Paolo Comi (Italtel)
— Antonello Corsi (Engineering Ingegneria Informatica S.p.A.)
— Ivo Degiovanni (INRIM)
— Alessandro Delvecchio (UNI)
— Oskar van Deventer (TNO, chair FGQT)
— Noel Farrugia (University of Malta)
— Giovanni Frattini (Engineering Ingegneria Informatica S.p.A)
— Thomas Gerster (PTB)
— Marco Gramegna (INRIM)
— Lukas Grünhaupt (PTB)
— Hugo Gelevert (TNO)
— Christian Goroncy (DIN)
— Olivier Dubuisson (Orange)
— Andreas Jenet (European Commission, JRC)
— Maran van Heesch (TNO)

— Loïc Henriet (Pasqal)
— Frank Hohls (PTB)
— Arne Hollmann (VDI)
— Ben Kassenberg (QuiX)
— Olga Kazakova (NPL)
— Jonas Keller (PTB)
— Claudius Klein (VDI)
— Sander Kossen (TNO)
— Stefan Kück (PTB)
— André Kulosa (PTB)
— Nataša Lalović (PTB)
— Thomas Länger (IDQ Europe GmbH, editor FGQT)
— Ben Lanyon (IQOQI)
— Wolfgang Lechner (UIBK)
— Bernard Lee (Senko)
— Matthieu Legré (IDQuantique, editor FGQT)
— Adam Miles Lewis (JRC)
— Tobias Lindstrom (NPL)
— Marius Loeffler (DIN, secretariat FGQT)
— Antonio Manzalini (TIM)
— Vicente Martín (Univ Politécnica Madrid)
— Tanja Mehlstäubler (PTB)
— Thomas Monz (Univ. Innsbruck)
— Ekaterina Moreva (INRIM)
— Olivier Le Moult (Orange)
— Niels Neumann (TNO, editor FGQT)
— Samira Nik (CEN/CENELEC)
— Tracy Northup (Univ. Innsbruck)
— Christian Ospelkaus (Univ. Hannover)
— Homer Papadopoulos (NCSR Demokritos, editor FGQT)
— Saverio Pascazio (INFN, Univ. Bari)
— Momtchil Peev (Huawei Technologies Duesseldorf GmbH)
— Richard Pitwon (Resolute Photonics)
— Angie Qarry (QDeepTech)
— Adriaan Rol (Orange Quantum Systems)
— Christian Roos (IQOQI)

— Maria Rossetti (UNI, editor FGQT)
— Ivan Rungger (NPL)
— Enrique Sanchez Bautista (Univ. Jülich)
— Félicien Schopfer (LNE)
— Hans Werner Schumacher (PTB)
— Sibylle Sievers (PTB)
— Nicolas Spethmann (PTB, vice-chair FGQT)
— Fabio Taucer (JRC)
— Francesco Tafuri (Univ. Napoli)
— Paolo Traina (INRIM)
— Christian Trefzger (DG CNECT)
— Daniele Tumietto (Economisti)
— Niels Ubbelohde (PTB)
— Pim Venderbosch (QuiX)
— Peter Verhoeff (TNO)
— Wouter Vlothuizen (TNO)
— Franziska Weickert (PTB)
— Benedict Wenzel (DIN, secretariat FGQT)
— Frank Wilhelm-Mauch (Research Center Jülich)
— André Xuereb (Univ. Malta)

1 Abbreviations, terms and acronyms

APD	Avalanche Photo Diode
API	Application Programming Interface
AWI	Approved Work Item (status in the development of an ISO standard)
BB84	Bennet Brassard 1984 quantum key distribution scheme
BEC	Bose-Einstein Condensation
CAGR	Compound Annual Growth Rate
CB	Certification Bodies
CCD	Charge-coupled device (electronic light sensor)
CCRA	Common Criteria Recognition Agreement
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN-CENELEC STAIR	CEN/CENELEC Working Group Standards, Innovation & Research
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
COM	Serial port interface on a personal computer
COTS	Commercial off-the-shelf
COW	Coherent One Way
CPU	Central Processing Unit
CSA	Cloud Security Alliance
CV-QKD	Continuous-variable quantum key distribution
CV	Continuous-Variable
CWA	CEN/CENELEC Workshop Agreement
CWDM	Coarse wavelength division multiplexing
DC	Direct current
DEMUX	Demultiplexer
DPS	Differential Phase Shift
DV	Discrete-Variable
DV-QKD	Discrete-variable quantum key distribution
DWDM	Dense wavelength division multiplexing
EMN-Q	European Metrology Network for Quantum Technologies
EN	European Standard

ERC	European Research Council
ESD	Electrostatic Discharges
ETSI	ETSI Telecommunications Standards Institute
ETSI ISG	ETSI Industry Specification Group (type of standards developing group)
ETSI TC Cyber	ETSI Technical Committee “Cyber”
EuroQCI	European Quantum Communication Infrastructure
EuroQCS	European Quantum Computing & Simulation
EuroQSM	European quantum sensing and metrology
FID	Free Induction Decay
FGQT	CEN/CENELEC Focus Group on Quantum Technologies
GaAs	Gallium-Arsenide
HAL	Hardware Abstraction Layer
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission, standards organization
IEEE	Institute of Electrical and Electronics Engineers (professional organization)
IETF	Internet Engineering Task Forcemult
InGaAs	Indium-Gallium-Arsenide
IR	Infrared spectrum
IRTF	Internet Research Task Force (research organization)
ISO	International Organization for Standardization, standards organization
ITSEF	Information Technology Security Evaluation Facilities
ITU	International Telecommunication Union (of the United Nations)
ITU-T	ITU Telecommunication Standardization Sector
IWA	ISO/IEC Workshop Agreement
JRC	Joint Research Center of the European Commission
JTC 1	Joint Technical Committee 1 (of ISO and IEC)
MKID	Microwave Kinetic Inductance Detectors
MoSi	Molybdenium silicide (MoSi2)
MUX	Multiplexer
MZI	Mach-Zehnder Interferometer
NbN	Niobium nitride
NbSi	Niobium silicide

NMI	National Metrology Institutes
NV	Nitrogen Vacancy
OPM	Optically Pumped Magnetometers
PAMP	Polarization of Atoms in a Magnetized Plasma
PCB	Printed Circuit Board
PCT	Patent Cooperation Treaty (international patent treaty)
PIC	Photonic Integrated Circuit
PID	PID-controller (proportional-integral-derivative controller)
PL	Photoluminescence
PNRD	Photon Number Resolving Detector
PP	Protection Profile
PQC	Post-Quantum Cryptography
PS	Phase Shifter
QCDM	Quantum Classical Division Multiplexing
QD	Quantum Dot
QIRG	Quantum Internet Research Group
QKD	Quantum Key Distribution
QMSI	Quantum Metrology & Sensing and quantum enhanced Imaging
QPU	Quantum Processor Unit
QSC	Quantum-Safe Cryptography
QSS-WG	Cloud Security Alliance (CSA) Quantum-Safe Security Working Group
QT	Quantum Technologies
QTSEF	Quantum Technology Security Evaluation Facility
QuantERA	Quantum Technologies European Research Area Network
Qubit	Quantum bit
QuIC	Quantum Internet Consortium
R&I	Research & Innovation
RF	Radio Frequency
RSA	Rivest-Shamir-Adleman public-key cryptosystem
SC27	Sub-Committee 27 (of ISO/IEC JTC1)
SDO	Standards Developing Organization
SEG	Standardization Evaluation Group

SEP	Standard-Essential Patent
SFR	Security Functional Requirement
SI	International System of Units
SiC	Silicon-carbide (Semiconductor)
SiPM	Silicon Photomultiplier
Si-SPAD	Silicon Single-Photon Avalanche Diode
SMF	Single Mode Fibre
SNR	Signal to Noise Ratio
SNSPD	Superconducting Nanowire Single-Photon Detector
SOG-IS	Senior Officials Group-Information Systems Security
SPAD	Single-Photon Avalanche Diode
SPDC	Spontaneous Parametric Down-Conversion
SQUID	Superconducting Quantum Interference Device (magnetometer)
ST	Security Target
TaN	Tantalum-Nitrogen
TBS	Tuneable Beam Splitter
TC	Technical Committee
TCP/IP	Transmission Control Protocol / Internet Protocol (Internet communication protocols)
TEC	Thermoelectric Cooling
TES	Transition Edge Sensor
TR	Technical Report
TRL	Technology Readiness Level (estimate for technology maturity)
TS	Technical Specification
TWPA	Traveling Wave Parametric Amplifiers
USB	Universal Serial Bus (digital interface)
UV	Ultraviolet
WDM	Wavelength Division Multiplexing
WG	Working Group
WIPO	World Intellectual Property Organization
WSi	Wolfram (Tungsten) Silicide

2 Introduction

2.1 General

More than one hundred experts joined at the start of FGQT of the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), and during the course of 30 meetings about 200 different experts were involved. These experts are active in different domains of quantum technologies and mapped with this document, most of the ongoing standardization activities, they defined needs and opportunities and put forward recommendations for further action to ensure that standards support the deployment of quantum technologies in the European industry. The mapping took place from the establishment of focus groups in June 2020 until today. Hence, the document informs the standardization needs and opportunities, in order to find adequate answers. Further, the document informs researchers and technical experts on those opportunities enabling all interested parties to participate through delegations of their respective National Standardization Bodies. Moreover, this document aims at informing and motivating researchers who receive public research grants to valorize their research results through engaging with standardization bodies.

The present roadmap document is structured as follows: Chapter 2 is for providing the reader an overview of the recent historical milestones and challenges that led to the establishment of the focus group. The chapter provides how quantum technologies may benefit economy and society and the chapter introduces the reader into the main concepts and the ecosystem of standardization.

Chapter 3 is related to the description of broad classes of quantum technologies, which include communication, computing and simulation and measurement and sensing.

Chapter 4 describes types of standards at hand and the different ongoing standardization platforms followed by areas of examples.

In chapter 5 we describe enabling technologies that form a basis for most of the quantum technologies, such as colour centres of nanodiamonds, ion traps, superconducting quantum circuits and travelling wave parametric amplifiers.

Chapter 6 describes quantum technologies components and subsystems

Chapter 7 analyses the standardization needs for quantum communication systems, which includes quantum key distribution.

Chapter 8 analyses the standardization needs for quantum computing and quantum simulation systems, in particular their modularity

Chapter 9 analyses the standardization needs for quantum metrology, quantum sensing and quantum imaging.

Chapter 10 describes the composite system of the quantum internet. We conclude the document with an outlook to the next steps. (chapter 12).

2.2 Quantum technologies and the significance of standardization

Quantum technologies allow us to engineer novel devices with the promise of many new applications that can help solve some of today's most pressing global challenges. Examples include novel methods for earth surveys in times of climate change, exploration of natural resources and information transmission and processing. These and other applications of quantum technologies are approaching the market and will be a pivotal factor for success in a wide and diverse range of industries and businesses. Quantum technologies are vital to Europe's independence and safety, as they affect the fields of information processing, storage and transmission. Similarly, novel devices facilitated by quantum technologies offer capabilities beyond any classical technique, such as higher sensitivity, smaller power consumption and automatic and maintenance-free quantum-referenced operation for more reliable industrial facilities.

NOTE Throughout the roadmap, the distinction between "classical" and "quantum" approaches and techniques is made at several occasions. We would like to stress that we use these words in order to distinguish between novel possibilities facilitated by quantum technology and established techniques based on classical physics and/or established technologies*. There is some similarity to the distinction between "classical mechanics" and "quantum mechanics" in physics. As in physics, "classical" does not mean out-dated or obsolete by any means. Indeed, solutions and techniques for sensing, communication and computing based on classical physics and/or established technologies are useful and necessary today and will be in the future – just as classical mechanics is still used in physics and many applications today. The new possibilities offered by QT will rather extend and complement existing technologies and not replace them.

Even though quantum physics is over a century old, in the last twenty years improvements in science and technology have led to a tremendous level of control over quantum systems at the most elementary level. It is now possible to routinely prepare, trap, manipulate and detect single quantum particles such as atoms, electrons and photons. Together with the possibility of creating and controlling distinct quantum states such as superposition states and entanglement, this second quantum revolution facilitates engineering of new classes of sensors, communication techniques and computers with unprecedented capabilities.

Many activities in QT are closely linked to research – in universities, research institutions as well as in industry. Already at this level, some form of standards or mutual understanding is needed for efficient communication and collaboration. As quantum technologies are maturing, it is important to prepare the field for standardization activities, thus facilitating and accelerating market uptake of quantum technologies. This idea is strengthened even further as quantum technologies are entering the political arena of various economies around the world, with more private and public initiatives entering into the quantum race.

Yet, there is a large variation in maturity of the different fields of quantum technologies, as seen via the technology readiness levels of the different domains. While some devices such as quantum computers are only recently approaching the market, others, such as magnetometers based on atomic vapours or superconducting quantum interference devices, are already well-established products. Hence, the level of maturity and the key-components of various quantum domains differ. Correspondingly, the standardization needs are different as well.

Standardization can lay the foundation for and stimulate the development of an economic system for quantum technologies within the EU, thereby enhancing science and industry and benefitting consumers within and outside Europe. For each, standardization is advantageous. For science, for instance, consensus is a prerequisite for efficient communication with the community and a fair and sensible comparison of results. Furthermore, standards allow for a flexible collaboration, as components are interchangeable and interoperable. Science therefore has to solve fewer technical problems, leading to growing science yields. For industry, standardization is required to transfer quantum technologies to the market in Europe and worldwide. Examples include terminology, performance tests and benchmarking methods of quantum devices, and interoperability and interchangeability of different quantum modules.

2.3 Ecosystem and cooperation in quantum technologies

In the last two decades, quantum science made significant progress and quantum technologies are about to become technologies that will impact our everyday life. Governments and companies are investing to unleash this potential. Several countries have positioned themselves to be leaders in areas such as computing, communication, sensing and imaging.

In order to continue at the forefront of this emerging technology and to participate in a global quantum industry, Europe has committed in making the best use of its excellence in science and engineering. The European Commission launched in October 2018 its EUR 1 billion Quantum Technologies Flagship on a 10-year timescale. It consists of a set of research and innovation projects selected through a peer-review process [4].

EU member states have also set aside individual public funding for research in quantum technologies. For example, in September 2018, the German federal government announced a EUR 650 million four years program for quantum technologies, which was increased to 2.6 billion in 2021 [5]. The German strategy targets several aspects of quantum technologies with a focus of transferring QT from fundamental research to market, from basic R&D to real-world commercialization. The UK government launched already in 2013 a GBP 270 million five-year investment on quantum technologies, which has been extended for another five years after the first phase. Further funding of GBP 1 billion was allocated in 2021 [5]. A key feature of the UK strategy is the establishment of four 'hubs' for computing, communication, imaging and sensing, including the National Quantum Computing Centre, with the goal of building the world's first universal quantum computer. The Netherlands invested EUR 765 million in QuTech, the quantum technology institute which aims to develop the building blocks for the first quantum computer in the coming 10 years. Denmark, Sweden, Finland, Austria, Hungary, France, Spain and Italy initiated substantial national quantum initiatives. In 2021, EU member states announced additional EUR 7.2 billion public funding [6].

The upcoming national quantum plan for China will be at least of the same order of magnitude as the European Commission's Flagship. China is building the National Laboratory for Quantum Information Sciences in Hefei, with over USD 1 billion in initial funding [7]. Chinese companies, including Baidu and Alibaba, have established their own initiatives in quantum computing, attracting top researchers to their teams. Alibaba plans to invest USD 15 billion into disruptive technologies in the years to come [7]. In 2021, China announced additional USD 15.3 billion public funding [6].

In December 2018, the United States' president signed a bill into law that devotes more than USD 1.2 billion to a national effort dedicated to quantum information science over the next 10 years. In 2020, the National Science Foundation additionally established three new "Quantum Leap Challenge" institutes to address critical challenges in quantum information science. The National Quantum Initiative Act represents a push to keep up with China and other countries in developing quantum technologies. In 2021 additional 1.9 billion public funding was announced [8]. A great advantage in the U.S. is the capacity of the private sector to complement publicly funded efforts in quantum technologies sector, and also funding via military agencies. The share of investments in quantum coming from venture-capital and other private-capital entities increased in the second half of 2021 and now account for more than 70 % of investments, up from 50 % in September 2021 [6]. There is a growing industrial interest in quantum information technology, including efforts at Google, Honeywell, Hughes Research, IBM, Intel, Microsoft and Northrop-Grumman. Several start-up companies, funded by venture capital and other equity sources have been established [9].

The Quantum Technologies Flagship sees its beginning in the 2016 published Quantum Manifesto, signed by 3 400 scientists calling for a quantum technologies initiative coordinated between academia and industry to move quantum technologies from laboratory to industry and to educate quantum technologies professionals in a combination of science, engineering and business [1]. With the launch in October 2018, the Flagship funds research and innovation.

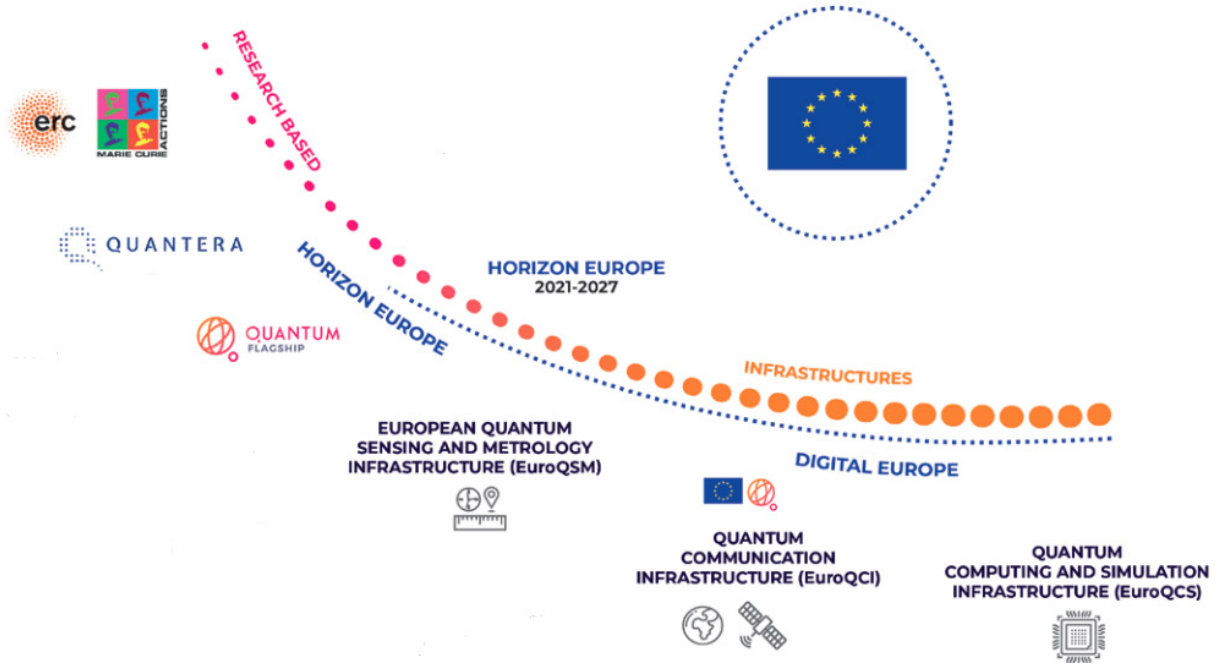


Figure 3 European Quantum Technologies ecosystem = Quantum Flagship + Quantera + EuroQSM + EuroQCI + EuroQCS + ERC/Marie Skłodowska Curie actions (adopted from [10])

European Union's long-term vision is the development of the quantum internet, where quantum computers, simulators and sensors are interconnected via quantum networks distributing information and quantum resources. The QT Flagship is the EU instrument to achieve this. It is a large-scale, long-term research initiative pooling resources in support of a commonly agreed science and technology roadmap, aiming to foster world-leading knowledge, technologies, and open research facilities for quantum in Europe. To unlock the full potential of QT, accelerate their development, and bring commercial products to the market, three goals underlie the QT Flagship's vision [10]:

— Consolidate and expand European scientific leadership and excellence in quantum research;

— Kick-start a competitive European industry in quantum technologies to make Europe a leader in the future global industrial landscape;

Make Europe a dynamic and attractive region for innovative research, business and investments in quantum technologies, accelerating their development and take-up by the market.

Key to the QT Flagship initiative's added value is its pan-European dimension that will allow to, inter alia, integrate national and European metrological and standardization institutes in developing quantum-based standards for the most mature technologies. In this context, the project Coordination and Support Action (EUR 2.7 million) is the central coordination and support project of the QT Flagship, responsible to identify and coordinate the relevant standardization and intellectual property protection actions.

Within the European QT ecosystem, other investment efforts exist, notably at the national level. A prominent example is the European Research Area Cofunded Action in Quantum Technologies (QuantERA) initiative, bringing together 31 organizations from 26 countries together with the European Commission supporting international research projects in the field of QT, with EUR 36 million invested so far.

The Digital Europe Programme, the first ever proposed digital capability building program of the Union for the period 2021 to 2027, will support the development of first quantum computers and their integration with high performance computers, as well as the development of a pan-European quantum communication infrastructure guaranteeing full security of communications and critical infrastructures.

The concept of 'Putting Science into Standards' workshop on quantum technologies was launched at the Quantum Flagship Kickoff Conference in Vienna on 29-30 October 2018 and first contacts were established. These workshops bring the scientific and standardization communities closer together by anticipating and bringing new issues requiring standards to the standardization community.

This led to a European Commission-led special session on standardization during the first European Quantum Technologies Conference 2019 in Grenoble (France) on 18 to 22 February, with contributions from CEN and CENELEC, and the German Institute for Standardization (Deutsches Institut für Normung e.V. (DIN)). There was a strong interest from sides of the Quantum Flagship Coordination and Support Action to establish a satellite session on standardization. The science community showed interest and willingness to formulate a roadmap for standardization. Following the 1st EQTC in Grenoble, the Putting Science Into Standards workshop "Standards4Quantum" was held in Brussels at CEN/CENELEC on 28-29 March 2019 involving stakeholders from industry, science community and standardizers, including the Coordination and Support Action of the QT Flagship, the European standardization organization for general devices, electronics and telecommunications CEN, CENELEC, and ETSI, as well as their national members such as DIN among others. There were also presence from members of the European metrology institutes Euramet and from NIST from the US.

For the first time, more than 80 quantum physicist and experts from different European countries working in different quantum disciplines gathered to discuss how to bring inventions to the market, thus completing the pathway of innovation. Planning at an early state and incorporating standardization can be crucial for accelerating market uptake of research findings. The workshop set the ground for bringing together the relevant stakeholders in the quantum technologies standardization value chain – research, standardization, industry and public administrations/institutions – and provided a timely opportunity for a balanced and representative overview on the status quo in quantum technologies, and for drawing informed conclusions on a strategic way forward.

Recommendations drawn from the Putting Science Into Standards workshop have been published in a Workshop report [11] and in a Science for Policy brief [12] and included:

— Call for fostered interaction with the Quantum Flagship;

— Stronger focus on the standardization of a quantum technology terminology and the development of an EU standardization roadmap for Quantum Technologies.

CEN Workshop Agreement(s) (CWA) could address terminology, whereas a standardization roadmap could be addressed by a Focus Group. Pro-active steps towards the creation of such a Focus Group or CWAs, including the identification of a supporting Secretariat, would be necessary.

Following a set of institutional arrangements, the Focus Group on Quantum Technologies (FGQT) was launched on 18th of June 2020, with DIN providing the secretariat and TNO the chair.

Moreover, the recommendations of a Policy Brief, based on the outputs of the above-mentioned workshop "Standards4Quantum", was included into the Strategic Research Agenda of the European Quantum Flagship.

2.4 Scope of the FGQT and the roadmap document

2.4.1 Scope of Focus Group on Quantum Technologies

The JRC Policy Brief [12] recommended concrete actions for addressing standardization for quantum technologies, which include the standardization of a terminology, the development of an EU standardization roadmap and the start of regular collaboration using lightweight standardization activities. The recommendations of the Policy Brief have been taken on board by the Quantum Flagship Coordination and Support Action, which has resulted in including in its work program further coordination of activities in the field of standardization. These are essentially reflected in three points in the proposed work program:

1) state of the art analysis;
2) identifying the standardization needs of the industry;
3) pushing forward standardization for QT.

Discussions on the coordination of these tasks took place at national and European level. A working group consisting of CEN/CENELEC, JRC, DIN and the Quantum Flagship Coordination Office was set up for this purpose and resulted in the formation of the CEN/CENELEC FGQT.

2.4.2 Scope of the quantum technologies standardization roadmap document

One central goal of the mid-2020 established CEN/CENELEC Focus Group Quantum Technologies (FGQT) is to develop a European roadmap on standardization of quantum technology. This roadmap offers to the science, research and industry communities a goal and a strategy to accelerate and foster innovation. This will facilitate the transfer of QT from research to market, from a European perspective and regarding the development worldwide. Furthermore, the roadmap aims to be a powerful tool enabling the main stakeholders to formulate, execute, check and revise a strategy for the standardization of QT.

In accordance to the Strategic Research Agenda for the Quantum Flagship [10] the CEN/CENELEC FGQT roadmap is structured around the four major areas of QT: communication, computing, simulation, and sensing and metrology. Furthermore, the roadmap also contains a section for an in-depth exploration of enabling technologies and a section where innovations and use cases are investigated.

The FGQT roadmap is intended to work as a guideline document in defining topics and a structure of QT fields, identifying separate steps and proposing a logical order in a larger development that might be followed at a later stage. Thus, it provides a basis for informed decision processes (i.e., investments in research) and a timeline for strategy as a reference.

This way, the roadmap reflects a common ground and defines a starting point for further development. It includes a state-of-the-art analysis, through standard and regulatory landscaping, including pre-normative documents at EU and international level and other existing schemes (e.g., de facto standards). Furthermore, the focus group promotes liaison with relevant existing CEN/CENELEC and ISO Technical Committees. While the development of standards itself is not within the scope of FGQT, the group works as a liaison office between scientists and the standardization organizations and thus fosters the future development of standardization for QT.

Another important aspect beyond the roadmap document itself lies in QT standardization community building and networking. FGQT provides a platform for communication, helping to develop a consensus, a “common view” and a “state-of-the-art”. In the process, this output will be updated regularly in the most recent FGQT roadmap to reflect the development in the field and, therefore, provides an overview feeding a communication and dissemination process.

3 Broad classes of QT for the benefit of economy and society

3.1 Provision of high security of communication

Following the white paper [13] released in 2015 by ETSI regarding the possible impact of quantum computing on the effectiveness of the existing cryptographic methods, the European Union [14] together with other authorities [15] and EU institutions, stated the need to develop new technical resources [16, 17] for cybersecurity.

These technical resources have to provide resistance to attacks using quantum computing and to secure essential services such as hospitals, energy grids and railways and ever-increasing number of connected objects in homes and factories [18].

Within this realm new techniques – post-quantum cryptography or quantum-safe cryptography (QSC) – have been proposed following the April 2016 NIST report [19] and the NIST invitation [17] for assessment of future quantum-safe cryptographic algorithms.

Furthermore, in 2017 the Commission Expert Group on Quantum Technologies Committee delivered a report indicating the ability to generate and use quantum states and resources for communication protocols (i.e., quantum random number generators (QRNG) for secret keys and quantum key distribution (QKD) for their secure generation).

According to the report, Quantum technology can influence cyber security by providing techniques taking advantage of quantum effects such as superposition, entanglement, teleportation, randomness and others. For example, QKD devices utilize QRNG systems and the entanglement phenomenon to agree on a secret key in order to establish a secure communication channel resistant to attacks by quantum computers.

Of course, the fact that QKD delivers a secret key between two parties does not mean that there are visible benefits in security and resistance to the application layer, meaning that QKD cannot address security by itself. But although there are shortcomings and the fact that QKD technology has several technical limitations, development of innovative QKD systems and integrating quantum-based systems into existing communication infrastructures might support the creation of high secure digital communication.

Thus, in 2019, all 27 EU member states have signed the EuroQCI declaration [20], towards the development of a quantum communication infrastructure covering the whole EU (EuroQCI) to safeguard sensitive data and critical infrastructures.

3.2 Novel ways of efficient simulation and computing

Quantum computers have offered new ways of performing computing and have opened the way to solving new or previously thought intractable problems. Whereas the power of classical computers scales linearly with the hardware, the computational power of quantum computers scales exponentially with hardware.

NOTE The term “classical” is discussed in some detail in section 2.2.

The fundamental units of classical computers, bits, are in a single definite state, whereas the fundamental units of quantum computers, qubits, can be in a superposition of multiple computational basis states. We can also perform operations on all definite states via the superposition at once.

This allows for solving faster specific problems by quantum algorithms than classical alternatives. This advantage can be polynomial, with the main example being the improved unstructured search with Grover’s algorithm. This advantage might however be nullified when implemented on hardware back ends due to overhead resulting from for instance error correction routines.

Other quantum algorithms provide an exponential speedup, which will likely prevail when implemented on actual hardware. Common examples of quantum algorithms that provide an exponential speedup are Shor’s algorithm which efficiently factors biprimes and the Harrow-Hassidim-Lloyd (HHL) algorithm which efficiently inverts a matrix – and thus solves a linear system of equations.

A third example is using quantum devices for analogue and digital simulation of quantum systems. By their very nature, quantum computers and quantum simulators can do this well due to the fact that the quantum character of the system is embedded in the quantum algorithm or in the rebuild controlled system representing a model of interest, which we cannot control directly. Hybrid techniques between these poles have been proposed.

Examples of applications are materials science, nuclear physics, particle physics, quantum gravity and chemistry. For the latter, we use quantum computers to efficiently simulate electronic structures and compute ground state energies, which are an ingredient to modelling chemical processes. These quantum algorithms can help efficiently develop new, and personalized, medicine.

3.3 Novel possibilities for measurement and sensing

The ongoing development of quantum metrology and sensing and quantum enhanced imaging (QMSI) technologies opens a wide scope of new or significantly enhanced devices and applications (for a detailed description see chapter 9). QMSI devices and applications can improve the accuracy and precision with which parameters of a wide range of systems can be measured or evaluated. Beyond these improvements they allow stepping over limitations related to conventional classical measurement strategies.

In general, the field of application for QMSI technologies - relying on quantum electronics, quantum clocks and atomic sensors and quantum photonics - span across physics, spintronics, chemistry, biology, medicine, materials science, as well as in quantum information, computation and communication. This illustrates the importance and cross-sectional character of QMSI technologies [2].

One key application for QMSI techniques and devices is the characterization and testing of QT components employed in all domains of QT, enabling the reliable commercial usage in the technology supply chain [21, 22]. A typical example can be the characterization, evaluation and benchmarking required for quantum computing to compare complementary architectures, inform development, and prioritize investment.

Another example of a novel application is the realization of SI base units outside of NMIs, which can include microwave and optical atomic frequency standards, Josephson voltage and quantum Hall resistance standards, miniature Kibble balances to realize the kilogram and nanophotonic or shot-noise thermometers [23]. These deployable quantum standards can dramatically shorten the calibration chains enabling more accurate end products.

In conclusion, the development of quantum-based measurement and sensing technologies can improve accuracy and precision even beyond the classical limit for a wide range of applications. Despite these applications, the development of the underlying enabling technologies has also a strong impact on many other QT components and subsystems.

4 Standardization

4.1 Relevance of standards for quantum technologies

For more than 25 years, the single market has provided a comprehensive and reliable legislative framework for conducting business across Europe. Since its creation, the European standardization policy played a fundamental role in its implementation and integration. It provides both harmonization and regulatory stability, which not only attracts investments, but also more importantly assures high safety standards for consumers and an adequate level of environmental protection. The economic benefit of standardization is estimated to be associated to 0.8-0.9 % of the GDP growth in countries such as Germany and France [24]. Standards effectively support trade, market access, quality of products and services, fairness, interoperability and innovation. Because of their role in protecting consumers, the health, safety, security and environment standards have a direct public interest. However, standards can also become a technical barrier to trade, as they can be adversely used as a tool to protect the single market and its strategic autonomy in fighting hostile trading practices, competition or procurement laws.

It is for these reasons that the EU QT Flagship has standardization widely included in its strategic research agenda and assures in the innovation strategy that its projects refer to standardization [11].

The European Standards Bodies (CEN, CENELEC and ETSI) define a *standard as "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."* Hence, standardization could be translated as any process used to develop and implement metrics (i.e., "standards") that specify essential characteristics of something whose control and uniformity are desired. This could be in the well-defined environment of the European Standards Bodies, but also the metrology institutes and other platforms. The definitions highlight those standards enable the communication and interaction among the community members, since members use the same vocabulary when they describe a corresponding technology, they measure with the same units and the measurement instruments produce comparable results.

Standards contribute to improve science:

It is important that scientist can communicate and exchange their research results or quantum technology hardware by using agreed vocabulary, definitions, units and interfaces. It is essential to undertake repeatable measurements and comparison in experiments. As standards are voluntary, the reduction of diversity should not limit scientific development. Looking from that angle one can say that scientists are among the first clients of standardization in the quantum technologies value chain.

Standards for innovators:

It is crucial when a company launches market with a new technology that the proposed product is compatible, safe and operates in an agreed environment. System integrators and service providers become the main clients for standardization.

Standards themselves can serve as framework conditions for research and innovation. This is especially the case for terminology and classification standards in the area of basic research. Metrology, measurement and testing standards are more relevant for applied research. Quality, health and safety standards are crucial for market penetration. Finally, compatibility standards can promote the diffusion of technologies and products especially in network industries.

Standardization can result in different products, which evolve over the time the technology is being developed and serve consequently different clients who are involved in the respective technology stage. At early technology readiness levels (TRL) main users (or clients) of standards produced during this phase

are found among the researchers, as agreements upon the vocabulary, the metrology and testing methods or operational procedures are being documented. Standards developed during the intermediate TRLs reflect the proven functionality of the technology, which however has not been integrated into the application or system. Physical interfaces, interoperability and quality metrics are of principal interest. Applied scientists, often from spin-offs, test in the beginning applications in laboratories and apply them in relevant environments. During TRL 7 to TRL 8 standards assure the service providers interoperable protocols, programming interfaces to integrate the technology into the system.

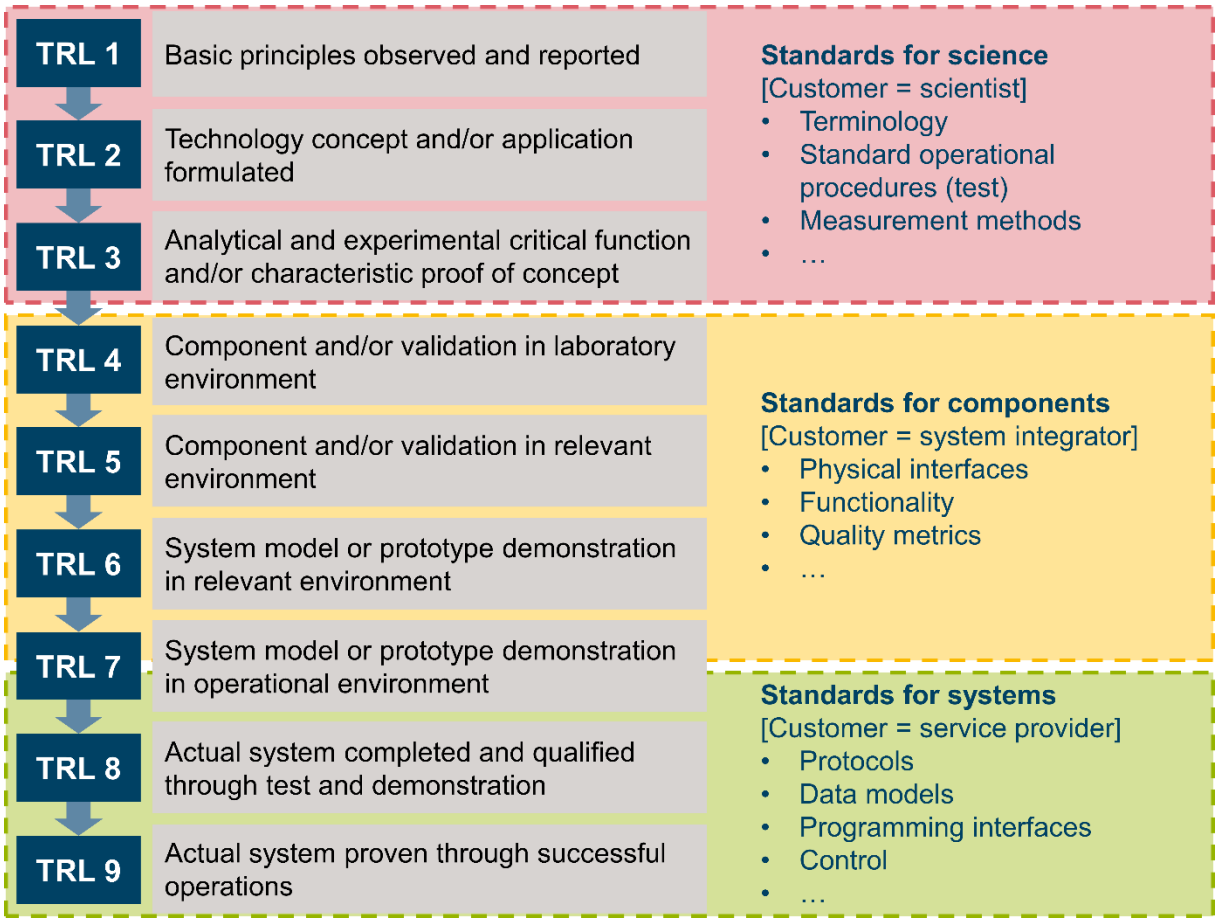


Figure 4 Technology readiness levels (TRL) and their relationship to standards and principal users

Technology readiness levels in the field of quantum technologies vary widely among the different fields. While several fields of quantum computing range are still at a conceptual state, some quantum sensing applications have reached TRL 9 and approach the market or are already commercially available in some cases.

Companies can use standardization as an effective strategic instrument. For example, standards can be used at an early stage of development to prepare the market for a new product, by defining common vocabularies, establishing the essential characteristics of a product or service. Additionally, standards can either supplement or complement governmental regulations. For example, in early stages of emerging research and technology fields, self-regulation via standardization allows stakeholders to set flexible framework conditions, which can later be transferred into governmental regulations.

Standards can also be used by the public sector in the context of public procurement, notably in tender specifications. The adoption of innovative standards in procurement schemes can for instance be used by governments to diffuse innovations to the private sector.

Standards for consumers:

Standards are equally providing an agreed level of reliability, guarantee for safety and security, hence building a trustful economic relationship. Standards promote transparency and trust to the innovation process, in helping to increase consumers' confidence. Standards for measurements and tests help innovative companies to demonstrate to the customers that their innovative products possess the features they claim to have, they are safe, of good quality and they help the environment.

4.2 Standardization products

4.2.1 General

Standardization is of great importance both at national and European level. Although European standardization activities are in the foreground in the CEN/CENELEC Focus Group Quantum Technologies (FGQT), which is coordinated by DIN, international and also relevant national standardization are presented, as a transnational harmonization of standardization documents is considered highly relevant. Standardization is becoming increasingly important both at European and international level in the quantum technology area. The results from the FGQT would highlight how the current state of the art in the quantum technology area would translate to standardization and associated application by industry.

This overview serves as the basis for future standardization activities in quantum technology. Knowing about existing standardization documents makes it possible to build on existing knowledge and avoid unnecessary duplication of work. In addition, existing gaps in standardization can be better identified and impulses for new standardization activities can be developed.

First of all, the different types of standardization documents and thus the different terms should be explained. A standardization document is generally a technical document that defines requirements for products, services or processes. However, there are differences in how they are created, which are illustrated below. For this purpose, Figure 5 shows various types of standardization documents depending on their development time and the degree of consensus in the documents.

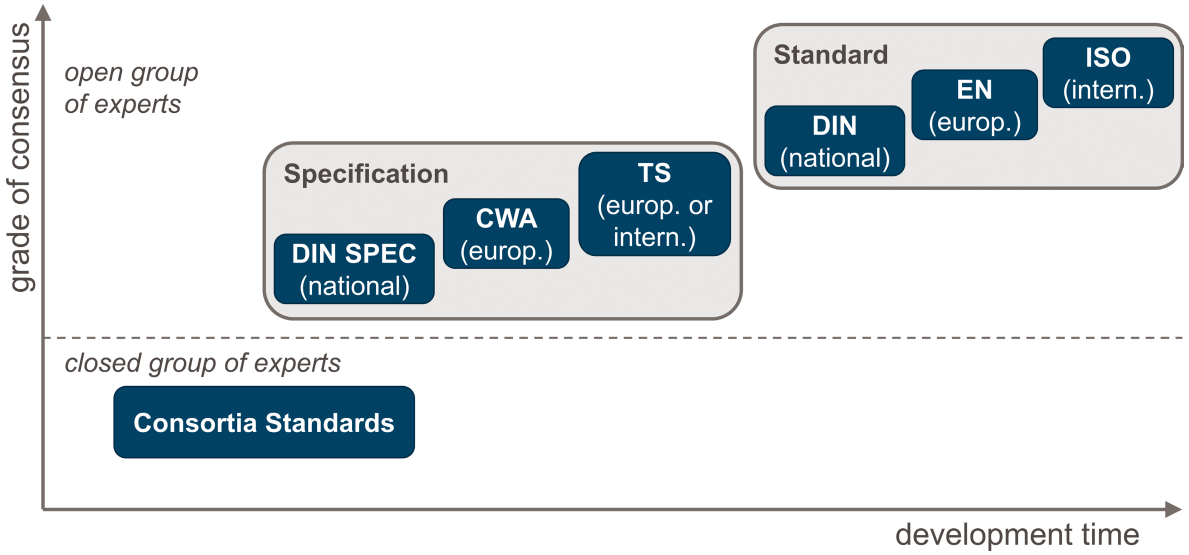


Figure 5 Examples of standardization documents

4.2.2 Consortia standards

Consortia standards shown in Figure 5 are usually drawn up in closed groups of experts. Among other things, they are characterized by the fact that not all interested parties are included in the creation process. The closed groups of experts named in the figure above can be, for example, industry-specific consortia that have been formed from different companies. Although these documents have some characteristics of a standardization document such as defined procedures or documentation rules, consortia standards are often not freely accessible and are developed in secrecy.

4.2.3 Standards

The work of European Standardization Organizations focuses exclusively on the transparent creation of standardization documents open to everyone and considered to take care of all stakeholder needs resulting in broadly accepted document achieved by consensus. This includes standards shown at the other end of the spectrum in Figure 5. Consensus means the general approval of the interested parties, which is characterized by the lack of sustained objection to central content. The main aim of the consensus is to take into account the views of all interested parties concerned and to dispel any counter-arguments. Standards are developed in different standardization committees within several standardization organizations. This development is described in section 4.3. In general, standards can be classified as follows:

— National Standards, e.g. DIN standards in Germany, UNE standards in Spain, etc.

— European Standards (EN standards), drafted at CEN, CENELEC or ETSI

— International Standards (ISO or IEC standards), drafted at ISO or IEC

4.2.4 Specifications

In contrast to a standard created with consensus, the standardization activities in research projects often focus on the creation of specifications. A specification is a public, freely available document that describes products, systems or services by defining characteristics and defining requirements. The specification is characterized by the fact that, compared to a standard, a consensus is not absolutely necessary and the involvement of all interested parties does not have to be guaranteed. A specification can be developed within a short period (approximately 6 months), which makes this tool attractive for research projects to transfer their project findings into a standardization document. Furthermore, specifications are developed by standardization committees or by temporary consortia under the umbrella of various standardization organizations. They can also serve as a basis for standards on European or international level. In general, specifications can be classified as follows:

— National Specifications e.g., DIN SPEC in Germany

— Technical Specifications (TS) or Technical Reports (TR) at European or international level, drafted by an established Technical Committee at CEN, CENELEC, ETSI, ISO or IEC.

— Workshop Agreements, drafted by a temporary consortium at CEN or CENELEC (CWA) or ISO or IEC (IWA)

— Group Specifications (GS) or Group reports (GR), drafted by an Industry consortium at ETSI

4.3 Standardization process

Every country participating in the European and international standardization world of CEN, CENELEC, ISO and IEC follow the so-called delegation principle. National standardization bodies send representatives to the European or international standardization committees of CEN, CENELEC, ISO and IEC to represent their national interests (see Figure 6).

NOTE JTC 22 is the new CEN/CENELEC Joint Technical Committee on Quantum Technologies, which is active from early 2023

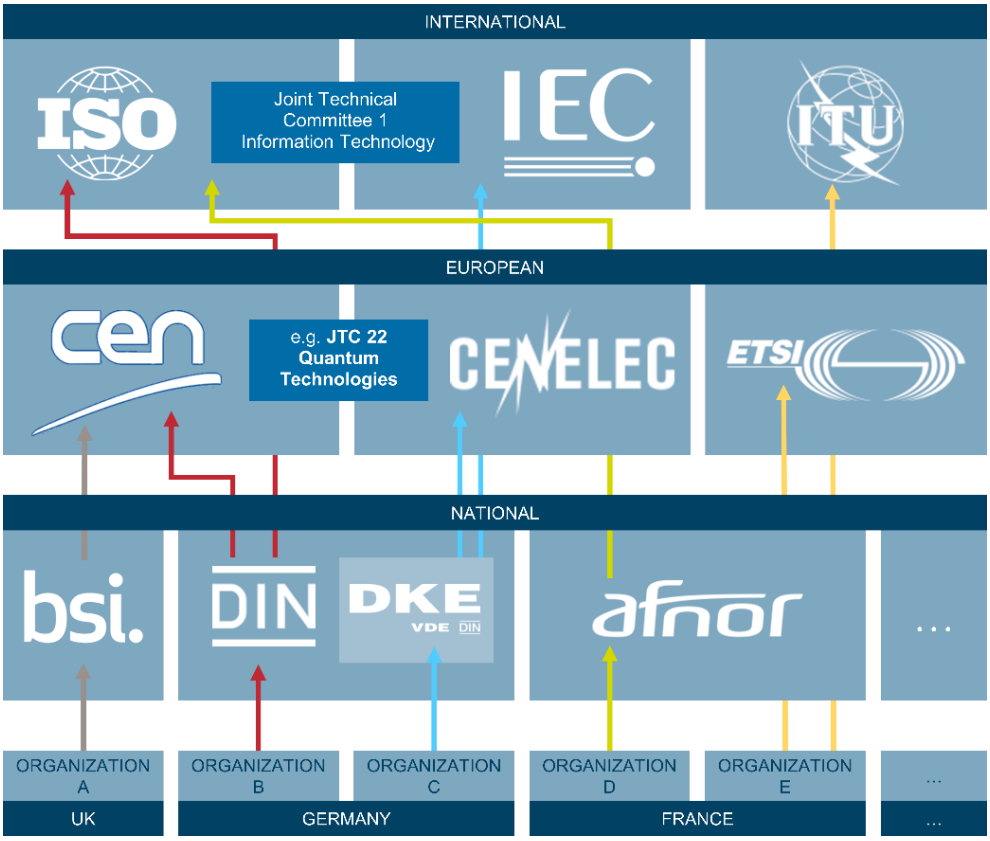


Figure 6 European and international standardization landscape

An important aspect of standardization work is to ensure that the documents do not contradict each other. The importance of European and international standardization has increased noticeably in recent years. Around 90 % of all standardization projects are nowadays carried out at European and international level.

The main goal of standardization at European level is to harmonize the national standards of the member states of the European Union. This includes on the one hand the uniform transfer of international standards and on the other hand the creation of European standards. The European standardization organizations CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization) and ETSI (European Telecommunications Standards Institute) are responsible for the organization of European standardization work. CEN is responsible for all non-electronic activities and CENELEC for electrotechnical standardization activities. ETSI is responsible for the standardization activities in the field of telecommunications at European level.

CEN and CENELEC are made up of the national standardization organizations. The other members are comprised of the national standardization organizations of the EU and EFTA (European Free Trade Association) member states as well as those states that intend to become members. In addition, there is particularly strong cooperation between CEN and CENELEC. In contrast, the members of ETSI are directly European companies, institutes and organizations.

The so-called delegation principle applies to CEN and CENELEC. This means that the members, the national standardization organizations, send their national experts to a European standardization body. In a national committee, known as the mirror committee, the work is discussed, existing results are discussed, and a national opinion is developed. This committee then votes on the final draft standards. Only when a sufficiently large majority of the national standardization organizations have voted for a draft standard is it accepted and published as a European standard (EN).

European standards shall automatically be adopted by the member states of the EU and opposing national standards withdrawn. As a result of this takeover obligation, the EN standards then become DIN EN standards in Germany (e.g., DIN EN 16575) or UNE EN standards in Spain. The obligation to adopt the national standards of the member countries does not apply to specifications, but is possible (e.g., NEN CEN/TS 17045).

The international standardization organizations ISO (International Organization for Standardization), IEC (International Electrotechnical Commission) and ITU (International Telecommunication Union) are responsible for organizing international standardization work. ISO is responsible for all non-electronic and IEC for electrotechnical standardization activities. The ITU is responsible for standardization activities in the field of telecommunications on an international level.

ISO and IEC are made up of the national standardization organizations. The ITU, on the other hand, is a special unit of the United Nations, whose 191 member states develop recommendations together with companies from the private sector and other regional and national organizations. Only when they are adopted by normative organizations such as ISO or ETSI as well as by national regulatory authorities they acquire the character of standards.

The so-called delegation principle also applies to ISO and IEC, so that the national standardization organizations also send their experts to the international standardization bodies. Also here the work is discussed in a national mirror committee, existing results are discussed, a national opinion is developed and the final draft standards are agreed. Only when a sufficiently large majority of the national standardization organizations have voted for a draft standard is it accepted and published as an international standard (ISO).

In contrast to European standardization, there is no obligation to adopt international standards in national standards. However, since international applicable standards are relevant for international trade or for global stakeholders, conflicting standards should be avoided. There is the possibility of adopting international standards in European and national standards and there are also parallel creation processes of standards at international and European level.

4.4 Standards developing organizations for quantum technologies

CEN/CENELEC FGQT

At European level several groups dealing with quantum technology exist. CEN and CENELEC established in 2020 the Focus Group on Quantum Technologies (FGQT) with more than 200 participants from all over Europe, which produced this present roadmap. The goal of the FGQT is to connect relevant European stakeholder in all fields of quantum technology and foster the interaction between them. The FGQT will collect all ongoing activities in the area of quantum technologies, identify current needs and envisage the initiation of standardization activities to support the European quantum technology industry.

CEN/CENELEC JTC 22 QT

The establishment of the new CEN/CENELEC Joint Technical Committee 22 on Quantum Technologies (JTC 22 QT) was agreed October 2022, based on among others earlier drafts of the present roadmap document. JTC 22 QT is expected to further develop the roadmap, to initiate actual standardization activities, and to coordinate this work in Europe as well internationally.

ETSI TC CYBER WG QSC and ETSI ISG-QKD

ETSI has established the first two specific standardization working groups for addressing quantum technologies, dealing with standardization of quantum communication.

The Industry Specification Group on Quantum Key Distribution (ETSI ISG-QKD) was formed in 2008 and aims to connect stakeholders from commerce, industry and science to develop ETSI Group Specifications describing quantum cryptography. The ETSI standardization work in ISG-QKD covers several levels: It starts with problem statements in the form of use cases, from which technical requirements can be derived. These requirements then form the base upon which a reference architecture is created. Various

different specifications describe in detail components, protocols and interfaces. A vocabulary is developed to guarantee common understanding of the technical terms used in standardization for quantum communication technologies. Special emphasis is given to security proofs and recently to security certification of quantum key distribution products.

The Technical Committee Cyber Security Working Group for Quantum-Safe Cryptography (ETSI TC CYBER WG QSC) originated from the ETSI ISG QSC (Industry Specification Group on Quantum-Safe Cryptography). It aims to assess and make recommendations for quantum-safe (i.e., safe from a quantum computer) cryptographic primitives protocols and implementation considerations. The focus is on the practical implementation of quantum-safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking and practical architectural considerations for specific applications.

These two ETSI groups together thus cover hardware and algorithmic methods for quantum-safe cryptography. The ISG-QKD directly addresses a quantum technology, while CYBER QSC is concerned with classical algorithms and protocols which are relevant to the threat posed by quantum computers and the secure implementation of QKD. It is to be noted that while Quantum-Safe Cryptography is not a Quantum Technology, it is inspired by and became highly attractive as a consequence of the cryptographic relevance of Quantum Computing. However, quantum cryptography and quantum information Theoretical security in itself require future consideration and standardization as a complementary technology to be integrated with QKD technology to provide end-to-end internet secure communication.

NOTE The term “classical” is discussed in some detail in section 2.2.

ITU-T SG11, SG13, SG17 and FG-QIT4N

The International Telecommunication Union (ITU) - Study Group 11 ‘Protocols’ is initiating work on classical protocols and interfaces for Quantum Key Distribution Networks.

The ITU Study Group 13 ‘Future networks’ works on general functional requirements for QKD networks. This work so far includes the study of a functional framework, the description of a generic functional architecture and a specific focus on key management function.

Further, it proposed the ITU-T Focus Group Quantum Information Technology for Networks (FG-QIT4N), established in 2020 to discuss pre-standardization issues regarding networks dealing with quantum information technology. FG-QIT4N has finished its work and published its deliverables [25, 26] and made available a recording [27] of its concluding information session.

Study Group 17 ‘Security’ is currently working on cybersecurity, security management, security architectures, frameworks and on quantum related communication at international level. Current areas of QKD standardization efforts within ITU-T include those listed below in no particular order of importance:

— Security – certification of QKD for market uptake;

— Interoperability – Integrate QKD-networks with other networks;

— Metrology – Specifying quantum-specific components;

— Usage policies – Embedding and use of applications.

ISO/IEC JTC 1

The following activities in quantum information have been undertaken by ISO/IEC JTC 1, the Joint Technical Committee on Information Technology:

ISO/IEC JTC 1/SC 7:
Subcommittee SC 7 ‘Software and systems engineering’ has investigated quantum computing standards related to software engineering,

ISO/IEC JTC 1/SC 27:
Subcommittee SC 27 ‘Information security, cybersecurity and privacy protection’, in its working group WG 3 ‘Security evaluation, testing and specification’, has started to develop standards dealing with security requirements and test and evaluation methods for QKD products. (ISO/IEC DIS 23837). Currently,

the work concentrates on the draft International standard ISO/IEC 23837 “Security requirements, test and evaluation methods for quantum key distribution —Part 1: Requirements” and “Part 2: Evaluation and testing methods” [28, 29].

ISO/IEC JTC 1/SC 38:
Subcommittee SC 38 ‘Cloud computing and distributed platforms’ has investigated quantum computing cloud services.

ISO/IEC JTC 1/WG 14:
The Working Group 14 ‘Quantum Computing’ was established in June 2020. It aims at a systems integration entity to focus on the JTC 1 quantum computing standardization program and maintains relationships with related ISO and IEC technical committees and other organizations. Aim is to identify gaps and opportunities and develop deliverables in the area of quantum computing. Current focus is to develop the (draft international) standard ISO/IEC DIS 4879 “Information technology — Quantum computing — Terminology and vocabulary” [30], maintain the study report of Quantum computing, and collect the use cases of Quantum computing.

IEC SEG 14

The Standardization Evaluation Group IEC SEG 14 on a quantum technology was established October 2022 and is focused on investigating current and future needs for standardization in the area of quantum technologies as well as developing a roadmap for standardization. SEG 14 will also make recommendations to the IEC Standardization Management Board (SMB).

IEEE

IEEE SA (Institute of Electrical and Electronics Engineers Standards Association) has since 2017 established several standardization working groups

— IEEE P1913 Software-Defined Quantum Communication [31];

— IEEE P2995 Trial-Use Standard for a Quantum Algorithm Design and Development [34]

— IEEE P3120 Standard for Quantum Computing Architecture [35]

— IEEE P3155 Standard for programmable Quantum Simulator [36]

— IEEE P7130 Quantum Technologies Definitions [32];

— IEEE P7131 Quantum Computing Performance Metrics & Performance Benchmarking [33].

IEEE nomenclature standards create a common language for the quantum computing field supporting American developers, scientists, entrepreneurs, investors, and potential customers.

IRTF and IETF-qirg

The Internet Research Task Force (IRTF) is the research and future-oriented branch of the IETF, the Internet Engineering Task Force, responsible for guiding the practical use and implementation of many protocols and systems used in today’s telecommunications networks.

The Internet Engineering Task Force (IETF) established in March 2020 the Quantum Internet Research Group (qirg) [37] aiming to support quantum internet and hence new communication and remote computation capabilities such as quantum secure communication, distributed quantum computing, and quantum-enhanced physical sensor systems. A key focus area for quantum networks will be cryptographic functions such as quantum key distribution or quantum byzantine agreement. Achievements so far are architectural principles for quantum internet and a description of applications and use cases for the quantum internet.

CSA QSS-WG

The Cloud Security Alliance (CSA) Quantum-Safe Security Working Group (QSS-WG) produces reports on the state of post-quantum cryptography.

The goal of this WG is to address key generation and transmission methods that will aid the industry in understanding quantum-safe methods for protecting their data through quantum key distribution (QKD), which is a physics-based technology to securely deliver keys, and post-quantum cryptography (i.e., no quantum but quantum-inspired cryptography) and mathematical algorithms that are resistant to quantum computing.

CCSA (China)

China Communication Standards Association (CCSA) established three main platforms relevant for standardization activities in the field of quantum technologies, namely:

— Quantum Communication and Information Technology Special Task Group, which carries out studies on quantum communication technologies, quantum communication network, and quantum computing technologies, as well as common key components for quantum information;

— Industrial Internet special task group, which focuses on studies on industrial internet related standards system and development of quantum information systems;

— The Navigation and Location Service group focusses on communication and navigation integration, which includes high precision position information.

Quantum-resistant algorithms

The Computer Security Resource Center (CSRC) of the US National Institute of Science and Technology (NIST - see below) has, in 2016, initiated a process to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms. In 2022 NIST has selected 1 algorithm for public-key encryption and key-establishment and 3 algorithms for digital signature [17]. These algorithms should replace most vulnerable current standards and establish keys used in public-key cryptography. It is expected that the first of the standards will be released publicly by 2024, and the United States government is starting to plan for their introduction, with the goal of mitigating as much as possible of the risk by 2035.

4.5 European and international metrology institutes

National metrology institutes (NMIs) play a very important role in quantum technology standardization, developing measurement techniques as well as contributing to standards-defining committees. Metrology is relevant to quantum technology in two ways: quantum devices are used in metrology as fundamental standards[1], and quantum devices and systems themselves require metrology for reliable functioning, interoperability and benchmarking. NMIs utilize metrology practices for quantum technology developments and also use quantum devices to advance metrology practices (quantum metrology) [38, 39, 40]. Within this framework, NMIs today uses quantum-based primary standards for frequency and time, including the realization of Universal Coordinated Time (atomic clock), voltage (Josephson junction) and electrical resistance (quantum Hall effect) and potentially, in future, for electrical current (single-electron pump). The roadmap for quantum technology in metrology is therefore linked to the move to using fundamental physical standards to define units, the starting milestone being the redefinition of the SI system [41] on 20th May 2019.

[1] The word “standard” in metrology may refer to the apparatus that is used to physically realize a quantity, such as an SI unit, rather than the document defining it.

EMN-Q

A group of European National Metrology Institutes (NMIs) and Designated Institutes (DIs) with important quantum technology activities have recently created the European Metrology Network for Quantum Technologies [22, 42], (EMN-Q) under the auspices of EURAMET. It currently comprises 18 partners[2] from 15 countries, and its objective is to support the competitiveness of the emerging European quantum industry. Specifically, the EMN-Q operates in all fields of metrology for quantum technology like quantum photonics, quantum clocks and atomic sensors as well as quantum electronics, thus covering the QT applications as communication, sensing and metrology, computing, simulation and basic research.

The EMN-Q will develop the European quantum metrology infrastructure by coordinating, pooling, and strengthening the national quantum metrology infrastructures.

The EMN-Q implements its strategy through coordination of national and European actions that will enable the European industry to succeed through improved reliability and interoperability of quantum technologies:

— Joint research on quantum metrology: Realization of units, calibration and measurement capabilities, quantum technology, standardization, and scientific excellence. Research on quantum metrology has been supported by the European metrology research programs and now by the European partnership on metrology.

— Coordination of European quantum metrology infrastructures: Leveraging resources of European NMIs and DIs, EMN-Q coordinates the development of new measurement capabilities and dedicated services to meet the rapidly growing needs of the European quantum industry.

Members of the EMN-Q are active in the CEN/CENELEC FGQT and contribute to this present roadmap, including by sharing relevant contents of its strategic research agenda and QT roadmaps.

NIST

The US National Institute of Standards and Technology (NIST), is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce, which contributes to American standardization activities. NIST participates in the ITU-T, ISO and ETSI work on quantum technology standards. Its renowned Physical Measurement Laboratory (PML) includes divisions for quantum electromagnetics [43], quantum measurement [44] and quantum physics [45].

Within the realm of the different divisions, different standard-setting activities have been produced in NIST, such as:

— superconducting photon detectors[3] [46];

— Web-based tools for quantum networks [47];

— the miniaturization initiative 'NIST on a Chip' [48], which will develop highly accurate quantum-based standards and sensors, often miniaturized to chip scale or smaller, traceable to the International System of Units (SI);

— algorithm for NV centre diamond magnetometry [49].

[2] EMN-Q member institutes (NMIs, DIs): CMI, DFM, METROSERT, MIKES, AALTO, LNE, LNE-LCM/CNAM, LNE-SYRTE, PTB, INRIM, JV, GUM, IPQ, CEM, RISE, METAS, UME, NPL [108]

[3] Single-photon detectors are key to research areas ranging from optical communication and astrophysics. To ensure their accuracy and reliability, photon detectors need to be evaluated and compared to some benchmark, ideally a formal standard. NIST is developing methods to do that and perform custom calibrations.

NMIJ and NICT

The National Metrology Institute of Japan's Research Institute for Physical Measurement carries out quantum metrology work in its time standards, quantum electrical standards and advanced quantum measurement groups.

The National Institute of Information and Communications of Japan has contributed to ITU-T SG 13 work on quantum networks and is a vice chair of FG-QIT4N. As a member of ETSI ISG QKD it currently focuses on an evaluation methodology for QKD implementations.

Various (U.S.A., Korea)

In the United States the standardization landscape is more diverse than in Europe, as there are more than 270 different standardization organizations, including NIST and IEEE already discussed in detail above. The American National Standards Institute (ANSI) coordinates the US contribution to international standardization. In the field of quantum technologies the following standard developing organizations are the most relevant: UL (ex Underwriters Laboratories), the American Society of Mechanical Engineers (ASME) and American Society for Testing and Material (ASTM).

Since 2008, standardization activities in the area of QKD have increased significantly and, in addition to the SDOs just mentioned, the following additional organizations have been identified as currently working on QKD:

— The Quantum Alliance Initiative with the Hudson Institute [50]

— Global Quantum Industrial Partners is an SK Telecom (Republic of South Korea) lead consortium aiming to promote ICT standards, interoperability and commercialization.

4.6 Supply-chain view on standards relevant to quantum technologies

4.6.1 Introduction

This section provides a supply-chain view on standards relevant to quantum technologies. It starts with a generic supply-chain view on standards. Next, it provides some hypothetical examples of business transactions relevant to quantum technologies. It concludes with guidelines for including the supply-chain aspect in a standardization roadmap (present document).

4.6.2 Supply-chain view on standards

Figure 7 provides an abstract supply-chain view on standards. The view includes two or more counterparties ("Party A", "Party B") that engage in a transaction. The transaction involves a product or service. Several aspects of that product or service may be standardized.

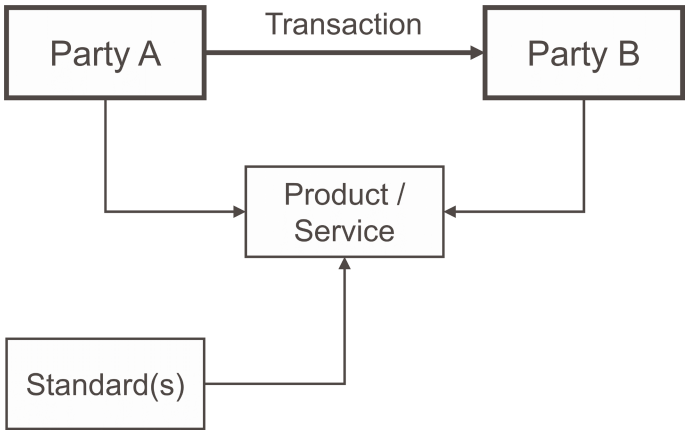


Figure 7 Abstract supply-chain view: a business transaction related to standards.

An example is a consumer who buys a television set in a shop. The counterparties in this example are the consumer and the shop. The product is the television set. One relevant standard is the electricity plug. Thanks to the standard, the plug fits into the wall socket in the consumer's home. The standard involves also voltage and frequency of the electric power. A benefit of the standard is hassle-free powering of the television set.

Another example is the same consumer buying a television service for their new television set. The counterparties are now the consumer and a television service provider. The product/service is the television service. A relevant standard is the encoding of the television signals, as the service only works if the television set can decode the provided television signals. A benefit of the standard is that the television set can continue to be used when switching between television service providers.

These two simplified supply-chain examples illustrate how standards facilitate transactions between two or more counterparties. Just try to imagine how complicated and expensive these transactions would have been, if each television set had its own incompatible plug, voltage and signal encoding.

4.6.3 Hypothetical transaction examples for quantum technologies

4.6.3.1 General

This section presents some hypothetical and abstract transaction examples related to quantum-technology supply chains. The markets for quantum technologies are mostly still embryonic, and it is not known what these different markets or their full supply chains may look like. However, some markets are already emerging. In particular, there are emerging markets of scientists and technology developers who are building quantum platforms and systems from components that implement enabling technologies, as illustrated in the "temple diagram" in the abstract (p. 7). Associated are markets for measurement equipment and measurement methods.

The purpose of this section is to provide inspiration for the initiation and development of standardization relevant to quantum technologies.

4.6.3.2 Buying an ion trap

Ion traps are a versatile quantum-technology component that can be applied in a variety of platforms and systems. A hypothesis is that there will be a market, where ion traps can be purchased as a unit that could be integrated into a platform or system. Standards may help enhance this emerging market for ion traps. One standardizable aspect is the characterization of ion traps that enable comparing and benchmarking between different ion-trap products and vendors. Another standardizable aspect may be the connection interfaces to integrate an ion trap into a platform or system.

The product in this example is an ion-trap product. The counterparties are the vendors and buyers of these ion traps. Standardizable aspects are technical characterization and interface specification of ion traps. A benefit of standardization would be the creation and growth of a market for ion-trap products.

NOTE This example may be applicable to many more enabling technologies that could be turned into a product.

4.6.3.3 Configuring a quantum simulator

Quantum simulators enable the simulation of e.g., chemical processes. A quantum simulator needs to be configured for a specific simulation task. Standards may provide a language to configure a quantum simulator.

The product in this example is a configurable quantum simulator. The counterparties are a chemical engineer who orders a quantum simulation, and a quantum engineer who configures/constructs the requested quantum simulator. A standardizable aspect is the language that describes the configuration. A benefit of standardization would be the creation and growth of a market for quantum simulators.

4.6.3.4 Developing an algorithm for a cloud quantum computer

Similar to the previous example would be quantum-computing capacity that is offered as a cloud service by multiple competing cloud-quantum-computing service providers.

The service in this example is a cloud-computing service. The counterparties are a developer with a quantum-computing task and a cloud-quantum-computing service provider. A standardizable aspect is an application programming interface. A benefit of standardization would be the creation and growth of a market for cloud-quantum-computing services.

4.6.3.5 Installing a QKD ground station

Quantum Key Distribution (QKD) enables a highly secure generation and distribution of cryptographic keys that does not rely on the unbreakability of mathematical algorithms. QKD has already been demonstrated in the space domain, involving orbital satellites. It is envisioned that a QKD network could be constructed with multiple satellites, multiple ground stations and multiple operators that operate different parts of the QKD network.

The product in this example would be the installation of a new QKD ground station. The counterparties are the operator of the ground station and the equipment vendor that provides the QKD equipment for the ground station. A benefit of standardization would be the creation and growth of a market for QKD equipment, as well as avoidance of vendor lock-in towards a specific QKD technology provider.

4.6.3.6 Buying quantum-technology measurement equipment

The specifications of quantum-technology platforms and systems as well as their enabling technologies need to be verifiable. Measurement equipment is required for this. Standards would specify what the measurable aspect is, and what the technical requirements that a specific measurement should satisfy are.

The product in this example would be measurement equipment that is used in a quantum-technologies context. The counterparties are the buyer and seller of the measurement equipment. Standardizable aspects are the measurement method itself, as well as characterizations of the fidelity of the measurements. A benefit of standardization would be the creation and growth of a market for measurement equipment for quantum technology set-ups.

4.6.3.7 Submitting a scientific article for peer review

Related to the previous example are scientific articles that involve measurements. If a measurement method is specified in a standard, then the author can reference that standard, instead of completely detailing it.

The product in this example is the submitted scientific article. The counterparties are the author and the peer reviewer. The standardizable aspect would be the applied measurement method. A benefit of this standardization is that it would make scientific articles on a specific measured feature better comparable, enabling benchmarking the results from the scientific article against its cited references.

5 Enabling technologies

5.1 Quantum channels

5.1.1 General / Principles /Overview

— Key subsystem: Quantum channel. A quantum communication system requires the access to a quantum channel. The quantum channel might vary depending on the technological choices of the basic components chosen to create and manipulate the quantum states. It might be required to transport electro-magnetic radiation or matter and can be adapted to situations like long distances -typical for telecommunications- or short distances -typical for communication inside a quantum device-, to different degrees of freedom of the physical system used to encode the information (phase, polarization, quadrature amplitudes, charge, flux, etc.), their dimensionality (qubits in two-dimensions, qubits in n-dimensions), etc.

— Types of quantum channels:

  - Direct transmission channel: Quantum systems are sent through a quantum channel that supports the transmission of the relevant degree of freedom used for encoding the quantum signals. It has limited reach due to loss or decoherence along the line. It can be also used, to create correlations, albeit with a limited reach. They can be concatenated, forming a multi-hop chain of direct transmission channels for longer reach. However, this is done by classical means: the quantum states are measured, so that no quantum correlations can be established between the initial and final point in the multi-hop chain.
  - Quantum correlation channel: A chain of direct transmission channels are used together with a quantum (repeater) protocol that involves the manipulation of the quantum states at the connection points and enables the efficient (polynomial with the length) establishment of correlations over long distances. These manipulations of quantum states are done at the quantum level, meaning that quantum correlations survive. These correlations allow, among other possibilities, quantum state transfer (teleportation). Quantum correlations channels always involve entanglement.

NOTE The term “classical” is discussed in some detail in section 2.2.

5.1.2 Standardization needs

Quantum transmission channels typically need to exhibit extremely low attenuation and reflectance in order to minimize decoherence, i.e., collapse of the wavefunction. As decoherence can be caused by direct measurement or by disruption to the photon propagation due to aberrations (imperfections) in the optical link constructed from passive optical components such as optical fibre, connectors, multiplexers, etc., the chances of transmitting a photon from transmitter to receiver without disruption, absorption or decoherence, decreases as the length of the any quantum channel increases and as the quality of the quantum channel decreases.

Another key performance parameter that has to be considered is the optical reflectance in the passive components that have to be deployed at the source, routing and reception nodes to direct the photons. Depending on how the quantum information is generated or processed, the passive components at the source, routing and receiving nodes may include non-linear crystals (e.g., BBO), polarization beam splitters, half wave plates, Wavelength Division Multiplexing (WDM) multiplexers and demultiplexers. Any boundaries, discontinuities or perturbations in refractive index may give rise to a reflection of the photons, which will contribute to return loss.

Compromises between performance and commercial viability would need to be considered in selection of the components used to build the quantum communication link.

Transmission of single or entangled photons over longer distances represent a considerable challenge and thus the optical insertion losses in the quantum channel must be minimized in all physical layer components used in the link.

Furthermore, it is crucial that at the connector interfaces such discontinuities are essentially eliminated through the design and quality of the mating connectors and associated fibres.

The higher densities of communication networks are leading to the miniaturization of cables, connectors, passive components and network accessories and infrastructures. The problems/gaps of the two fundamental components of a physical layer quantum link (optical fibres and optical connectors) as well as other passive components are following:

1) *Problems/gaps of the ultra-low loss optical fibres*

To miniaturize the size of network elements there is a need for:

— newer classes of performance requirements and test methods to ensure the requirements of the optical transport system

— new optical fibre designs, including alternatives to all glass silica-based fibres such as plastic or plastic clad silica, and

— new designs of optical fibres optimized for ultra-tight bends.

New classes of fibres like the Hollow core fibre [51], enable faster signal propagation and have greater imperviousness to noise, and recent developments [52] are trying to reduce their high attenuation losses to the levels of the conventional silica fibres.

2) *Problems/gaps of the ultra-low loss pluggable optical connectors*

Since light does not propagate through the whole optical fibre, but only through the core, the relative dimensions of the core and cladding of the optical fibre have a big impact on the connector quality. There is need for improvement of the material quality and the manufacturing process of the fibres to reduce further the insertion loss and return loss in the connectors by tightly controlling the three main parameters of the fibre:

a) the core-cladding concentricity;

b) core ovality; and

c) cladding ovality.

3) *Problems/gaps of the ultra-low loss optical MUX/DEMUX*

WDM schemes such as DWDM or CWDM allow multi-wavelength transmission over single fibre and is common to existing national and international networks. Multiplexing quantum and classical channels together over single-mode fibre (SMF) as part of a “Quantum Classical Division Multiplexing” (QCDM) scheme would provide a practical route to quantum communication over existing infrastructure, however compromises would need to be made as both classical and quantum channels have their own requirements. For instance classical channels use optical amplification technologies such as EDFAs to extend signal reach. The purpose of quantum channels, however is to convey signals as far as possible while preserving the quantum state. Optical amplification would essentially destroy the quantum state of propagating signals, as if they had been measured.

Therefore, quantum channels would need to be multiplexed onto the common fibre such as to bypass amplification nodes.

Critical parts of a WDM link are its MUX and DEMUX components. Although both classical and QKD channels would benefit from an ultra-low loss MUX and DEMUX, manufacturers have to sacrifice channel isolation for ultra-low loss and vice versa. Traditionally, conventional classical signals on WDM networks require high channel isolation to prevent crosstalk, which will inevitably increase the noise. While, in classical channels, the signal-to-noise-ratio and channel losses can be compensated through the use of optical amplification, this is not a viable option for quantum channels.

Hence, until technology advancement permits the production of an ultra-low loss MUX/DEMUX with high isolation, it would be advisable to transmit the classical and QKD channel separately for the moment.

5.2 Colour centres in (nano)diamonds and other crystals (e.g., SiC)

5.2.1 Introduction

The aim of this roadmap section is to identify the existing pre-normative gaps and standardization needs preventing effective exploitation of spin's superior quantum coherence in the NV centres for quantum sensing and quantum information processing. To the best of our knowledge, there are no standards related to NV-centre based sensors. Due to lack of common standards and procedures (as seen in Table 1), the commercial outcomes for both quantum sensing and communication are often incomparable and lacking in cross-producer reproducibility. Lack of standards for quantum sensor industry is commonly seen as a barrier to market acceptance of new relevant products. The standardization will help multiple industries in the quantum technology sector. The existence of a standard that stakeholders can adhere to would therefore significantly de-risk further investments in the market.

Table 1 Already Existing Documents

Standardization Activity	ID	Title	Category	Link
Quantum Flagship	Quantum Flagship Strategic Research Agenda	Quantum Flagship Strategic Research Agenda	Quantum Technology	https://ec.europa.eu/digital-single-market/en/news/new-strategic-research-agenda-quantum-technologies https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65402
BSI	BBSS EIENC 6622660077--33--11::22001144	Luminescent nanomaterials — Quantum efficiency	Quantum Technology	N/A

5.2.2 General description

A negatively charged NV centre in diamond is an excellent example of a room temperature quantum system with a great applicability in many interdisciplinary fields [53, 54, 55, 56, 57, 58], including magnetometry, thermometry, strain and pH measurement, even in biological systems.

Several instances of NV centres applications as quantum sensors are available in literature and some possible market applications have already emerged (as described below). Other systems, e.g., SiC and hBN, are currently also under intense study and can be exploited in principle [59, 60].

5.2.3 Principles

An NV colour centre in diamond is formed by one N and three C atoms (Figure 8a). This configuration makes the ground state |g> of the NV centre an electronic spin triplet system with S=1 (Figure 8b). The optical transition can be non-resonantly excited typically by a green laser, resulting in a broadband fluorescence spectrum in the 637 nm to 800 nm wavelength range (zero-phonon-line at 637 nm, see Figure 8c).

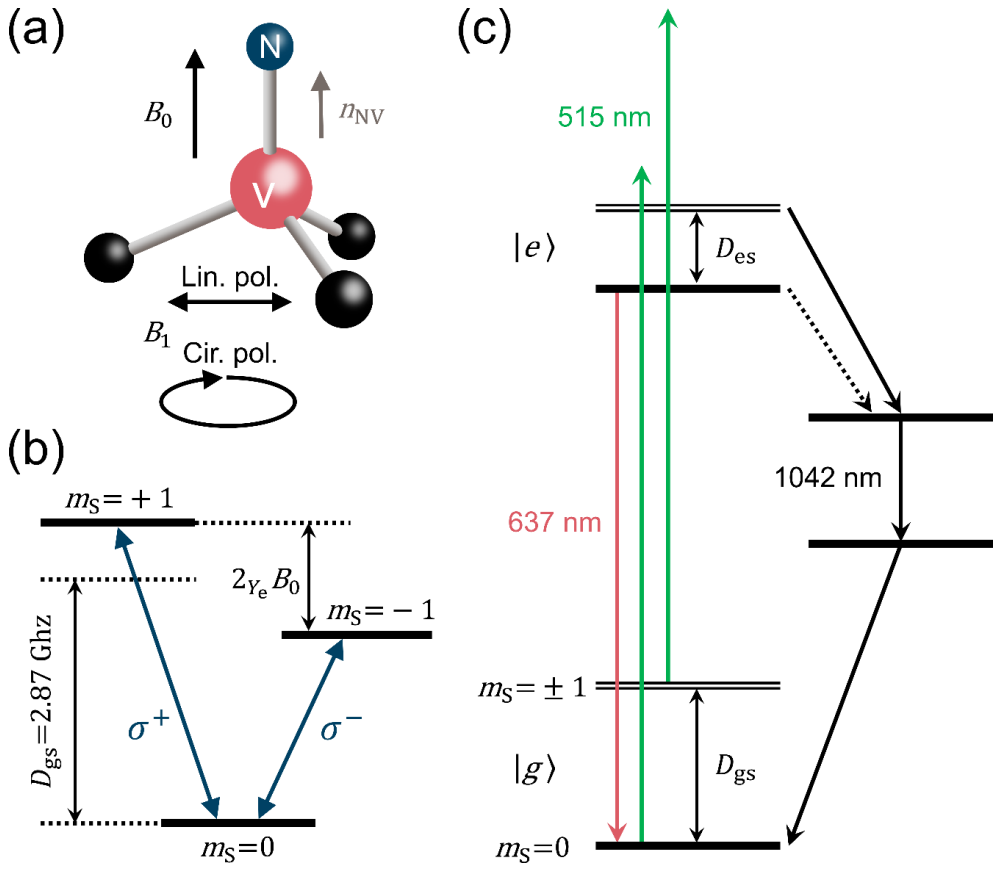


Figure 8 a) Schematics of an NV centre. b) Spin triplet ground state. c) Energy level diagram [54].

A specificity of the system is that if the electron is in the spin state |m=±1>, two decay paths are possible, with different associated photoluminescence (PL) emission. Remarkably, this allows the optical read-out of the spin state of the NV centre at room temperature. Furthermore, it enables high sensitivity measurements of magnetic and electric fields, temperature and strain to be performed due to the long spin coherence times.

5.2.4 Pre-normative gaps

The main identified pre-normative gaps concern material, infrastructure and device standardization (as discussed in detail below). With a number of commercial applications already entering the market in the field of quantum solid state centre magnetometry, we believe that timely development of the relevant standards will support and stimulate current and near-future quantum products.

We can also expect the development of a standard to stimulate a discussion among all existing and potential stakeholders. While we expect that a final standard will take some time to develop, the mere existence of such an activity will help all parties involved and prevent proprietary products from becoming de facto standards.

5.2.5 Standardization needs

In respect to pre-normative gaps and industrial applications outlined above, we identify the following three groups of standardization needs:

— Material standardization: characterization methods for colour centres in solids, allowing for reliable and comparable spec sheets in terms of purity of the base material, chemical type, density, spatial distribution of colour centres. Specifically:

  - Technique of synthesis of the base material;

- Native defect concentration, spatial distribution, lifetime;
- Doping technique;
- Type, density, lateral position and depth of implanted colour centres;
- Photoluminescent properties (photon flux, spectrum, autocorrelation properties);

— Infrastructure standardization: guideline for development of characterization infrastructure and defining measurement procedures and figures of merits. Specifically:

Magnetometry/sensing:

- Sensitivity, i.e., the weakest signal (normalized to the square root of the measurement time) that is detectable with a measurement system;
- Environmental working conditions (e.g., temperature, pressure, external electromagnetic fields);
- Optical excitation power, power density;
- Bias magnetic field (amplitude, orientation);
- Biocompatibility, i.e., determined measurement conditions (optical excitation power, microwave power & polarization, functionalization) that are non-detrimental to the normal physiology of living cells/tissue;

Microwave engineering:

- Microwave power & polarization;
- Geometry of the antenna delivering the microwave;
- Contrast and linewidth of the ODMR resonance dip;
- Excitation pulse sequences;

— Device standardization: performance of colour centres in quantum sensing and imaging as well as quantum computing and simulation.

The examples of crucial measurements that need to be defined include:

- Achievable sensitivity (magnetic/electric field, temperature, strain);
- Photoluminescence properties;
- Quantum coherence properties (via Rabi, Ramsey and Hahn Echo protocols);
- Biocompatibility conditions.

5.2.6 Overview (commercial sectors and markets)

For quantum communication, NV centres provide robust room-temperature single-photon sources which can be used both as light sources for secure communication and as a means for quantum random number generation. Efforts to develop a 'quantum internet' based on distributed entanglement are underway in Europe and the US, with diamond colour centres the leading candidate for local memories and quantum repeaters (see e.g., OpenQKD[4] [61]). Diamond chips containing 10 000 or more quantum memory nodes also offer enormous potential for quantum computing and simulation, providing a degree of scalability that competing technologies may struggle to achieve. However, due to absence of common standards and procedures (as reflected in Table 1), the commercial outcomes are often incomparable and lacking in cross-producer reproducibility. Lack of standards for quantum sensor industry is commonly seen as a barrier to market acceptance of new relevant products. The standardization will help multiple industries

[4] OpenQKD.eu Horizon 2020 research and innovation project

in the quantum technology sector. The existence of a standard that stakeholders can adhere to would therefore significantly de-risk further investments in the market.

In respect to existing commercial technologies, we identify the following sectors and the major players:

— Quantum computation: Quantum Brilliance [62]

— Quantum imaging: QNami [63] (Horiba), QZabre [64], Attocube [65], NVISION [66], Zeiss [67]

— Quantum sensing: Bosch [68], THALES [69], Lockheed Martin [70]

— Material production/development: Element Six [71]

Among the major players must be considered the Quantum Flagship initiative projects:

— AsteriQs [72]

— MetaboliQs [73]

The potential buyers broadly range from fundamental and applied researchers to developers in quantum communication and sensing and further applications of the technology in finance, military and defence, Life Science, etc.

Markets: The global quantum sensors market is expected to grow from $ 161 M in 2019 to $ 300 M by 2024 with a compound annual growth rate (CAGR) of 13.2 % during 2019-2024 [74] (alternative figures provide $ 320 M by 2023 [75] and $ 545 M in 2030 [76], see Figure 9). The market is still challenged by a number of factors, which include high cost and the challenge of product reliability, fragmentation, availability of competing technologies, unestablished supply chain and limited demonstrated applications. The majority of current products on the quantum sensor market are designed for research and development activities. However, companies are starting to focus on the development and commercialization of NV centre sensors for industrial applications, e.g., communication, finance, military and defence, life science, etc. The current supply chain includes material suppliers and advanced material developers, component and device manufacturers. The stakeholders are a good mixture of well-known large corporations as well as established SMEs and start-ups. There are over 30 companies worldwide now involved in diamond magnetometry. For example, several large and well-established companies are developing ensemble magnetometry systems for engineering applications, while a number of spin-outs offer products involving scanning probe nanomagnetometry aimed at research markets.

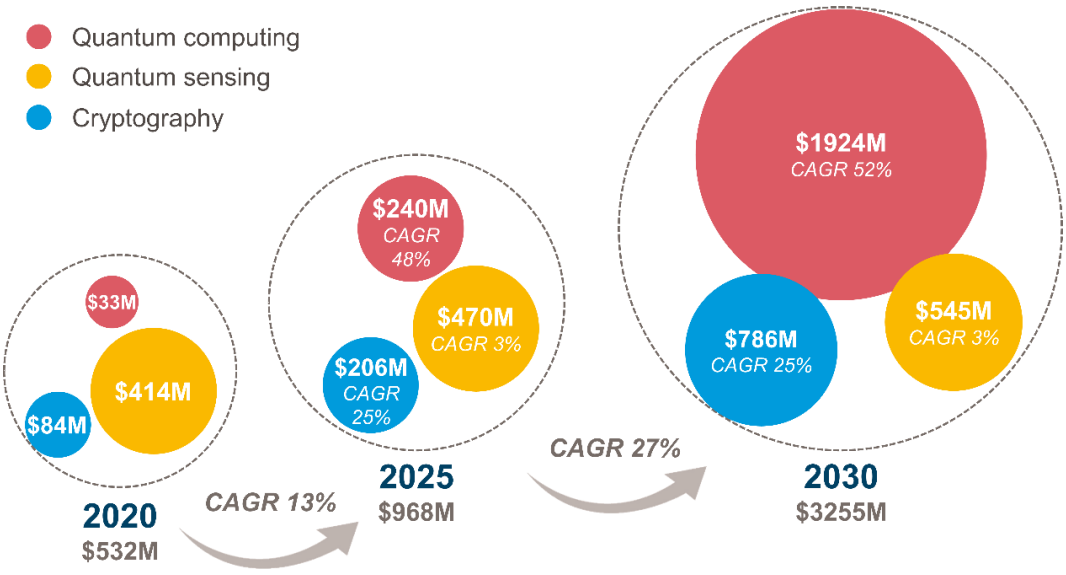


Figure 9 Quantum technology market forecast [76]

5.3 Ion traps

5.3.1 General

5.3.1.1 Already existing documents

Table 2 Already Existing Documents

Standardization Activity	ID	Title	Category	Link
Quantum Flagship	Quantum Flagship Strategic Research Agenda	Quantum Flagship Strategic Research Agenda	Quantum Technology	https://ec.europa.eu/digital-single-market/en/news/new-strategic-research-agenda-quantum-technologies https://ec.europa.eu/news-room/dae/document.cfm?doc_id=65402

5.3.1.2 General description

Ion traps enable the storage, cooling, and manipulation of charged particles.

This platform constitutes a fundamental building block for a wide range of applications over several subfields of QT: quantum computation, quantum simulation, quantum communication and quantum metrology.

The good isolation of the trapped particles from environmental disturbances allows for, e.g., exceptionally long coherence times for quantum information stored in atomic qubits and the use as frequency references with unprecedented accuracy.

Examples for specific products that can be derived from this platform include atomic clocks, gravitational sensors, quantum computers, quantum simulators. Related services could, e.g., consist of the reliable characterization to allow for comparable hardware platforms. These products and services are relevant for both science and industry. Several companies are already developing QT based on ion traps.

A range of technologies exist within the field of ion trapping. These include:

— Paul ion traps, with both DC and RF electric field confinement; linear traps

— Electrode structure: 3D (classical blade/rod or chip-based traps), 2D (surface electrode traps)

— Penning ion traps: DC electric and magnetic field confinement

— Optical dipole traps for ions

— Traps for operation at room temperature or in cryogenic environments

— Single vs. multiple potential minima (e.g., segmented linear trap, surface trap array)

— Different addressing technologies: Optical addressing or microwave addressing of qubits

— Integrated optical / electronic / microwave components

— Shuttling, non-shuttling geometries

5.3.2 Pre-normative gaps

While ion traps have been developed and used in scientific research for decades, considerable commercial interest for their use in QT applications has only arisen very recently. As such, there are essentially no existing standards for this rapidly growing field.

5.3.3 Standardization needs

We propose here a list of quantities whose standardization would be favourable to guarantee comparability of ion traps and interoperability with other related components.

What are the requirements/parameters?

— *Comparable and complete description of relevant specifications of an ion trap, as detailed below;*

— *Comparable means: need to specify all parameters required to transfer results to other ion species or operating conditions;*

— *"Specification sheet" for ion traps as a base requirement for commercialization; including key indicators, as detailed below.*

What are examples of parameters that need to be specified?

— Technical drawings:
  - Electrode geometry, with indicated trapping sites;
  - Dielectric surfaces closest to the ions;
  - Mounting and connection requirements / constraints;
  - Optical access and achievable detection numerical aperture;

— Maximum bakeout temperature;

— Confinement parameters (for each dimension, with indication of ion mass and charge, (RF drive frequency if applicable)):
  - Achievable trapping frequency, potential depth (corresponds to maximum safe RF and DC voltages);
  - Anharmonic potential terms and loss parameter;
  - Upper bound on heating rates (at given trapping frequency);
  - Mathieu q parameter (RF confined dimensions only);

— RF ion trap capacitance;

— DC control capabilities (e.g., principal axis rotation / radial mode splitting in linear traps) (Alternatively: 3D data of electrode electric potentials at 1 V);

— Temperature increase per RF power (under specified heat sinking conditions and drive frequency);

— Transfer functions for temporal confinement changes such as shuttling operations (due to, e.g., integrated filters);

— Excess micromotion:
  - minimal value of RF electric field (in specified volume, for given RF field gradients in all RF-confined dimensions);
  - range of compensation fields;

— Vacuum compatibility: Bound on achievable pressure via collision rate measured with ion (indicate ion mass, charge, confinement parameters, laser cooling parameters (if applicable));

— (Optional: Included atom sources (ablation targets, ovens));

— (Optional: Integrated microwave electrode RF properties, max currents, achievable fields, and gradients at given trapping sites);

— (Integrated optical / electronic component specifications – development in a too early stage);

— For cryogenic traps:

- Power dissipation under specified operating conditions;
- Connection heat load;
- Component CTEs;

— For trap arrays:

- Distance between trap sites;
- Crosstalk of control voltages for different sites.

What are examples of crucial measurements that need to be defined (of the above)?

— *Achievable trapping frequencies (maximum RF and/or DC voltages);*

— *Heating rates;*

— *Minimal excess micromotion;*

— *Upper bound on collision rate and lower bound on ion lifetime (need to specify laser cooling conditions and statistics requirements).*

5.4 Superconducting quantum circuits

Microfabricated chip-scale superconducting circuits have been used in applications for several decades. While not mass-produced, there are sectors where for example sensors made from superconducting circuits are in widespread use. Important examples include sensors for magnetometry, radio astronomy and single-photon detection.

Currently, most of these circuits are conceptually simple and involve only a small number of elements. Large-scale circuits are used in a very limited number of applications; most notably in voltage metrology and more recently near-quantum limited microwave amplifiers. Large-scale digital superconducting high-speed electronics based on e.g., rapid single flux logic (RSFQ) is a well-established field but has as of yet had limited real-world impact.

There are several foundries for superconducting circuits that circuit designers can access either commercially or via academic/government sponsored programs. Since the circuits are fabricated using the same lithographic processes used for semiconductor circuits, the same *de facto* industry standards for exchange of information are used for exchange of information between designers and foundry (e.g., the GDSII file format for the physical layout). The relative simplicity of the abovementioned circuits means that the use of these formats combined with a so-called Design Rule document (text document describing the features of the process issued by the foundry) typically provide enough information for designers. Usually, only a relatively small number of parameters (such as layer assignments, critical current density, sheet resistance etc.) need to be defined in the Design Rule document.

Conversely, in the semiconductor industry where circuits are extremely complex, designers use so-called Process Development Kits (PDKs). These are typically provided by the foundries and contain highly sophisticated models and vast amount of information about a specific process line in a specific semiconductor fab. The PDKs are also typically made to be used with proprietary design software. Although a number of attempts have been made by industry bodies to standardize PDKs this has not yet been successful and no SDO has attempted to introduce standards for any part of this workflow.

The rapid progress of superconducting quantum computing means that we can expect to soon be dealing with circuits with many thousands of circuit elements. This will require a much more sophisticated workflow and more advanced processing than what has hitherto typically been used. Already, workflows using script-based designs combined with RF modelling software to (in-part) autogenerate the physical layout of circuits have found widespread use.

As complexity continues to increase and e.g., 3D integrated circuits become more common, standards for information exchange between designers and foundries could become relevant. However, two factors need to be considered. Firstly, superconducting quantum computers operate at microwave frequencies

which means the precise *physical layout* is more important than in most semiconductor circuits; this means that a high-level cell-based approach is not always appropriate since e.g., controlling RF crosstalk is hugely important; optimizing the physical layout is paramount and cells cannot always be easily reused. Secondly, the fact that these are *quantum* circuits means that they are extremely sensitive to their environment. As of yet there is no practical way to in practice model the full performance of even single qubits since this depends on a complex interaction between the design, the materials used and the many variables in the fabrication process. Currently, there is not even agreement about the best way to report measured metrics of superconducting quantum circuits. This and many other issues will need to be resolved before something akin to a PDK can be created for superconducting quantum processor foundries.

Whereas standardization of the fabrication process and information exchange relevant for superconducting circuits is very challenging, one area where standardization could be directly relevant in the near-term is in the *packaging* of superconducting circuits. This would parallel the development of semiconducting circuits where a number of standards are defined by e.g., IEC exist for popular package formats (such as BGA, DIL etc.). These new standards could extend existing standards or where appropriate create new ones. The latter could for example include standards for high-density RF interfaces suitable for operation at cryogenic temperatures and in high vacuum.

5.5 Traveling wave parametric amplifier

5.5.1 General

5.5.1.1 Already existing documents

Table 3 Already Existing Documents

Standardization Activity	ID	Title	Category	Link
Quantum Flagship	Quantum Flagship Strategic Research Agenda	Quantum Flagship Strategic Research Agenda	Quantum Technology	https://ec.europa.eu/digital-single-market/en/news/new-strategic-research-agenda-quantum-technologies https://ec.europa.eu/news-room/dae/document.cfm?doc_id=65402

5.5.1.2 General description

Traveling wave parametric amplifiers (TWPA) are microwave amplifiers typically operating in the frequency range of approximately 2 GHz to 10 GHz. Based either on the non-linearity provided by Josephson-junctions or the kinetic inductance of disordered superconductors these devices find application as the first amplifier of the amplification chain for the readout wiring of superconducting qubits or microwave kinetic inductance detectors (MKID) for radio-astronomy. Due to their operating principle, theoretically such amplifiers allow amplification with the smallest possible added noise of half a photon. Despite the fact that practical implementations have not shown quantum limited noise in TWPAs yet, these devices still provide significant increase in SNR for the readout of superconducting qubits and are an essential enabling technology for quantum computing based on superconducting circuits. Additionally, these devices may also boost SNR for the readout of MKID, which are deployed to telescopes in multiple locations.

Results on TWPAs have first been published in 2012 and since then the concept has been continuously developed due to its strong potential.

5.5.2 Pre-normative gaps

While TWPAs have been developed and used in scientific research for about ten years, considerable commercial interest for their use in QT applications have only arisen recently. Although figures of merit such as bandwidth, amplification, and noise are routinely reported in scientific publications, there are no existing standards for the data measured and reported for data sheets of TWPAs, which are on the cusp of becoming commercially available.

5.5.3 Standardization needs

We propose here a list of quantities whose standardization would be favourable to guarantee comparability of TWPAs and interoperability with other related components. Ideally these parameters should be reported in a standard data sheet provided to potential customers by suppliers of such devices.

Examples of parameters (i.e., what would ideally be included in a TWPA datasheet) that need to be specified are:

- Technical drawings:
  - RF-packaging dimensions with indication of available holes/threads usable for mounting and ensuring thermalization of the device;
- Available options for connectors: should be one of already available standard RF-connectors, e.g., SMA or other;
- Typical pump frequency;
- Typical pump power referred to the input of the device package;
- Magnetic field / current bias to tune the operation point.

Examples of crucial measurements that need to be defined are:

- Power gain defined as the mean of transmission over the device's bandwidth with an active pump minus the mean of transmission over the same bandwidth corrected for the device's input loss. Measurements of the power gain profile are to be provided in the datasheet at a minimum frequency resolution of 10 MHz or lower;
- Saturation power, defined as the signal power where the stated power gain decreased by 1 dB;
- Bandwidth, defined as the lowest and highest frequency point where the amplification decreases by −3 dB below the stated amplification value. In the presence of gain-ripples the gain profile will be smoothed suitably;
- Gain ripple, defined as the standard deviation of the power gain over the quoted bandwidth. Additionally, the maximum value of positive and negative deviation from the quoted power gain shall be provided;
- Added noise, defined as the mean of the added noise in the quoted bandwidth. Additionally, like for the power gain profile in the data sheet the added noise spectrum shall be shown in the quoted bandwidth at a minimum frequency resolution (and identical frequency points as for the power gain) of 10 MHz or lower.

5.6 Semiconductor quantum dots for quantum electronics

5.6.1 General description

Nanofabricated semiconductor quantum dots as an essential circuit element for quantum electronics allow to confine, control and examine single or few electron(s) or hole quantum states. The possible quantum technology applications range from single charge control for single electron based sensing and metrology to full quantum state control for quantum computation, simulation and communication.

A number of different semiconductor material platforms are in use. The most common ones are heterostructures of the III-V compounds gallium arsenide (GaAs) and aluminium gallium arsenide ($Al_xGa_{1-x}As$) and more recently the group IV element silicon (Si), but many other materials are also in use, both conventional like other III-V compounds (e.g., indium arsenide) or germanium (Ge) (mostly in conjunctions with silicon for strained heterostructures) and also unconventional materials like gapped 2d or 1d materials (e.g., bilayer graphene or semiconducting carbon nanotubes).

The confinement of the electrons typically combines different techniques: an initial confinement to a thin sheet of few nanometre extension is realized at interfaces of semiconductors with different bandgap (e.g., GaAs and $Al_xGa_{1-x}As$ or silicon and germanium compounds) or at the interface between the semiconductor and a dielectric (e.g., the Si-SiO_2 interface). The further confinement of the remaining degrees of electron movement is realized by electric gating or by removal of material (etching). The typical required length scales range from few 100 nm down to 10 nm, depending on the material system and the intended application. Electric control of the quantum dot state is realized by electric gates and contacts.

The fabrication of quantum dots uses nanofabrication techniques established for conventional microelectronics, but in most cases specially adopted for quantum device fabrication and realized in R&D scale cleanroom facilities. There was also some research on using standard silicon MOS processes for fabrication of quantum dots in the last 20 years. Only recently a major semiconductor manufacturer implemented the fabrication of integrated quantum dot circuits in a state of the art industrial silicon microelectronics fabrication line and demonstrated the scalable fabrication of semiconductor quantum dots.

5.6.2 Pre-normative gaps

While quantum dots have been developed and used in scientific research for decades, considerable commercial interest for their use in QT applications has only arisen very recently. As such, there are essentially no existing standards for this rapidly growing field, which appears at the transition to practicable quantum circuits.

5.6.3 Standardization needs

Here we propose to identify sets of different quantities that can be used to characterize technology platforms and individual quantum dot devices, to be used as basis of quantum dot application development and for application dependent selection of the device technology platform, of manufacturing service providers or of individual quantum dot devices.

Material platform:

— Quantum dot host material (semiconductor system/ material stack, doping, purity);

— Interface and surface quality (roughness, trap density);

— Charge carrier density and mobility.

Fabrication:

— Confinement of the quantum dot (geometrical, interface, trap and/or gate-defined);

— Fabrication technology, depending on semiconductor system;

— Reproducibility in terms of:

- On-wafer deviations in one fabrication batch;
- Several wafer batches for mass production.

Basic quantum dot properties:

— Charge level description at working point(s):
- Definition of working point;
- Threshold voltages and uniformity;
- Charging energies;
- Capacitance matrix elements;
- Tunnel coupling;
- Charge noise;
- Temperature requirements;

— Quantum state description:
- Orbital;
- Spin.

Quantum dot node level description

Interface description:

— For use-ready devices:
- Device geometry (die size, bond pad positions);

— For quantum dot circuit node:
- Definition of geometry node;
- Interconnects;
- Constraints (e.g., cross coupling sensitivity).

Technology, environmental and handling constraints:

— Constraints for further processing, bonding, packaging:
- Temperature/time for heating steps;
- Sensitivity to solvents/acids/gases;
- Protection against electrostatic discharges (ESD);

— Storage conditions;

— Treatments before mounting and cooling in cryostat;

— Cooling procedure (electrical conditioning, cooling rates).

5.7 Timeline for standardization of enabling technologies

A timeline is a very helpful tool to get an overview and to define the necessary steps in the standardization process. Due to different technologies and also varying development stages of the enabling technologies in chapter 5, a generalized approach may not cover all different aspects for each one, but can create a comprehensive framework for this task.

In Figure 10 an estimated timeline is shown in the scheme. It starts at the tipping point (here t = 2023) between R&D prototyping and commercialization. Three main, partly overlapping tasks are identified, Parameters & Testing, Small Series Production and Mass Production.

A full scale mass production is estimated to take place after 3 to 5 years of development.

This framework of a timeline can be used for all enabling technologies with small adaptions in timing and individual standardization activities.

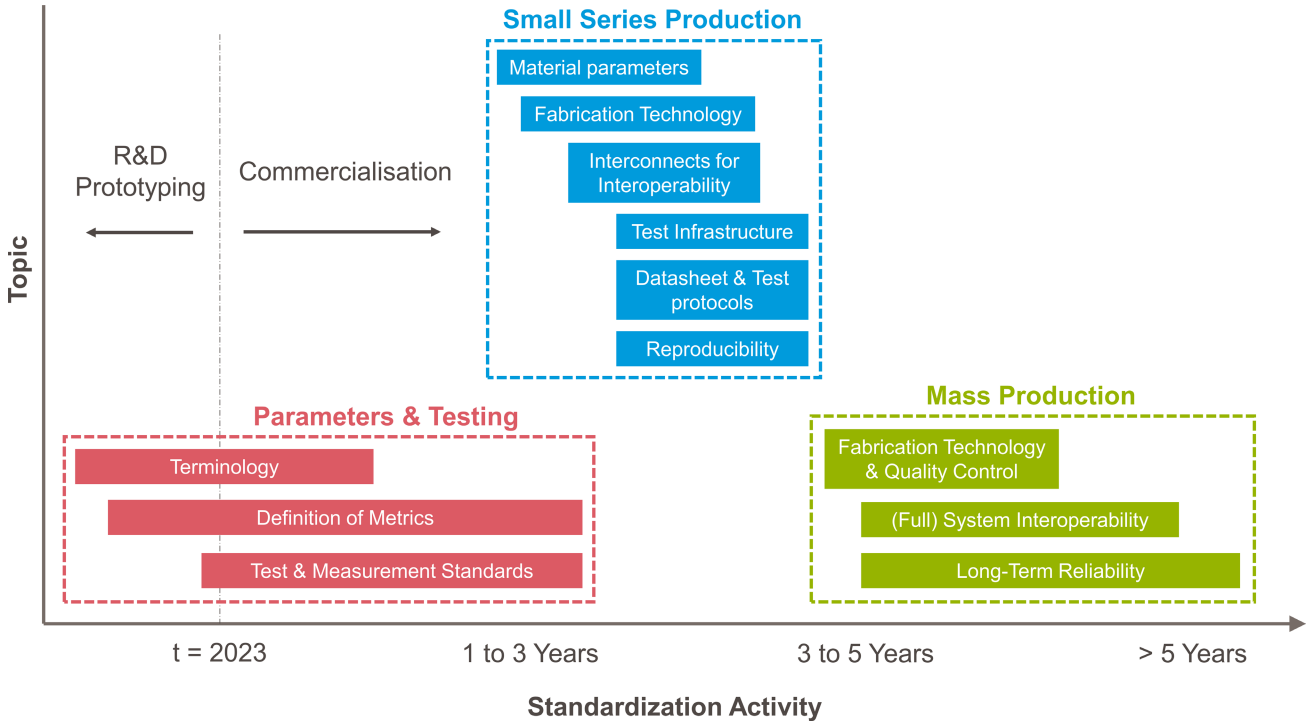


Figure 10 Timeline proposal for standardization activity starting in 2023. This can be an example for a mature enabling technology like ion traps. In contrast, a technology more likely on research level, e.g., single-electron sources based on semiconductor quantum dots, may not require a start before 2025 to 2028.

6 QT components and subsystems

6.1 Introduction

QT components and subsystems are stand-alone and essentially quantum devices that are widely used in different user-oriented QT systems. Thus, QT components and subsystems are universal building blocks that cannot be uniquely assigned to a single QT system class or "pillar" and are mainly aimed to serve QT producers providing a dedicated, highly specialized functionality.

6.2 Single-photon sources

6.2.1 General / Principles / Overview

What is a single-photon source?

A perfect single-photon source is a light source that emits light as single particles or photons, i.e., in which two or more photons are never emitted simultaneously. This distinguishes them from coherent light sources (lasers) and thermal light sources such as incandescent light bulbs. Thus, a single-photon source is a one-photon number state generator.

The proof that a single-photon source is emitting single photons is performed by demonstrating photon anti-bunching [77], i.e., that the time between two successive photons is never less than some minimum value.

Single photon characteristics of a source is proven by means of a Hanbury Brown & Twiss interferometer, which is used to measure the intensity correlation function of a radiation source. The light from the radiation source is split by a beam splitter and imaged onto two SPAD detectors. The signals of the detectors after detection of a photon are recorded by means of correlation electronics, where the signal of a SPAD detector is electrically delayed. This measurement is equivalent to measuring $<I(t)><I(t + \tau)>$, the time average of the intensity at detector 1 and the time average of the intensity delayed by τ at detector 2. By normalization, the intensity correlation function is obtained in form of a histogram of the time delay between two photons and the coincidence count. For a single-photon source, a clear notch around zero delay is observed.

What kind of single-photon sources exist?

Single photon generation occurs when a source produces only one photon within its fluorescence lifetime after being optically or electrically excited. The most widely studied and also most common sources of single photons are single atoms, ions or molecules, Rydberg atoms, diamond colour centres, and quantum dots. These sources are also called deterministic single-photon sources and they produce so-called "photons on demand". In contrast, we speak of "heralded single-photons", when pairs of single photons are generated, e.g., by spontaneous parametric down-conversion, and a photon detected by one detector "heralds" another in corresponding optical path.

It should be noted that an easy-to-implement source that approximates a single-photon source can be realized by attenuating a laser beam; this reduces its intensity and thus the average number of photons per pulse. Since photon statistics follow a Poisson distribution, one can achieve sources with a well-defined probability ratio for the emission of one versus two or more photons. For example, a mean value of $\mu = 0.1$ leads to a probability of 90 % for zero photons, 9 % for one photon, and 1 % for more than one photon. Strictly speaking, however, these are not single-photon sources, since it is not possible to completely eliminate two-photon emission. Nevertheless, these sources can certainly be used for various applications.

True single-photon sources can be realized in several ways [78, 79]:

— Single atoms, ions or molecules: Atoms, ions, and molecules can be individually trapped and stored in cold traps. By means of second order correlation measurements it was found that it is indeed a source of single photons, i.e., a second photon is emitted only after the ion has absorbed another photon.

— Colour centres in solids: Colour centres in solids are isolated defects, e.g., a single ion in a diamond or in a semiconductor with a small band gap. These defects are firmly localized in the solid, and further experimental requirements, such as a low temperature or a strong magnetic field, are not essential. The defects can be of various types, such as foreign atoms, molecules, imperfections, etc. The best-known representative is the nitrogen-vacancy centre (NV centre) in diamond.

— Quantum dots: Semiconductor quantum dots (QD) are atomic structures selectively deposited on a semiconductor substrate. The best known and most widely studied and developed are InGaAs structures on a GaAs substrate. Due to the high technological maturity in creating and processing defined semiconductor structures, single-photon sources based on quantum dots are efficient and offer the possibility to generate indistinguishable photons if appropriately patterned.

— Parametric fluorescence: Parametric fluorescence (SPDC, “spontaneous parametric down conversion”) offers another interesting method for the generation of single photons. Here, a suitable nonlinear crystal is used to convert a short wavelength photon into two long wavelength photons of twice the wavelength. These two photons are correlated, under certain circumstances they can be even indistinguishable and entangled. An advantage of these SPDC sources is that one of the photons can be used (by its detection) to determine at what time the other single photon is present (the so-called "heralded photon").

There is a vast amount of literature on the above single-photon sources, excellent reviews can be found in [78, 79].

Applications of single-photon sources

Single-photon sources have the potential to be used in a wide range of applications. Well-known and widely discussed is their use in quantum key distribution, quantum computing and metrology, the so-called “quantum-enhanced metrology”.

6.2.2 Pre-normative gaps

The following pre-normative gaps were identified:

— Performance of system;

— Definition of metrics.

6.2.3 Standardization needs

For the description of a single-photon source, several parameters are necessary and should be clearly defined. These are:

— Photon rate: the number of photons emitted within a typical time duration, usually within 1 second. This is the product of a variety of factors including:

  - Excitation efficiency;
  - Emitter quantum efficiency;
  - Emitter excited state lifetime;
  - Coupling efficiency of emitted photons to external optics.

  It is important to know the overall photon production efficiency. This can be measured by using a pulsed excitation scheme and ensuring that the emission rate is saturated (excitation efficiency ~ 1). The photon production efficiency of the source is then the detected photon rate divided by the excitation rate. This excitation rate should be significantly longer than the excited state lifetime.

— Wavelength and spectrum: Single-photon sources do not emit photons at one specific wavelength, so the spectrum of their emission should be measured in a traceable manner. As wavelength, either the peak wavelength λ_{peak}, the mean wavelength λ_{mean} or the median wavelength λ_{median} should be stated;

— Bandwidth: the bandwidth of the emission of a single-photon source is determined by the full-width at half-maximum of the emission spectrum;

— Stability: In general, the stability describes the fluctuations of a single-photon source with respect to several parameters, e.g., photon rate, polarization etc.;

— Photon statistics: An ideal single-photon source emits exactly one photon per time interval. Other, quasi single-photon sources emit either zero or more than one photon per time interval. Possible ways to describe the photon statistics is to use correlation functions, second order and higher;

— Spectral diffusion: The spectral diffusion describes the temporal change in the emission spectrum of the single-photon source;

— Coherence time: The coherence time can be considered as the dephasing time of the excited state, and, from the quantum optics point of view, as the duration of the wave train that is associated with the emitted photon;

— Indistinguishability (Purity): Indistinguishability describes, how equal two photons, emitted from the same source are. Typically, this is measured by the Hong-Ou-Mandel experiment, the descriptive parameter is the visibility;

— Polarization.

6.3 Entangled-photon sources

6.3.1 General / Principles / Overview

Entanglement in quantum optics is a physical phenomenon that occurs when photons are created or are interacting with each other, so that the quantum state of each photon in the group cannot be described independently of the state of the other photons. This is true even if the distance between the particles becomes macroscopically large. Entanglement is not present in classical mechanics; it is a special feature of quantum mechanics.

NOTE The term “classical” is discussed in some detail in section 2.2.

What are entangled-photon sources?

An entangled photon source is a source, which produces entangled photons as described above.

What kind of entangled-photon sources exist?

Entangled photons can be generated by parametric fluorescence (parametric down-conversion) in non-linear optical crystals. In this process, an entangled pair of photons, each with half the energy, is generated from a photon of higher energy in the crystal. The directions in which these two photons are emitted are strongly correlated with each other and with the direction of the emitted photon, so that the entangled photons produced in this way can be used efficiently in experiments.

Certain types of atoms can be excited by a laser in such a way that they also emit a pair of polarization-entangled photons when they return to their ground state. However, these are emitted almost uncorrelated in any spatial direction, so they cannot be used very efficiently.

Further methods are using indistinguishable single photons, which are entangled, e.g., at a beam splitter, four-wave mixing or two photon emission from a quantum dot.

6.3.2 Pre-normative gaps

The following aspects require standards:

— Performance of system;

— Definition of metrics and vocabulary.

6.3.3 Standardization needs

For the description of an entangled-photon source, several parameters are necessary and should be clearly defined. These are:

— Definition of different measures of entanglement;

— Entanglement fidelity;

— Indistinguishability;

— Photon pair rate.

6.4 Single-photon detectors

6.4.1 General / Principles / Overview

What are single-photon detectors?

A single-photon detector is able to detect light at the single-photon level. It may be classified as photon-number-resolving or non-photon-number resolving. For the first type, the output signal is proportional to the number of photons absorbed within its response time. The second type produces a single output pulse regardless of the number of incident photons simultaneously 'detected' within its response time. This type of detector is widely commercialized, whereas the photon-number-resolving detectors are still very much research laboratory devices. The overall detection efficiency is the result of the absorption efficiency and the conversion efficiency of the absorbed photon(s) into a measurable output electrical signal.

What kind of single-photon detectors exist?

Different types of single-photon detectors have been developed and used in different kinds of applications [78, 79]. In the following, these types will be briefly presented and discussed with respect to their general characteristics as well as their advantages and disadvantages. Comprehensive overviews of the different detector types including a detailed description of their operation can be found in [78, 79].

Detectors can be operated in either gated or free-running (continuously-gated) mode. Gated mode means that the detector is only single-photon sensitive for a finite time interval ('gate'), while free-running means that it is continuously single-photon sensitive, excluding the time required for it to reset after a detection. Gated mode is usually used when the dark count probability (see below) of the device is relatively high.

Avalanche photodiode detector (APD) and single-photon avalanche photodiode detector (SPAD): An APD is a highly sensitive semiconductor photodiode detector that exploits the photoelectric effect to convert light into electricity. From a functional point of view, an APD can be considered as the semiconductor analog to the photomultiplier. APD arrays are now also commercially available. The principle of operation is basically as follows: By applying a high reverse bias voltage, APDs exhibit an internal current amplification effect due to impact ionization (the so-called "avalanche effect"). Avalanche photodiodes are therefore more sensitive than other semiconductor photodiodes. When very high gain is required (up to 10^6), the detectors are operated with a reverse voltage above the breakdown voltage of a typical APD. In this case, the signal current of the photodetector must be limited and quickly reduced. Therefore, active and passive current shutdown techniques are used for this purpose. These special APDs, so called SPADs are also called "Geiger mode detectors". This mode of operation is particularly useful for single-photon detection, provided that the dark count rate and the so-called "after-pulsing probabilities" are sufficiently low. In principle, any semiconductor material can be used for a SPAD detector. The following have been developed so far:

— Silicon: Silicon detects photons in the near ultraviolet, visible, and near infrared spectral regions (approximately 300 nm to 1000 nm) with low noise, low dark count rate, and low after-pulsing. Si-SPADs are the most advanced, sensitive and reliable detectors and are available in different quality levels (mainly in terms of detection efficiency and dark count rate).

— Germanium (Ge) detects in the infrared spectral range up to a wavelength of 1.7 µm but has a high detector noise.

— InGaAs detects in the wavelength range between 0.9 µm and about 1.7 µm and is thus suitable for high-speed optical fibre telecommunication. It is typically used as a heterostructure diode, with InP as the substrate and multiplication layer.

— Other SPADs have been developed for ultraviolet (gallium nitride) and mid-infrared (HgCdTe) spectral regions.

A special form of Si-SPADs are the so-called silicon photomultipliers (SiPM). A SiPM consists of an array of several avalanche photodiodes on a common silicon substrate, which are operated in Geiger mode. This makes it possible in principle to detect single photons as well as many photons simultaneously. This is achieved by connecting many (up to 1000) small APD cells (approximately 10 µm to 100 µm) in parallel.

Transition Edge Sensor (TES) Detector: A transition edge sensor (TES) is a cryogenic energy sensor or cryogenic particle detector that exploits the strongly temperature-dependent resistance of the superconducting phase transition.

Superconducting Nanowire Single-Photon Detector (SNSPD): This detector is based on a current-biased superconducting nanowire (or better "nanostripe"). It is currently the fastest single-photon detector for photon counting. The nanowire is cooled well below its critical superconducting temperature and biased with a DC current that is close to the critical current of the nanowire. A photon incident on the nanowire disrupts the Cooper pairs and reduces the local critical current below that of the bias current. This leads to the formation of a localized non-superconducting region or hotspot with a finite electrical resistance, which can be detected. The SNSPD does not have the intrinsic energy or photon number resolution of a TES but is significantly faster than conventional TES detectors and operates at higher temperatures. Several companies are commercializing complete single-photon detection systems based on superconducting nanowires.

Applications of single-photon detectors

The applications of single-photon detectors are manifold. Medicine, biology, astrophysics, but also emerging application fields such as quantum cryptography and quantum computing and, last but not least, scientific research in the field of experimental quantum optics and quantum physics. In summary, single-photon detectors are becoming increasingly important in areas where weak photon fluxes need to be measured that are not measurable, or only poorly measurable, with conventional detectors.

6.4.2 Standardization needs

Regarding the metrological characterization and the standardization needs of single-photon detectors, there are quite few normative documents available so far, see e.g., the guidelines of the European Telecommunications Standards Institute listed above. In the ETSI standard GS QKD 011 “Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems” (2016-05), prepared among others with the participation of various national metrology institutes by the “Industry Specification Group (ISG) on Quantum Key Distribution (QKD)”, the parameters for the description of components for quantum communication were defined, see following list. The document is focused on gated detectors and describes in detail the measurement procedures for the following parameters:

— Detection probability: The probability that a photon incident at the optical input is detected within a detection gate;

— Detector gate repetition rate: The repetition rate of the time intervals in which a detector has single photon sensitivity;

— Dark count rate probability: For a gated detector, this is the probability that a detector will register a detection event in a gate of specified duration when no optical illumination is present. For a free-

running detector, this is the probability that a detector will register a detection event in 1 s or other specified time interval when no optical illumination is present;

— After-pulse probability: the probability that a detector will register a false detection event in the absence of irradiation, assuming that a true photon detection event is present in the preceding detection gate;

— Dead time: The time interval after a detection event during which the detector is unable to provide an output signal;

— Recovery time: The smallest period of time after which the detection efficiency is independent of the previous photon detection history;

— Jitter: The uncertainty in determining the arrival time of a photon at the optical input;

— Spectral sensitivity: The photon detection efficiency as a function of the wavelength of the incident photons;

— Temporal sensitivity: The photon detection efficiency as a function of the arrival time of the incident photons with respect to the gate;

— Back flash emission: the secondary photon emission that arises from the avalanche of charge carriers that occurs during the detection of a photon.

ETSI group report "ETSI GR QKD 003 V2.1.1 (2018-03) Quantum Key Distribution (QKD); Components and Internal Interfaces" notes the developing importance of solid-state and superconducting free-running detectors for telecom wavelengths; these types of detector are also commonplace for the visible and near-infrared spectral regions. The IEC 61788-22 series defines international standards for superconductor electronic devices. IEC 61788-22-3, currently in the committee draft stage, is a standard for the measurement of dark count rate of SNSPDs, referred to in that document as superconducting strip photon detectors. Test standards addressing free-running detectors – solid-state and superconducting – will be required.

6.5 Single-electron sources

6.5.1 General description and overview

A single-electron source emits a single electron within one cycle of its operation. This definition is generally also extended to sources emitting a well-defined number n of electrons in one cycle. For an ideal single-electron source this number is the same in every cycle of its operation.

Different realizations of single-electron sources have been pursued [80]. Most of these rely on the same basic principle: the charging energy necessary when adding an extra electron to a small, confined space is used to select the target electron number n. Realization of this type of single-electron sources are most notably:

a) Multiple in series connected metal or semiconductor single electron transistors with fixed tunnelling barriers and operated by a sequence of control gate voltages applied sequentially to the single electron transistors;

b) Surface acoustic wave operated single-electron sources where the surface acoustic wave generates a moving confinement potential (quantum dot) in a piezoelectric semiconductor, which is used to select and transfer a single electron;

c) Hybrid superconductor-normal-metal turnstiles using both the charging and the superconductor gap;

d) Tuneable barrier single-electron sources in which the coupling of a lithographically defined quantum dot is modulated between strong coupling to a contact and strong isolation to select, transfer and emit n single electron per cycle.

Other recently investigated schemes are:

e) Superconductor based quantum phase slip devices, relying on a kind of dual to the Josephson effect;

f) Optical pumped exciton separation, relying on the self-limited generation and separation of single excitons in a quantum dot.

One common application of all these schemes is to use the transfer of single quantized charge for the generation of a quantized current, e.g., for the direct first principal realization of the unit ampere in the new SI. The current is given by $I = n \times e \times f$ with e the elementary charge, one of the fundamental constants fixed in the new SI system, f the periodic operation frequency and n the number of electrons transferred in each cycle.

Semiconductor quantum dot based single-electron sources [b) and d) in the above list] in high-quality semiconductors can emit quasi-free ballistic single-electron wave packets. It has been proposed to use these for quantum state metrology, for electro-magnetic sensing or for quantum state transfer. For example, the on-demand generation of single electrons and the precise control of their emission time enables picosecond time-resolution in signal processing applications. The realization of such schemes is presently an active research topic.

6.5.2 Pre-normative gaps

The following pre-normative gaps were identified:

— Definition of performance metrics;

— Definition of characterization procedures;

— Definition of parameters for description of system level and handling requirements for applications.

6.5.3 Standardization needs

Parameters describing required and allowed operation conditions:

— Device temperature constraints;
  - Heat load during operation, thermal resistance;

— Magnetic field (required/allowed);

— Voltage bias requirements and tolerance (including AC noise tolerance);

— Drive signal requirements;

— Constraints for interoperability;

— Other environmental constraints (RF noise/signal tolerance / EMF considerations).

Charge transfer metrics:

— Real operation frequency range;

— Effective charge transfer frequency (n×f);

— Accuracy of charge transfer:
  - Traceability to SI-units;
  - Different operation parameters (e.g., frequency);
  - Long-term stability.

Single-electron wave packet metrics (for applications of quasi-free single electron wave packets):

— Wave packet energy and energy tuning range;

— Wave packet description (level of detail depending on target application):
  - Width of distribution characterizing emission in time and energy;

- Energy-time distribution function;
- Energy-time correlation function;
- Indistinguishability between independently generated wave packets (quantum state purity if applicable);
- Tunability of wave packet properties;

— Multi-electron emission properties (if applicable) in addition to individual electron wave packet description:

- Energy/time correlations;
- Spin correlations.

System and handling requirements:

— Requirements for electrical control lines;

— Device handling considerations (storage conditions, ESD);

— Cooldown procedure (cooldown rate, control line biasing requirements);

— Aging of performance metrics.

6.6 Quantum random number generators

6.6.1 General

An additional subsystem that plays a role in many scenarios is the quantum random number generator (Quantum RNG, QRNG): Its purpose is to generate random bit sequences. It can be used for many practical purposes but is typically used as a subsystem of QKD systems: to generate the random sequences required in QKD systems.

6.6.2 Projected standards

S: Quantum Random number generators

S: Existing standards for RNGs which can also be relevant to QRNGs

TR: Statistical analysis of numerical output – this refers to various test suites such as TESTU01 etc.

K: Device-dependent QRNGs

K: Device-independent QRNGs

K: calibration procedures, characterization, stability, side-channels, attacks, countermeasures, modelling, entropy estimation, randomness extraction, 'health tests'

"S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e., hints towards potential standards, or indications of applicability, etc.

6.6.3 Considerations

Maybe QRNGs should be stated as a subset of RNGs, e.g., following the AIS terminology.

6.7 Quantum memories

6.7.1 General

Future quantum networks are expected to provide the basis for large-scale quantum communication and distributed quantum computing. These networks will require quantum entanglement to be shared between distant quantum memories.

Quantum memories are prospective and essential quantum technology sub-systems in quantum information processing that aim to "store" and reproduce on demand quantum states, received from any quantum process, including quantum algorithms. Therefore, in quantum computing, quantum memories can be used e.g., as identity quantum gates [81], while in quantum communication they will be acting as essential components of quantum repeaters [82, 83].

Important characteristics of quantum memories are the time of storage and fidelity of the stored (reproduced) state with respect to the original one.

6.7.2 Projected standards

It is expected that standards are developed that specify the mentioned time and fidelity of storage as well as the entanglement fidelity

6.7.3 Gaps

No standards are available.

7 Quantum communication systems

7.1 Overview

Quantum communication enhance classical communication or enable new possibilities through the transmission/distribution of quantum states. To transmit quantum states it is not only necessary to have the ability to create and manipulate quantum states, but also to provide quantum channels to distribute these states. Thus, the distinct requirement of quantum communication compared to other quantum technology areas is the ability to create, maintain and put to use quantum channels. Simultaneously all types of quantum communication require specific quantum information processing protocols.

NOTE The term "classical" is discussed in some detail in section 2.2.

A quantum channel can be used to directly transmit the quantum states of interest or to create quantum correlations between distant quantum communication systems. The latter quantum correlations can be used to transmit quantum states or to perform a range of operations that can yield classical correlations that cannot be obtained by any classical physical process.

Physical media capable to support quantum channels include optical fibre (see section 5.1 "Quantum channels"), free space, superconducting wires, waveguides. It is to be noted that, since quantum states have to be manipulated and transmitted in quantum communication systems, these are extremely sensitive to imperfections, noise or physical impairments in the devices and the quantum channel (e.g., losses in optical fibre). Also, since (unknown) quantum states cannot be copied, amplification cannot be used. Given losses along the quantum channel, imperfect coupling or detectors, this imposes strict limits on the maximum range of direct quantum signal transmission and other means (quantum repeaters) will have to be used, once they become practically available, to establish long range quantum communication.

To perform the quantum state manipulation and transmission required by a quantum communication system, a set of basic components is needed:

— Basic components or subsystems.

The production of quantum communication systems requires the development of a complete set of components. This is referred to as supply chain in the Strategic Research Agenda of the Quantum Flagship. The supply chain for quantum communication includes at least the following items:

— Sources of quantum states (to be sent along a quantum channel);

— Means for quantum state preparation;

— Quantum memories and their interfaces;

— Physical realizations of quantum channels (optical fibres, waveguides…);

— Detectors of quantum systems (receiving the input of a quantum channel);

— Signal processing subsystems;

— Post-processing subsystems (for key distillation or teleportation).

NOTE Several of these subsystems are generic and may be used in other fields of quantum technologies, beyond quantum communication. See also the respective sections in chapter 6 "QT components and subsystems".

Moreover, although in principle not relevant for standardization, education and training has been recognized as a key issue for quantum technologies and in this sense also specifically for the development of quantum communication systems.

The basic components and subsystems can be integrated to functional QT systems:

— Quantum communication systems (built out of the first level components/ subsystems to serve a specific purpose required by a use-case (see chapter 11)).

With the basic components and subsystems identified, quantum communication systems can be built. These systems will address the two main classes of applications that have been identified in the Strategic Research Agenda of the Quantum Flagship: Quantum security networks and quantum information networks (see chapter 3 and chapter 10). Quantum security aims at guaranteeing confidentiality and authenticity of digital data (possibly together with other technologies) potentially against arbitrary attackers, even with quantum computers at their disposal.

— Fundamental quantum communication systems: Building on top of the basic components/ subsystems and having access to a quantum channel, several high level quantum communication systems can be built. These include:

  - Quantum Key Distribution (QKD) systems (or modules as defined by ETSI ISG QKD): To create a secret key shared between two users at both ends of a quantum channel with security independent of assumptions on a potential attacker. Two QKD systems connected by a quantum channel are known as a QKD link. Current QKD systems are limited to the use of direct transmission channels and thus have limited reach. Unlimited reach of current QKD links can be achieved through their concatenation, which requires an additional trust assumption on the intermediate nodes (trusted-node model);
  - Quantum repeaters (section 7.12): Allowing the establishment of quantum correlations end-to-end and with unlimited reach and thus end-to-end quantum channels. This enables quantum communication without restrictions for all quantum communication protocols, including quantum state transfer and QKD protocols.

Typically quantum communication systems utilize many QT subsystems, such as quantum channels (section 5.1), quantum random number generators (section 6.6) and for a significant classes of quantum communication systems, single-photon sources and their approximations (section 6.2), single-photon detectors (section 6.4), coherent quantum receivers and, in some cases entangled-photon sources (section 6.3).

7.2 The relevance of quantum-safe cryptography

Quantum-Safe Cryptography (QSC) refers to cryptographic algorithms, both symmetric and asymmetric (public-key cryptography) that are thought to be secure against a cryptanalytic attack by a quantum computer [17, 84, 85] . The technology is also referred to as quantum-proof, post-quantum or quantum-resistant.

The Terms of Reference [86] of the CEN/CENELEC FGQT includes the following statement: “as quantum technologies have different areas of application, the FGQT will develop a roadmap for potential standardization of issues relevant to QT”. This raises the question whether or how QSC is relevant to quantum technologies.

QSC itself is not a quantum technology. It does not rely on any quantum-mechanical effects such as superposition and entanglement. However, the same is true for the control subsystem for quantum computers, and many subsystems of quantum communication systems. Still, these are relevant for quantum technologies, as the latter pose significantly different requirements than readily available technical solutions. So no direct quantum-based functionality does not automatically imply irrelevance for quantum technologies.

One way of looking at QSC is as a complementary [87], supporting technology for Quantum Key Distribution (QKD) networks and other types of quantum-communication networks, e.g., entanglement distribution networks. Most or all quantum-communication networks require a supporting classical digital communication network running in parallel. This supporting network may provide protocol support, synchronization support and other. Given potential high-security applications for quantum-communication networks, it makes sense to put high security requirements on the supporting network as well. QSC is one of the technologies that may be applied for this purpose, e.g., supporting the mutual authentication and the privacy of the pre-shared secret of communicating parties.

Another way of looking at QSC is as a partially competing [88] technology to QKD. Both technologies aim to secure communication channels. QSC relies on mathematical primitives, whereas QKD relies on physical primitives. The two technologies have different cost structures and offer different types and levels of assurance. Both technologies have active standards development, associated product development and pilot implementations. This suggests that there are relevant markets for both technologies, and there may be significant differences between these markets. Note also that from a purely practical point of view the combination of algorithmic and physical approaches "increases security", as indeed it pushes significantly up the needed resources bar for potential attackers.

Note that many of the statements above have their controversy. People may disagree to qualifying QSC as a potential complementary supporting technology for QKD. People may disagree about the value of the one type of security primitive compared to the other: mathematical versus physical. People may disagree about the potential market sizes of the different technologies.

These controversies could also be seen as standards' needs. For example, the potential complementarity between QSC and QKD could be explored in a Technical Report. The arguments pro/con QSC and QKD could be explored in another Technical Report, providing consensus-based agree-to-disagree views. Performing such explorations in a consensus-driven SDO context, like CEN/CENELEC, has referential value over similar analyses in blogs and peer-reviewed papers.

7.3 Organization of quantum-communication roadmap

The quantum-communication/quantum-key-distribution roadmap presented in sections 7.3 to 7.12 of the present document is expanding upon a roadmap document [89] published by the OpenQKD project of the Horizon 2020 research and innovation program.

Based on the categorization scheme of this publication an initial partitioning for quantum communication (QC) and quantum key distribution (QKD) standards was developed by members of the FGQT group, and sent out with a request for comments on the FGQT mailing list. The received comments were fed back into the initial scheme, leading to the first version of the QC/QKD roadmap.

The current scheme involves 8 categories of quantum technologies in the field of QC/QKD that are deemed to be reasonable for mapping out the entire field of potential standards — as a basis for further consideration and derivation of strategic road mapping information:

— QKD protocols;

— QKD transmitter modules;

— QKD receiver modules;

— Generic QKD components;

— Single link QKD;

— Basic standards related to QKD and Quantum Communication;

— Security evaluation/certification of Quantum Key Distribution;

— Quantum repeaters.

The section 7.11 "Security evaluation/certification of quantum key distribution" has a unique significance in the scheme as it contains the "central" standards used for security evaluation and certification according to EN ISO 15408 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model" [90][5] (Common Criteria (CC)) of QKD products (i.e., of QKD components, links, probably also networks)—while related background documents for security evaluation and certification can be found in other sections.

5 See also common criteria publications [109]

Standard documents in this section are:

- Catalogues of specific security functional requirements (SFRs);
- Test and evaluation methods;
- Sample Protection Profiles (PP), i.e., security specifications according to CC;
- Catalogues of attack methods; and
- Specific information on background documents, potentially also from the other sections of the QC/QKD roadmap, necessary and essential for the security specification of QKD products.

Each category has four sub-sections:

— **Projected standards**

This is a list of (existing or hypothetical) standards and other related documents considered useful in that category. This list was elaborated through expert interviews (we asked for a wish list) and supports the bootstrapping process of the QC roadmap. This sub-section shall be removed in later versions of the roadmap.

"S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e., hints towards potential standards, or indications of applicability, etc.

— **Existing standards**

Existing standards in that sub-category at the point of time given in the "Organization of quantum-communication roadmap" section above.

— **Considerations**

Specific considerations and notes, concerning the state of standardization in the particular category; any other considerations and comments of interest;

— **Gaps**

Results of a gap analysis; missing standards; any strategic information derived from the expertise of the experts involved in the particular sub-category

7.4 Types of standards

We are following here the approach of the OpenQKD project, which is mapping EN 45020 [91] common types of standards to a particular grid of standards types, more suitable and better applicable to the QC/QKD field.

EN 45020 defines some common types of standards as shown in Table 4. The following terms and definitions are not intended to provide a systematic classification or comprehensive list of possible types of standards. They indicate some common types only. These are not mutually exclusive; for instance, a particular product standard may also be regarded as a testing standard if it provides test methods for characteristics of the product in question.

In the following table the EN 45020 types of standards are mapped to a grid, more suitable to the field of QC/QKD. The abbreviations (2nd column) are subsequently used in the "Existing standards" subsections. This mapping is an adaptation of a similar mapping from the OpenQKD roadmap [89].

Table 4 Types of standards as defined in EN 45020

Type of standards	Definition
Basic standard	Wide-ranging coverage or contains general provisions for one particular field
Terminology standard	Concerned with terms, accompanied by their definitions etc.
Testing standard	Concerned with test methods, sometimes supplemented with other provisions related to testing
Product standard	Specifies requirements to be fulfilled by product or group of products, to establish its fitness of purpose
Process standard	Specifies requirements to be fulfilled by a process, to establish its fitness of purpose
Service standard	Specifies requirements to be fulfilled by a service, to establish its fitness of purpose
Interface standard	Specifies requirements concerned with the compatibility of products and systems at their point of connection
Standard on data to be provided	Contains a list of characteristics for which values or other data are to be stated for specifying the product, process or service

Table 5 QKD standard categories mapped to EN45020 standard types

			Type of standards								
			Basic standard	Terminology standard	Testing standard	Product standard	Process standard	Service standard	Interface standard	Standard on data to be provided	Informative
QKD standard categories	**SG**	**Security evaluation: generic standards**	**X**		**X**	**X**					
	SM	**Security evaluation: evaluation methodology and testing standards**	**X**		**X**	**X**					
	SB	**Security evaluation: background documents**	**X**		**X**	**X**	**X**	**X**	**X**	**X**	
	ME	Metrology standards (Testing, calibration, characterization, stability, attacks, countermeasures)		**X**	**X**				**X**		**X**
	KM	Key management and key delivery Interface standards					**X**		**X**		
	QN	QKD Network standards	**X**					**X**	**X**		**X**
	SA	Satellite modules and networks	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
	WP	White papers, technical reports and supporting documentation									**X**
	VC	Vocabulary and general standards	**X**	**X**	**X**						**X**
	OT	Other standards									**X**

7.5 QKD protocols

NOTE We note here that as QKD protocols are to be used in the security domain, they need to be proven secure (acceptance by the scientific community) and consequently endorsed by public regulatory bodies.

7.5.1 Projected standards

S: BB84 (Bennet Brassard 1984 quantum key distribution scheme) and decoy state BB84

S: CV (Continuous-Variable) Gaussian and discrete modulation

S: Distributed phase reference protocols, like DPS (Differential Phase Shift), COW (Coherent One Way), and Round Robin

S: Measurement device independent and device independent protocols

S: Twin-field QKD systems

K (for all S): protocol definition, security proofs and analysis, pre- and post-processing

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e., hints towards potential standards, or indications of applicability, etc.

7.5.2 Existing (or developing) standards

SDO	Document number	Document title	Version	publ. date
ETSI	GS QKD 005	Quantum Key Distribution (QKD); Security Proofs **(SG)** (update in preparation, V1.1.1 published 2010-12)	V1.4.2	*Stable draft (2022-06-17)*
ETSI	GR QKD 019	Quantum Key Distribution (QKD); Design of QKD interfaces with Authentication **(SG, SB)**	V0.0.92	*Early draft (2022-06-20)*

7.5.3 Considerations

Also considered should be (not in the projected standards list): single-link BB84 (with true single-photon sources, i.e., without the need of decoy states).

Different modulation schemes like polarization, phase, and variants like time-bin need to be considered including consequences, like the necessity of phase-randomization and differences in detection schemes.

Additional standards for DPS and COW (having similar realizations, but different security proofs) need to be considered.

CV Discrete modulation: Here we can think of protocols exploiting constellations of coherent states instead of the Gaussian modulation: this could be relevant considering the current optical communication based on this kind of modulation.

In addition to the quantum steps and variations in the protocol it is also important that steps in the post processing protocol are treated correctly.

7.5.4 Gaps

An important question remains how best to support the acceptance of particular QKD protocols for security certification. Standards developing organizations or groups, like e.g., the ETSI ISG-QKD, can potentially play an important role but peer review in academic publications, as well the involvement of other communities, including national agencies and prospective users etc., are also likely to be important.

The rigorous influence of finite size effects especially at highly fluctuating channels is still under research.

The security parameter "epsilon" is currently treated as an upper bound specified in a data sheet. An adaptation to match security requirements on request as well as a real-time evaluation to estimate its real value could be required from applications with high security levels.

Currently, several research institutions, as well as QKD system producers are known to work on a formalization of security proofs of QKD protocols. The way to address it will likely be to construct a consecutive chain of formal arguments. To our knowledge, no published (or publishable) information on this subject is currently available.

7.6 QKD transmitter modules

7.6.1 Projected standards

S: DV (Discrete-Variable) QKD transmitter module (fibre/free space) with different degree of qubit modulation

S: CV QKD transmitter module (fibre/free space)

S: Entanglement sources

K (for all S): calibration procedures, characterization, stability, attacks, countermeasures

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e. hints towards potential standards, or indications of applicability, etc."

7.6.2 Existing standards

SDO	Document number	Document title	Version	publ. date
ETSI	GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems **(ME, SB)**	V1.1.1	*2016-05*
ETSI	GS QKD 013	Quantum Key Distribution (QKD); Characterisation of optical output of QKD transmitter modules **(ME, SB)**	V0.1.0	*Stable draft (2021-09-20)*
ISO/IEC	23837-1	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements **(SG)**		*is being finalized, publication imminent*
ISO/IEC	23837-2	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 2: test and evaluation methods **(SM)**		*is being finalized, publication imminent*

7.6.3 Considerations

While calibration refers to the initial setting up of the device, characterization refers to the measurement of parameters of the output photon states.

ETSI GS QKD 011 "(…) gives specifications and procedures for the characterization of optical components for use in QKD systems. Examples of specific tests and procedures for performing such tests are given.

Due to their importance in the security of a QKD system, particular attention is given to active optical components such as optical sources and single-photon detectors." (p. 13)

ETSI GS QKD 013 "(…) defines procedures for characterizing specific properties of complete QKD transmitter modules. These procedures are limited to characterizing the signals emitted by the transmitter under operational conditions." (p. 13)

ISO/IEC 23837 (all parts): 1st DIS (draft international standards) was approved at the Oct 2022 WG3 meeting of ISO/IEC JTC 1/SC 27. ISO/IEC 23837 (all parts) specifies security functional and assurance requirements also for QKD transmitter modules (also called "sources"), as well as receiver modules ("detectors").

7.6.4 Gaps

There are technologies which are not (yet) covered in the existing standards. For these, additional standards may be required (cf. section 6.4 "Single-photon detectors").

Side channels regarding qubit generation, like influence of independent parameters (e.g., wavelength, chirp) from qubit values need to be considered.

These standards should be referenced in QKD protocol (security proof) standards. The suitability and completeness of the standards for their intended use needs to be assessed.

7.7 QKD receiver modules

7.7.1 Projected standards

S: DV QKD receiver module (fibre/free space)

S: Measurement device independent receiver modules (fibre/free space)

S: CV QKD (coherent) receiver module (fibre/free space)

K (for all S): calibration procedures, characterization, stability, attacks, countermeasures

S: Hybrid DV-CV QKD receiver module

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e. hints towards potential standards, or indications of applicability, etc."

7.7.2 Existing standards

SDO	Document number	Document title	Version	publ. date
ETSI	GS QKD 011	Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems **(ME, SB)**	V1.1.1	*2016-05*
ISO/IEC	23837-1	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements **(SG)**		*is being finalized, publication imminent*
ISO/IEC	23837-2	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 2: test and evaluation methods **(SM)**		*is being finalized, publication imminent*

7.7.3 Considerations

ISO/IEC 23837 (all parts): 1st DIS (draft international standards) was approved at the Oct. 2022 WG3 meeting of ISO/IEC JTC 1/SC 27. ISO/IEC 23837 (all parts) specifies security functional and assurance requirements also for QKD transmitter modules (also called "sources"), as well as receiver modules ("detectors").

The underwater realm has specific and somehow mandatory requirements that are rather different with respect to those concerning the free space or terrestrial ones, such as the positioning of the parties, the extremely noisy environment that may drastically change also with the depth, the eventual integration with the acoustic technology usually employed in current underwater technology, the needed different wavelength, and thus detectors, that should be used in optical underwater communication to avoid water absorption.

Detector parameters of real systems deviate from their ideal models. For DV-QKD, the influence of the overall QKD system (measurements from lately recovered detectors compared to detectors without recent photon detection) may cause dependencies between measured values. For CV-QKD, the calibration process to normalize shot noise in order to retrieve excess noise is critical for trusted-detector models as well as for CV-QKD systems operating in the high loss regime.

7.7.4 Gaps

The gaps are similar as for the QKD transmitter modules.

Detector side channels enabled previous quantum hacking attacks. The calibration of detectors at operation environments (e.g., correct temperature for relevant environments) as well as the continuous monitoring of the correct behaviour to properly detect incoming light must be ensured after device fabrication, as well as over the entirely lifetime of the system.

7.8 Generic QKD components

7.8.1 Projected standards

S: Generic QKD components; the objective here is to fix the specific requirements on QT subsystems that are specifically required for QKD purposes

K: properties, measurement, characterization, interfaces, COTS telecom components, components for different QKD protocols, electronics

S: QKD integrated optics

K: check existing [test] standards

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e. hints towards potential standards, or indications of applicability, etc."

7.8.2 Existing standards

SDO	Document number	Document title	Version	publ. date
ETSI	GR QKD 003	Quantum Key Distribution (QKD); Components and Internal Interfaces **(ME, SB)**	V2.1.1	*2018-03*

7.8.3 Considerations

ETSI GR QKD 003 identifies common components for several QKD system types.

7.8.4 Gaps

The ETSI GR QKD 003 standard identifies relevant (and partially common) components of different QKD system types (generic systems, weak laser pulse, entanglement-based, continuous-variable based systems). This is meant as "preparatory action" (p. 6) for further "(…) definition of properties of components and internal interfaces of QKD Systems." Here, respective standardization projects need to be started, and priorities attached to these activities (coordination).

The influence of the quantum channel, like types of fibres (SMF, hollow-core fibres, multi-core fibres, few-mode fibres) and their properties (e.g., dispersion), as well as deficiencies of optical telescopes might need to be considered here.

7.9 Single link QKD

7.9.1 Projected standards

S: QKD key management and key interfaces

S: QKD control and system management interface

K: issue commands like start, stop, get, set, adjust wavelength

S: Digital channel authentication protocols

S: Underwater QKD

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e. hints towards potential standards, or indications of applicability, etc."

7.9.2 Existing standards

SDO	Document number	Document title	Version	publ. date
ETSI	GS QKD 004	Quantum Key Distribution (QKD); Application Interface **(KM)**	V2.1.1	*2020-08*
ETSI	GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API **(KM)**	V1.1.1	*2019-02*
ETSI	GS QKD 015	Quantum Key Distribution (QKD); Quantum Key Distribution control interface for software defined Networks **(KM, QN)**	V2.1.1	*2022-04*
ETSI	GS QKD-020	Quantum Key Distribution (QKD); Interoperable KMS API **(KM, QN)**	V0.0.1	*Early draft (2021-12-06)*
ETSI	GR QSC 001	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework **(QN, SB)**	V1.1.1	*2016-07*
ETSI	GS QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios **(QN, SB)**	V1.1.1	*2017-02*
IEEE	P1913	Software-Defined Quantum Communication **(QN, SB)**		*Drafting*

7.9.3 Considerations

Existing standards cover the interfacing with QKD modules, on the one hand, to hand over keys (key delivery API), and on the other hand, to manage the QKD module, a QKD link, or even an entire QKD network.

7.9.4 Gaps

Further attention should be directed towards the harmonization of key handover and QKD module management interfaces. Check if there are already redundant interfaces standards.

In ETSI GS QKD-020 two QKD manufacturers are driving the revision of an interoperable KMS API.

7.10 Basic standards related to QKD and quantum communication

7.10.1 Projected standards

S: Vocabulary and ontology

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e. hints towards potential standards, or indications of applicability, etc."

7.10.2 Existing standards

SDO	Document number	Document title	Version	publ. date
ETSI	GR QKD 007	Quantum Key Distribution (QKD); Vocabulary **(VC)** (update in preparation, V1.1.1 published 2018-12)	V1.3.2	Early draft (2021-11-18)
ETSI	GS QKD 002	Quantum Key Distribution (QKD); Use Cases **(OT)**	V1.1.1	2010-06

7.10.3 Considerations

Terminology problems, i.e., no universally accepted dictionary for QKD related terms, which have persisted long time in QKD seem to gradually have been reduced and eliminated. Most of the published standards have their terminology sections, and a consistent effort is being undertaken to use harmonized terminology.

7.11 Security evaluation/certification of quantum key distribution

Security evaluation and consequently certification of QKD modules and products is an indispensable prerequisite for their accreditation and qualified deployment in telecom networks. Several steps towards such a certification have already been undertaken, yet no actual certification of a QKD link — not even of a single component — has already been achieved.

A security evaluation of a product is always being carried out against its security specification. Currently, two parallel attempts towards basic security specifications for QKD modules, as well as towards an evaluation methodology are under way, involving experienced standards developing organizations (SDO) committees. An actual IT security evaluation facility (ITSEF) and an actual certification body (CB) are also involved: the ETSI ISG-QKD, together with the German ITSEF DT-Sec, and under guidance of the German CB "Bundesamt für Sicherheit in der Informationstechnik (BSI)", has developed a sample CC Protection Profile (PP) for a QKD link, which is going to be evaluated by another accredited ITSEF. The ISO/IEC JTC 1/SC 27/WG 3, who are also the maintainers of the EN ISO 15408 "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model" [90] standard itself, have developed a catalogue of CC security functional requirements, as well as a related evaluation methodology.

In addition, several mostly small and medium enterprises are working towards the security certification of QKD components, especially of the so-called Key Management System (KMS), which is a collective term for the subsystem managing the generated keys in a QKD link, as well as for wider network and internetwork protocols.

7.11.1 Projected standards

S: Catalogues of QKD security functional requirements

S: QKD link sample protection profile

S: QKD network sample protection profile

S: Evaluation methodology for QKD links

S: Evaluation methodology for QKD networks

TR: QKD known attacks

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e. hints towards potential standards, or indications of applicability, etc."

7.11.2 Existing standards

SDO	Document number	Document title	Version	publ. date
ETSI	GS QKD 008	Quantum Key Distribution (QKD); QKD Module Security Specification **(SG)**	V1.1.1	2010-12
ETSI	GS QKD 010	Quantum Key Distribution (QKD); Implementation security: Protection against trojan horse attacks in one-way QKD systems **(SB)**	V.0.4.1	Stable draft (2021-09-20)
ETSI	GS QKD 016	Quantum Key Distribution (QKD); Protection Profile (PP) (TB Approval was for planned: 2022-09-22) **(SG)**	V.0.7.1	approved – to be published
ISO/IEC	23837-1	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 1: Requirements **(SG)**		approved – to be published
ISO/IEC	23837-2	Information security – Security requirements, test and evaluation methods for quantum key distribution – Part 2: test and evaluation methods **(SM)**		approved – to be published

7.11.3 Considerations

The ISO/IEC 23837-1 and -2 and the ETSI GS QKD 016 approaches towards common criteria security specification/evaluation/certification are different in the sense that the first one involves a catalogue of generic security functional requirements for the specification (PP and ST) of QKD modules (Part 1) and a connected test and evaluation methodology (Part 2), while the latter approach proposes a specific CC protection profile for a pair of prepare and measure QKD modules. Both propose specific security functional requirements (SFRs) for QKD modules. But while the ISO puts their QKD SFRs in the "trusted path"

class, the ETSI puts theirs in the FCS "cryptographic support" class. Otherwise, their QKD SFRs ("families") are very similar, but the exact differences and implications need to be assessed in detail. In the medium term, a harmonization of the two approaches would probably make sense. Further open issues remain with the question who will actually carry out the security testing and evaluation of the quantum optical subsystem? Respective QTSEFs (quantum technology security evaluation facilities) need to be established. There are ongoing activities in this direction (the EU intends to fund equipment for such a lab [92]). Another lab shall reportedly be set up in Madrid. These reports will be detailed in further versions of this roadmap section.

Once the ISO/IEC security standards, as well as the ETSI PP will be readily available, actual efforts towards certification need to be undertaken, based on these standards. Such evaluations need to be prepared and supported through feasibility studies (of detailed plans on how to "organize" such a certification) and pre-evaluations (to increase the chances of a positive evaluation outcome).

7.11.4 Gaps

Several of the gaps related to "background documents" were taken/inspired by the presentation "QKD certification documents, follow up#2, 'Beyond the Protection Profile'" held by Dirk Fischer of the German BSI (Bundesamt für Sicherheit in der Informationstechnik) at the recent ETSI ISG-QKD meeting #32 on 20 June 2022. The presentation slides are available for ISG-QKD members on the meeting documents website.

The very important issue of background documents for security certification of QKD products needs to be addressed here.

Background documents are documents required for a security evaluation—beyond the actual security specification documents (PPs, STs, and other documents directly related to EN ISO 15408 CC certification). Potential background documents are in the "existing standards" tables identified by the category "CB: Security evaluation: background documents".

Background documents are documents with widely accepted contents (standards, technical reports) supporting the creation and evaluation of EN ISO 15408 Common Criteria (CC) security specifications, in particular, of Protection Profiles (PPs) and Security Targets (STs).

Background documents contain:

— specifications of cryptographic functions and protocols;

— specifications of quantum optical components and subsystems;

— including related characterization and testing methods;

— specifications of QKD protocols and security proofs;

— CC formal supplementary documents (according to selected evaluation assurance level, EAL);

— related CC evaluation methodologies;

— other technical background;

— attack methods and attack rating methodologies.

The list of required background documents needs to be systematically developed, and the subsequent "writing" of these documents needs to be coordinated among involved and interested standards developing organizations (SDOs). This coordination function will be addressed in future versions of the QC/QKD roadmap.

Currently, in the ETSI ISG-QKD, an activity to systematically identify required background documents for QKD security specification according to the group's ETSI GS QKD 016 Protection Profile, is being triggered and shall be started in January 2023.

The proposed approach towards identifying (some of) the necessary background documents is to walk through the PP and find the relevant SFRs where choices regarding conventional or quantum cryptography are needed. Here background documents will likely be necessary.

Generally, the "catalogue" of background documents needs to be established through experts consultations in the relevant SDOs.

Such a catalogue needs to be developed in close cooperation with information technology security evaluation facilities (ITSEFs), i.e., the evaluation labs, and, most importantly, with the certification bodies (CBs) that will ultimately decide the applicability of the referenced background documents.

Further common understanding and awareness of the issue of "background documents" needs to be built through joint activities (e.g., meetings) of the relevant stakeholders (QKD experts, ITSEFs, CBs).

The roles (leading roles, contribution roles) need to be clarified among the stakeholders (and among SDOs).

The following are reasons why these background documents are needed:

— QKD products are "highly individual implementations" and much of the functionalities;

— Cannot be covered with the generic SFRs of the CC catalogue;

— The CC catalogue only covers the "functional domain"; and

— Individual "security features" are not covered by CC catalogue;

— PPs contain developer created SFRs;

— The CC are explicitly indifferent towards cryptography;

— Cryptography needs to be "defined" through accepted background documents;

— ITSEFs will need the background documentation for their evaluation/certification procedures.

An analysis of best practices in related domains is advised:

— Common Criteria Recognition Agreement (CCRA);

— Senior Officials Group-Information Systems Security (SOG-IS) agreement.

7.12 Quantum repeaters

7.12.1 General

While the problem of losses over optical fibres applies both to classical and quantum communication, quantum repeaters are quantum communication systems that allow the distribution over longer distances of input quantum signals, as the latter do not allow simple amplification [93]. Specifically, since copying of not pre-determined quantum states is impossible (no cloning theorem), the principle is that input quantum states are teleported to a further destination by utilizing a previously generated distributed entanglement.

The basic concept of a quantum repeater protocol has been modified since its original proposal [94] and different classes of quantum repeater designs have been put forward. Although entangled quantum memories – a potential core element of a class of quantum repeaters – have been demonstrated [95] recently still no stable prototypes have been hitherto implemented. It would be beneficial for a future quantum repeater to be able to communicate with a number of other quantum repeaters in its vicinity to allow eventually end-to-end quantum circuit switching on demand, subject to respective steering commands in a (composite) full quantum network. In other words, future quantum repeaters need to be equipped with mechanisms for directional and/or wavelength switching.

7.12.2 Projected standards

The different classes of prospective quantum repeaters are to be standardized after these reach practical-prototype level of development (TRL 7). From a present-day perspective, it appears appropriate to standardize these both with respect to the needed background resources (e.g., pre-distributed entanglement) and the probability of quantum state "retransmission" by a quantum repeater.

Projected standards should also be related to the utility of quantum repeaters in composite quantum communication networks aka "the quantum internet".

7.12.3 Gaps

Due to the early stage of development no relevant standards are available. There are some standardization efforts towards composite systems but no dedicated ones that deal explicitly with quantum repeaters.

7.13 Additional standardization needs

According to the discussion above we distinguish between standardization needs for basic components, usually driven more by the technological content and those arising for the quantum communication systems and subsystems, that have a broader scope and that, for a successful industrialization, will have to interact with standards coming from the application field of the specific use-case that they address.

From basic components:

— Many basic components can be used for different purposes (e.g., single-photon detectors/sources for quantum communication but also for quantum sensing or computing). Either a comprehensive characterization is done such that manufacturers of systems can choose components that fit their purpose/use-case or specific sets of characterizing measurements have to be defined for each purpose/use-case;

— The precise definition of the key concepts and procedures in order to have a scientific consensus about the measurements and magnitudes involved in the characterization in the sense mentioned in the introduction has to be done;

— Many of the basic components will comply already with some other standards required for they usage as part of opto-electronic circuits (e.g., driving voltages for a laser, control/data buses, etc.):

  - Standards for basic component characterization:
    - Sources of quantum systems:
      — i.e., single quantum sources;
    - Detectors for quantum systems:
      — Note interaction with existing standards (e.g., ITU-T wavelength grid);
    - Quantum memories and their interfaces:
      — Note interaction with quantum computing;
    - Means for quantum state preparation;
    - Means for quantum state analysis:
      — These last two are of general use in quantum technologies;
    - Physical substrates for the quantum channel (optical fibres, waveguides…):
      — Note interaction with existing standards (e.g., for optical fibres).

From quantum systems and subsystems:

— Define standard requirements needed for quantum communication systems:

- Compliance with sets of basic characterization measurements that makes the basic components appropriate for a given use-case (e.g., different for QKD than for biological sensors…);
- Compliance with existing standards for classical communication systems sharing the same or similar purpose:
  - Standards about physical integration: Power supply, size, connectors…;
  - Standards about logical integration (software) in a telco/security ecosystem (logical interfaces for control, management, key provisioning…);
  - Safety standards (standard regulations. e.g., harmless, not dangerous EM radiation emitted, etc.);

— Standards for verification of key functionality defined in the characterization of components for a given purpose (appropriate for a purpose i.e., a given use-case);

— Security standards:
- Certification of quantum communication systems (protection profiles, targets of evaluation…);
- Analysis of applications, protocols and software;

— Standards for interoperability:
- Low level: Emitter/receivers from different manufacturers;
- High level: At the quantum communication system (e.g., QKD link) level;

— Standards for quantum networks:
- Architectures;
- Control and management;
- Integration in telecommunication/security infrastructures (depending on the type of utilization of quantum networks):
  - Integrations in operations systems support;
  - Integration in security infrastructures (secure networking protocols, key management, combination of security primitives…), see security standards above;
  - Routing protocols:
    — For quantum level signals (quantum states routing);
    — For classical level products (secret key routing);
  - Quantum/classical coexistence:
    — High level: At the network/system level;
    — Low level: At the quantum state transmission level (co-propagation).

8 Quantum computing and quantum simulation systems

8.1 Introduction

8.1.1 General

Quantum computing and simulation as an area covers many different implementations, and several enterprises are developing solutions for a mature quantum computer. The concept of a "modular quantum computer", well known from digital computing, has created a new market which has attracted many small enterprises to develop dedicated modules which are competing with more monolithic full-stack organizations. The availability of a supply chain of such modules from different vendors will enable research teams to concentrate their research on breaking new grounds, without spending much effort on duplicating known solutions. This is where standardization can play an important role.

From a standardization point of view, this market requires a subdivision of the field of quantum computing and simulation into a variety of modules that can interwork with each other through well-defined interfaces (hardware and software), and a consensus on the functional and performance requirements of each module of interest. Instead of communicating such requirements with a single or small number of local suppliers, research teams can save effort by communicating these requirements with relevant standardization bodies.

This is where standardization can play an important role. It will increase the availability of mature hardware and software solutions in return, as well as knowledge on requirements and solutions from others.

It may be worth noting that a quantum simulator is a dedicated quantum computer, designed for solving specific problems as well as studying well defined quantum systems. They may be programmable up to a certain level. The modularity described in this present document covers both quantum computers and quantum simulators, since they use the same hardware components.

8.1.2 Current developments

Although many different implementations do exist, the two leading quantum computing architectures in the European Quantum Flagship are based on different device technologies: Trapped ions and superconducting qubits. These two architectures satisfy the five required criteria for quantum computing defined by DiVincenzo [96]:

— A scalable physical system with well characterized qubits;

— The ability to initialize the state of the qubits to a simple fiducial state;

— Long relevant decoherence times;

— A "universal" set of quantum gates;

— A qubit-specific measurement capability.

Other qubit and platform types include impurity spins in solids, neutral Rydberg atoms, topological qubits and photonic qubits, and these need to be considered as future candidates for quantum computing and require further development.

The developments on quantum computing architectures can be roughly grouped into three categories:

— Those technical approaches that show theoretical merit to be pursued for several reasons, yet have not satisfied the DiVincenzo criteria;

— those systems that have fulfilled the DiVincenzo criteria, yet need to improve on system size and system control to find applications in advanced quantum algorithms, and;

— quantum architectures that are at the threshold of fault-tolerant quantum computing with sufficiently large quantum registers to realize logical qubits for large-scale quantum computation.

8.2 Modularity and layering of hardware stack

8.2.1 General

Quantum computing is an area covering many different implementations. A convenient way of specifying its requirements is via a stack of layers, as shown in Figure 11. The layers are chosen in such a manner that the functionality of each layer can be described in an independent manner. This causes that the interworking between these layers can be described through well-defined interfaces at the boundaries of these layers. Note that such an interface can be virtual (hidden internally within the implementation of the same origin) or real (between implementations of different origin).

The stack covers both hardware and software layers, while some layers are a mix of both. The software layers are drawn in Figure 11 above the hardware layers with another colour. These software layers are described in more detail in section 8.3, and may include (from bottom to top) software drivers, hardware abstraction layers, register level programming layers, assembly, etc. The aim is that higher software layers are more agnostic to differences in hardware architectures.

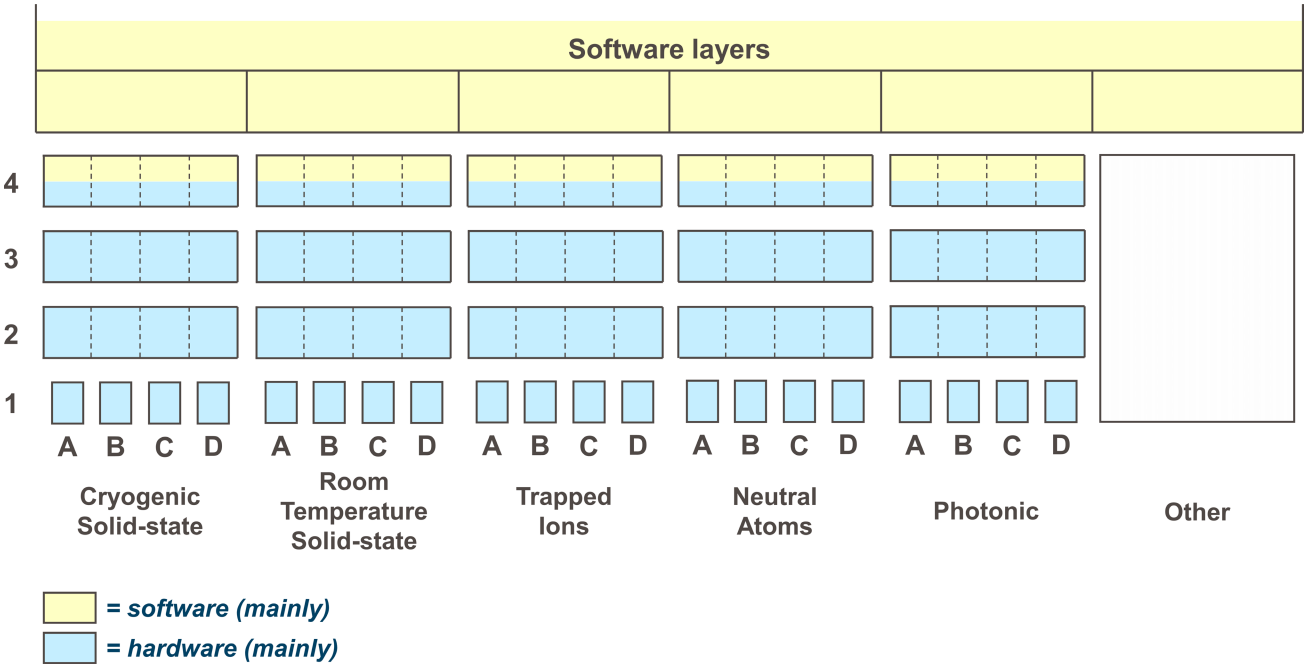


Figure 11 A possible break-down of quantum computing into layered stacks, accounting for different architectures

The layered approach allows for using different hardware stacks for specifying the requirements of different architecture families. Each architecture family can have multiple members (A, B, C, ...) and the description of its hardware layers (1,2,3,4) may account for differences between these members. The diagram in Figure 11 has illustrated this symbolically by drawing different “boxes” in the layers for different members of the same family.

All these hardware stacks can make use of the same layering approach:

— Device holder, which may include one or more quantum devices, housing, shielding, magnets, i/o connection, etc.;

— Control highway, which may include wiring and/or fibres, free-space optics, active devices (amplifiers), passive devices (attenuators, filters, couplers), opto-electronic (photo diodes), thermalization means, vacuum feed-through, i/o connection, etc.;

— Control electronics/optics, which may include output generators, input analysers, signal processing, i/o connection, as well as low-level firmware to guide the generation of signals and the read-out of their response;

— Control software, which may include calibration means, low-level code to translate instructions from higher software layers into commands for guiding the control electronics/optics.

So far, the following architecture families have been identified (in arbitrary order):

— Cryogenic solid-state based;

— Room temperature solid-state based;

— Trapped ions;

— Neutral atoms;

— Photonic quantum computing;

— Other solutions.

These architectures are described below in further detail.

A module is an implementation that may be constructed from (smaller) modules and components. It could offer the functionality of a single layer, of multiple layers, or just of a fragment of a layer. A module may also support different operating modes, such that it complies with the requirements of multiple members and/or multiple architecture families. As such, the functionality of a module may cover multiple layers and/or families and/or members.

8.2.2 Cryogenic solid-state based quantum computing architectures

The members of this architecture family have in common that they all make use of a cryostat, where the quantum devices in a holder are controlled from outside the fridge by room-temperature electronics. Consequently, a huge amount of control channels is required to interconnect those two, especially when many qubits are to be controlled in a single fridge.

The following members have been identified within this architecture family:

— Superconducting:
  - Transmons;
  - Flux qubits;

— Semiconductor spin qubits;

— Topological qubits;

— Artificial atoms in solids.

The layers in the stack describing this architecture family involves:

— [HL1] Quantum devices – The modules in hardware layer HL1 are typically operating at cryogenic temperatures and may be implemented as chip and/or on PCB. It could have though requirements on shielding, operating temperature, magnetic aspects, etc.

— [HL2] Control highway – Hardware layer HL2 covers all infrastructure needed for transporting microwave, lightwave, RF and DC signals (via electrical and/or optical means) between the control electronics at room temperature and the quantum device at cryogenic temperatures. It is a mix of transmission lines, filtering, attenuation, amplification, (de)multiplexing, etc. A huge number of control channels are required to control many qubits in a single fridge (which clarifies the name) and this can easily become very bulky. It could have tough requirements on aspects like heat-flow, thermal noise and vacuum properties.

— [HL3] Control electronics – Hardware layer HL3 covers all electronics for generating, receiving, and processing microwave, RF and DC signals. Some implementations make use of routing/switching and/or multiplexing of control signals at room temperatures. It may have some firmware on board to guide the signal generation and signal processing.

— [HL4] Control software – Layer HL4 can be a mix of hardware and low-level driver software for instructing the control electronics. It also has a software interface to higher layers for receiving sequences of instructions about when, where and what pulses are to be generated, how to process and read-out the response and means for performing calibration.

Further details about solid-state based quantum computing have been elaborated in Annex B.

8.2.3 Room-temperature solid-state based quantum computing architectures

The members of this architecture family have in common that solid-state qubits are all operating at room temperatures. Examples of members in this architecture family are:

— Artificial atoms in solids, such as NV centres;

— Optical quantum dots.

8.2.4 Trapped-Ion quantum computing

The members of this architecture family can operate either at room temperature or at cryogenic temperature (4K). Quantum devices are controlled by electronics operating either at room temperature or under cryogenic conditions. For a larger number of qubits, the required amount of routing signals becomes bulky, and efficient thermal management, low-noise electrical and magnetic components are required.

— Room temperature:
  - Optical qubits;
  - Raman qubits;
  - Spin (microwave) qubits;

— Cryogenic (4K):
  - Optical qubits;
  - Raman qubits;
  - Spin (microwave) qubits.

The layers in the stack describing this architecture family involves:

— [HL1] Quantum devices – The modules in hardware layer HL1 are typically operating either at room temperature or at cryogenic temperatures and may be implemented stand-alone, as chip and/or on PCB (printed circuit board). The device may have though requirements on materials compatibility, shielding, operating temperature, electrical and magnetic aspects, vacuum properties, etc.

— [HL2] Control highway – Hardware layer HL2 covers all infrastructure needed for routing light, microwave signals, RF and DC signals between the control electronics at room temperature and the quantum device at room temperature or cryogenic temperatures. It is a mix of transmission lines, filtering, attenuation, amplification, (de)multiplexing, etc. The number of control channels required to control many qubits in single vacuum housings rapidly grows with the complexity and capabilities of the quantum devices. Stringent requirements to convey on efficient thermal management, low-noise (electrical and magnetic) environment and materials with low outgassing (especially for the room temperature) vacuum components need to be taken into account during design, development and production.

— [HL3] Control electronics – Hardware layer HL3 covers all electronics for generating, receiving, and processing microwave, RF and DC signals. Some implementations make use of routing/switching

and/or multiplexing of control signals at room temperatures and at cryogenic. It may have some firmware on chip/board to route signal preparation, control, and processing/readout.

— [HL4] Control software – Layer HL4 can be a mix of hardware and low-level driver software for instructing the control electronics. It also has a software interface to higher layers for receiving sequences of instructions about when, where and what pulses or signals are to be generated, how to process and read-out the response, and means for performing calibration.

8.2.5 Neutral atoms

Systems of individually-controlled neutral atoms, interacting with each other when excited to Rydberg states, have emerged as a possible platform for quantum information processing. The two main examples are ensembles of individual atoms trapped in optical lattices or in arrays of microscopic dipole traps separated by a few micrometres. In these platforms, the atoms are almost fully controllable by optical addressing techniques.

The layers in the stack describing this architecture family involves:

— [HL1] Quantum devices – The modules in hardware layer HL1 are typically operating either at room temperature and in a high-vacuum enclosure. Unlike in solid quantum processors, e.g., superconducting, silicon or NV qubits, the register in an atomic QPU is not permanently built but is reconstructed after each processing. The device may have requirements on operating temperature, electrical and magnetic aspects and vacuum properties.

— [HL2] Control highway – Hardware Layer HL2 covers all infrastructure needed for routing optical light originating from laser sources (fibres, free-space optics), active devices acting on laser light such as acousto-optics deflectors and modulators, electro-optics modulators, digital micro-mirror devices. Attenuators, filters, and couplers can also be incorporated. Piezo-electric devices for mechanical control. Microwave signals, RF and DC signals complement the control over qubits.

— [HL3] Control electronics – Hardware layer HL3 covers all electronics for generating, receiving, and processing optical, microwave, RF and DC signals.

— [HL4] Control software – Layer HL4 can be a mix of hardware and low-level driver software for instructing the control electronics. The control software is responsible for the orchestration of the various phases in a compute cycle (loading of the atoms, re-arrangement of the register of qubits, measurement). Automatic calibration procedures are typically integrated at the control software layer. This layer also has a software interface to higher (calibration-independent) layers for receiving sequences of instructions at the level of laser pulses.

8.2.6 Photonic quantum computing

These architectures have in common that the quantum information during computing is encoded into photonic properties. We can divide different families of photonic quantum computers in two categories, universal and non-universal quantum computers. Non-universal quantum computers cannot perform every task but can at least perform one task.

Non-universal photonic quantum computing families that are identified are:

— Boson sampling;

— Gaussian boson sampling.

Universal families that are identified are:

— Knill-Laflamme-Milburn scheme (This was a theoretical proof-of-principle, but not practically feasible);

— Measurement based quantum computing using cluster states;

— Continuous variable quantum computing.

The layers in the stack describing this architecture family involves:

— [HL1] Quantum photonic devices – The modules in hardware layer HL1 contains sources, detectors, (non)linear optical devices, and feedback mechanisms. These devices are combined into a quantum photonic architecture.

— [HL2] Control highway – Hardware layer HL2 covers all wiring infrastructure (optical and electrical) needed for controlling the quantum photonic devices.

— [HL3] Control electronics – Hardware layer HL3 contains all electronics and/or optics to control and read-out the quantum photonic devices. It may have some firmware on board to guide the signal generation and signal processing.

— [HL4] Control software – Layer HL4 can be a mix of hardware and low-level driver software for instructing the control electronics. It also has a software interface to higher layers for receiving sequences of instructions about when, where and what signals are to be generated, how to process their response

Further details about photonic-based quantum computing have been elaborated in Annex C.

8.3 Modularity and layering of software stack

8.3.1 General

Broadly speaking, quantum software is all the software that is related to quantum technology systems, including quantum programs executed on quantum devices, control software, and more.

A convenient way of specifying quantum software for quantum computing is via a stack of layers, specialized by application area. The layers are chosen in such a manner that the functionality of each layer can be described in an independent manner, as shown in Figure 12. The interworking between these layers can be described through well-defined interfaces.

In the following subsections, the layers of the software stack are described and discussed, using a bottom-up approach (i.e., from the control software to the applications / services supporting use cases).

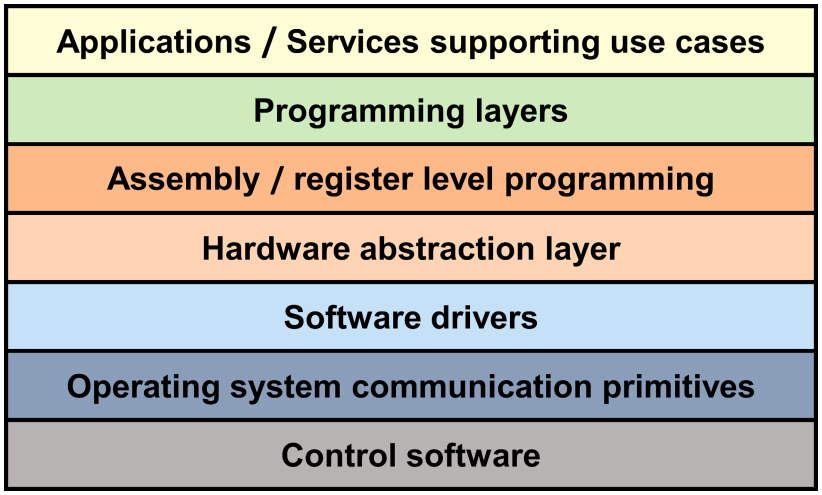


Figure 12 A possible break-down of software layers for quantum computing.

8.3.2 Control software

Placed on top of quantum hardware (described in section 8.2), control software for quantum computing delivers high-performing qubit operations to higher level of abstraction in the quantum software stack with minimal user intervention. This control software layer is the same as hardware layer HL4 from the previous section 8.2.

Control software may include calibration means, low-level code to translate instructions from higher software layers into commands for guiding the control electronics/optics, and comprises the techniques used to define error-robust physical operations and associated supporting protocols designed to tune-up and stabilize the hardware.

Control software for quantum hardware is typically stored on classical digital computers, i.e., there is a very strict separation between the place where the control software is stored and the quantum registers.

NOTE The term "classical" is discussed in some detail in section 2.2.

In the long term, control software may work in concert with Quantum Error Correction (QEC), which is supposed to lay at the assembly / register level programming layer, to provide broad coverage of various error types. More specifically, control software could improve the efficiency of QEC, i.e., reduce resource overheads required for encoding, by homogenizing error rates and reducing error correlations.

8.3.3 Operating system communication primitives

A quantum computer must be provided with an operating system (OS), which is a resource manager for the underlying quantum hardware, provided with built-in networking functions allowing multiple users and applications to use the resources as remote clients. To an application, it appears as if it has its own resources and is protected from other applications. Applications can make use of facilities only as offered by the OS. For example, the OS provides communication primitives (e.g., based on the POSIX standard for the sockets interface [97]) and only by means of these primitives should it be possible to pass messages between client applications and the quantum computer.

8.3.4 Software drivers

In the layered view illustrated in Figure 12, software drivers are components that are plugged into the operating system and allow hardware-abstraction programs to call the control software of the underlying quantum hardware. If the hardware changes, the software drivers must change as well.

8.3.5 Hardware abstraction layer

The hardware abstraction layer (HAL) should allow quantum computer users, such as application developers, platform and system software engineers and cross-platform software architects, to abstract away the quantum computer implementation details while keeping the performance. The hardware may change, but the QASM-like programs (belonging to the upper assembly / register level programming layer) should be still able to work.

Among all software layers for quantum computing, this is the one that requires the most urgent standardization effort. The hardware abstraction layer should provide Application Programming Interfaces (APIs) to the upper layer, decoupling from the different types of quantum hardware technologies (see section 8.2 for some examples).

8.3.6 Assembly / Register level programming

This layer concerns QASM (i.e., quantum assembly) languages that describe quantum computations according to one specific model (e.g., circuit model, measurement-based model, quantum annealing model), with a per-architecture instruction set.

An example is OpenQASM [98], which targets IBM Q devices and enables experiments with small depth quantum circuits. OpenQASM represents universal circuits over the CNOT plus SU(2) basis with straight-

line code that includes measurement, reset, fast feedback, and gate subroutines. OpenQASM possesses a dual nature as an assembly language and as a hardware description language.

A different example is NetQASM [99], which is a platform-independent and extendable universal instruction set with support for local quantum gates, digital classical logic, and quantum networking operations for remote entanglement generation. NetQASM consists of a specification of a low-level assembly-like language to express the quantum parts of quantum network program code.

Due to the huge diversity of quantum computing architectures, it is not likely that a unique, widely accepted QASM would emerge and later become a standard.

8.3.7 Programming layers

The specification of quantum algorithms using QASM languages is not easy for programmers. Indeed, QASM programs are usually generated by a software library, from a piece of code written in a common programming language, such as Python.

In general, the programming layers include all the languages, libraries, and software development facilities (e.g., software development kits, debugging tools, quantum compilers) used by developers for coding quantum algorithms or high-level applications that use predefined quantum algorithms as subroutines.

Quantum compilation is the problem of translating an input quantum circuit into the most efficient equivalent of itself, considering the characteristics of the device that will execute the computation and minimizing the number of required two-qubit gates. The most advanced quantum compilers are noise-adaptive, i.e., they take the noise statistics of the device into account.

8.3.8 Applications / Services supporting use cases

To effectively support industrial and research use cases, quantum applications must be executed in suitable environments. Currently, some vendors provide access to quantum devices via user-friendly cloud platforms. The quantum programs must be locally compiled for a specific device and submitted for batch processing to the remote platform. However, other paradigms are emerging. For example, the quantum internet will enable networked quantum applications, whose execution will involve multiple quantum nodes and will be characterized by interleaved digital classical and quantum message passing.

8.4 Benchmarking

Well-defined and standardized methods to characterize and to benchmark quantum computing devices are necessary to compare different architectures. This facilitates reliable key characteristics of a device-under-test. Agreed ways of specifying characteristics are relevant for components in supply chains, to identify the optimal implementation for the application at hand. But agreed methods are also relevant for comparing the performance across modules, architectures or platforms as a whole.

In general, we identify two approaches. The first approach (“bottom-up”) identifies key parameters (or metrics) including measurement protocols, as well as what measurements are to be performed to specify a relevant characteristic of the device-under-test. The second approach (“top-down”) employs to-be-defined algorithms that can be run on the device-under-test. The output of the algorithm will offer the desired characterization of the device-under-test.

The bottom-up approach is usable for individual components of a quantum computer system. Measurements have to be reliable, well-defined, and ideally traceable to SI units. In this way, a high degree of trust and comparability can be achieved via connecting to established metrology (see chapter 9 on quantum metrology). This is particularly important in cases where quantum computers are assembled employing components of different parties (see section 4.6 supply chain). We note that in chapter 5 “Enabling Technologies” possible parameters can be found.

8.5 Characterization and benchmarking of quantum computing devices

Quantum computing can be implemented by employing different architectures. Examples are given in section 8.2. Several different implementations are available nowadays for exploring applications, i.e., running algorithms, often via online access (see Use Case section 2.1 “Using a Quantum Computer as Secondary Processor in the Cloud”).

Well-defined and standardized methods to characterize and to benchmark quantum computing devices are necessary to compare different architectures. This facilitates giving reliable key characteristics of a device-under-test, relevant for components in supply chains, to compare performance across platforms and to identify the optimal implementation for the application at hand.

We identify two general approaches: In one approach (“bottom-up”), key parameters (or metrics) are identified, including measurement protocols, and measurements are performed, realizing a characterization of the device-under-test. The second approach (“top-down”) employs to-be-defined algorithms that can be run on the device-under-test, the output of the algorithm realizing a characterization of the device-under-test.

The bottom-up approach is usable also for individual components of a quantum computer system. Measurements have to be reliable and ideally traceable to SI units. In this way, a high degree of trust and comparability can be achieved via connecting to established metrology (see section 9.1 Quantum Metrology). This is particularly important in cases where quantum computers are assembled employing components of different parties (see section 4.7 Supply Chain). We note that in chapter 5 Enabling Technology possible parameters can be found. In the layer model as illustrated in section 8.2.1 the bottom-up approach is implemented in the lower layers.

The “top-down” approach aims at defining a standardized set of algorithms. Two limiting cases can be identified: A “query of parameter values” or execution of fundamental operations (for instance one-qubit and two-qubit gates) on the underlying device-under-test, which can be thought of as a self-diagnosis. Note that in this case the characterization depends on the measurement capabilities of the platform itself, is not independent (i.e., implemented and performed by hardware manufactured by the vendor itself) and not traceable to SI units. However, implementation of this way of characterization can be light-weight and easy to handle. The reported values of parameters provide the characterization of the device-under-test. Alternatively, a more complex set of algorithms can be defined and executed on the device-under-test. Subsequently, parameters for success and performance can be defined and determined. This approach emphasizes the application, however, connection to the underlying hardware and implementation can be challenging, depending on the chosen metric. In the layer model as illustrated in section 8.2.1 the top-down approach is implemented in the higher layers.

The above outlined standardization of characterization and benchmarking for quantum computer devices can serve several purposes:

— define generally accepted set of key parameters, measurement protocols and algorithms for reliable characterization;

— establish quality standards and, perspectively, certification of quantum computer components;

— guarantee quality of components in supply chains;

— help to compare complementary architectures in a well-defined manner, important both for further development and application;

— inform about performance of quantum computer devices.

8.6 Timeline for standardization of quantum computing and quantum simulation

Figure 13 shows an estimated timeline for the start of standardization activities in the areas of quantum computing and quantum simulation. This is not meant as an exhaustive list but is meant to give some idea of the range of activities one can expect will start in the next few years. Indeed, as is indicated in the timeline, some activities are already ongoing: a quantum computing vocabulary is being developed by ISO/IEC and IEEE is actively working on metrics and benchmarking (please see Annex A for comprehensive list). Several proposals for work that could potentially start in 2023 are at the time of this writing under active consideration by SDOs.

Quantum computing and simulation as areas encompass many technological platforms which are also used for e.g., sensing, timing and metrology. In many cases one can therefore expect synergy between standardization activities. For example, ion-trap based quantum computing is an emerging area, but ion traps have been used for e.g., timing applications for a long time and the technology is therefore more mature – and possibly ready for start of initial standardization activities – than one might initially assume.

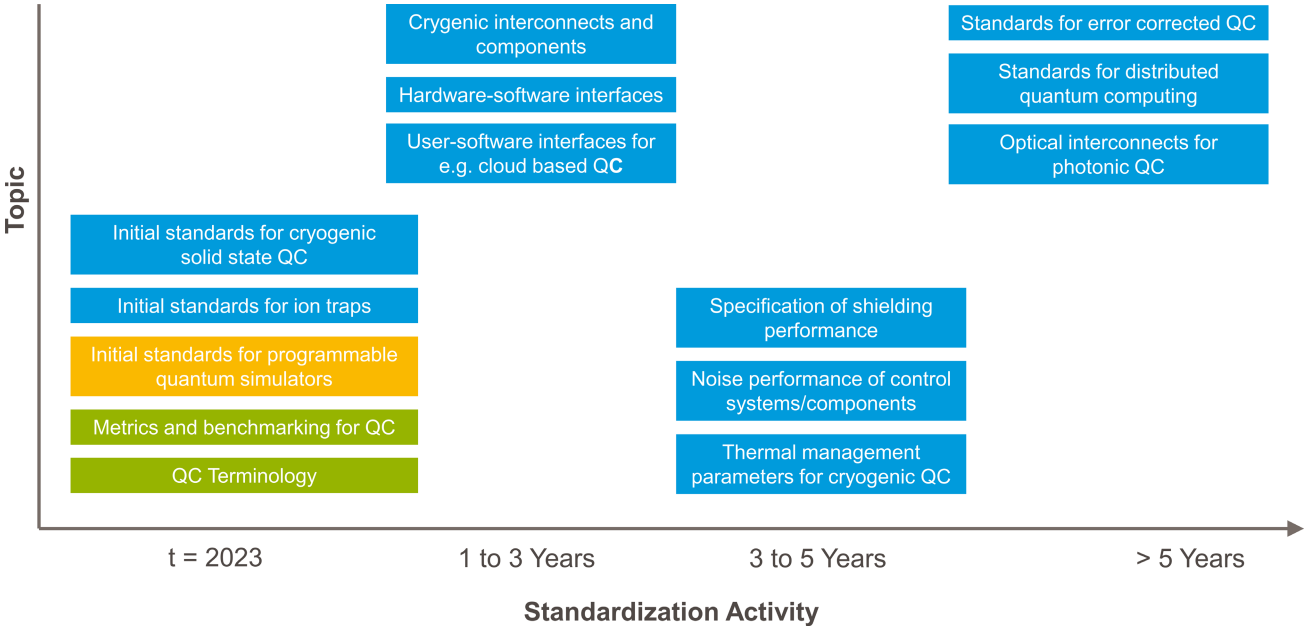


Figure 13 Possible timeline for start of standardization activities in the area of quantum computing and quantum simulation. The topics in green are already ongoing, topics in yellow are under active consideration.

9 Quantum metrology, quantum sensing and quantum imaging

9.1 Overview

9.1.1 General

Quantum metrology and sensing and quantum enhanced Imaging (QMSI) exploit the properties of quantum states and peculiar phenomena, such as entanglement and non-classical correlations in a wide range of physical platforms, from condensed matter to single photons, through NV-centres, cold atoms, ions, or single electrons. QMSI devices significantly improve the accuracy and precision with which parameters of a wide range of systems can be measured or evaluated. Beyond, they allow stepping over limitations related to conventional classical measurement strategies, as the environment-induced noise from vacuum fluctuations (the so-called shot noise), or the dynamically induced noise in the position measurement (the standard quantum limit) or the diffraction limit. QMSI devices span a range from fundamental research to practical applications in industry, in the field of physics, chemistry, biology, medicine, materials science, as well as in quantum information, computation and communication.

NOTE The term “classical” is discussed in some detail in section 2.2.

We identify two major domains of applications and related standardization needs:

1) Novel applications enabled by QMSI; and
2) Characterization, benchmarking, and evaluation for reliable QT.

9.1.2 Novel applications enabled by QMSI

9.1.2.1 Traceability and realization of SI base units outside of NMIs

Since the 2019 revision of the SI-System [100] all base-units are defined in terms of physical constants, several of them from the quantum realm, and can be in principle realized anywhere without the need of a traceability chain to unique physical artefacts, due to quantum technologies for most of them. This opens the opportunity to realize SI-units with the best accuracy outside NMIs and achieving miniaturized, simpler to operate, intrinsically accurate and quantum-referenced sensors is now an exciting challenge. However, designing and building quantum measurement standards remains a complex and demanding procedure. Things can go wrong, leading potentially to incorrect operation. In the future a world-wide quality network, mainly backed by the international network of NMIs, needs to ensure the reliability of these efforts [23].

Examples include microwave and optical atomic frequency standards, Josephson voltage and quantum Hall resistance standards, miniature Kibble balances to realize the kilogram and nanophotonic or shot-noise thermometers. These deployable quantum standards can dramatically shorten the calibration chains enabling more accurate end products. They are designed for easy operation allowing for use without the need for highly trained specialists.

National metrology institutes are a relevant resource for developing advanced measurement science, technology transfer, standardization, and measurement & calibration services for QMSI devices and applications. To strengthen this role, the European NMIs, organized in EURAMET [101], decided to establish a new sustainable body called European Metrology Network for Quantum Technologies (EMN-Q) [22]. EMN-Q in close cooperation with standardization institutes (like CEN/CENELEC) should identify and develop the next generation QT in sensing and metrology [42].

9.1.2.2 Novel and improved sensing and metrology devices

QMSI includes the fields of quantum electronics, quantum clocks & atomic sensors and quantum photonics. Without addressing all possible applications ranging from SI traceability to ultra-low noise measurements below the standard quantum limit or high-precision measurement at the nanoscale with single quantum systems, some examples for relevant QMSI technologies of scientific and technological interest are listed in the following [2]:

a) Quantum electronics: Single-electron sources (for the SI-realization of the ampere and single-electron quantum optics, realization of the "quantum metrological triangle"), Josephson junctions (for quantum voltage standard), quantum Hall effect (for quantum resistance standard);

b) Quantum clocks: Atomic clocks (for new time standards and chip scale atomic clocks to address GNSS (Global Navigation Satellite System) resilience, network synchronization, Time Stamping, Basic research, etc.);

c) Atomic sensors: Atom interferometers for gravimeter (for climate research, civil engineering, hydrocarbon and mineral exploration, GNSS-free navigation), magnetometers based on cold atoms or NV-centres in nanodiamonds (for brain imaging, hearth imaging, metrology, navigation);

d) Quantum photonics: Single-photon sources and detectors (for ultraprecise quantum interferometers, phase discrimination for quantum communication, twin beam and squeezed light, super-resolution, sub-shot-noise imaging, quantum enhanced microscopy, quantum enhanced displacement sensing, quantum illumination and quantum radar/LiDAR, quantum reading, quantum ghost imaging and spectroscopy, quantum photometry and quantum physics based primary standards).

The examples above include both SI measurement standards used for traceability and novel QT-based measurement devices. Typically, these can be thought of as devices with improved properties, as for example sensitivity, range or drift, but otherwise serving the same purpose of measuring a certain quantity. Therefore, no additional standardization might be needed for the device as such. However, in any case, the underlying enabling technology and QT components and subsystems may require standardization, as discussed in chapter 5 & 6. For example, an ion optical clock requires characterization of the employed ion trap and a magnetometer based on NV centres requires a standardized description of the material used. These aspects are described in chapter 5. This shows the general and cross-sectional character of metrology.

9.1.3 Characterization, benchmarking, and evaluation of quantum technologies

QMSI techniques and devices are playing a major role for characterization and testing of QT components employed in all domains of QT and are a prerequisite for commercial usage of QT in the worldwide technology supply chain (see chapter 4). Metrological characterization and qualification are underlying a responsible quantum innovation and industrialization, in particular by providing competent, independent and unbiased test and evaluation from the level of enabling technology over sub-systems/components, up to the system/platform level, as illustrated in the temple scheme in the abstract of this document. Several national metrology institutes from around the world are developing corresponding testing facilities [23, 22, 42] . Furthermore, recently, several testbeds are initiated on national as well as the EU level [21].

For example, characterization, evaluation, and benchmarking are required for quantum computing in order to compare complementary architectures, inform development and prioritize investment. Reliable characterization of components is furthermore important to help establish technological supply chains as discussed in chapter 4: Properties of, for example, trapped ion or superconducting quantum processor chips need to be well defined to build more complex systems out of these core components. Examples for corresponding standardization needs are given in chapter 5.

9.2 Quantum magnetometers

9.2.1 General description and overview

In our definition, quantum magnetometers (QMs) are spin-based devices that measure the magnetic flux density in units Tesla (T). QMs are sensitive in a field range spanning orders of magnitude from fT to several T. They are in the process of being commercialized in a wide range of applications, similarly to their conventional counterparts including position control, airborne and seaborne navigation, geomagnetic exploration, automotive engineering, magnetic materials characterization, high current detection, and battery diagnostics. Moreover, their high sensitivity at lowest magnetic fields promotes the usage of QMs in medical applications like magnetoencephalography mapping [102, 103].

QMs are devices that take advantage of the properties of an ensemble of quantum spin systems susceptible to applied magnetic fields. The Zeeman effect causes a modification of the energy levels and depending on the kind of spins involved, electronic, nuclear, or total spins, and on the magnetic field coupling, the transition between levels is characterized by distinctive frequencies. Non-equilibrium occupation of certain quantum states is necessary to induce single or multi-level switching and to obtain a measurable signal. Optical pumping, radio frequency excitation or auxiliary magnetic fields are mechanisms to force the ensemble in the desired state and the consecutive read-out happens spontaneous or photon induced. [102, 103]

Different kinds of atoms in an ensemble are used as QMs. The list of examples includes but is not limited to:

i) **Optically pumped magnetometers** (OPMs). In OPMs the out of equilibrium distribution of Zeeman states and the read-out process are stimulated by frequency-tuned laser excitation. Evaporated alkali elements, such as K, Rb or Cs, are typical field sensitive atoms. OPMs operate in contrast to highly sensitive superconducting quantum interference devices (SQUIDs) at room temperature with comparable sensitivity. Therefore, they are predestined for medical diagnostics like magnetoencephalography and magnetocardiography. One major limitation of OPM's sensitivity is quantum noise. Advanced QT techniques, such as optical and spin squeezing, are further developed to improve performance and to introduce OPMs on the market.

ii) **Nuclear spin magnetometers**. Nuclear magnetic resonance techniques on e.g., ^{3}He and $^{129/131}$Xe nuclei with spin S = 1/2, 3/2 received considerable attention in recent years, because they provide experimental results with superior absolute accuracy and high spatial resolution. The population of different quantum states is stimulated by optical hyperpolarization and PAMP (polarization of atoms in a magnetized plasma). Because of their time stability, ^{3}He OPMs are utilized for absolute field measurements in experiments to survey the limitations of the Standard Model in physics.

iii) **Co-magnetometers.** They combine OPMs and nuclear spin magnetometers in one device. In co-magnetometers, either two different quantum states in one kind of atom or two individual quantum states in two different types of atoms are employed. Systematic uncertainties on the magnetic field due to particle motion or leakage currents are suppressed giving rise to highest absolute measurements of the magnetic field. Another advantage of co-magnetometers is that two measurements are carried out simultaneously for exactly the same probe volume.

iv) **Protons.** Protons in water samples or aqueous solutions are nuclear spin magnetometers. They are considered the metrological gold standard for traceable magnetic field measurements with highest absolute accuracy. The proportionality factor γ of the measured Lamor frequency $\omega = \gamma B$ in respect to the applied field B is known with 10^{-8} relative uncertainty based on CODATA [104]. Depending on the magnetic field range and probe size, different types of NMR techniques are employed, i.e., free induction decay (FID) (10 μT – 2 mT), absorption (1 mT – 0.3 T), or a water flowing (nutation) technique (0.1 mT – 100 mT). Proton FID on rubber samples is used at magnetic fields up to several T. Devices are commercially available for this field range, however, the lack of normative standards created an industrial defacto standard without metrological traceability.

v) **Bose-Einstein condensation (BEC) magnetometers**. BEC magnetometers or single domain ferromagnetic BEC magnetometers are based on trapped cold atoms. They combine high sensitivity to magnetic fields (0.3 nT) with μm resolution. The 2-dimensional BEC is trapped by a microfabricated wire carrying electrical currents on an atom chip. The BEC density is a measure of the magnetic landscape, and it is experimentally probed with an imaging laser beam. The sensitivity of BEC magnetometers depends on the chemical potential, which is orders of magnitude lower than the critical BEC temperature.

9.2.2 Pre-normative gaps

— Definition of performance metrics

— Definition of characterization procedures

— Definition of environmental standard conditions during characterization procedures

9.2.3 Standardization needs

Standardization needs can be grouped in three main topics:

a) Standardization of the employed atomic ensemble:
   - Isotope type and grade;
   - Chemical parameters: Composition, purity, contamination (water etc.);
   - Physical parameters: Density, pressure, temperature;

b) Infrastructure standardization and guidelines on measurement protocol:
   - Theoretical and/or experimental estimation of intrinsic distortion of the to be measured magnetic field by magnetic properties (e.g., susceptibility, material impurities) of the magnetometer setup including samples, holders, supporting materials, excitation and detection units;
   - Standardization of geometric parameters of probe bodies, e.g., material, deviation from ideal shapes, surface roughness, manufacturing procedures;
   - Reference probes;
   - Biocompatibility, when used close to biological objects, cells, living organisms;

c) Definition of device performance under standardized conditions:
   - Background AC/DC magnetic field compensation, radio frequency noise tolerance;
   - Temporal stability of residual field, influence of magnetic field anisotropy;
   - Thermal conditions, stability;
   - Data sampling rate/time;
   - Sensitivity, resolution, signal to noise ratio, energy resolution per bandwidth, shot-noise.

10 Composite systems

10.1 Overview

In chapter 7, the standardization roadmap for quantum communication systems was presented, with an emphasis on components. In this section, the focus is on quantum networks as composite systems.

A quantum network is an arrangement of quantum communication systems and their connecting quantum channels enabling quantum state transfer (direct transmission channels) or establishing quantum correlations (quantum correlations channel) between quantum states at some or all nodes of the network. The goal is to pack the quantum functionality of a quantum network into a well-defined subdomain that "fits" in existing infrastructures. Quantum networks belong to two types:

— Multi-hop networks: when only direct transmission channels are available, thus direct transmission of quantum states or quantum correlation establishment can be done only over limited distances (typically metro or regional area). Long distance quantum correlation establishment is impossible but classical correlations that are not feasible outside the quantum regime can be achieved through classical concatenation of these channels and additional trust (see above), thus limiting the access to quantum capabilities (no end-to-end quantum key distribution), since no quantum correlations can be established between the initial and end points of the multi-hop link. Note that these types of networks are not necessarily static as direct quantum transmission channels can be established on demand between end points by a switching mechanism (wavelength switching, if required, is also feasible).

— End-to-end networks (sometimes called quantum information networks or full quantum networks): allow full connectivity among all the quantum systems in the network through quantum correlation channels of very long range (potentially unlimited distance). These networks would allow (communication-wise) the unrestricted implementation of any quantum communication protocol, including QKD without the need of trusted nodes (also called trusted repeaters). Note that a routing mechanism shall be implemented to dynamically establish different end-to-end configurations.

NOTE The term "classical" is discussed in some detail in section 2.2.

A basic classification can be drawn

a) Quantum key distribution networks :
   - Trusted repeater type;
   - End-to-end quantum communication type;

b) Quantum information networks.

According to the main implementation domain the following distinct case can be identified: terrestrial networks, space borne networks, mixed versions.

10.2 Trusted repeater networks

10.2.1 General

Trusted repeater networks are the multi-hop networks described above. They are a transient solution on the road towards full quantum networks addressed in the next subsection and can only serve for key distribution end-to-end albeit at the expense of the additional assumption of the availability of trusted locations that was outlined above.

QKD trusted repeater networks have the advantage that they can be implemented almost immediately with presently available technology. The arguably first operational network of this kind was the BBN DARPA one in 2007. Shortly afterwards the EU FP6 SECOQC project launched a protocol-wise systematic trusted repeater network with six nodes and 9 links was demonstrated. The respective network software

was later released under an open source license and became the basis for further developments and progress.

Several trusted repeater QKD networks of metropolitan area size, with dozens of QKD links, have recently been rolled out in funded projects, and there are currently several national and international plans and programs to establish such infrastructures for actual use. The most prominent example of such an international plan is the European Union's EuroQCI initiative.

10.2.2 Projected standards

S: QKD key forwarding

S: QKD node control and management

S: QKD system interoperability

TR: QKD and key management

S: QKD network control, and management

S: QKD orchestration among networks

S: Secure QKD nodes

S: Hybrid space/terrestrial QKD networks

NOTE "S:" denotes a standard; "TR:" technical report; "K:" keywords, i.e. hints towards potential standards, or indications of applicability, etc."

10.2.3 Existing standards

SDO	Document number	Document title	Version	publ. date
ETSI	GS QKD 004	Quantum Key Distribution (QKD); Application Interface **(KM)**	V2.1.1	*2020-08*
ETSI	GS QKD 014	Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API **(KM)**	V1.1.1	*2019-02*
ETSI	GS QKD 015	Quantum Key Distribution (QKD); Quantum Key Distribution control interface for software defined Networks **(QN)**	V2.1.1	*2022-04*
ETSI	GS QKD 017	Quantum Key Distribution (QKD); Network architectures **(QN)**	V0.0.9	*Early draft (2021-09-05)*
ETSI	GS QKD 018	Quantum Key Distribution (QKD); Orchestration Interface of Software Defined Networks **(QN)**	V1.1.1	*2022-04*
ETSI	GS QKD-020	Quantum Key Distribution (QKD); Interoperable KMS API **(QN, KM)**	V0.0.1	*Early draft (2021-12-06)*
ETSI	GR QSC 001	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework **(QN, SB)**	V1.1.1	*2016-07*
ETSI	GS QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios **(QN, SB)**	V1.1.1	*2017-02*

SDO	Document number	Document title	Version	publ. date
IEEE	P1913	Software-Defined Quantum Communication **(QN)**		*Drafting*
ITU-T SG 13	Y.3800 (ex Y.QKDN_FR, Corrigendum 1)	Framework for Networks to supporting Quantum Key Distribution **(QN, VC)**		*2020-04*
ITU-T SG 13	Y.QKDN_Arch	Functional architecture of the Quantum Key Distribution network **(QN)**		*Drafting*
ITU-T SG 13	Y.QKDN_KM	Key management for Quantum Key Distribution network **(QN, KM)**		*Drafting*
ITU-T SG 13	Y.QKDN_SDNC	Software Defined Network Control for Quantum Key Distribution Networks **(QN)**		*Drafting*
ITU-T SG 13	Y.QKDN_CM	Control and Management for Quantum Key Distribution Networks **(QN)**		*Drafting*
ITU-T SG 13	Y.QKDN_BM	Business role-based models in Quantum Key Distribution Network **(QN)**		*Drafting*
ITU-T SG 13	Y.QKDN-req	Functional requirements for quantum key distribution network **(QN)**		*Drafting*
ITU-T SG 13	Y.QKDN-qos-gen	General Aspects of QoS on the Quantum Key Distribution Network **(QN)**		*Drafting*
ITU-T SG 13	Y.QKDN-qos-req	Requirements for QoS Assurance of the Quantum Key Distribution Network **(QN)**		*Drafting*
ITU-T SG 17	X.cf-QKDN	Use of cryptographic functions on a key generated in Quantum Key Distribution networks **(QN, SB)**		*Drafting*
ITU-T SG 17	X.sec-QKDN-ov	Security requirements for quantum key distribution networks - Overview **(QN, SG)**		*Drafting*
ITU-T SG 17	X.sec-QKDN-km	Security requirements for quantum key distribution networks - Key management **(QN, SG)**		*Drafting*
ITU-T SG 17	X.sec-QKDN-tn	Security requirements for quantum key distribution networks -Trusted node **(QN, SB)**		*Drafting*

10.2.4 Considerations

Contemporary trusted repeater networks have much higher demands than their “historic” predecessors. Many questions are open: e.g., do they need the functionality to exchange keys between peers in different local subnets, is the architecture built upon fixed (unchangeable) QKD links or should the integration of advanced functionality with variable (switched) connection of QKD modules to different peers also be

feasible? Further, must the use of "unorthodox" QKD link configuration, like three-device-systems (Entanglement source in the middle, or MDI paradigms) be addressed, or control functionalities allowing to change the wavelength in the quantum channel during quantum key generation be an option and open the way for future QKD-SDN designs?

Many of these options are in fact features that are being developed by individual teams, and are also brought forward towards standardization—but without much coordination. So there are currently several parallel developments ongoing world-wide (there are currently at least four approaches to developing protocols and implementations for QKD trusted repeater networks).

10.2.5 Gaps

There is a high need for coordination, especially in the development of QKD trusted repeater network protocols, to avoid incoherent developments and inefficiencies and to facilitate compatibility and convergence. The situation threatens to develop as it happened in the field of cloud computing, where dozens of SDOs have proposed literally hundreds of standards—while the de-facto standards are being set by the dominant market players (cf. Amazon AWS) outside of any consensual process.

10.3 Full quantum networks

10.3.1 General

These networks will fulfil multiple (quantum-specific) communication purposes and would be in the position not only to enable long distance quantum communication but also distributed quantum computing and metrology. For this reason, a more popular term had been coined, namely the "quantum internet". This notion is certainly appealing. At the same time, it might lead to certain misinterpretations. While full quantum networks would allow leveraging the full potential of distributed quantum technologies, the "quantum internet" is by no means a replacement or an upgrade of the traditional internet. It is rather an addition that will bring about numerous novel functionalities as a co-network to the existing and truly indispensable one.

In fact, quantum networks would strongly rely on existing protocols that are implemented in already existing network communication standards. A quantum network main purpose is to physically transport entanglement and state-superpositions. This requires functionality such as addressing, routing, quality and error management, similar to functions that are implemented in different layers of the internet (if we refer to the OSI model). These managerial functions require communication between different users/layers in a network and it is obvious that to this end existing classical communication channels available are to be used. Moreover, in analogy to traditional communication, functionality should be independent of / agnostic to concrete physical mechanisms.

10.3.2 Application areas

The quantum internet has potential applications in each of the quantum technology pillars. Below we discuss some of these. Note that even though each of the pillars is addressed, implementing a quantum internet is initially a quantum communication task.

Secure communication: Communication protocols have been constructed that have been theoretically proven to be secure. Behind these lie the impossibility of making an identical copy of an unknown arbitrary quantum state as a consequence of the "no-cloning" theorem. Quantum states can be used to transfer non-classically feasible correlations between parties that exchange them. Strong correlations, in turn, allow the mutual agreement on secret strings (symmetric keys). Simultaneously, gain of information through eavesdropping is limited by an increase of the quantum bit error rate and for this reason can be traced and eradicated. This gain limitation is a consequence of the impossibility of faithful cloning and is not feasible classically.

Equivalently, key distribution can be based on entanglement. The best-known case is that of qubit pairs, each pair behaving as one joint quantum system, even if its constituents are physically separated by significant distances. Local measurements of both qubits exhibit maximal correlations that can be used in analogy to the case discussed above to agree upon a symmetric secret key. Utilization requires classical information sharing between the two communicating parties. Note also that deviation from a maximal degree of correlation is a signature of eavesdropping and can be used to test the presence of adversarial activity.

In the case of quantum computing state-superpositions and entanglement are used to perform efficient calculations, albeit at the expense of a massive amount of highly specialized infrastructure. The quantum internet allows disjoint less massive quantum computers to exchange qubits and entanglement, thus get coupled and act as a single powerful quantum computer.

In the case of metrology: Quantum mechanics can improve measurement precision, e.g., enhancing the resolution of telescopes or very accurate timing applications. The quantum internet allows optical telescopes to have large baselines, by getting synchronized. Further, entanglement shared via the quantum internet allows to achieve very accurate angle of arrival estimates. This in turn allows separate optical telescopes to act as a virtually single larger one. Similar argument holds for timing applications to achieve extremely precise imaging.

10.3.3 Considerations

Here we briefly consider a number of questions relevant for full quantum networks:

— How can quantum states be transported coherently, whereby this transport has to be over long distances?

— How can entanglement be generated between two arbitrary nodes of the network? Specifically, what protocols should be used to achieve sufficient fidelity?

It is to be noted that multiple protocols to this end are known. Users can for instance directly send quantum states as carriers of quantum information (note that there is a maximal loss that this approach can sustain). Another option is based on “quantum teleportation”, which, based on shared entanglement and classical communication, enables the distant transfer a quantum state. These and other protocols all have performance characteristics. Furthermore, in noisy settings, clearly this operation will lead to imperfect transfer of quantum states. A strategy to find adequate solutions in different situations appears to be the development of a tool-box that holds different protocol implementations and lists these in conjunction with their characteristics. This tool-box would allow for quick evaluation of the resulting fidelity for different use cases and optimal utilization of a certain implementation.

— How can the quantum operations be best coordinated to achieve sufficient performance of the full quantum network?

To guarantee adequate performance of full quantum networks, it is important that the different nodes are simultaneously controlled so that an aligned set of quantum operations can be performed. These quantum operations include, but are not limited to, sharing entanglement between nodes, manipulation of quantum states by local operations in a node and (partial) measurements of quantum states.

Necessary tasks to achieve full quantum networks functionality include:

— Quantum states (qubits) routing and sharing of classical information, whereby the non-physical network segments should be agnostic of the functionality details (in analogy to TCP/IP);

— Design of quantum repeaters to allow for transport of quantum states over long distances;

— (Dynamic) Interconnection of quantum devices and nodes, respectively definition of appropriate interfaces;

— Development of methods to distribute classical information pertaining to quantum states, whereby the information is uniquely assigned to the respective states;

— Understanding the scalability of the capacity of network performance and throughput, as a function of relevant degrees of freedom;

— Design and implementation of appropriate network protocols, that would allow seamless overall operation of full quantum networks integrating and binding segments on different layers of abstraction through inter-segment (vertical) interfaces.

A more specific technical issue related to the quantum physical segment is e.g.:

— Appropriate communication electromagnetic wavelengths for different communication media, whereby loss minimization is the prime concern.

10.3.4 Projected standards

The technology of the quantum communication systems needed for realizing full quantum communication networks (such as e.g., quantum repeaters) is still to be developed. However, already now, it is to be recommended to develop standards on the general architectures of these networks as their functionality is clearly foreseeable. The respective interfaces can also (at least preliminarily) be designed already now. The process of standardization must be open and allowing extensions and complemented with the development and maturing of the technology.

Initial considerations (QIRG of IRTF) have been started and these concentrate predominantly on the functionality of the physical layer, while simultaneously emphasizing the necessity that higher layers should be agnostic of the underlying physical mechanisms.

10.3.5 Gaps

Full scale standards are generally not yet developed. Specifically, the overall design and operation of the full quantum networks and their interaction with classical communication ones needs yet to be scrutinized in detail.

10.4 Security evaluation / certification of quantum communication networks

This is a necessary activity, specifically for the utilization of quantum communication networks (both in the versions of trusted repeater networks and full quantum communication networks) as composite quantum-based security infrastructures. At present this activity has not been initiated as the major focus currently is on certification of plain (single link) QKD (see section 7.9 above). It is, however, clearly foreseeable that security certification of quantum communication networks will follow. For this reason, we tag it in the present roadmap, as a future necessary standardization activity. It is also clear that this certification activity has to be synchronized and harmonized with security certification of separate quantum communication systems.

11 Use Cases

Use cases can help identify standardization needs in many different areas, even if the technology itself is not ready for standardization.

Use cases are for instance relevant to identify:

— Challenges of quantum computing

— The necessity of mitigation to quantum-safe encryption and communication

— Basic approaches to quantum-safe encryption and communication, including post-quantum cryptography, quantum networks and hybrid forms thereof.

— Fundamental blocks of realizing quantum hardware

— Concrete network and infrastructure designs and how these should be integrated.

Additionally, the three application areas – computing, communication and simulation – identified within the European quantum flagship are of special importance.

Finally, apart from the application of quantum technology, also the integration within classical processes is relevant for use cases and the value of classical computing, information and communication within computational pipelines.

NOTE The term “classical” is discussed in some detail in section 2.2.

More Information on use-cases of quantum technologies can be found in the document “FGQT Q05 Use Cases” [105].

12 Conclusions and next steps

12.1 General

This roadmap document is the results of two years of work, over 30 meetings and over 300 contributions of the CEN/CENELEC Focus Group on Quantum Technologies (FGQT). The following sections provide an overview of topics for standardization, based on analyses earlier in this document, and an outlook.

12.2 Topics for standardization

12.2.1 Continue roadmapping and use cases

The market for quantum technologies continues to evolve. Whereas a significant part of the quantum-technologies market are currently components and products aimed at quantum-technological research and development at the time of writing this document, this will change over time. As a consequence, use cases and standards needs will evolve. This means that there will be continuous need to analyse use cases and to evolve the standardization roadmap.

The following are example standards documents that could be produced for this.

Type	**Scope**
Technical Report	Quantum Technology Roadmap
Technical Report	Quantum Technology Use Cases

The documents would be informative Technical Reports, e.g., subsequent releases of the two documents produced by FGQT. Their purpose would be to communicate and coordinate European standardization strategies.

12.2.2 Quantum computing

Modularity and layering are key words for quantum computing, both hardware and software.

The following are example standards-oriented documents that could be produced for this.

Type	**Scope**
Technical Specification	Modularity and layering of the quantum-computing software stack
Technical Specification	Cryogenic solid-state quantum computing
Technical Specification	Photonic quantum computing
Technical Specification	Ion-trap-based quantum computing
Technical Specification	... more, based on market need ...

These documents would be normative Technical Specifications. Their purpose would be to support the purchasing processes for constructing quantum computers. Other normative documents could relate to characterization, calibration and testing of quantum-computing components and (sub)systems. There could also be informative documents for dedicated quantum-computing use cases.

12.2.3 Quantum metrology, sensing and imaging

Metrology is transversal through all aspects of quantum computing, quantum communication and quantum sensing/imaging. The purpose of standards in this area would be certification for quantum-technology components and products on the market. These include applications of quantum metrology, sensing and imaging, e.g., standards for datasheets for single-photon sources and single-photon detectors.

The following are example standards documents that could be produced for this.

Type	Scope
Technical Report	Standardization needs from network of European metrology institutes (NMIs/DIs, Euramet EMN-Q)
Technical Specification	Characterization of single-photon sources
Technical Specification	Characterization of single-photon detectors
Technical Specification	Characterization of QKD transmitters/receivers
Technical Specification	Characterization of Quantum Random Number Generators
Technical Specification	Characterization of sub-shot noise imaging devices
Technical Specification	Characterization of quantum magnetometers
Technical Specification	Characterization of Quantum clocks (and chip scale atomic clocks)
Technical Specification	Characterization of atomic interferometers/quantum sensors
Technical Specification	Quantum physics based primary standards (quantum electronics, quantum clocks, quantum photonics, quantum photometry)
Technical Specification	Characterization of Quantum gravimeters/gradiometers
Technical Specification	Characterization of high-precision force sensors (GNSS)
Technical Specification	Characterization of Quantum radar/lidar (quantum illumination devices)
Technical Specification	Characterization of spin-qubit-based sensing devices
Technical Specification	Characterization of NV centres based microscopes
Technical Specification	Characterization of nano-optomechanical sensors
Technical Specification	Characterization of NV centres based high-precision electric/magnetic field measurement sensors
Technical Specification	... more, based on market need ...

The purpose of the informative Technical Report is coordination with strategic research agenda's on quantum technologies. The purpose of the normative Technical Specifications is to form a basis for datasheets of such components in the market.

Obviously, coordination will be needed with specific application areas, like quantum computing and quantum communication, as different characteristics may be relevant in different application areas.

12.3 Next steps

Having identified needs for Technical Report and Technical Specifications on quantum technologies above, a next question is how to organize the work to assure that those are created. The work should be organized such that on the one hand European interest are guarded, and the EC and European Quantum Flagships have hooks of control. On the other hand fragmentation should be avoided, and the focus should be on Europe's position in a global market. This requires discussion and proposals at the European level, as well as global coordination with ISO, ITU, ETSI and other relevant standards-developing initiatives. The present document provides a base for such discussion, proposals and coordination.

Based on among others the present document, CEN/CENELEC decided October 2022 to establish JTC 22 QT, the Joint Technical Committee Quantum Technologies.

Annex A

Existing standards initiatives

A.1 Standardization

In standardization processes, parties collaborate in order to grow a market together and create an ecosystem, which is beneficial for all participating parties. Standards are (being) written in different contexts. An example are standards for electronic consumer devices, where both producers of devices and producers of content have a common interest. Without a standardized and shared interface, extra effort is required to bring the content to the devices. Therefore, by having a standardized interface between the device side and the side of the content developers, each party individually has a larger market reach than in a fragmented market without such interoperability.

Another example are standards for network interconnection. Service providers (e.g., telephony, mobile, internet) typically have a geographically concentrated market. Through interconnection, consumers of one service provider can reach more and other consumers of other service providers than in a fragmented market without such interconnection.

There are many more examples. All examples have in common that multiple parties have interests that are at least partially aligned, where they need each other to grow a market together.

The success of a standard is measured by its level of adoption. Many standards fail because they are too early (i.e., standardization needs are formulated, while the market is still heavily changing), too late (i.e., fragmented proprietary standards already established) or not needed. For example, the market for 3D-TV turned out to be non-existent despite huge development, standardization and marketing efforts. Or a market is winner-takes-all, like Facebook for social networking.

NOTE The analyses in Annex A were made mid-2020

A.2 Current state of quantum technology standardization and patents

A.2.1 General

This section provides on overview of current quantum related standardization efforts and applications for patents [106, 107]. In section A.2.2 we explain how we gathered and processed information. An overview of the standardization efforts is given in section A.2.3 and an overview of the patents can be found in section A.2.5. In section A.2.6 we align the two in order to see if there is coherence between the two.

A.2.2 Data collection

In the following sections an overview is given of different standards and patents on quantum related technologies. Both are included as a first analysis showed that the number of standards related to quantum is very limited.

To create an overview of the standards, we considered both already existing standards as well as standardization initiatives at different standardization organizations, including IETF, ETSI, ISO, NIST and the Chinese CCSA. For this, publicly available data is used. Additionally, we contacted the standardization organizations. We have however not obtained a response yet. We also included standards that are still in progress, as well as study groups if no standard was issued yet, but efforts are made.

To create an overview of the patents, we used the publicly available patent database provided by the World Intellectual Property Organization [107]. We queried the database with the following search terms: quantum computing, quantum sensing, quantum communication, quantum key distribution (QKD), post-quantum cryptography (PQC), and quantum algorithms. We searched the front page of the

patents in this database for matches with these specific keywords and included the patent in the database if there was a match. Within these results all family members of one patent application are listed as an independent dataset. A simple patent family is a collection of patent documents that are considered to cover a single invention. The technical content covered by the applications is identical.

We double checked the results via using the database Espacenet. We have seen discrepancies between the results from the two publicly available databases. These discrepancies occur due to the different coverage of the international available patent sources and the listed status of families. Our search for the exact sources of those discrepancies was not conclusive, which is why a more thorough analysis was undertaken using the listed commercially available software solutions, PatBase and PatSnap.

We considered all patents available in the WIPO-database, not just the patents that are still valid. Furthermore, with patents we have to consider the region of application. Therefore, as country we listed the country of applicability and not the country of origin of the applicant.

The information that was found is stored in two databases, keeping the division between the current standards and the current patents. The data was further subdivided in different subdomains, as there is not one quantum technology. The considered subdomains are: quantum communication; quantum key distribution (QKD); quantum sensing; quantum computing; and, post-quantum cryptography (PQC). For the patents we also considered quantum algorithms as a subdomain, whereas for the standards we added an extra subdomain on definitions. The definitions-subdomain was added in order to deal with standards that cover multiple of the aforementioned subdomains by providing more general terminology.

A second subdivision is made considering the focus area of the standards. Here we distinguish between protocols, applications, hardware and vocabulary. The focus area is assigned manually. The number of patents in the database does not allow for such a manual assignment.

Finally, the contributors to standards and the applicants of the patents are classified as being a company, a university, a standardization organization or a research institute. For the patents we used an automated Python-script to make this classification. For instance, if in the name of the applicant appeared the substring ‘univ’, it was classified as University. Similarly, if one of the substrings ‘inc.’ or ‘ltd.’ appeared, it was classified as company. For company a few other substrings were also used as trigger, based on often seen contributors. If a classification based on these and other rules was not possible, it was listed as unknown.

A.2.3 Overview of quantum standardization

A.2.3.1 Introduction

To provide a clear overview of the current standards and standardization efforts related to quantum, we have made various visualizations based on the created database for standards. The overview of all found standards is provided in this Annex.

A.2.3.2 Standardization efforts per country

First, we consider the activities per country. Here we distinguish between contributors and contributions. The contributors are sole parties, which can contribute to multiple standards. In Figure A.1 the number of contributors per country is illustrated and Figure A.2 shows the number of contributions by these contributors grouped per country. Countries are indicated by their three letter country codes, as described in the ISO 3166 international standard.

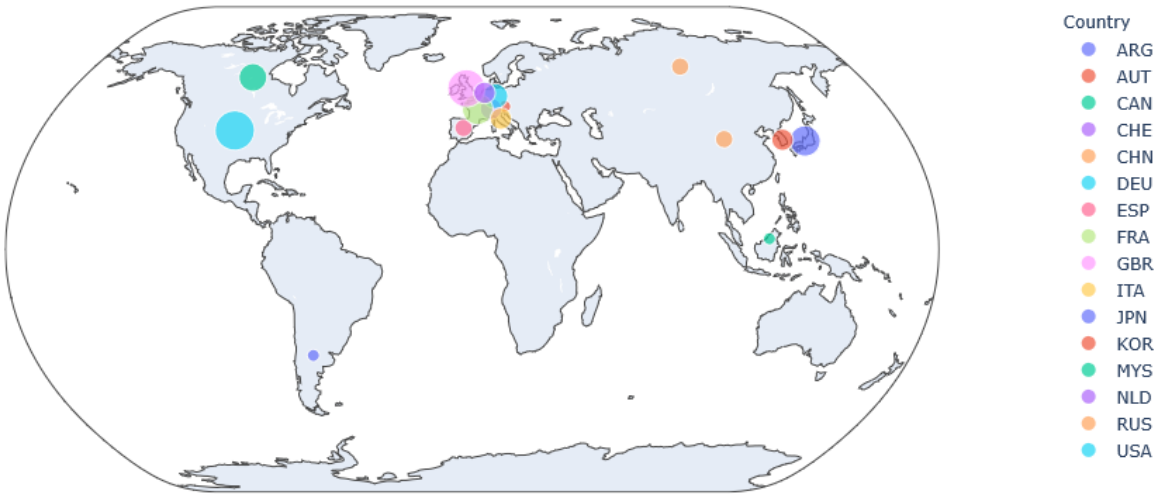


Figure A.1 Number of contributors to standards per country

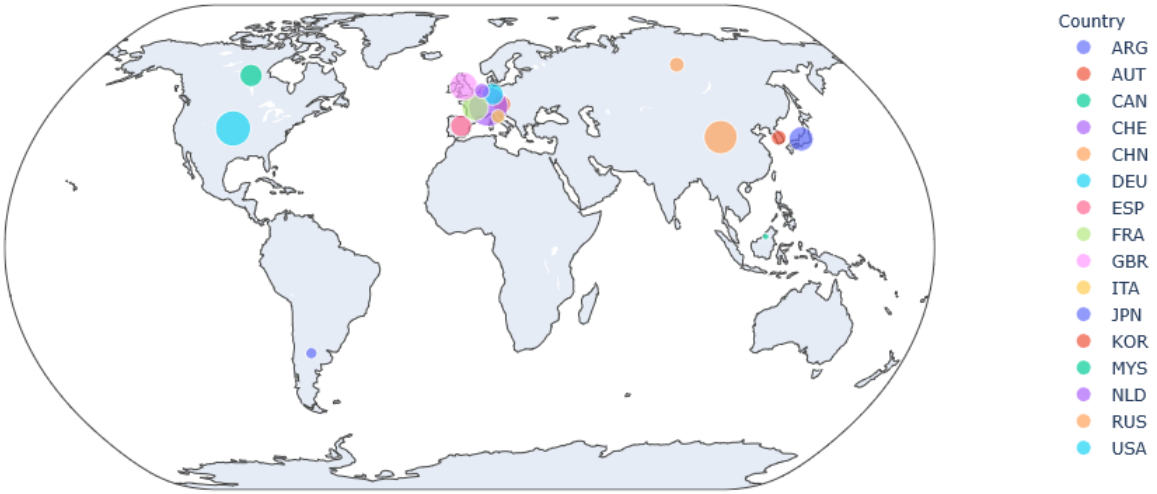


Figure A.2 Number of contributions to standards per country. Different contributions by a single contributor are counted separately

The differences between the two figures follows from the fact that a single contributor can contribute to multiple standards. Sometimes the contributors to a standard are not known as not all standardization organization provide this information as open access. In these cases, the standardization organization was listed as the sole contributor. It also happened that the standardization organization was indeed one of the contributors. The difference between these two situations should be clear from the context.

Interestingly, we see no activity regarding standardization from India and Australia, while it is publicly known that these countries are investing in quantum technology. This can either mean that there is no activity in these countries related to standardization, or that certain standards or standardization organizations are missing in this overview. We furthermore do see activity in at the standardization organization of China CCSA, obtained from [108]. It is not clear which parties contributed to the standards and what the latest status is. In this case, we listed CCSA as the sole contributor, hence, it is likely that there are still contributors missing in the overview. For the standards issued by the ITU we used a similar approach, as also for their standards the contributors were not always publicly available.

In Figure A.3 and Figure A.4, respectively, we show the classification of the contributors and the corresponding contributions for each country. Interestingly, both Switzerland (CHE) and China (CHN) have

only three and two contributors, respectively. There are over twenty contributions from both countries to standards. Note however, that in both numbers efforts by the standardization organization ITU and CCSA are included, based in Switzerland and China, respectively. For their standards it was not always known which parties contributed. As not all contributors are known, the standardization organizations themselves are also incorporated as a contributor.

Interestingly, in the figures it is seen that there are many contributions from companies, namely more than half of the individual contributors to standards is classified as a company. This proves that there is also a significant investment in quantum technology from businesses and effort to create a market for quantum technologies together with other parties.

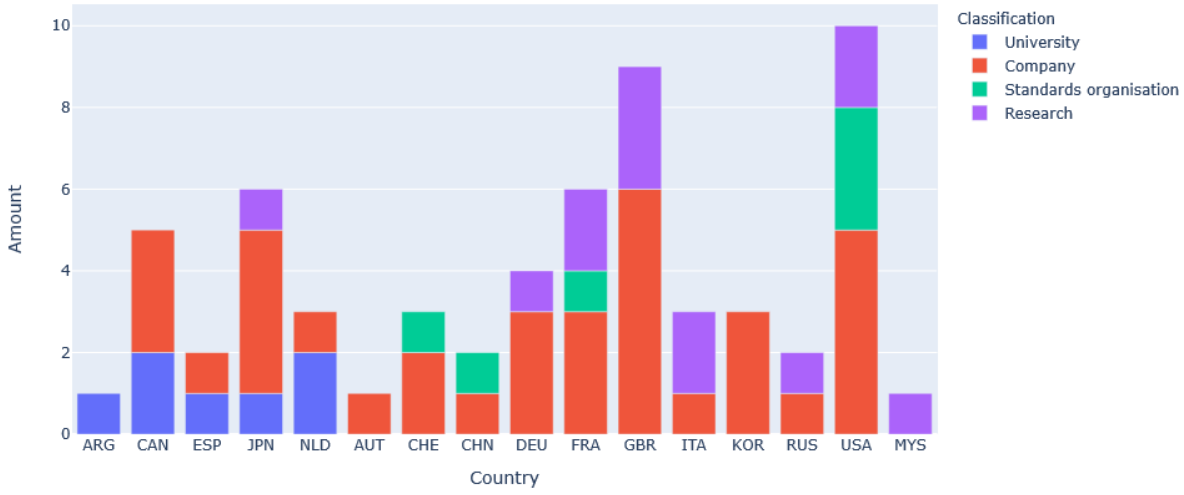


Figure A.3 Number of contributors to standards per country classified as company, university, research organization (RTO) or standardization organization

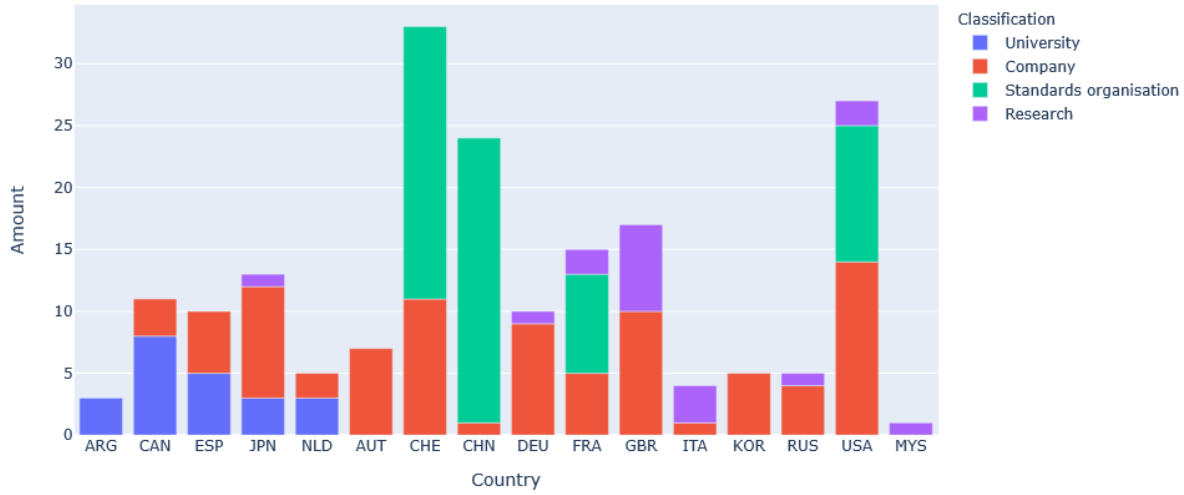


Figure A.4 The contributions per country, with the classification of the contributor

A.2.3.3 Standards per subdomain

We divided the standards in different subdomains: quantum communication; quantum key distribution (QKD); quantum sensing; quantum computing; post-quantum cryptography (PQC); and definitions. The results of this subdivision are shown in Figure A.5. In Figure A.6 a similar subdivision is given, but then in the focus areas which are: protocols, applications, hardware and vocabulary.

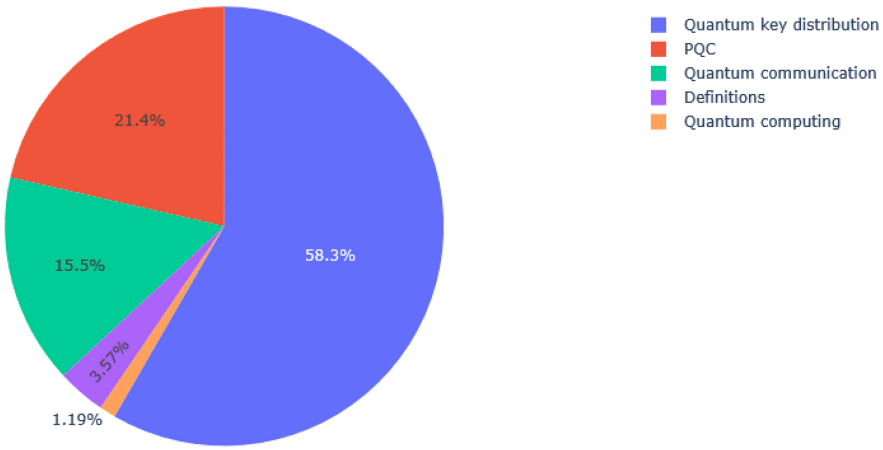


Figure A.5 Distribution of the standards, divided in different subdomains

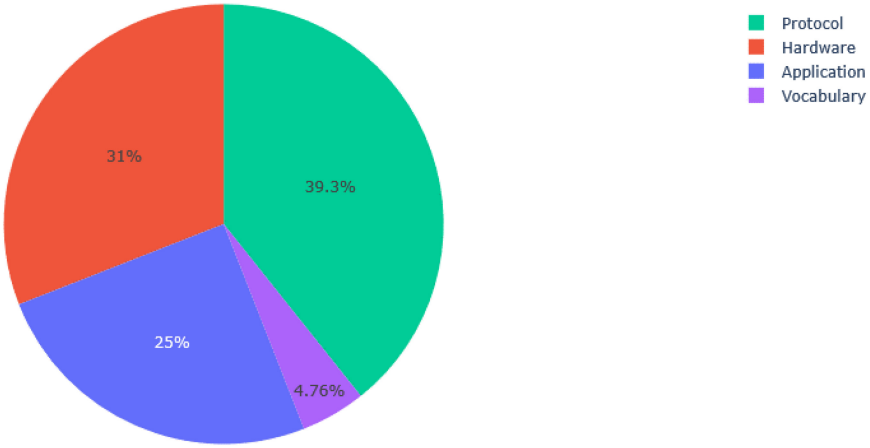


Figure A.6 Distribution of the standards, divided in focus areas

Note that even though it appears as if most standards on quantum key distribution relate to protocols, this is not the case. In Figure A.7 we compare the subdivision in focus areas and subdomains for the standards. We see that only for quantum key distribution and quantum communication, standards cover all focus areas.

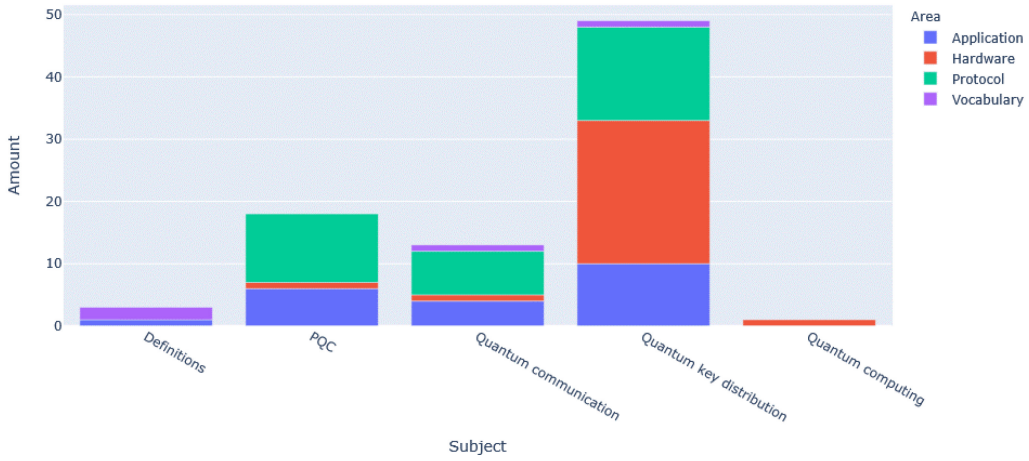


Figure A.7 The subdomains of standards versus the focus areas

We see that the main effort in standardization is on post-quantum cryptography and quantum key distribution. Furthermore, we see that there are multiple standards on protocols.

A.2.4 Standards per standardization organization

In Figure A.8 and Figure A.9 we consider all standards grouped per standardization organization that has issued them. In our analysis we also found standards that are still in draft or for which the current status was unknown. These are also incorporated.

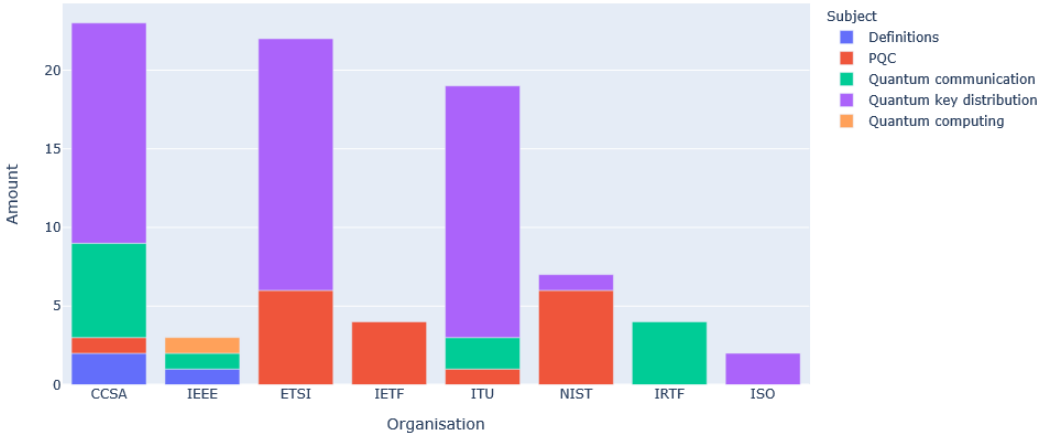


Figure A.8 Number of standards per standardization organization, subdivided in different subdomains

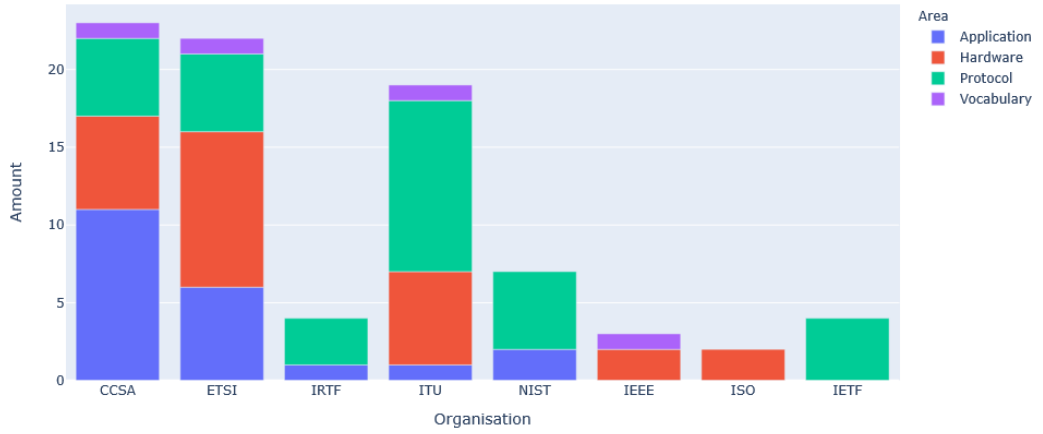


Figure A.9 Number of standards per standardization organization, subdivided in focus areas

The number of standards is expected to grow in the next few years, as currently many standardization organizations have an active quantum standardization process.

A.2.5 Overview of quantum patents

A.2.5.1 Introduction

There are currently only a limited number of standards related to quantum. To see where possible future standardization interests of parties are, we constructed a similar database for patents.

A.2.5.2 Patents per country or region

The first results are shown in Figure A.10 and Figure A.11, where we show the number of parties that have a patent in a specific country or region and the total number of patents in that region, respectively.

The international PCT-applications, are indicated by the circle in Nigeria and the circle in Italy represents the European patent applications.

We note that there are numerous patents that are valid only in specific countries. The circles in specific countries, such as Panama, Denmark, Spain or Brazil indicate patents that are only issued in that specific country. Furthermore, opposed to the standardization efforts, here we do see activity in China, India and Australia. Recall that patent applications in multiple countries or regions (patent family), it appears multiple times in the database. For instance, a patent that was issued in China, in the United States of America, and issued for all other countries besides these two, appears three times in the database.

The number of patents filed in China and the United States of America is higher than the number of patents filed for worldwide. This implies that multiple patents are only valid in China/the United States of America and not in the rest of the world.

Figure A.10 Number of parties with a patent filed in a country. The circle at Italy represent Europe, and the circle at Nigeria represents worldwide issued patents

Figure A.11 Number of patents filed for that specific country. Europe is represented by the circle in Italy and the circle at Nigeria represents the patents issued worldwide

In Figure A.12 we see the number of patents valid in a certain country or region with a classification based on the applicant of the patent. The data is ordered considering the number of patents owned by companies.

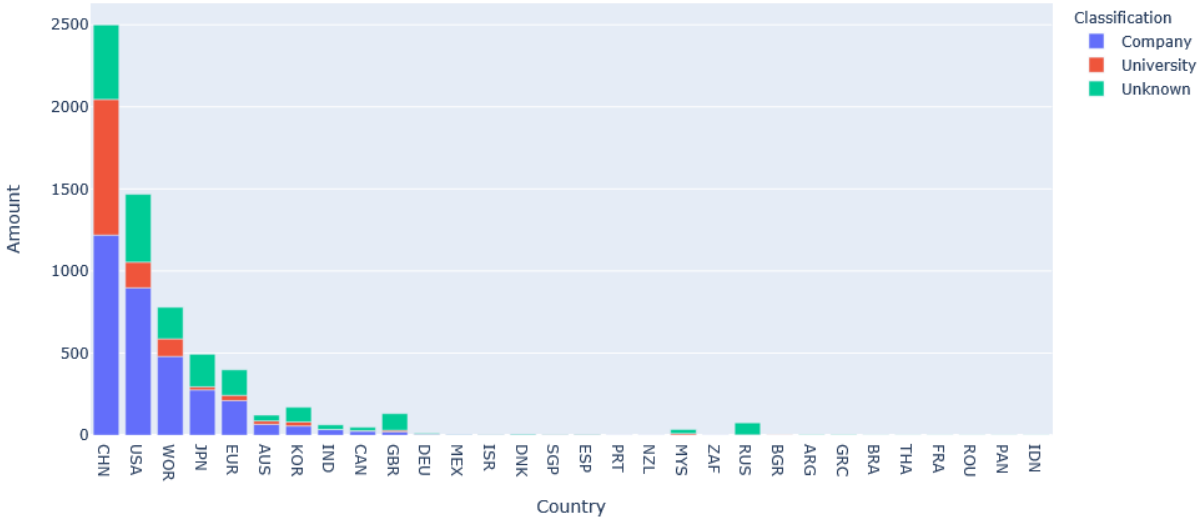


Figure A.12 Number of valid patents per country. Here WOR and EUR indicate patents that are valid worldwide and in Europe, respectively

A.2.5.3 Patents per subdomain

In Figure A.13 we show the number of patents per subdomain, these subdomains are the same domains as considered for the standards. The subdomains are assigned based on the search results, e.g., patents found with search query quantum sensing are also assigned quantum sensing as subdomain. Only a limited number of patents appeared for different subdomains. In these cases, the subdomain was assigned manually. We see that most patents relate to quantum communication and quantum key distribution. The bulk of the standards have one of the latter two as subdomain.

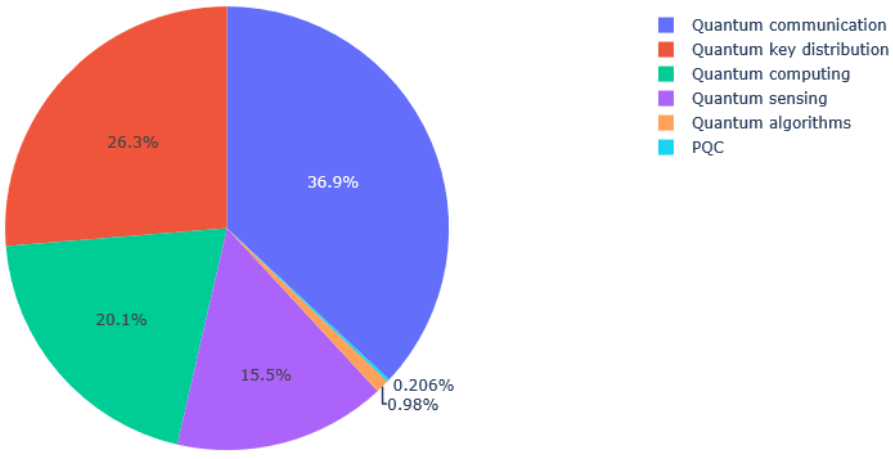


Figure A.13 The subdivision of the patents with respect to the different subdomains

We note that the number of patents in the subdomains PQC and quantum algorithms is very limited.

Regarding the overlap between patents and existing standards in the field of quantum technologies, the software PatSnap offers an option to filter out those results, where the so-called Standard-Essential Patents (SEP) stem from standards issued by major Standard Organizations. A SEP is a patent that claims

an invention that must be used to comply with a technical standard. SEP are listed by Standard Organizations as essential. The system of PatSnap includes SEP data from major Standards Organization (International Telecommunications Union (ITU), European Telecommunications Standards Institute (ETSI), American National Standards Institute (ANSI), European Committee for Standardization (CEN), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE) and International Organization for Standardization (ISO)).

This search displays just 140 SEP for the four subdomains Quantum Sensing, Quantum Key Distribution, Quantum Communication and Quantum Algorithms. 37 of them are listed in the search results for all the categories, 33 in three categories, 34 in in two categories and 36 in just one category.

Quantum Computing

— European Telecommunications Standards Institute (ETSI) lists 66 SEP, whereas the number of patents related to International Electrotechnical Commission (IEC) and International Telecommunications Union (ITU) was 2 and 1, respectively.

Quantum Sensing

— European Telecommunications Standards Institute (ETSI) lists 86 SEP, whereas the number of patents related to ITU and IEC was 9 and 2, respectively.

Quantum Communication

— European Telecommunications Standards Institute (ETSI) lists 96 SEP, whereas the number of patents related to ITU, IEC, and Institute of Electrical and Electronics Engineers (IEEE) was 11, 2, and 1, respectively.

Quantum Algorithms

— European Telecommunications Standards Institute (ETSI) lists 64 patents SEP, whereas the number of patents related to ITU and IEC was 7 and 1, respectively.

A.2.6 Alignment between standards and patents

By considering both the information on the standards and the patents, we can analyse if they show similar patterns. In Figure A.14 we see the number of standards and the number of patents. As the number of entries in the databases differed significantly, we used a double y-axis, with the tick values for the patents on the left-hand side, and those of the standards on the right-hand side. We consider each of the subdomains separately.

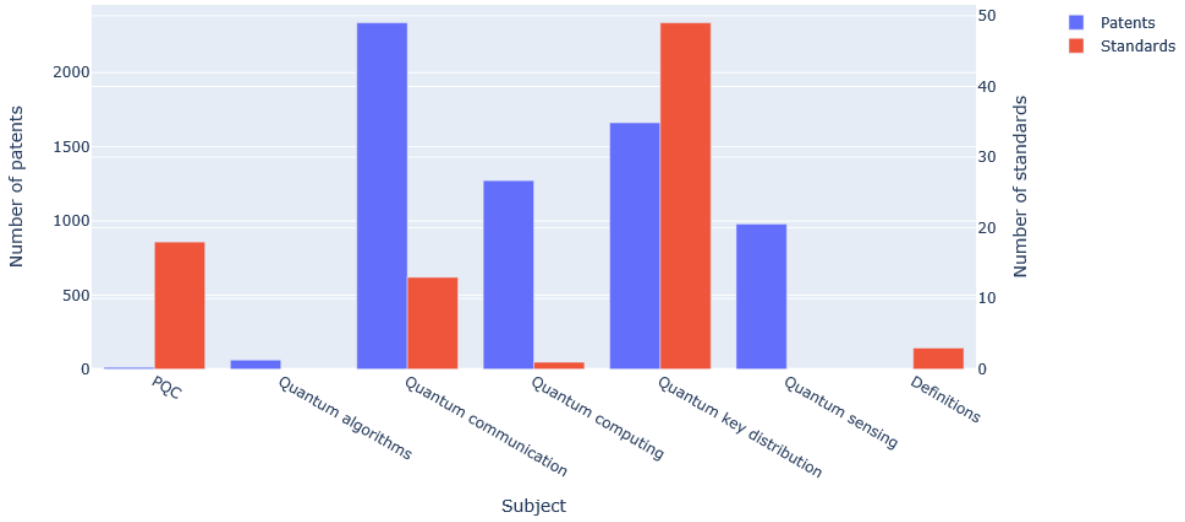


Figure A.14 The number of patents and standards divided in the different subdomains. Note the use of a double y-axis

Considering the cumulative number of patents and standards over the years, we obtain the figure as illustrated in Figure A.15. Note that the last few years, the number of patents increased significantly, as well as the number of standards. The number of patents is significantly larger than the number of standards. However, as patents are usually valid for twenty or thirty years, patents from before 1990 will likely not be valid anymore. Also note that the plot for standards extends beyond 2020, the year of writing this report. This follows from the known plans of NIST and IRTF to have standards in the next few years on post-quantum cryptography and quantum communication respectively, which we incorporated in the analysis. For 2020, only standards and patents issued in the first two months are incorporated. Therefore, we expected that these numbers will increase during the rest of the year.

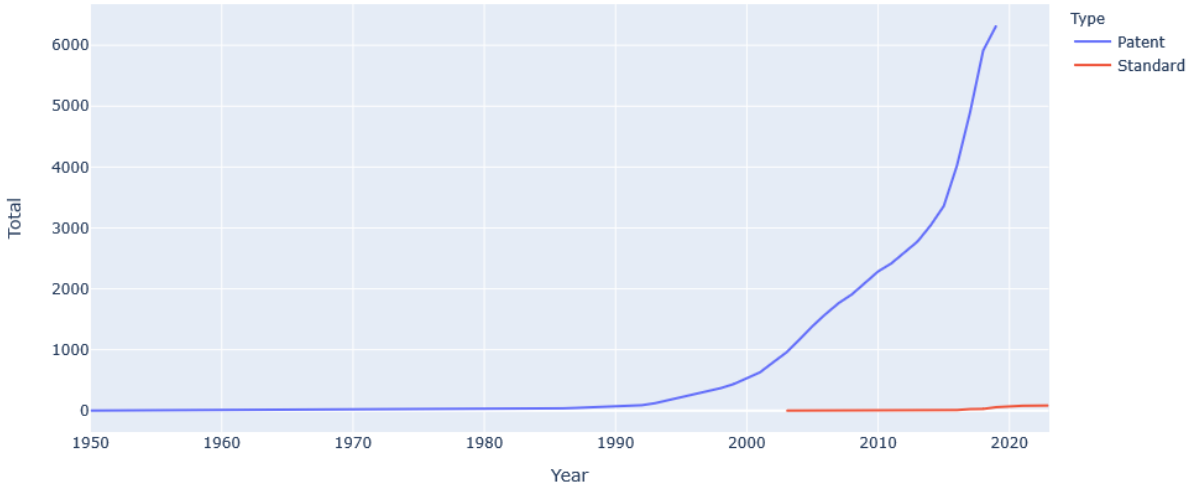


Figure A.15 Cumulative number of patents and standards per year

In our analysis we focused on the available standards and patents related to quantum technology. The patents were incorporated in the analysis as the number of standards was limited. Considering patents could later provide insights in the interests of organizations and academic institutes and potentially be used to predict a trend in the development of quantum standards.

The number of standards considering quantum computing and quantum sensing is very limited. Instead, most of the current quantum related standards are on post-quantum cryptography, quantum key distribution and quantum communication and focus on the security domain. An explanation for this might be the early stage of development of the aforementioned fields. Companies are still trying different ways to exploit the quantum effects for computation and sensing applications and hence, standardization has not been the main concern as of yet. Another explanation might be that companies and organization aim to cover the whole production pipeline of quantum computers and sensors themselves, thereby limiting the need of standardized interfaces with external platforms of other parties. This is however an assumption that needs verification.

We note that there appears to be little participation from Indian and Australian parties in the standardization activities of well-known standardization organizations and that the efforts of Chinese parties are mainly limited to the Chinese CCSA standardization organization. It is interesting to know why this is the case. This could however be a blind spot in the conducted research.

We see a significant increase in the number of standards and the number of patents over the years. We expect that as the technology will continue to evolve, this upward trend will continue.

Lastly, we note that the diversity of contributors to standards and applicants for patents. For both, we see both universities and companies active. This indicates that quantum technology is beyond the stage of pure academic research, at least for some focus areas.

A.3 Long-list of the standards and standards-in-progress

Below we see a list of the current standards and the standards in progress. The standard name and the title of the standards is given. The standardization organization and the applicable subdomain are given between brackets.

— draft-dahlberg-ll-quantum-03: The Link Layer service in a Quantum Internet (IRTF, Quantum communication)

— draft-irtf-qirg-principles-02: Architectural Principles for a Quantum Internet (IRTF, Quantum communication)

— draft-van-meter-qirg-quantum-connection-setup-01: Connection Setup in a Quantum Network (IRTF, Quantum communication)

— draft-wang-qirg-quantum-internet-use-cases-02: Applications and Use Cases for the Quantum Internet (IRTF, Quantum communication)

— GR QKD 003 V2.1.1: Quantum key distribution (QKD); Components and Internal Interfaces (ETSI, Quantum key distribution)

— GR QKD 007 V1.1.1: Quantum key distribution (QKD); Vocabulary (ETSI, Quantum key distribution)

— GS QKD 002 V1.1.1: Quantum key distribution (QKD); Use Cases (ETSI, Quantum key distribution)

— GS QKD 004 V1.1.1: Quantum key distribution (QKD); Application Interface (ETSI, Quantum key distribution)

— GS QKD 005 V1.1.1: Quantum key distribution (QKD); Security Proofs (ETSI, Quantum key distribution)

— GS QKD 008 V1.1.1: Quantum key distribution (QKD); QKD Module Security Specification, (ETSI, Quantum key distribution)

— GS QKD 011 V1.1.1: Quantum key distribution (QKD); Component characterization: characterizing optical components for QKD systems, (ETSI, Quantum key distribution)

— GS QKD 012 V1.1.1: Quantum key distribution (QKD); Device and Communication Channel Parameters for QKD Deployment (ETSI, Quantum key distribution)

— GS QKD 014 V1.1.1: Quantum key distribution (QKD); Protocol and data format of REST-based key delivery API (ETSI, Quantum key distribution)

— ISO/IEC WD 23837-1: Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements (ISO, Quantum key distribution)

— ISO/IEC WD 23837-2: Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods (ISO, Quantum key distribution)

— IEEE P7130: Standard for Quantum Technologies Definitions (IEEE, Definitions)

— IEEE P7131: Standard for Quantum Computing Performance Metrics & Performance Benchmarking, (IEEE, Quantum computing)

— GR QSC 001 V1.1.1: Quantum-safe algorithmic framework (ETSI, PQC)

— GR QSC 003 V1.1.1: Case Studies and Deployment Scenarios (ETSI, PQC)

— GR QSC 004 V1.1.1: Quantum-Safe threat assessment (ETSI, PQC)

— GR QSC 006 V1.1.1: Limits to Quantum Computing applied to symmetric key sizes (ETSI, PQC)

— TR 103 570 V1.1.1: Quantum-Safe key Exchanges (ETSI, PQC)

- TR 103 617 V1.1.1: Quantum-Safe Virtual Private Networks (ETSI, PQC)
- Unknown 0: Mixing Preshared Keys in IKEv2 for Post-quantum Security (IETF, PQC)
- Unknown 1: Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2) (IETF, PQC)
- Unknown 2: Framework for networks supporting QKD (ITU, Quantum key distribution)
- Unknown 3: Security guidelines for applying quantum-safe algorithms in 5G system (ITU, Quantum key distribution)
- TR.sec-qkd: Technical Report: Security framework for quantum key distribution in telecom network (ITU, Quantum key distribution)
- X.cf_QKDN: Use of cryptographic functions on a key generated in quantum key distribution networks (ITU, Quantum key distribution)
- X.sec_QKDN_km: Security requirements for quantum key distribution networks - key management (ITU, Quantum key distribution)
- X.sec_QKDN_ov: Security requirements for quantum key distribution networks – overview (ITU, Quantum key distribution)
- X.sec_QKDN_tn: Security requirements for quantum key distribution networks - trusted node (ITU, Quantum key distribution)
- X.1702: Quantum noise random number generator architecture (ITU, PQC)
- Y.3800: Overview on Networks Supporting Quantum key distribution (ITU, Quantum key distribution)
- NIST PQC 1: PQC data encryption (NIST, PQC)
- NIST PQC 2: PQC digital signatures (NIST PQC)
- NIST PQC 3: PQC key encapsulation (NIST PQC)
- NIST PQC 4: PQC Stateful hash-based signatures (NIST, PQC)
- draft-ietf-ipsecme-ikev2-multiple-ke: Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IETF, PQC)
- draft-ietf-ipsecme-qr-ikev2-11: Mixing Preshared Keys in IKEv2 for Post-quantum Security (IETF, PQC)
- X.5Gsec-q: Security guidelines for applying quantum-safe algorithms in 5G systems (ITU, Quantum key distribution)
- FG QIT4N: Evolution and applications of quantum information technology for networks (ITU, Quantum communication)
- FG QIT4N: Terminology and use cases for QIT for networks (ITU, Quantum communication)
- SG17: Security (ITU, Quantum communication)
- QKDN_KM: Key management for Quantum key distribution network (ITU, Quantum key distribution)
- Y.QKDN_Arch: Functional architecture of the Quantum key distribution network (ITU, Quantum key distribution)
- Y.QKDN_CM: Control and Management for Quantum key distribution Networks (ITU, Quantum key distribution)
- Y.QKDN_SDNC: Software Defined Network Control for Quantum key distribution Networks (ITU, Quantum key distribution)

- Y.QKDN_BM: Business role-based models in Quantum key distribution Network (ITU, Quantum key distribution)
- Y.QKDN-req: Functional Requirements for Quantum key distribution Network (ITU, Quantum key distribution)
- NISTIR 6977: Vulnerabilities in Quantum key distribution Protocols (NIST, Quantum key distribution)
- NISTIR 8105: Report on Post-Quantum Cryptography (NIST, PQC)
- NISTIR 8240: Report on Post-Quantum Cryptography (NIST, PQC)
- Y.QKDN-qos-gen: General Aspects of QoS on the Quantum key distribution Network (ITU, Quantum key distribution)
- Y.QKDN-qos-req: Requirements for QoS Assurance of the Quantum key distribution Network (ITU, Quantum key distribution)
- IEEE PAR 1913: Software-Defined Quantum Communication (IEEE, Quantum communication)
- DGS/QKD-0013_TransModChar: Quantum key distribution (QKD); Characterization of Optical Output of QKD transmitter modules (ETSI, Quantum key distribution)
- DGS/QKD-015_ContIntSDN: Quantum key distribution (QKD); Control Interface for SDN (ETSI, Quantum key distribution)
- DGR/QKD-017_NwkArch: Quantum key distribution (QKD); Network architectures (ETSI, Quantum key distribution)
- DGS/QKD-0010_ISTrojan: Quantum key distribution (QKD); Implementation security: protection against Trojan horse attacks in one-way QKD systems (ETSI, Quantum key distribution)
- RGS/QKD-004ed2_ApplIntf: Quantum key distribution (QKD); Application Interface (ETSI, Quantum key distribution)
- RGS/QKD-0005ed2_SecProofs: Quantum key distribution (QKD); Security Proofs Revision (ETSI, Quantum key distribution)
- DGS/QKD-016-PP: Quantum key distribution (QKD); Common criteria protection profile for QKD (ETSI, Quantum key distribution)
- Unknown 3: Quantum Communication Terminologies and Definitions (CCSA, Definitions)
- Unknown 4: Quantum Secure Communication application scenario and requirements (CCSA, Definitions)
- Unknown 5: Quantum key distribution (QKD) application interface (CCSA, Quantum key distribution)
- Unknown 6: Technical requirements for quantum key distribution (QKD) systems Part I: Decoy-state BB84 (CCSA, Quantum key distribution)
- Unknown 7: Test methods of optical quantum key distribution (QKD) system (CCSA, Quantum key distribution)
- Unknown 8: Technical Specification of WDM Systems with the Support of Quantum key distribution (CCSA, Quantum key distribution)
- Unknown 9: Quantum Secure Communication Network Architecture (CCSA, Quantum communication)
- Unknown 10: Technical Requirements of Co-Fiber Transmission System for Quantum key distribution and Classic Optical Communication (CCSA, Quantum key distribution)

- Unknown 11: Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 1: Optical Source (CCSA, Quantum key distribution)
- Unknown 12: Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 2: Single photon detector (CCSA, Quantum key distribution)
- Unknown 13: Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 3: Quantum random number generator (QRNG) (CCSA, Quantum key distribution)
- Unknown 14: Requirements of encrypted data carried in MPLS PW in quantum secure communication network (CCSA, Quantum communication)
- Unknown 15: Study on security issues of Quantum key distribution (CCSA, Quantum key distribution)
- Unknown 16: Study on test and evaluation of Quantum Secure Communication System (CCSA, Quantum communication)
- Unknown 17: Study on the Co-Fiber Transmission of Quantum key distribution and Classic Optical Communication Systems (CCSA, Quantum key distribution)
- Unknown 18: Study on Generating and Testing method of Quantum Random Number (CCSA, PQC)
- Unknown 19: Study on quantum key distribution key components and modules technical requirements (CCSA, Quantum key distribution)
- Unknown 20: Study on Quantum Secure Communication Network Management (CCSA, Quantum communication)
- Unknown 21: Study on CV-QKD technique (CCSA, Quantum key distribution)
- Unknown 22: Study on software defined QKD network (CCSA, Quantum key distribution)
- Unknown 23: Study on trusted relay node in QKD network (CCSA, Quantum key distribution)
- Unknown 24: Study on Quantum Secure Communication Technology (CCSA, Quantum communication)
- Unknown 25: Study on optimization protocol based on decoy state methods (CCSA, Quantum communication)

A.4 Detailed tables of current standardization efforts related to quantum communication technologies

NOTE The overviews provided in this Annex A.4 were made mid-2020.

Table B.1 List of standards on security of cryptographic modules

Number	Name	Publ. date	SDO	Com-mittee	Subject	Category	Comment	Hyperlink
FIPS PUB 140-3	Security Requirements for Cryptographic Mod-ules	2019-03-22	NIST		General	Security		https://csrc.nist.gov/publications/detail/fips/140/3/final
EN ISO/IEC 19790:2020	Information technology - Security techniques - Se-curity requirements for cryptographic mod-ules (ISO/IEC 19790:2012, Corrected version 2015-12)	2020-03-18	CEN		General	Security		https://standards.iteh.ai/catalog/standards/cen/543fdbea-52bf-4549-8a5a-d07f8b91625b/en-iso-iec-19790-2020
ISO/IEC 15408-1:2009	Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Intro-duction and general model	2009-12; 2014-01	ISO/IEC		General	Security		https://www.iso.org/standard/50341.html

NOTE Existing standards in the field of QKD, as well as standards under development, are listed directly in the chapter 7 “Quantum Communication Systems.

Table B.2 List of standards on QRNG technology

Number	Name	Publ. Date	SDO	Committee	Subject	Category	Comment	Hyperlink
Recommendation for the generation of random bits								
SP 800-90A Rev. 1	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	2015-06	NIST		RNG	General	Deterministic methods	https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final
SP 800-90B	Recommendation for the Entropy Sources Used for Random Bit Generation	2018-01	NIST		RNG	General	Design and test of entropy sources	https://csrc.nist.gov/publications/detail/sp/800-90b/final
SP 800-90C (Draft)	Recommendation for Random Bit Generator (RBG) Constructions	In draft	NIST		RNG	General	Using 800-90A and 800-90B	https://csrc.nist.gov/publications/detail/sp/800-90c/draft
Testing								
AIS 20	W. Schindler: AIS 20: Functionality classes and evaluation methodology for deterministic random number generators, Version 2.0, English Translation	1999-12-02	BSI		RNG	Testing		https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_Functionality_Classes_Evaluation_Methodology_DRNG_e.html

Number	Name	Publ. Date	SDO	Committee	Subject	Category	Comment	Hyperlink
AIS 31	W. Killmann, W. Schindler : A Proposal for: Functionality Classes and Evaluation Methodology for True (Physical) Random Number Generators, Version 3.1, English translation	2001-09-25	BSI		RNG	Testing		https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_evaluation_methodology_for_true_RNG_e.html
	W. Killmann, W. Schindler, "A proposal for: Functionality classes for random number generators“, Version 2.0	2011-09-18	BSI		RNG	General		https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.html https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_Functionality_classes_for_random_number_generators_e.html
	Evaluation of random number generators Version 0.10	2013	BSI		RNG	Testing		https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_AIS_31_Evaluation_of_random_number_generators_e.pdf?__blob=publicationFile&v=1
ISO/IEC 18031 :2011	Information technology — Security techniques — Random bit generation	2011-11	ISO/IEC		RNG	General	Specifies main characteristics and security requirements	https://www.iso.org/standard/54945.html

Number	Name	Publ. Date	SDO	Committee	Subject	Category	Comment	Hyperlink
ISO/IEC 18031: 2011/AMD 1:2017	Information technology — Security techniques — Random bit generation — Amendment 1: Deterministic random bit generation	2017-02	ISO/IEC		RNG	General		https://www.iso.org/standard/63755.html
ISO/IEC 20543 :2019	Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408	2019-10	ISO/IEC		RNG	Testing		https://www.iso.org/standard/68296.html
X.1702	Quantum noise random number generator architecture	2019-11-13	ITU-T	SG13	QRNG	General	Recommendation	https://www.itu.int/rec/T-REC-X.1702
SP 800-22 Revision 1a	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	2020-04	NIST		RNG	Testing		https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

Number	Name	Publ. Date	SDO	Committee	Subject	Category	Comment	Hyperlink
TestU01	Pierre L'Ecuyer and Richard Simard, TestU01 A Software Library in ANSI C for Empirical Testing of Random Number Generators, 2013	2009-08-18	U Montreal		RNG	Testing		http://simul.iro.umontreal.ca/testu01/tu01.html
Ent	John Walker. Ent: A pseudo-random number sequence testing program	2008-01-28	Fourmilab		RNG	Testing		http://www.fourmilab.ch/random/
ANSI X9.82-1-2006 (R2013)	Random Number Generation - Part 1: Overview and Basic Principles.	2006-07-26	ANSI	ASC-X6	RNG	General		https://webstore.ansi.org/standards/ascx9/ansix9822006r2013
ANSI X9.82: Part 2-2015	Random Number Generation - Part 2: Entropy Sources.	2015-09-25	ANSI	ASC-X7	RNG	General		https://webstore.ansi.org/standards/ascx9/ansix982part2015
ANSI X9.82: Part 3-2007 (R2017)	Random Number Generation - Part 3: Deterministic Random Bit Generator Mechanisms.	2011-11-11 2017-02-01	ANSI	ASC-X8	RNG	General		

Number	Name	Publ. Date	SDO	Committee	Subject	Category	Comment	Hyperlink
ANSI X9.82: Part 4–2011 (R2017)	Random Number Generation - Part 4: Random Bit Generator Constructions.	2007-09-11 2017-01-27	ANSI	ASC-X9	RNG	General		https://webstore.ansi.org/standards/ascx9/ansix982part2011r2017

A.5 Standards for quantum sensing and quantum metrology

No standards for quantum sensing and quantum metrology have been identified at the time of writing this Annex.

Annex B

Cryogenic solid-state quantum computing

B.1 Scope and objectives

The scope of this annex are the hardware layers and control software dedicated to cryogenic solid state quantum computing. This is an architecture family of which all members make use of a cryogenic fridge, and where the quantum device(s) are controlled from outside the fridge by room-temperature control electronics. Consequently, a huge number of I/O channels is required to interconnect the qubits within these quantum devices with room temperature electronics.

So far, the following members have been identified within this architecture family: superconducting transmons, superconducting flux qubits, semiconductor spin qubits, topological qubits and artificial atoms in solids.

The objective is to create a first document, out of a series of documents, that is restricted to provide functional descriptions of the involved layers and to identify associated functional requirements. The specification of limiting requirements and associated values is explicitly out-of-scope of this first document. On the other hand, descriptions of multiple best-practices on implementations are within scope as long as their description does not exclude similar other solutions.

As such, this annex may serve as a good starting point for collecting ideas to feed initial standards on cryogenic quantum computers.

B.2 Normative references

[1] <a first reference>

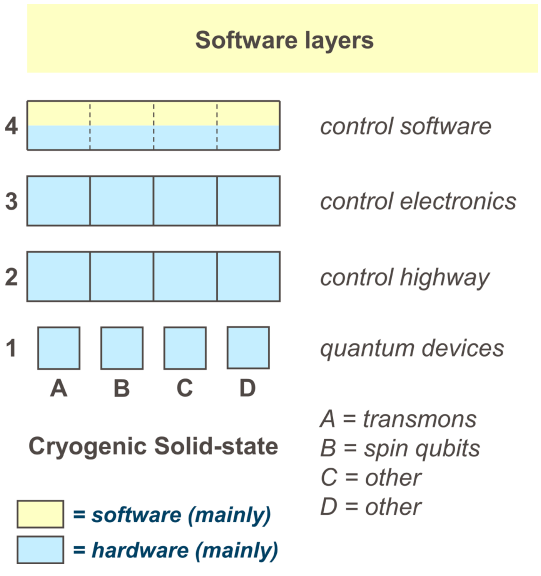
[2] <more references as needed>

B.3 Terminology and abbreviations

B.3.1 Terminology

For the purposes of the present document, the following terminology and definitions apply:

Hardware stack
A layered description of functionality covering a specific quantum computing architecture family accounting for different members. Cryogenic solid-state quantum computers is an example of such an architecture family, and implementations based on transmons and spin-qubits are examples of its members. Where needed, a layer may distinguish between different solutions for different members, and may consist of hardware and/or (low level) software.



Quantum devices
The modules in hardware layer 1 that are typically operating at cryogenic temperatures and may be implemented as chip and/or on PCB.

Control highway
The modules in hardware layer 2 that cover all infrastructure needed for transporting microwave, lightwave, RF and DC signals (via electrical and/or optical means) between the control electronics at room temperature and the quantum devices at cryogenic temperatures. It is a mix transmission lines, filtering, attenuation, amplification, (de)multiplexing, etc. A huge number of control channels are required to control many qubits in a single fridge (which clarifies the name) and this can easily become very bulky.

Control electronics
The modules in hardware layer 3 that cover all room-temperature electronics for generating, receiving, and processing microwave, lightwave, RF and DC signals. Some implementations make use of routing/switching and/or multiplexing of control signals at room temperatures. It may have some firmware on board to guide the signal generation and signal processing.

Control software
The modules in layer 4, which can be a mix of hardware and low-level driver software, for instructing the control electronics. It may also have means to enable calibrating and benchmarking purposes. It has a software interface to higher layers for receiving sequences of instructions about when, where and what pulses are to be generated.

B.3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

FGQT CEN/CENELEC Focus Group on Quantum Technologies

PCB Printed Circuit Board

DC Direct Current

RF Radio Frequent

B.4 Overview of concepts

A quantum schedule describes when which operation should be applied on what. At the gate level, the quantum schedule is equivalent to a circuit diagram. A circuit diagram specifies the order in which gates and measurements are applied to qubits. At the pulse level, the quantum schedule is equivalent to a pulse diagram. A pulse diagram specifies at what time, which pulses are applied to which location on a quantum device (a port) and at which frequency (a clock). The hardware-instruction level description specifies when which instructions need to be executed in the control electronics in order to generate the desired pulses at the quantum device. The hardware-instruction level description is implementation-specific.

Table B.1 Overview of concepts and their representation at different levels of abstraction

	Abstraction layer	**Quantum-circuit level**	**Quantum-device level**
	Describes	Gates acting on ideal qubits	Signals on a quantum device
When	Schedule	Order of operations	Timing of operations
What	Operation	Unitaries and POVMs	Parameterized wave-forms and acquisition protocols
Where	Resource	Qubits	Ports & clocks

EXAMPLE Resources on a transmon device

Resources denote where an operation should be applied. Here we explain these concepts using a simple cQED device shown in Figure B.1. These concepts should be easy to generalize to other devices and systems.

For many systems, it is possible to associate a qubit with an element or location on a device that a signal can be applied to. We call such a location on a device a port. Here, qubits and ports are represented as strings (e.g., P0, feedline_in, q0:mw_drive, etc.). A port can be associated with a qubit by including the qubit name in the name of the port (separated by a colon :).

Besides the physical location on a device, a pulse is typically applied at a certain frequency. A reference clock can be used to track the phase of a certain transition or simply to ensure the signal ends up at the right frequency. Similar to ports, reference clocks can be associated with qubits by including it in the name, but this is not required to account for non-qubit elements. If the frequency of a clock is set to 0 (zero), the pulse is applied at baseband and is assumed to be real-valued.

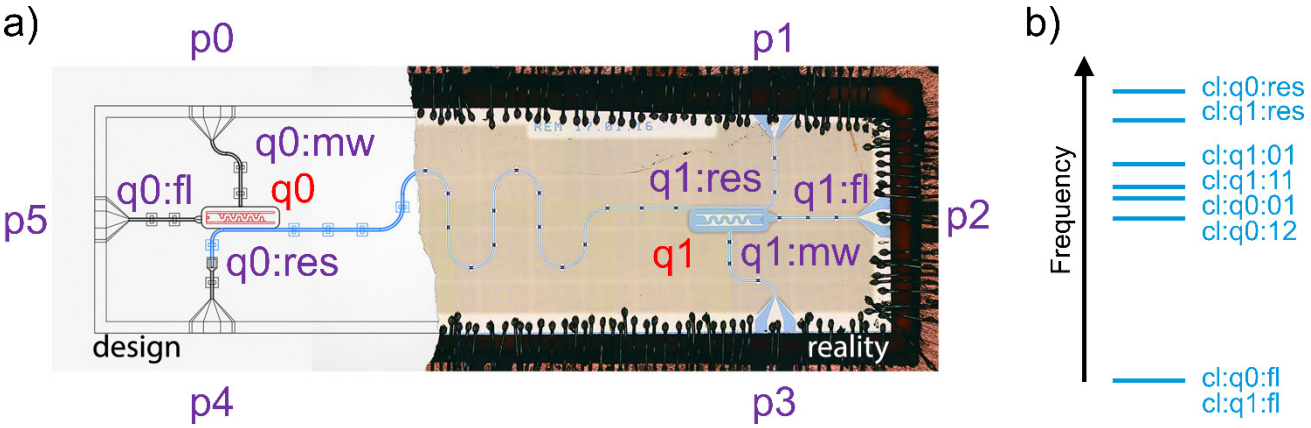


Figure B.1 Device image [109]

Resources are used to indicate on what operations are applied. (a) Ports (purple) indicate a location on a device. By prefixing the name of a qubit in a port name (separated by a colon :) a port can be associated with a qubit (red), but this is not required. (b) Clocks (blue) denote the location in frequency space and can be set to track the phase of a known transition. By prefixing the name of a qubit in a clock name (separated by a colon :) a clock can be associated with a qubit (red), but this is not required.

B.5 Layer 1 – Quantum devices

Quantum devices of cryogenic solid state quantum computers are typically operating at cryogenic temperatures. They may be implemented stand-alone, as chip and/or on PCB.

This section is currently a place holder for functional descriptions and associated functional requirements, to be elaborated in further detail during a follow-up activity.

The functional requirements may identify topics such as materials compatibility, shielding, operating temperature, electrical and magnetic aspects, vacuum properties, etc.

B.6 Layer 2 – Control highway

B.6.1 General

The control highway enables the transportation of downstream and upstream signals between control electronics, operating at room temperature, and quantum devices, operating at cryogenic temperatures.

Figure B.2 shows an *example* of a possible control highway dedicated to a *transmon* quantum computer. The I/O channels of *spin-qubit* quantum computers may be different, but this example alone may be sufficient to get basic understanding of various functional requirements for future standardization.

In this example, the I/O of each qubit is handled via three channels: one for microwave control signals, another one for flux control and a third one for read-out. The response signals of two or more qubits may share a common read-out channel to reduce the overall number of channels. Travelling wave amplifiers may be used for amplifying these response signals, and they need an extra TWPA pump channel for powering. As such, a 50 qubit transmon quantum computer may have 102 or more I/O channels.

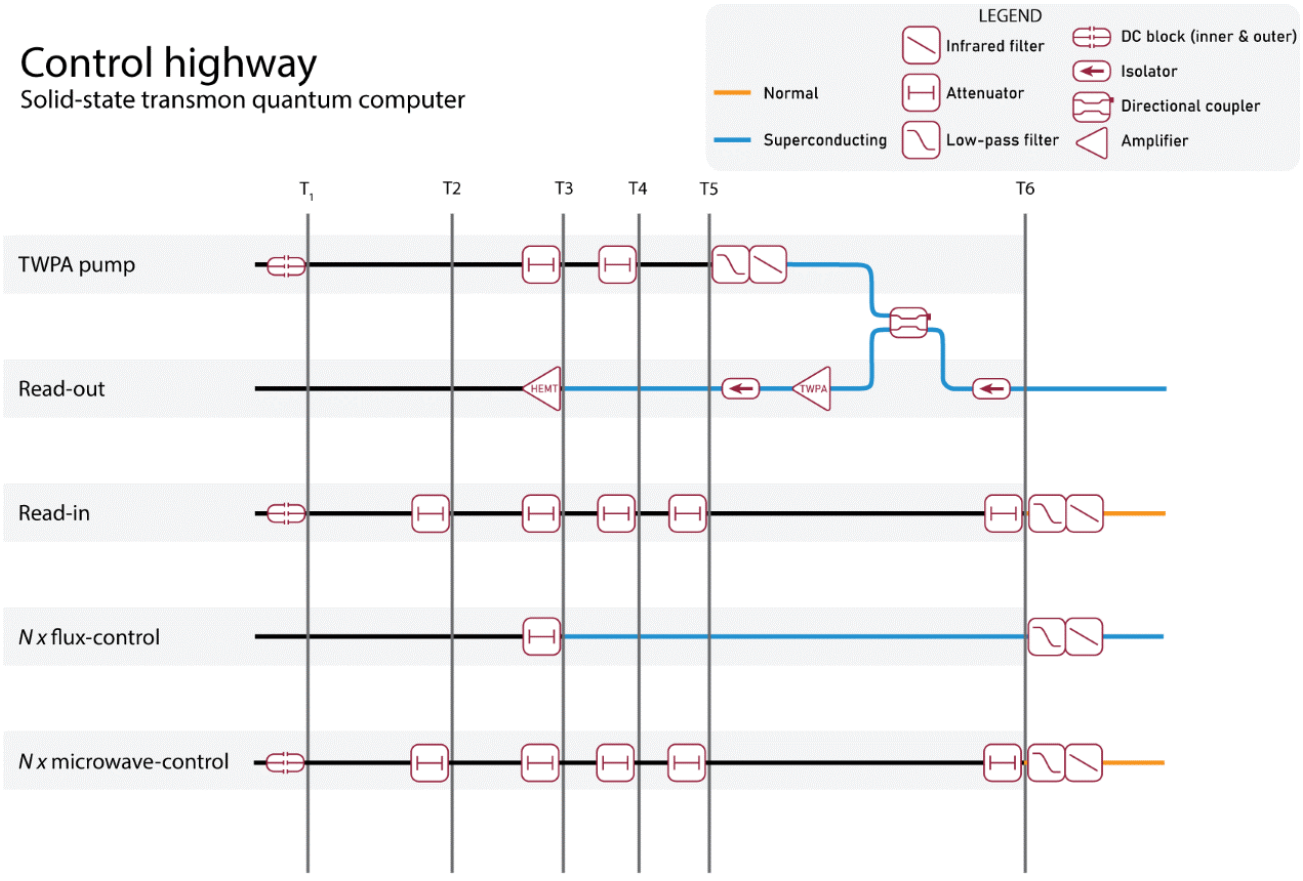


Figure B.2 An example of a control highway applicable to a particular transmon architecture

The involved I/O channels may be build-up from a variety of building blocks, for instance from transmission lines, attenuators, directional couplers, low-pass filters, infra red filters, DC-blocks, superconducting sections, amplifiers, isolators, circulators as well as thermalization means and vacuum feed troughs.

B.6.2 Consideration of relevant requirements

The *transmission requirements* on the control highway are to be defined in detail, and these requirements are highly dependent on the specific architecture and use case. The same applies to various *interconnection* and *footprint requirements.* But there are more issues of relevance that are to be specified, which may be less obvious. Their relevance is explained below.

Heat flow considerations. A cryogenic fridge cools the setup in multiples stages, with temperatures from T1, T2, T3, and so on, down to the lowest temperature; usually down to the milli-Kelvin range. The control highway has to bridge a temperature drop of about 300 K, and these channels will leak heat from room temperature into the fridge down to the quantum device. This will challenge the cooling mechanism of the fridge, and may prevent desired temperatures at the quantum device. Most of the heat flows through the metallic parts of the cabling, mainly through the shielding of coaxial cabling or ground planes of stripline cabling.

To minimize that heat flow, the cabling should have low thermal conductance, and be thermalized at each temperature stage. Most of the heat flow through the cabling will then flow via the thermalization into the cooling mechanism. The residual heat flow to a next stage in the fridge will then be minimized.

A superconducting transmission line at one of the bottom sections may be used to reduce the heat flow even further. Superconductors tend to combine low thermal conductance with high electrical conductance, which is the opposite behaviour of metals.

Due to the large number of channels, this thermal leakage cannot be ignored and puts limits on the lowest temperatures that can be achieved since the cooling capacity of the fridge is limited. This puts a maximum on the number of channels.

This explains the need of various *thermal requirements* on the control highway as a whole.

Noise considerations. Each I/O channel suffers from adding some noise to the signal. Even passive lines generate at least thermal noise. Without any loss in a channel, and (hypothetical) noise-free control electronics, this noise would be at least the thermal noise of a 50 ohm resistor at room temperature. Therefore, attenuators are placed at different temperature stages, to achieve noise temperatures that are only slightly above the temperature of each stage. Attenuation values between 40 to 80 dB are not uncommon.

The lowest achievable noise level (in absence of any signal) occurs when all attenuation is concentrated in the stage with the lowest temperature. However, under operational conditions, signals will be dissipated in the attenuators, which is the reason why attenuation has to be distributed. The reason is explained below.

— At first, the dissipation of signal in the attenuator results in more heat power that should flow away via the cooling mechanism of the fridge. Since this cooling capacity is limited, with the lowest capacity at the coolest stages, this dissipation can easily overload the cooling. This is one reason why attenuation has to be *distributed*, which also increases the noise at the end of the chain.

— Secondly, the dissipation of signal power in the attenuator will increase the *hot-spot temperature* of the internal resistors. That temperature will raise above the outside temperature of the attenuator, which is usually thermalized at the stage temperature. This raise increases the thermal noise as well, which will be most pronounced by the last attenuator at the lowest temperature. Preventing all dissipation at a single spot by proper distribution of attenuation will reduce this noise. So even with infinite cooling capacity, attenuation has to be distributed because of noise.

— The increase of hot-spot temperature can be reduced by effective *hot-spot cooling*. It requires attenuators with high thermal conductance between internal hot spots and external thermalization points. Unfortunately, the thermal conductance of many materials is low at cryogenic temperatures, which challenges effective hot-spot cooling.

This may illustrate that effective hot-spot cooling and distribution of attenuation is essential to minimize the noise at the end of the I/O chain. The optimum distribution is use-case dependent, such as available cooling capacity of the fridge and used signal powers.

This explains the need of various *noise requirements* on the control highway as a whole.

Vacuum considerations. A vacuum is needed as heat insulation to reach the low temperatures for cryogenic quantum devices. Once a vacuum pump has achieved the desired vacuum level, leakage from outside will gradually raise this level. It may be obvious that this puts strong vacuum requirements on the feed-throughs between outside and inside the fridge.

In addition, materials inside vacuum, and cavities within constructions, may suffer from *out-gassing.* This will gradually fill the vacuum with unwanted particles. And even when this out-gassing stops after a while, it may occur again after reopening the fridge when materials and cavities act like a sponge.

But outgassing is also strongly temperature dependent. At low temperatures almost all outgassing is stopped since most materials will freeze at cryogenic temperatures. This may suggest that outgassing is mainly a room-temperature issue.

However the main problem with leaks and outgassing is that the gases may condense and freeze at the colder parts of a cryostat which dissipates energy and uses part of the available cooling power. This explains the need of various *vacuum requirements* on the control highway as a whole.

B.6.3 Functional description

These requirements could involve:

— Functional description of all I/O chains, including length of each temperature stage, position of thermalization and desired components in each chain. It could highlight typical differences between solutions for transmons, spin-qubit and others;

— Description of additional means to simplify characterization, inspection and/or calibration of the overall setup;

— Description of signal levels, shapes and frequency bands for both downstream and upstream I/O channels.

B.6.4 Transmission requirements

These requirements could involve:

— Requirements on step and/or impulse *response* of the full chain, when the chain is terminated by a realistic impedance. This could involve rise-time, overshoot, and ringing. Note that when the impedance of a quantum device is quite different from 50 ohm, it may not be useful to specify response under 50 ohm conditions.

— Design values (target) as well as masks for upper and lower limits of the *transmission* in the desired pass-band of interest when the chain is terminated by a realistic impedance. This could be offered for the full chain, as well for each stage and/or segment/component. Note that requirements on *reflection* can be made superfluous by setting meaningful transmission and response requirements on the full chain

— Masks for upper limits on low-pass filtering for *out-of-band* frequencies. These masks may be specified up to one or two decades above the highest pass-band frequencies, to reduce out-of-band noise

(IR-filtering). If pulses are to be modulated on 8 GHz, these masks may even be specified up to 100GHz or more.

— Requirements on DC/low-frequency characteristics, for instance to separate bias currents from signals. When the pass-band has a lowest break frequency, then the design of that separation can be simplified if that break frequency can be set as high as possible. This could involve DC-resistance as well, if a particular channel should operate from DC.

— Requirements on EL-FEXT (Equal-Level Far End Crosstalk) between I/O channels. This is the ratio between signal level and crosstalk level (from another channel), as observed at the end of an individual I/O channel. EL-FEXT is indicative for the expected signal-to-noise ratio in each channel, which requires the cumulation of crosstalk from all other channels.

— Requirement on NEXT (Near End Crosstalk) from a downstream I/O channel to an upstream I/O channel. Note that requirements on NEXT between two downstream channels can be made superfluous when meaningful EL-FEXT requirements are set.

B.6.5 Thermal requirements

These requirements could involve:

— Maximum passive heat flow through an I/O channel;

— Requirements on superconducting sections, for reducing the heat flow;

— Maximum signal dissipation in each stage (attenuators), at given signal power, to prevent that the resulting active heat flow overloads the cooling capacity per stage;

— Transversal thermal conductivity of an I/O channel near thermalization clamps;

— Transversal thermal conductivity of attenuators to minimize raise of hot-spot temperatures.

B.6.6 Noise requirements

These requirements could involve:

— Requirements on maximum thermal noise temperatures at the end of downstream I/O channels, under passive conditions (in absence of any signal);

— Requirements on hot-spot cooling and distribution of attenuators to restrict the raise of noise temperatures. These raises occur when signals are heating-up attenuators and therefore produce higher thermal noise levels. Such raise may be too high when the locations of the attenuators are sub-optimal and/or the cooling of hot-spots inside attenuators is inadequate;

— Requirements on noise generated within cryogenic amplifiers.

B.6.7 Vacuum requirements

These requirements could involve:

— Leakage requirements on the vacuum feed-through;

— Out-gassing requirements of the used materials and constructions.

B.6.8 Shielding and magnetic requirements

These requirements could involve:

— Non-magnetic requirements of dedicated connectors and other devices;

— Shielding around (groups) of I/O channels and components;

— Residual magnetic fields allowed in shielded environment;

— Maximum external magnetic fields to avoid saturation of shields.

B.6.9 Interconnection requirements

These requirements could involve:

— Interconnection between I/O chains and quantum devices. This may be performed by specifying preferred connectors or by specifying geometries to make a more permanent interconnection between cabling and these devices;

— Interconnection between I/O chains and control electronics. This may be performed by specifying preferred (bus) connectors;

— Means for organizing a massive number of wiring between fridge and control electronics. It could be performed by specifying lengths of cabling outside the fridge or preferred intermediate (bus) connectors at some patch panel outside the fridge.

B.6.10 Footprint requirements

These requirements could involve:

— Mechanical/dimensional requirements on thermalization clamps around cabling;

— Mechanical/dimensional requirements on vacuum feed-throughs;

— Mechanical/dimensional requirements on holes in the plates on each stage;

— Ways to organize thousands of channels for controlling > 1000 qubits in a single fridge.

B.7 Layer 3 – Quantum control electronics

The control electronics is primarily intended for generating the desired pulses to control the quantum devices in layer 1, and to read-out their response. It covers all room-temperature electronics for generating, receiving, and processing microwave, lightwave, RF and DC signals. Some implementations make use of routing/switching and/or multiplexing of control signals at room temperatures. It may have some firmware on board to guide the signal generation and signal processing.

This section is currently a place holder for functional descriptions and associated functional requirements, to be elaborated in further detail during a follow-up activity.

The functional description may include the blocks for generating and detecting pulses, as well as for multiplexing and/or routing/switching functionality (when appropriated). It may also describe various best-practices on interfacing with the control software in layer 4.

The functional requirements may identify topics such as signal levels, pulse shapes, noise, sensitivity, dynamic range, etc.

B.8 Layer 4 – Quantum control software

This layer covers hardware-specific software to control what pulses are to be generated by the control electronics in layer 3, and also covers all kinds of means for calibration and benchmarking the system as a whole and how to interface with higher software layers.

This section is currently a place holder for functional descriptions and associated functional requirements, to be elaborated in further detail.

The functional description may include the needs for enabling calibration and benchmarking

Annex C

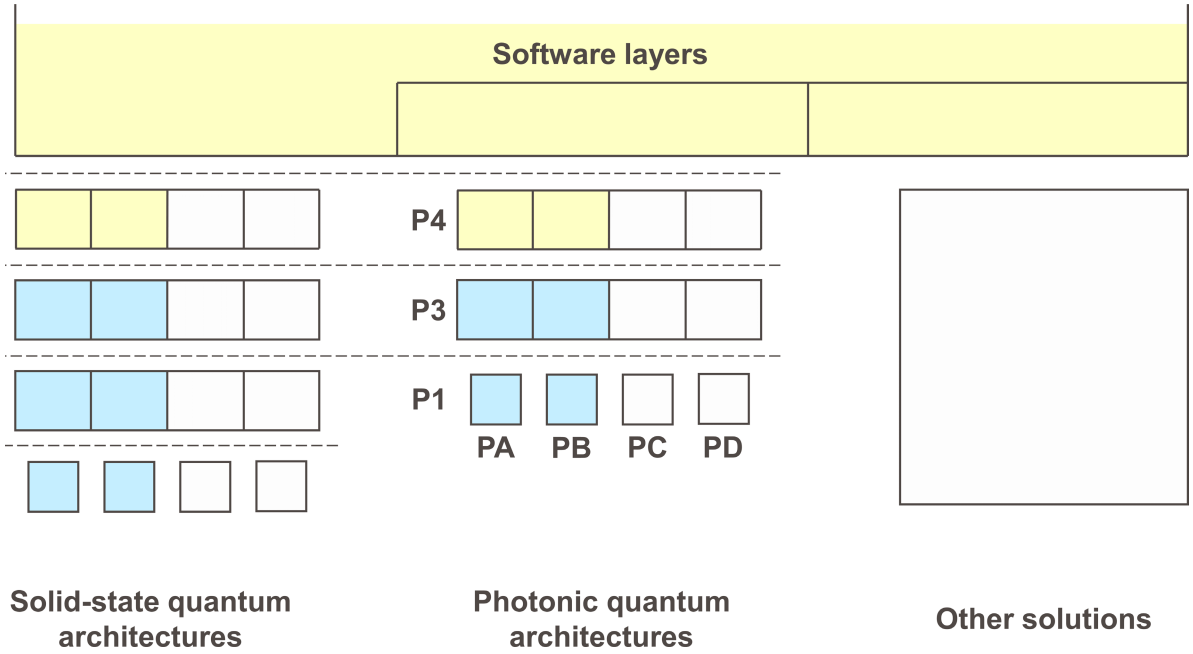
Photonic quantum computing

C.1 Scope and objectives

The aim of this annex is to break-down the hardware stack of quantum computers based on photonic architectures into smaller layers and modules. The functionality of each of the identified modules must be identified in such a manner that they can interwork with each other via well-defined interfaces. This annex is also the natural place to collect what kind of requirements on these modules deserve a specification in future standards. The specification of actual values is beyond the scope of this present annex.

As such, the structure identified in this annex could grow into a (future) dedicated standard on photonic quantum computing.

C.2 Terminology



Key

	Layers		Architectures
P1	Quantum photonic devices	PA	Boson sampling
P3	Quantum control Electronics	PB	Gate based quantum computing
P4	Quantum control Software	PC	(some future development)
		PD	(some other future development)

Figure C.1 A possible break-down into various modules for photonic quantum computing architectures

C.3 Functional description of a quantum photonic processor

C.3.1 Quantum photonic processor

A linear quantum photonic processor is a multimode quantum interferometer, which can perform any unitary transformation on the creation and annihilation operators of a photonic quantum state. This state is a superposition of creation and annihilation operators of the optical modes of the interferometer. The user is responsible for the photonic quantum state that serves as the input to the processor. The unitary transformation of the creation and annihilation operators is fully controllable by the user. These devices have multiple applications in photonic quantum computing. For example, linear gates can be encoded in combination with photonic qubit encoding. Also, they can be used to implement (Gaussian) boson sampling. For this application certain optimization problems can be mapped onto unitary transformation that are implemented on the quantum photonic processor. A certain quantum photonic state can then be sent through the processor and the resulting output distribution will correspond to the optimal solution or an approximation of the optimal solution for the implemented optimization problem.

C.3.2 Optical interface

The main component of a quantum photonic processor is a photonic integrated circuit (PIC), which interfaces with the user via optical fibres. The PIC contains a network of interconnected waveguides. These waveguides support only a single polarization and can be designed for a specific wavelength. The photonic quantum state enters and exits the PIC via polarization maintaining optical fibres. The wavelength and polarization of the input state must match the design wavelength of the PIC.

C.3.3 Photonic integrated circuit components and layout

C.3.3.1 General

The most fundamental components of a quantum photonic processor are waveguides, couplers, and phase delays. A waveguide guides the light over the processor without altering the photonic state it is guiding. Two waveguides can be connected by a coupler. In the coupler, the photons have a probability of coupling to the other waveguide depending on the coupling ratio of the coupler. A coupler is created by bringing two waveguides close enough together so that guided modes can evanescently couple from one waveguide to another. A phase delay adds an additional phase to photons passing through that component. A phase delay can be induced through various means. The thermo-optic effect, where the refractive index of a material changes with temperature, can be used to create a phase delay in a waveguide by heating it using resistive heaters. Additional stress in a waveguide also changes its refractive index. This can be induced using piezo-electric tuners.

C.3.3.2 Unit cell

With the fundamental linear quantum photonic processor components, a unit cell can be defined that allows for all arbitrary unitary transformations on two modes. There are multiple possibilities to define a unit cell. An example is shown in Figure C.1. This example consists of a tuneable beam splitter (TBS), designed as a Mach-Zehnder interferometer (MZI), and a phase shifter (PS). The TBS controls the interference between the two modes and the phase shifter controls the phase of the two output modes. The PS induces a phase delay on one of the waveguides to create a phase difference between them. The configuration shown in Figure C.1 is an example of an asymmetric unit cell where there is tuning element on only one of the arms of the MZI. Symmetric designs are also possible with tuning elements on both arms of the MZI. A symmetric unit cell does not require tuning elements outside of the MZI.

C.3.3.3 Network

Unit cells are combined into a network with a specific topology such that it can perform any unitary transformation on the creation and annihilation operators of the state, see Figure C.3 for an example. A square topology is shown in Figure C.3 [110], but other topologies such as a triangular layout [111] also exist.

C.3.4 Implementing unitary transformations

A unitary transformation is implemented on the network by setting the phase shift of each unit-cells' TBS and PS. The phase is set by applying a specific voltage across the resistive heaters or piezo-electric tuner. The voltage-phase relation is determined by characterizing the phase delays. The phases that are required to implement the unitary are determined by performing a decomposition algorithm on the unitary. The decomposition algorithm depends on the structure of the network and of the unit-cells [110, 111].

To implement a specific transformation, the user passes the phases necessary for that transformation to the quantum photonic processor. Another possibility is that the quantum photonic processor accepts a unitary transformation directly and performs the decomposition

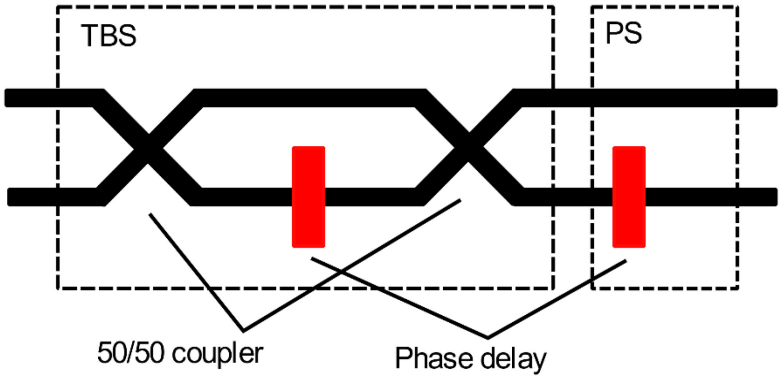


Figure C.2 An example of a unit cell in a quantum photonic processor. The unit cell consists of two input and output waveguides on which a tuneable beam splitter (TBS) and a phase shifter (PS) are applied. The TBS is built of a Mach-Zehnder interferometer (MZI), which consists of two 50/50 couplers and a phase delay on one of the arms. The TBS can be tuned to a specific splitting ratio by tuning the phase delay. The PS consists of a phase delay on one of the two arms, which induces a tuneable phase difference between the two arms.

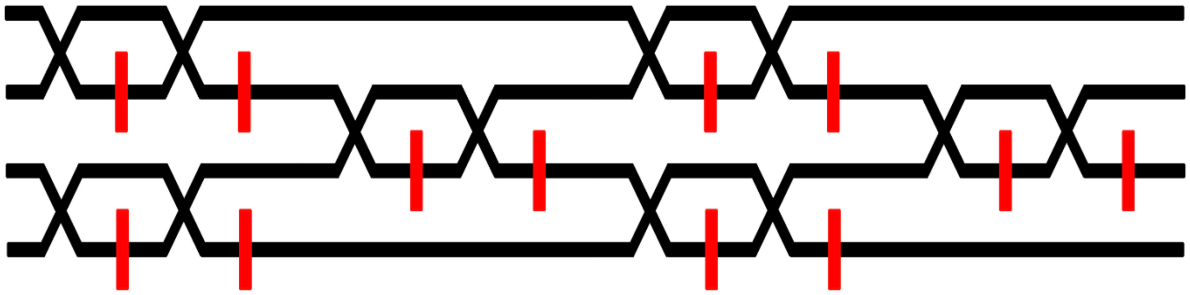


Figure C.3 An example network of a 4 mode quantum photonic processor. Six unit cells are combined using the architecture of Clements [110].

C.4 Quantum photonic devices

C.4.1 Introduction

This section contains all quantum photonic devices that are necessary for a photonic quantum computing architecture. This includes sources, detectors, (non)linear optical devices, and feedback mechanisms. These elements can be combined in various ways to create different types of photonic quantum computers. For example, a boson sampler needs a set of photon sources, a photonic processor (linear optical device) and a set of photon detectors.

The different devices are shown in Figure C.4 where the devices are split up into minimally required devices and additional devices. The minimally required devices for a photonic quantum computer are sources, detectors, and linear optics. The additional devices are nonlinear optics and feedback. They add functionality and allow for different computing protocols to be used and therefore allows different applications to be run.

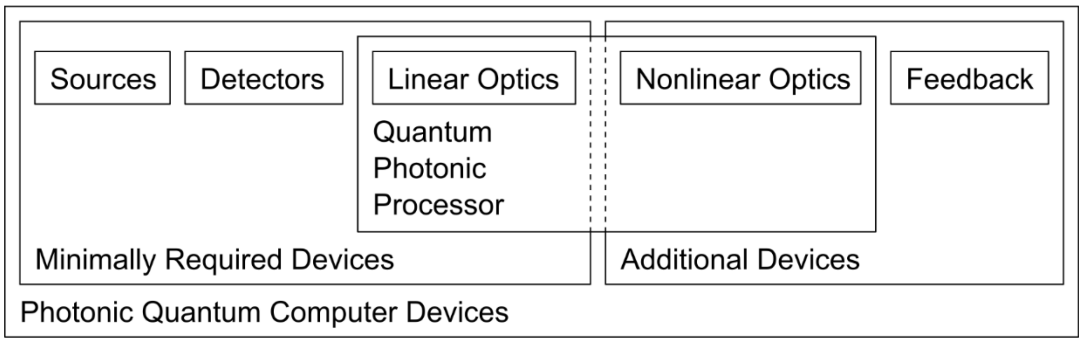


Figure C.4 A diagram of the photonic quantum computer devices organized into several categories. The devices are split up into minimally required devices and additional devices, where sources, detectors and linear optics belong to the former category, and nonlinear optics and feedback to the latter. A quantum photonic processer consists of linear optical devices, but it can also include nonlinear optical devices.

C.4.2 Photonic sources

Examples of various elements are listed below together with their requirements:

— Examples:
  - Spontaneous Parametric Down-Conversion (SPDC);
  - Quantum dot;
  - Ring resonator;
  - etc.;

— Requirements:
  - Generation rate (number of photons per second);
  - Wavelength (centre wavelength of the photon's spectrum);
  - Spectrum (wavelength distribution of the photons);
  - Repetition rate of pump laser;
  - Efficiency (probability of generating a single photon (pair) per pump pulse);

— Distinguishability (wavefunction overlap integral of the photons).

C.4.3 Photonic detectors

— Examples:
  - Avalanche Photo Diode (APD);
  - Superconducting Nanowire Single-Photon Detector (SNSPD);
  - Photon Number Resolving Detector;
  - etc.;
— Requirements:
  - Efficiency as a function wavelength (probability that a photon with a specific centre wavelength is detected);
  - Dark counts (number of detections per second without incoming photons);
  - Jitter (timing inaccuracy);
  - Dead time (time that detectors are insensitive to incoming photons after a detection event);
— Pulse shape (temporal shape of the electrical signal generated by the detectors).

C.4.4 Linear optics

— Examples:
  - Waveguides;
  - Directional couplers;
  - Ring resonators;
  - Tuneable beam splitters;
  - Phase shifters;
  - etc.;
— Requirements:
  - Loss;
  - Fidelity, measure of accuracy for operation implementation;
  - Tunability, degree of control over the operations;
  - Dispersion;
  - Number of input and output modes (physical waveguides);
— Circuit depth, number layers of optical elements.

C.4.5 Nonlinear optics

— Examples:
  - Quantum dot;
  - Doped waveguide (gain region);
  - etc.;
— Requirements:
  - Loss;
  - Gain;

- Efficiency;

— etc.

C.5 Quantum control electronics

This section contains all electronics that is needed to control the quantum devices in lower layers. And the connections to a PC so that the control signals can be sent to the control electronics.

— Examples:
  - TEC + PID;
  - Drivers for tuneable elements on photonic processor;
  - (Micro)Processor for drivers and TEC;
  - Time tagger for detector signals;
  - (Bias current source for detectors);
  - Connection hardware (USB/COM);
— Requirements:
  - to be identified.

C.6 Quantum control software

This layer contains the low-level driver software that is needed to drive the control hardware and communicate with higher software layers.

Covers:

— Software driver.

Requirements:

— Connection protocol (for instance serial or API);

— Speed;

— Features.

Literature

[1] A. de Touzalin, C. Marcus, F. Heijman, I. Cirac, R. Murray, T. Calarco, „Quantum manifesto: A new era of technology," p. 20, 2016.

[2] O. van Deventer, N. Spethmann, M. Loeffler *et al.*, „Towards European Standards for Quantum Technologies," *EPJ Quantum Technologies 9, 33,* 2022.

[3] R. Lewis, M. J. Everitt, „Special Issue on Quantum Standardization," *EPJ Quantum,* 2022-2023.

[4] D. Castelvecchi, „Europe shows first cards in €1-billion quantum bet," *Nature,* Nr. 563, pp. 14-15, 2018.

[5] Qureca, „Overview on quantum initiatives worldwide – update 2022," 10 3 2022. [Online]. Available: https://qureca.com/overview-on-quantum-initiatives-worldwide-update-2022/.

[6] N. Mohr, M. Masiowski, M. Zesko, H. Soller, „Quantum Technology Monitor," p. 53, 2022.

[7] E. B. Kania, „China's Quantum Future: Xi's Quest to Build a High-Tech Superpower," *Foreign Affairs,* 26 September 2018.

[8] US National Science and Technology Council, „National Quantum Initiative Supplement to the Presidents FY 2022 Budget," 12 2021. [Online]. Available: https://www.quantum.gov/wp-content/uploads/2021/12/NQI-Annual-Report-FY2022.pdf.

[9] C. Monroe, *American Leadership in Quantum Technology,* Washington D.C.: US Government., 2017.

[10] European Quantum Flagship, „The Quantum Flagship officially presents the Strategic Research Agenda to the European Commission," 3 3 2020. [Online]. Available: https://qt.eu/app/uploads/2020/04/Strategic_Research-_Agenda_d_FINAL.pdf.

[11] A. Jenet, C. Trefzger, A. M. Lewis, F. Taucer, L. Van Den Berghe, A. Tüchler, M. Loeffler, S. Nik, „Standards4Quantum - Making Quantum Technology Ready for Industry," *JRC Conference and Workshop Report,* 2020.

[12] A. Jenet, C. Trefzger, F. Taucer, A. M. Lewis, L. Van den Berghe, A. F. Tuechler, S. Nik, „Making Quantum Technology ready for Industry," *JRC Science for Policy Briefs 2019,* Nr. JRC117356, 2019.

[13] ETSI, *Quantum Safe Cryptography and Security - An introduction, benefits, enablers and challenges,* ETSI, 2015.

[14] European Commission, „The Cybersecurity Strategy," [Online]. Available: https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy.

[15] European Data Protection Supervisor, „TechDispatch #2/2020: Quantum Computing and Cryptography," 2020. [Online]. Available: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-22020-quantum-computing-and_en.

[16] European Quantum Flagship, [Online]. Available: https://qt.eu/.

[17] NIST, „Post-Quantum Cryptography," [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography.

[18] European Commission, „Cybersecurity Policies," [Online]. Available: https://ec.europa.eu/digital-single-market/en/cybersecurity.

[19] NIST, „NISTIR 8105 - Report on Post-Quantum Cryptography," April 2016. [Online]. Available: https://doi.org/10.6028/NIST.IR.8105.

[20] European Commission, „The future is quantum: EU countries plan ultra-secure communication network," 13 June 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

[21] European Commission, „Framework Partnership Agreements for open testing and experimentation and for pilot production capabilities for quantum technologies (FPA)," [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl4-2021-digital-emerging-02-22;callCode=null;freeTextSearchKeyword=quantum;matchWholeText=true;typeCodes=1,0;statusCodes=31094501,31094502,31094503;.

[22] EURAMET, „EMN for Quantum Technologies," [Online]. Available: https://www.euramet.org/european-metrology-networks/quantum-technologies/.

[23] A. Tzalenchuk, N. Spethmann, T. Prior *et al.*, „The expanding role of National Metrology Institutes in the quantum era," *Nature Physics,* Nr. 18, pp. 724-727, 2022.

[24] K. Blind, A. Jungmittag, A. Mangelsdorf, „Der gesamtwirtschaftliche Nutzen der Normung," DIN, 2011.

[25] ITU-T, „ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N)," [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx.

[26] ITU-T, „Focus Groups publications," [Online]. Available: https://www.itu.int/pub/T-FG.

[27] ITU-T, „Info session on FG-QIT4N deliverables to ITU-T Study Groups 11 and 13," [Online]. Available: https://www.itu.int/en/ITUT/focusgroups/qit4n/Pages/SG11&13.aspx.

[28] „ISO/IEC DIS 23837-1, Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements," [Online]. Available: https://www.iso.org/standard/77097.html.

[29] „ISO/IEC DIS 23837-2, Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods," [Online]. Available: https://www.iso.org/standard/77309.html.

[30] „ISO/IEC DIS 4879, Information technology — Quantum computing — Terminology and vocabulary," [Online]. Available: https://www.iso.org/standard/80432.html.

[31] IEEE, „P1913 Software-Defined Quantum Communication," [Online]. Available: https://standards.ieee.org/ieee/1913/6720/.

[32] IEEE, „P7130 Standard for Quantum Technologies Definitions," [Online]. Available: https://standards.ieee.org/ieee/7130/10680/.

[33] IEEE, „P7131 Standard for Quantum Computing Performance Metrics & Performance Benchmarking," [Online]. Available: https://standards.ieee.org/ieee/7131/10681/.

[34] IEEE, „P2995 Trial-Use Standard for a Quantum Algorithm Design and Development," [Online]. Available: https://standards.ieee.org/ieee/2995/10633/.

[35] IEEE, „P3120 Standard for Quantum Computing Architecture," [Online]. Available: https://standards.ieee.org/ieee/3120/10751/.

[36] IEEE, „P3155 Standard for programmable Quantum Simulator," [Online]. Available: https://standards.ieee.org/ieee/3155/10845/.

[37] IETF, „Quantum Internet Research Group (qirg)," [Online]. Available: https://datatracker.ietf.org/rg/qirg/about/.

[38] Bureau International des Poids at Mesures, „BIPM Workshop: The Quantum Revolution in Metrology," [Online]. Available: https://www.bipm.org/en/bipm-workshops/quantum-metrology.

[39] E. O. Göbel, U. Siegner, Quantum Metrology: Foundation of Units and Measurements, Weinheim: Wiley-VCH, 2015.

[40] C. Williams, „The SI and Quantum Metrology," *Proceedings of the International School of Physics Enrico Fermi,* Nr. 196, 2017.

[41] Bureau International des Poids et Mesures, „The International System of Units (SI)," [Online]. Available: https://www.bipm.org/en/measurement-units/.

[42] I. P. Degiovanni, M. Gramegna, S. Bize, H. Scherer, C. Chunnilal, „EURAMET EMN-Q: The European metrology network for quantum technologies," *Measurement: Sensors,* Nr. 18, 2021.

[43] NIST, „Quantum Electromagnetics Division," [Online]. Available: https://www.nist.gov/pml/quantum-electromagnetics.

[44] NIST, „Quantum Measurement Division," [Online]. Available: https://www.nist.gov/pml/quantum-measurement.

[45] NIST, „Quantum Physics Division," [Online]. Available: https://www.nist.gov/pml/quantum-physics.

[46] NIST, „Counting Photons Is Now Routine Enough to Need Standards," [Online]. Available: https://www.nist.gov/news-events/news/2019/12/counting-photons-now-routine-enough-need-standards.

[47] NIST, „Web-Based Tools for Quantum Networks," [Online]. Available: https://www.nist.gov/pml/quantum-networks-nist/web-based-tools-quantum-networks.

[48] NIST, „NIST on a Chip Technology," [Online]. Available: https://www.nist.gov/noac/technology.

[49] NIST, „OptBayesExpt documentation," [Online]. Available: https://pages.nist.gov/optbayesexpt/.

[50] Hudson Institute, „Quantum Alliance Initiative," [Online]. Available: https://www.hudson.org/policy-centers/quantum-alliance-initiative.

[51] MDPI, „Special Issue "Hollow Core Optical Fibers"," [Online]. Available: https://www.mdpi.com/journal/fibers/special_issues/hollow_core_optical_fibers.

[52] H. Sakr, Y. Chen, G. T. Jasion *et al.*, „Hollow core optical fibres with comparable attenuation to silica fibres between 600 and 1100 nm," *Nature Communications,* Nr. 11, 2020.

[53] L. Rondin, J.-P. Tetienne, T. Hingant, J.-F. Roch, P. Maletinsky, V. Jacques, „Magnetometry with nitrogen-vacancy defects in diamond," *Rep. Prog. Phys. 77 056503,* 2014.

[54] E. Abe, K. Sasaki, „Magnetic resonance with nitrogen vacancy centers in diamond - microwave engineering, materials science, and magnetometry," *J. Appl. Phys. 123, 161101,* 2018.

[55] G. Balasubramanian *et al.*, „Nitrogen-Vacancy color center in diamond - emerging nanoscale applications in bioimaging and biosensing," *Current Opinion in Chemical Biology 20, 69,* 2014.

[56] B. S. Miller *et al.*, „Spin-enhanced nanodiamond biosensing for ultrasensitive diagnostics," *Nature 587, 588,* 2020.

[57] T. Fujisaku *et al.*, „pH Nanosensor Using Electronic Spins in Diamond," *ACS Nano 13, 11726,* 2019.

[58] G. Kucsko *et al.*, „Nanometer scale thermometry in a living cell," *Nature 500, 54,* 2013.

[59] F. Pan *et al.*, „First-principles prediction of the negatively-charged nitrogen-silicon-vacancy center in cubic silicon carbide," *J. Appl. Phys. 108, 043917,* 2010.

[60] S. Castelletto, A. Boretti, „Silicon carbide color centers for quantum applications," *J. Phys. Photonics 2, 022001,* 2020.

[61] OpenQKD, [Online]. Available: https://openqkd.eu/.

[62] Quantum Brilliance, [Online]. Available: https://quantumbrilliance.com/.

[63] Qnami, [Online]. Available: https://qnami.ch/.

[64] QZabre, [Online]. Available: https://qzabre.com/.

[65] Attocube, „Customized Microscopes for low temperature," [Online]. Available: https://www.attocube.com/en/products/microscopes/customized-low-temperature-microscopes/combined-atomic-force-and-confocal-microscope.

[66] NVISION, [Online]. Available: https://www.nvision-imaging.com/.

[67] Zeiss, [Online]. Available: https://www.zeiss.com/corporate/int/home.html.

[68] Bosch, [Online]. Available: https://www.bosch.com/research/fields-of-innovation/smart-sensors/.

[69] THALES, [Online]. Available: https://www.thalesgroup.com/en/thales-and-quantum-technologies.

[70] Lockheed Martin, [Online]. Available: https://www.lockheedmartin.com/en-gb/index.html.

[71] Element Six, [Online]. Available: https://www.e6.com/en/.

[72] AsteriQs, [Online]. Available: https://www.asteriqs.eu/.

[73] MetaboliQs, [Online]. Available: https://www.metaboliqs.eu/.

[74] BCC Research, „Quantum Sensors: Quantum Entanglement for Communications and Beyond," BCC Publishing, 2019.

[75] Market Research Future, „Global Quantum Sensor Market," 2020.

[76] Yole Developpment, „Quantum Technologies 2020 report," 2020.

[77] S. Wolf, S. Richter, J. von Zanthier, F. Schmidt-Kaler, „Light of Two Atoms in Free Space: Bunching or Antibunching?," *Phys. Rev. Lett. 124, 063603,* 2020.

[78] M. D. Eisaman *et al.*, „Single-photon sources and detectors," *Review of Scientific Instruments 82, 071101,* 2011.

[79] A. Migdall, S. V. Polyakov, J. Fan, J. C. Bienfang, Single-Photon Generation and Detection: Physics and Applications, Experimental Methods in the Physical Sciences, Bd. 45, Academic Press, 2013.

[80] J. P. Pekola, O. P. Saira, V. F. Maisi, A. Kemppinen, M. Möttönen, Y. A. Pashkin, D. V. Averin, „Single-electron current sources: Toward a refined definition of the ampere.," *Reviews of Modern Physics, 85(4),* p. 1421–1472, 2013.

[81] A. Lvovsky, B. Sanders, W. Tittel, „Optical quantum memory," *Nature Photon 3,* p. 706–714, 2009.

[82] D. Lago-Rivera, S. Grandi, J. V. Rakonjac, A. Seri, H. de Riedmatten, „Telecom-heralded entanglement between multimode solid-state quantum memories," *Nature 594,* pp. 37-40, 2021.

[83] Y. Yu, F. Ma, X. Y. Luo *et al.*, „Entanglement of two quantum memories via fibres over dozens of kilometres," *Nature 578,* p. 240–245, 2020.

[84] BSI, „Post-quantum cryptography," [Online]. Available: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Post-Quanten-Kryptografie/post-quanten-kryptografie_node.html.

[85] ENISA - European Union Agency for Cybersecurity, „Post-Quantum Cryptography: Current state and quantum mitigation," [Online]. Available: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

[86] CEN-CENELEC FGQT, „CEN-CENELEC FGQT Terms of Reference," [Online]. Available: https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q01_termsofreference.pdf.

[87] ISARA, „Quantum Key Distribution and Quantum-Safe Cryptography: two (complementary) approaches to becoming quantum-ready," [Online]. Available: https://www.isara.com/blog-posts/qkd-qsc-becoming-quantum-ready.html.

[88] techUK, „Cutting through the hype – Post-Quantum Cryptography vs Quantum Key Distribution," [Online]. Available: https://www.techuk.org/resource/cutting-through-the-hype-post-quantum-cryptography-vs-quantum-key-distribution.html.

[89] M. Loeffler, C. Goroncy, T. Länger, A. Poppe, A. Neumann, M. Legré, I. Khan, C. Chunnilall, D. Lopéz, M. Lucamarini, A. Shields, E. Spigone, M. Ward, V. Martin, „Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution online (5/2021)," 2020. [Online]. Available: https://openqkd.eu/wp-

content/uploads/2021/03/OPENQKD_CurrentStandardizationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf.

[90] „ISO/IEC 15408-1, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model," 2022. [Online]. Available: https://www.iso.org/standard/72891.html.

[91] *EN 45020:2006, Standardization and related activities - General vocabulary (ISO/IEC Guide 2:2004).*

[92] European Commission, „DIGITAL Europe Work Programme 2021-2022, p.103," [Online]. Available: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital.

[93] W. J. Munro, K. Azuma, K. Tamaki, K. Nemoto, „Inside quantum repeaters - Selected Topics in QuantumElectronics," *IEEE Journal of 21, 1,* 2015.

[94] H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, „Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters 81, 5932,* 1998.

[95] European Quantum Flagship, „Entangled quantum memories for a quantum repeater: A step closer to the Quantum Internet," [Online]. Available: https://qt.eu/about-quantum-flagship/newsroom/entangled-quantum-memories/.

[96] D. P. DiVencenzo, „The Physical Implementation of Quantum Computation," 13 04 2000. [Online]. Available: https://arxiv.org/abs/quant-ph/0002077.

[97] IEEE/Open Group 1003.1-2017, *Standard for Information Technology - Portable Operating System Interface (POSIX(TM)) Base Specifications, Issue 7.*

[98] IBM, „OpenQASM 3.x Live Specification," [Online]. Available: https://github.com/openqasm/openqasm.

[99] A. Dahlberg *et al.*, „NetQASM -- A low-level instruction set architecture for hybrid quantum-classical programs in a quantum internet," 2021. [Online]. Available: https://arxiv.org/abs/2111.09823.

[100] Bureau International des Poids at Mesures, „SI Brochure: The International System of Units (SI), 9th edition," 2019. [Online].

[101] EURAMET, [Online]. Available: https://www.euramet.org/.

[102] D. Budker *et al.*, „Quantum sensors for high precision measurements of spin-dependent interactions," 2022. [Online]. Available: https://arxiv.org/abs/2203.09488.

[103] M. Mitchell, A. S. P., „Colloquium: Quantum limits to the energy resolution of magnetic field sensors," *Rev. Mod. Phys. 92,* 2020.

[104] P. J. Mohr, D. B. Newell, B. N. Taylor, „CODATA Recommended Values of the Fundamental Physical Constants: 2014," *Journal of Physical and Chemical Reference Data 45, 043102,* 2016.

[105] CEN/CENELEC, „FGQT Q05 Use Cases," 2023. [Online]. Available: https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/quantum-technologies/.

[106] M. Travagnin, „Patent analysis of selected quantum technologies, EUR 29614 EN," Publications Office of the European Union, Luxembourg, 2019. [Online]. Available: https://publications.jrc.ec.europa.eu/repository/handle/JRC115251.

[107] World Intellectual Property Organization, [Online]. Available: https://wipo.int/portal/en/index.html, with search function https://patentscope.wipo.int/search/en/search.jsf.

[108] ITU & CCSA, „Presentation for the ITU on standardization efforts by the ITU and CCSA," [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/S6AP1-Wei%20Qi_Presentation.pdf.

[109] C. Dickel, „Scalability and modularity for transmon-based quantum processors," 2018. [Online]. Available: https://doi.org/10.4233/uuid:78155c28-3204-4130-a645-a47e89c46bc5.

[110] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, I. A. Walmsley, „Optimal design for universal multiport interferometers," *Optica 3,* pp. 1460-1465, 2016.