National Physical Laboratory

NPL REPORT TQE 27

# ENGAGING UK INDUSTRY IN THE DEVELOPMENT OF NEW STANDARDS FOR QUANTUM TECHNOLOGIES

JOHN DEVANEY

SEPTEMBER 2023

# Engaging UK Industry in the development of new standards for quantum technologies

John Devaney
Science & Engineering Directorate

ISSN 1754-2995

https://doi.org/10.47120/npl.TQE27

National Physical Laboratory
Hampton Road, Teddington, Middlesex, TW11 0LW



Approved on behalf of NPLML by
Dr Rhys Lewis, Head of Quantum Programme

## GLOSSARY/ABBREVIATIONS

| Term | Definition |
|---|---|
| **BEIS** | Department for Business, Energy & Industrial Strategy |
| **BSI** | British Standards Institution |
| **DCMS** | Department for Digital, Culture, Media and Sport |
| **EMN-Q** | European Metrology Network for Quantum Technologies |
| **ETSI** | European Telecommunications Standards Institute |
| **FG-QIT4N** | Focus Group on Quantum Information Technology for Networks (in ITU-T) |
| **FGQT** | Focus Group on Quantum Technologies (in CEN/CENELEC) |
| **IEEE** | Institute of Electrical and Electronics Engineers |
| **IEC** | International Electrotechnical Commission |
| **ISO** | International Organization for Standardization |
| **JTC 1/SC 27** | Joint Technical Committee 1, Subcommittee 27 (under ISO/IEC) |
| **JTC 1/WG 14** | Joint Technical Committee 1, Working Group 14 (under ISO/IEC) |
| **ITU-T** | International Telecommunication Union, Telecommunication Standardization Sector |
| **ITU-T/SG 13** | ITU-T Study Group 13, Future networks |
| **ITU-T/SG 17** | ITU-T Study Group 17, Security |
| **NIST** | National Institute of Standards and Technology (the United States' National Metrology Institute) |
| **NMI** | National Metrology Institute |
| **NPL** | National Physical Laboratory |
| **NQCC** | National Quantum Computing Centre |
| **NQTP** | National Quantum Technology Programme |
| **QKD** | Quantum Key Distribution |
| **QRNG** | Quantum Random Number Generator |
| **QT&**E | Quantum Test and Evaluation |
| **SDO** | Standards Development Organisation |
| **SME** | Small-to-Medium Enterprise |
| **WG** | Working Group |

# EXECUTIVE SUMMARY

Under the UK National Quantum Technologies Programme (NQTP), one of the key areas of work is described as “Strengthen engagement in international standards and benchmarking”. This report from the National Physical Laboratory (NPL) covers UK and international activity in quantum technology standards development and NPL’s involvement in that process.

This report provides an update on standards development in quantum computing, quantum communications, quantum imaging, and quantum sensors and timing.

NPL delivered a well-attended on-line workshop with high-profile speakers on quantum computing standardisation. For the work identified as a priority to start effectively and efficiently, NPL and other NMIs will take leadership in developing the standardisation strategy. Three more workshops will be organised by NPL on quantum communication, quantum imaging, and quantum sensors and timing. The goal will be to seek similar direction for appropriate standards development.

The establishment of the NPL Centre for Quantum Standards will focus quantum technology standards activity for optimum effectiveness, with the NPL Quantum Standards Manager as a dedicated resource.

# CONTENTS

# 1 INTRODUCTION

This report is an output from the NPL quantum programme for the period April 21 – March 22. This period is the second year of a four-year programme to enable the capabilities and expertise of the National Physical Laboratory (NPL) to fully support the UK National Quantum Technology Programme (NQTP) and the UK's aspirations for economic growth based on quantum technologies. The NPL programme is funded by the government department of Business, Energy and Industrial Strategy (BEIS).

The NQTP vision to create a quantum-enabled economy is described in the 2020 strategic intent document for the national programme (UK National Quantum Technologies Programme Board, 2020). The strategic intent document details four main objectives and several key areas within those themes which are required to deliver the desired outcomes and benefits for the UK.

Under the objective of "Stimulate market growth, unleash innovation, and create a thriving ecosystem", one of the key areas of work is described as "Strengthen engagement in international standards and benchmarking".

In this report we describe the activities undertaken to raise awareness in the UK quantum community of the importance of standards and the importance of the UK community engaging with the standards development process. We describe current standards development and UK involvement and the activities undertaken to build relationships with the quantum community around the world to find common standards needs and priorities. The report describes a workshop on quantum computing standards that was organised for the UK community by NPL and other partners from the NQTP. The report concludes with a proposal based on the outputs from the UK workshop on how to best deliver the prioritised quantum computing standards.

## 1.1 QUANTUM TECHNOLOGY STANDARDS ACTIVITY IN 2022

### 1.1.1 Introduction

Within the NPL Quantum Technologies Programme there are four focus areas: quantum computing, quantum communications, quantum imaging and quantum sensors and timing. Standardisation activity is at different stages of development and across several different SDOs for each of these areas.

A list of quantum technology standards published and in draft is in Appendix 2.

A BSI committee for quantum standards was established with NPL support in March 2021. The committee now has 67 members. So far, its main activity has been to mirror and contribute to ISO/IEC/JTC 1/WG 14, Quantum computing, and to the CEN/CENELEC Focus Group on Quantum Technologies (FGQT). BSI's remit is to mirror and contribute to activity in CEN/CENELEC in Europe and ISO/IEC globally, but the committee can also act as an information-sharing forum for other standards development in, for example ETSI, ITU-T or IEEE.

The CEN/CENELEC FGQT was established to create a roadmap for quantum technologies that could then be used as a guide to the need for standardisation, and it has mainly collected information about the current state-of-the-art. NPL experts have contributed, particularly on single-photon sources and detectors, and on quantum communications.

### 1.1.2 Quantum computing

Quantum computing is the area where the need for standards is most apparent, particularly around benchmarking of performance. The workshop described in the next section brought forward many of the needs and concerns in developing standards for quantum computing.

A working group (WG 14, Quantum computing) was established under ISO/IEC/JTC 1, Information technology, following a proposal from the Standardization Administration of China (SAC) in 2020. SAC was awarded the secretariat of the WG. Its only work item is a "terminology and vocabulary" for quantum computing. NPL experts are contributing to development of the draft standard.

Project committees have been established in IEEE to develop standards for Quantum Technologies Definitions (P7130) and Quantum Computing Performance Metrics and Performance Benchmarking (P7131). Work has only just begun in these committees, but IEEE project committees are expected to work more quickly, with more frequent meetings than ISO and IEC. NPL experts are signed up to observe and participate.

#### 1.1.3 Quantum communications

Quantum communications standards, particularly around quantum key distribution (QKD), have been in development for some time, primarily in ETSI.

NPL experts contributed to drafting of GS QKD 016, Protection Profile, GS QKD 013, Characterisation of Transmitter Modules, GS QKD 010, Protection Against Trojan-Horse Attacks and the revision of GS QKD 007, Vocabulary and GS QKD 005, Security Proofs. NPL experts participated in the 30th and 31st meetings of ETSI ISG-QKD (June 2021 and December 2021) and all monthly teleconferences.

NPL experts also contributed comments on ISO/IEC 23837, Security Requirements and Test and Evaluation Methods for QKD, which were mainly accepted by ISO/IEC JTC 1/SC 27/WG 3, Security evaluation, testing and specification.

Standards for quantum random-number generation (QRNG) are also under development with contributions from NPL experts. Comments were contributed to the revision of ISO/IEC 18031, Random bit generation and accepted by ISO/IEC JTC 1/SC 27/WG 2, Cryptography and security mechanisms. QRNG standards are expected to start development in ETSI soon.

Standards for QKD networks are most likely to be developed in ITU-T and the ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N) was established in 2019 to do pre-standardisation work on the topic. It has produced nine deliverables. NPL will nominate experts to participate in the development of full standards.

#### 1.1.4 Quantum imaging, and quantum sensors and timing

Commercial development in these topics is still in its very early stages. The European Metrology Network for Quantum Technologies (EMN-Q) was established under the auspices of EURAMET to co-ordinate and share information about advances and opportunities in quantum measurement technologies. NPL experts participate in its work. EMN-Q has three sections: clocks, photonics and computing.

EMN-Q aims to become is to become the central contact point to stakeholders interested in metrology for quantum technologies by:

- contributing to standardisation and certification of quantum technologies;
- promoting the take-up of metrology in the development of these technologies;
- supporting industrial needs in synergy with the technological objectives of the EC Quantum Flagship and national quantum technology programs; and
- promoting the use of quantum measurement techniques where advantageous for "classical" technical areas.

The three UK/NPL reps are Rachel Godun, Chris Chunnilall (who is also vice-chair) and Tobias Lindstrom. Rhys Lewis is the UK “vote holder”, “primary contact” and “cross-sectional expert”.

## 1.2 THE VALUE OF METROLOGY UNDERPINNING STANDARDS

The UK measurement infrastructure relies on the existence of standards to support the metrology needed for validation of new products and services. Metrology, the science of measurement, oversees the maintenance and improvement of this measurement infrastructure, continually responding to evolving societal needs. By achieving global agreement on how measurements should be made, expressed and used, metrology has generated systems and frameworks for measurement quantification and through these underpins consistency and assurance in all measurement. Anyone using this validated measurement system will benefit from their measurements being stable over time, comparable with others and accurate, allowing known confidence in measurement results.

Adopting the principles of metrology has the following benefits:

- Improves the effectiveness and efficiency of science and the trust in its outcomes
- Reduces waste and increases value for money and productivity
- Unlocks the potential of innovation faster, allowing earlier market entry
- Decreases the time to implement change and add value
- Is essential for the development and assessment of evidence-based policy and accelerates progress in science and in society

Each of these benefits is supported by a solid evidence base.

Embracing the measurement infrastructure is an essential requirement for reproducibility of outcomes and therefore progress in science and in society. The virtuous circle of improved measurement, driving improved technology, driving improved measurement, is the motor that propels economic and social progress.

The application of metrology is universally relevant across all sectors and to all users of measurement. Metrology should be part of everything and a partner of everyone. All elements of the economy including the SME community should be encouraged to take advantage of the UK measurement infrastructure including the national metrology institute capabilities. Increasing the adoption of better measurement will provide significant competitive advantage for the UK, in industry and academia.

## 2 QUANTUM COMPUTING STANDARDS WORKSHOP, 15 MARCH 2022

This workshop was held to review the rapidly developing field of standards for quantum computing, promoting the importance of collaboration and co-ordination between industry, academia and government. The workshop explored the barriers to organisations getting involved in the standards development process, the emerging topic of benchmarking for quantum computing hardware and software, and how we align as a quantum community to best represent the UK internationally were among the topics discussed.

The workshop brought together UK industrial, governmental and academic organisations, along with experts from outside the UK, all involved in quantum computing, to exchange ideas about the need for standards, discuss which topics to pursue, and which standards development organisations (SDOs) would best serve the needs of UK stakeholders.

The workshop was organised by an NPL project manager supported by other NPL experts and project managers, in consultation with BSI and the BSI committee for quantum technologies. The workshop was structured in two parts.

The first session was introduced by Rhys Lewis, Head of Quantum Programmes, NPL, followed by presentations with Q&A from leading figures in quantum computing:

- Sir Peter Knight FRS NPL and Imperial College
- Will Lawson BEIS Technology Strategy and Security team
- Stephanie Ifayemi DCMS lead on Digital Standards
- Barbara Goldstein NIST Programme Manager
- Thomas Lubinski QED-C and Quantum Circuits, Inc. USA

The second session was a panel discussion hosted by John Devaney, Quantum Standards Manager, NPL. The panel consisted of:

- Elham Kashefi School of Informatics, University of Edinburgh
- Marco Ghibaudi Riverlane
- Rob van den Brink Delft Circuits, The Netherlands
- Thomas Lubinski QED-C

The panellists agreed that the scoping and terminology work already happening in a few SDOs (CEN/CENELEC, ISO/IEC/JTC 1, and IEEE at very least) was the ideal and necessary first step in standards development for quantum computing. There was also good agreement that the growing market for quantum computing products and services need standards development to get underway as soon as possible. That is, development of standards that will give some assurance about the performance/characteristics of the products and services being marketed.

The question of where standardisation should happen was met with slightly different but not necessarily contradictory opinions. There was agreement that standards could be developed in any organisation that was open to involvement from all stakeholders and followed a fair and transparent process of standards development. There was some agreement that standards could begin their development in any SDO (or national standards body [NSB]) and be adopted and/or developed further by others, particularly global SDOs with the greatest reach. There was also some agreement that stakeholders have to have ownership of the standards relevant to them, which might mean that they prefer an SDO with which they are already familiar.

The question of hardware benchmarking took up a large part of the discussion. The Quantum Economic Development Consortium (QED-C) advocates an “application oriented” approach, which executes familiar quantum algorithms and small programs over a range of problem dimensions to gauge how well—and how quickly—a quantum computer performs quantum operations.

There is an overlap in membership between QED-C and IEEE, but IEEE project committee P7131 will consider all and any approaches to benchmarking as potentially suitable for standardisation.

Another consideration in developing benchmarking standards will be consideration of what a quantum computer should be or might be capable of. Should we, for example, include performance of Shor’s algorithm (to find the prime factors of an integer) as a benchmark although no quantum computer today is large enough to handle the process?

The possibility was raised that there might be problems (e.g. optimal molecule design) where quantum computers provide a solution but we cannot know whether it is the best or correct solution. In contrast, conventional computer benchmarking involves running laborious calculations (e.g. calculating pi to a certain precision) where we know the right answer with absolute certainty. How can we benchmark in such situations?

Discussion shifted from “where” standardisation might happen to “how”. A quantum computer can be described as a complex systems-of-systems, where the performance of the whole depends on the interaction between the parts. Will the standards developed will recognise this complex reality, specifying performance for the system as a whole rather than each constituent part?

Regardless of where and how standardisation might happen for quantum computing, there was agreement that the end goal has to be consensus and convergence, avoiding lasting conflict and fragmentation.

# 3 UPDATE ON CO-ORDINATION OF UK ENGAGEMENT IN QUANTUM TECHNOLOGY STANDARDS DEVELOPMENT

## 3.1 INTRODUCTION

As stated earlier, a UK quantum standards committee run by BSI with NPL support was established in 2021. The committee mirrors standards development in ISO/IEC/JTC 1 and CEN/CENELEC, and monitors activity in ITU-T. It will also mirror a newly agreed Strategy Advisory Group in IEC.

In addition, NPL has appointed a full-time Quantum Standards Manager to consult with UK quantum technology stakeholders, co-ordinate UK input to standards development, to monitor European and international quantum standards development and, where appropriate, to intervene in or lead the standards development process.

## 3.2 PRIORITIES FOR THE UK

As the panel and contributors to the quantum computing workshop largely agreed, the time has come for significant standards development in support of the sector. In the next year, NPL experts will participate in and, where appropriate, lead the strategic analysis of quantum computing standards needs. Where the analysis identifies the need for new committees, working groups and/or work items, NPL experts will submit or contribute to appropriate proposals and be prepared to lead the development work.

Standards development for QKD and QRNG have proliferated, with NPL experts contributing in the preferred forum of ETSI. This participation will continue. A workshop, led by NPL in consultation with BSI, will be held this year to update UK stakeholders on progress in QKD and QRNG standards, and to consult on where future priorities lie, also including the topic of quantum networks. Meanwhile, in the area of quantum networks, NPL will monitor and participate in new standards development, particularly in ITU-T. NPL will publicise ongoing activity and collect UK contributions towards new standards.

Workshops, also led by NPL in consultation with BSI, will be held this year to bring UK stakeholders involved in quantum imaging and sensing together with the purpose of identifying topics where standards would support the sector.

## 3.3 WORKING ACROSS THE NQTP

NPL's Quantum Standards Manager will work with the other members of the NQTP, particularly the Quantum Hubs, to ensure that stakeholders not already involved in standards development or the BSI committee are aware of standards in development, proposed standards and opportunities to contribute and get involved.

NPL will continue to report to the NQTP boards.

## 3.4 POSSIBLE FURTHER WORK TO ESTABLISH PRIORITY AREAS FOR QUANTUM TECH STANDARDS

### 3.4.1 JOINT SURVEYS AND ANALYSIS WITH NIST AND OTHER NMIS

NPL is intends to make detailed analysis of the standards needs in each area of quantum technology, for publication with the highest profile possible, and in collaboration with other NMIs including NIST. These analyses would demonstrate the UK's readiness to lead on standards development in close collaboration with others and provide both a reference and a starting point for strategic development in the major SDOs.

### 3.4.2 STRATEGY WORK IN ISO/IEC/JTC 1

BSI, on behalf of UK stakeholders, has proposed a global survey of quantum technology standardisation needs to ISO/IEC/JTC 1. The work was approved in May to report back in November 2022. The anticipated outcome is that BSI will propose establishment of a quantum technology subcommittee to JTC 1, with a particular focus on quantum computing.

The commissioned and highly publicised content outlined in 3.5.1 would provide a solid foundation for the work in JTC 1. A Strategic Evaluation Group (SEG) on quantum technology has already been approved by IEC, with leadership from the Korean NSB, KATS. The UK-led strategic work could and should be developed in regular communication and cross-participation with the IEC group. Both pieces of work will have to recognise the scope of their parent organisations: information technology in JTC 1, electrotechnical products and services in IEC.

The collaboration with other NMIs would demonstrate their effectiveness in meeting the needs of this nascent industry. UK leadership for the new subcommittee would be the likely outcome.

## 3.5 REPORTING WITHIN GOVERNMENT

There should be a forum for cross-government awareness of quantum standards activity. NPL would prepare a regular brief on the current position for this group.

## 4 CONCLUSION

This report has described the second year of work delivered under the NPL quantum programme in support of strengthening UK industry engagement in international standards and benchmarking.

A workshop on quantum computing standards organised by NPL with partners from the UK quantum programme has confirmed the need to start work on quantum computing standards as soon as possible, in whichever standards body/bodies will most benefit UK stakeholders. For this work to start effectively and efficiently, NPL and other NMIs need to demonstrate leadership in developing the standardisation strategy.

Three more workshops will be organised by NPL on quantum communication, quantum imaging, and quantum sensors and timing. The goal will be to seek similar direction for appropriate standards leadership and development.

The establishment of the NPL Centre for Quantum Standards will focus quantum technology standards activity for optimum effectiveness, with the NPL Quantum Standards Manager as a dedicated resource.

## 5 REFERENCES

UK National Quantum Technologies Programme Board, 2020. Strategic Intent. [Online] Available at: https://uknqt.ukri.org/files/strategicintent2020/#:~:text=The%20NQTP%20Partners%20are%20committed,innovate%20and%20grow%20with%20confidence [Accessed 2022].

# APPENDIX : QUANTUM TECHNOLOGY STANDARDS PUBLISHED AND IN DRAFT

*General quantum technology*

| IEEE | |
|---|---|
| In draft | |
| P7130 | Standard for Quantum Technologies Definitions |

*Quantum communications*

NOTE Does not include (quantum) random number generation standards publications.

| ETSI | |
|---|---|
| Published | |
| ETSI GS QKD 002 V1.1.1 (2010-06) | Quantum Key Distribution (QKD); Use Cases |
| ETSI GR QKD 003 V2.1.1 (2018-03) | Quantum Key Distribution (QKD); Components and Internal Interfaces |
| ETSI GS QKD 004 V2.1.1 (2020-08) | Quantum Key Distribution (QKD); Application Interface |
| ETSI GS QKD 005 V1.1.1 (2010-12) | Quantum Key Distribution (QKD); Security Proofs |
| ETSI GR QKD 007 V1.1.1 (2018-12) | Quantum Key Distribution (QKD); Vocabulary |
| ETSI GS QKD 008 V1.1.1 (2010-12) | Quantum Key Distribution (QKD); QKD Module Security Specification |
| ETSI GS QKD 011 V1.1.1 (2016-05) | Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems |
| ETSI GS QKD 012 V1.1.1 (2019-02) | Quantum Key Distribution (QKD); Device and Communication Channel Parameters for QKD Deployment |
| ETSI GS QKD 014 V1.1.1 (2019-02) | Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API |
| ETSI GS QKD 015 V2.1.1 (2022-04) | Quantum Key Distribution (QKD); Control Interface for Software Defined Networks |
| ETSI GS QKD 018 V1.1.1 (2022-04) | Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks |

| | |
|---|---|
| ETSI White Paper No. 27 | Implementation Security of Quantum Cryptography: Introduction, challenges, solutions |
| ETSI GS QKD 018 V1.1.1 | Quantum Key Distribution (QKD) Orchestration Interface of Software Defined Networks |
| | |
| In draft | |
| ETSI GS QKD 013 V1.1.2 | Quantum Key Distribution (QKD); Characterisation of Optical Output of QKD transmitter modules |
| ETSI GS QKD 016 V1.1.1 | QKD Common Criteria Protection Profile for QKD |
| ETSI GS QKD 017 V1.1.1 | Quantum Key Distribution (QKD) Network architectures |
| ETSI GS QKD 019 V1.1.1 | Quantum Key Distribution (QKD) Design of QKD interfaces with Authentication |
| **ISO/IEC** | |
| In draft | |
| ISO/IEC 23737-1 | Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements |
| ISO/IEC 23837-2 | Information technology security techniques — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods |
| **IEEE** | |
| In draft | |
| P1913 | Software-Defined Quantum Communication |
| **ITU-T** | |
| Published | |
| Y.3800 Cor1 | Overview on networks supporting quantum key distribution |
| Y.3801 | Functional requirements for quantum key distribution networks |
| Y.3802 Cor1 | Quantum key distribution networks – Functional architecture |
| Y.3803 | Quantum key distribution networks – Key management |
| Y.3804 | Quantum key distribution networks – Control and management |

| | |
|---|---|
| Y.3805 | Quantum key distribution networks – Software-defined networking control |
| Y.3806 | Quantum key distribution networks – Requirements for quality of service assurance |
| Y.3807 | Quantum key distribution networks – Quality of service parameters |
| Y.3808 | Framework for integration of quantum key distribution network and secure storage network |
| Y.3809 | A role-based model in quantum key distribution networks deployment |
| Y.3810 | Quantum key distribution network interworking - Framework |
| Y.3811 | Quantum key distribution networks - Functional architecture for quality of service assurance |
| Y.3812 | Quantum key distribution networks - Requirements for machine learning based quality of service assurance |
| Y Suppl 70 | ITU-T Y.3800-series – Quantum key distribution networks - Applications of machine learning |
| X.1710 | Security framework for quantum key distribution networks |
| X.1712 Cor1 | Security requirements and measures for quantum key distribution networks – key management |
| X.1714 | Key combination and confidential key supply for quantum key distribution networks |
| In draft | |
| Y.QKDN-iwfr | Quantum key distribution networks - interworking framework |
| Y.QKDN-iwrq | Quantum key distribution networks - interworking requirements |
| Y.QKDN-ml-fra | Quantum key distribution networks - functional requirements and architecture to enable machine learning |
| Y.QKDN-rsfr | Quantum key distribution networks - resilience framework |
| Y.supp.QKDN-roadmap | Standardization roadmap on Quantum Key Distribution Networks |
| Y.TR-QEFN | ITU-T's Views for Quantum-Enabled Future Networks |

*Quantum computing and simulation*

| | |
|---|---|
| **IEEE** | |
| *In draft* | |
| *P1913* | Software-Defined Quantum Communication |
| *P1943* | Standard for Post-Quantum Network Security |
| P2995 | Trial-Use Standard for a Quantum Algorithm Design and Development |
| P3120 | Standard for Quantum Computing Architecture |
| P3155 | Standard for Programmable Quantum Simulator |
| P3172 | Recommended Practice for Post-Quantum Cryptography Migration |
| P7130 | Standard for Quantum Computing Definitions |
| P7131 | Standard for Quantum Computing Performance Metrics & Performance Benchmarking |
| **ISO/IEC** | |
| *In draft* | |
| ISO/IEC 4879 | Information technology -- Quantum computing -- Terminology and vocabulary |
| **CEN/CENELEC** | |
| *In draft* | |
| No identifier | Quantum Technologies Standardisation Roadmap |