Single-Photon Detection in Quantum Communication and Quantum Networks: Roles, Requirements, and Defense-Related Challenges

Augusto Ribeiro Rodrigues and Rene Felipe Keidel Spada
Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos/SP – Brasil

***Abstract*— Quantum communication and quantum networks are applications of second-generation quantum technologies with direct relevance to secure and resilient information exchange in civil, governmental, and defense-related scenarios. In operational contexts, these technologies may support satellite and free-space optical links, distributed sensing, quantum-secured communication layers, and future command-and-control infrastructures. Since many architectures use light to carry quantum states, single-photon detection is a crucial stage between optical quantum transmission and classical information processing. This paper reviews the role of single-photon detectors in quantum communication and quantum-network systems, emphasizing system-level functions, performance parameters, and technological constraints. In quantum key distribution, efficiency, dark counts, timing jitter, dead time, and count rate affect error rates, secret key rate, and transmission distance. In networks, single-photon detectors support heralding, Bell-state measurements, entanglement swapping, and node synchronization.**

***Keywords*— Single-Photon Detectors, Quantum Communication, Quantum Networks**

I. Introduction

Quantum technologies can be understood as a set of scientific and technological developments based on the control, manipulation, and exploitation of intrinsically quantum properties, such as superposition, entanglement, tunneling, energy quantization, and the quantization of radiation. Although quantum mechanics has already produced profound technological impacts throughout the twentieth century, it is common to distinguish between a first and a second quantum revolution. The first quantum revolution was mainly associated with the understanding of the quantum laws governing matter and radiation, enabling consolidated technologies such as semiconductors, transistors, lasers, image sensors, magnetic resonance imaging, and atomic clocks [1], [2]. In this stage, quantum effects were essential for explaining and designing devices, but the coherent control of individual quantum states was not usually exploited as a technological resource in itself.

The second quantum revolution, in contrast, is characterized by the ability to prepare, control, manipulate, and measure individual or highly controlled quantum systems, such as photons, atoms, ions, electrons, spins, molecules, and quasiparticles [1], [2]. In this context, properties that were previously treated mainly as conceptual aspects of quantum theory, such as superposition and entanglement, become physical resources for information processing, transmission, and measurement [3]. Therefore, contemporary quantum technologies do not merely represent a further miniaturization of classical technologies, but rather a change of paradigm: they seek to directly exploit properties with no classical analogue in order to obtain new capabilities, higher precision, or enhanced security in specific applications.

In general, the field is commonly organized into four major areas: quantum computing, quantum simulation, quantum communication, and quantum sensing/metrology [3], [4]. These areas support emerging capabilities in secure communication, information processing, precision measurement, navigation, and sensing, with increasing relevance for civil, industrial, and defense-related applications [2], [5]–[7]. Fig. 1 places these capabilities in a defense-related context.

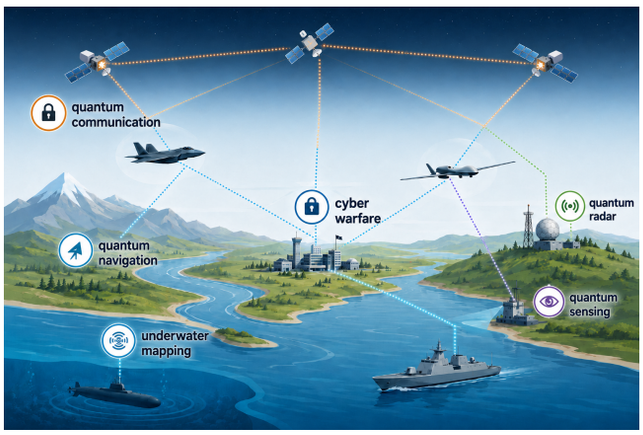

Fig. 1. Strategic context of quantum technologies in defense-related applications. Adapted from [2].

Among these areas, quantum communication and quantum networks are of particular interest for this work. They provide a route toward architectures for transmitting, distributing, and processing information with potential implications for secure communication, distributed quantum information processing, clock synchronization, and the interconnection of future quantum processors [8]–[10]. From a defense perspective, secure and resilient information exchange is critical for command-and-control, strategic communications, cyber defense, space systems, and distributed sensing [2], [11]. Thus, quantum communication should not be understood only as point-to-point protected transmission, but also as part of broader networked architectures combining quantum states, entanglement, and classical control channels [9].

Quantum key distribution (QKD) is one of the most mature examples of quantum communication, since it uses quantum states and measurement principles to support the secure distribution of cryptographic keys [8], [10]. However, deploy-

A. R. Rodrigues, augustoarr@ita.br; R. F. K. Spada, rfkspada@ita.br.

ment still depends on engineering factors such as secret key rate, transmission distance, cost, implementation security, and compatibility with existing communication infrastructure [12]. These aspects affect operational scenarios, where quantum-secure links must operate under realistic loss and noise conditions while satisfying reliability requirements associated with governmental, industrial, or defense applications.

A central feature of many quantum communication and quantum-network proposals is the use of light as a carrier of quantum states. Photons are suitable for communication because they can propagate through optical fibers and free-space links, encode information in degrees of freedom such as polarization, phase, and time-bin, and preserve quantum coherence over long distances more effectively than many matter-based carriers, although they remain susceptible to loss, dispersion, and background noise [8], [10]. In satellite and free-space quantum communication, these features are used for extending secure links over large distances, especially where terrestrial fiber infrastructure is limited or unavailable [11], [13]. Consequently, several protocols operate in the single-photon regime, relying on individual photons or weak optical pulses whose security and functionality depend on their quantum nature [14], [15].

This makes the generation, transmission, manipulation, and detection of individual photons or weak optical states a requirement for many optical quantum communication and quantum-network systems. Although complete architectures also require sources, memories, repeaters, optical control elements, and classical post-processing, single-photon detectors (SPDs) occupy a central position. They form the interface through which extremely weak optical quantum signals are converted into measurable electrical events, directly affecting the extraction of information from received quantum states [16], [17]. In protocols such as QKD, entanglement distribution, quantum teleportation, and heralded-state preparation, the detection event often defines whether a transmission, distribution, or post-selection process was successful [8]–[10].

The performance of SPDs is commonly characterized by parameters such as detection efficiency, dark count rate, timing jitter, dead time, afterpulsing probability, maximum count rate, wavelength sensitivity, photon-number resolution, and operating conditions [16]–[18]. In practical quantum communication links, weak signals, channel losses, background noise, imperfect sources, and finite event rates couple detector specifications directly to system performance. Detection efficiency determines the probability of registering valid photons, whereas dark counts and background events introduce false detections that increase error rates and reduce link reliability. Timing jitter affects synchronization, coincidence measurements, time-bin encoding, and high-rate operation, while dead time and saturation constrain the maximum count rate and scalability of real implementations.

At the system level, SPD performance connects device characteristics to protocol operation: efficiency and noise affect the probability and reliability of received events, whereas timing response, recovery time, and wavelength sensitivity constrain synchronization, event rates, and compatibility with fiber, free-space, and integrated platforms [16]–[18]. This article reviews, from an integrative literature-based perspective, how detector performance conditions the reliability, security, and maturity of optical quantum communication and quantum-network systems, including strategically relevant applications in communications, photonics, and defense-related infrastructures.

II. Review Methodology

This work adopts an integrative literature review approach to examine how SPDs contribute to quantum communication and quantum-network architectures. Instead of conducting a systematic bibliometric mapping, the review synthesizes representative literature from quantum information, optical communication, photonics, and single-photon detection.

The reviewed corpus was organized to cover four complementary groups of studies: foundational works on quantum communication and quantum networks; protocol-level analyses in which detector imperfections affect metrics such as quantum bit error rate (QBER), secret key rate, transmission distance, heralding probability, or entanglement distribution rate; technical reviews and representative studies on SPD platforms, including single-photon avalanche diodes (SPADs), superconducting nanowire single-photon detectors (SNSPDs), and transition-edge sensors (TESs); and recent works discussing integration, scalability, wavelength compatibility, and deployment challenges in fiber, free-space, satellite, or integrated photonic architectures [8]–[10], [16]–[19].

Priority was given to review papers, protocol-level analyses, and detector-technology studies that explicitly relate detector parameters, such as efficiency, noise, temporal response, wavelength compatibility, integration potential, and scalability, to communication or networking performance [12], [20], [21]. This focus makes it possible to identify the detector characteristics that most directly constrain and enable optical quantum information systems for communication and networking applications.

The analysis was organized according to two complementary axes. The first concerns quantum communication links, especially quantum key distribution, where SPDs affect signal reception, error probability, secret key rate, and maximum transmission distance [8], [10], [12]. The second concerns quantum networks, where detection events are involved not only in final readout, but also in heralding, Bell-state measurements (BSM), entanglement-distribution protocols, synchronization, and node-to-node connectivity [9], [22]. This organization highlights how the same detector parameters acquire different relevance depending on whether the detector operates in a point-to-point communication link or as part of a multi-node quantum-network architecture.

III. Single-Photon Detectors in Quantum Communication

In quantum communication systems, SPDs provide the measurement interface for weak optical states used to encode and transmit information. This role is evident in QKD, where the receiver must register individual detection events associated with quantum states prepared by the transmitter [8], [10], [14]. In this context, the detection process is directly connected to the feasibility of the protocol: valid detections contribute to the raw key, while incorrect or spurious detections may increase the QBER and reduce the amount of secure information that can be extracted after error correction and privacy amplification [8], [10]. For civil, governmental, and

defense communication links, reliable key generation requires the receiver to distinguish valid quantum signals from losses, device noise, and environmental background.

Fig. 2 illustrates the functional role of the SPD in a point-to-point optical quantum communication link. Alice transmits weak optical quantum signals through a quantum channel affected by attenuation and background noise. At Bob's receiver, the attenuated quantum signals are registered by the SPD, which converts photon arrivals into discrete electrical detection events. These events do not directly constitute the final key or accepted data; instead, they provide the raw detection records that are filtered, checked, corrected, and compressed during classical post-processing steps such as basis sifting, parameter estimation, error correction, and privacy amplification. Therefore, the SPD is not merely an optical receiver, but a system-level component that affects the reliability, security, and usability of the received quantum information.

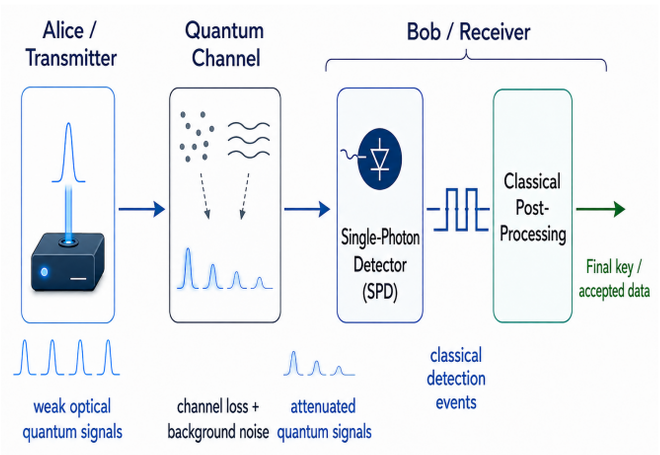

Fig. 2. Point-to-point optical quantum communication link, highlighting the SPD-based conversion of attenuated quantum signals into classical detection events.

The performance of SPDs is better understood within a link-budget framework, where detector parameters are related to source intensity, channel loss, and noise rather than treated as isolated device specifications. In a representative weak-pulse optical link, assuming Poissonian photon statistics, this balance can be expressed by estimating the probability of registering at least one signal-related detection event per optical pulse:

$$p_{\mathrm{sig}} = 1 - \exp\left(-\mu \cdot \eta_{\mathrm{ch}} \cdot \eta_{\mathrm{det}}\right), \tag{1}$$

where μ is the mean photon number per pulse, η_{ch} is the channel transmittance, and η_{det} is the detector efficiency. If p_{dc} denotes the dark-count probability within the detection gate, the total click probability can be written as

$$p_{\mathrm{click}} = 1 - (1 - p_{\mathrm{sig}}) \cdot (1 - p_{\mathrm{dc}}), \tag{2}$$

which is equivalent to

$$p_{\mathrm{click}} = 1 - (1 - p_{\mathrm{dc}}) \cdot \exp(-\mu \cdot \eta_{\mathrm{ch}} \cdot \eta_{\mathrm{det}}). \tag{3}$$

For low-probability events, this expression reduces approximately to $p_{\mathrm{click}} \simeq p_{\mathrm{sig}} + p_{\mathrm{dc}}$. In gated operation, for $D_{\mathrm{cr}} \cdot \Delta t_{\mathrm{gate}} \ll 1$, p_{dc} may be related to the dark count rate by $p_{\mathrm{dc}} \simeq D_{\mathrm{cr}} \cdot \Delta t_{\mathrm{gate}}$, where D_{cr} is the dark count rate and Δt_{gate} is the effective detection window. Thus, detector noise, temporal gating, and channel attenuation enter the same link-level probability budget [8], [10], [16], [17].

This balance directly affects the QBER, especially in high-loss regimes. Under the same low-probability approximation, a simplified error model can be expressed as

$$\mathrm{QBER} \simeq \frac{e_{\mathrm{opt}} \cdot p_{\mathrm{sig}} + e_{\mathrm{dc}} \cdot p_{\mathrm{dc}}}{p_{\mathrm{click}}}, \tag{4}$$

where e_{opt} represents optical or alignment-related errors and $e_{\mathrm{dc}} \simeq 1/2$ represents the random contribution of dark-count events to the bit error probability. This form makes explicit why dark counts become increasingly relevant as the transmission distance increases: channel attenuation reduces p_{sig}, while p_{dc} remains associated with the detector and the detection window. In the high-loss limit, the relative contribution of false detections increases, raising the QBER and reducing the usable key rate [8], [10], [12].

Temporal parameters also impose limits on communication performance. Timing jitter affects the assignment of detection events to the correct temporal window, which is critical in high-rate protocols, time-bin encoding, coincidence measurements, and free-space or satellite links subject to variable background conditions. Dead time limits how rapidly the detector can recover after an event and may lead to saturation when the photon flux or repetition rate increases. Therefore, high detector efficiency alone is not sufficient for quantum communication: low noise, precise timing, fast recovery, wavelength compatibility, and stable operating conditions are also required to translate photon arrivals into reliable system-level performance [16]–[18], [20].

As a result, SPD performance should be treated as part of the link budget rather than as an isolated receiver specification. In high-loss or high-rate regimes, efficiency, dark-count probability, timing jitter, dead time, and saturation jointly determine the usable detection window, the balance between signal-related and noise-related events, and the rate at which valid detection records can be supplied to classical post-processing [10], [16], [18]. The detector therefore constrains the operational range of the link through measurable quantities such as click probability, QBER, secret key rate, and timing stability.

IV. Single-Photon Detectors in Quantum Networks

Quantum networks are not simply an extension of point-to-point quantum communication links. While a point-to-point link connects two users through a quantum channel, a quantum network involves multiple nodes capable of sharing, processing, and measuring quantum states across a distributed architecture [9], [22]. Such networks may support entanglement distribution, quantum teleportation, secure multi-user communication, distributed quantum information processing, and the interconnection of future quantum processors [9]. In strategic and defense-related contexts, quantum networks are linked to future infrastructures for secure command-and-control links, distributed sensing, clock synchronization, and the integration of ground, airborne, and space assets [2]. These applications impose requirements related to synchronization, node coordination, reliability, and scalability.

Fig. 3 illustrates a quantum-network architecture in which remote nodes send photonic states to an intermediate SPD-assisted BSM stage. In this type of architecture, the detector is not restricted to the final readout of a received signal. Instead, detection events at the intermediate measurement node can herald successful operations, identify BSM outcomes, and support entanglement swapping, thereby contributing to the establishment of quantum correlations between distant nodes without requiring direct detection at the final nodes. Detection therefore acts not only as the final stage of information readout, but also as an operational condition for the generation, verification, and connectivity of distributed quantum states.

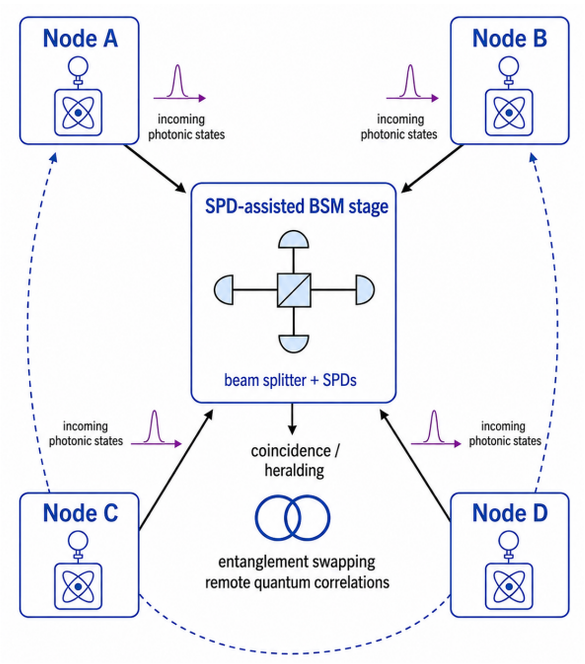

Fig. 3. Quantum-network architecture with an intermediate SPD-assisted Bell-state measurement stage, highlighting incoming photonic states, coincidence detection/heralding, and entanglement swapping for the establishment of remote correlations.

At the protocol level, SPDs support heralding, BSM operations, and coincidence-based validation. A heralding event can indicate the generation, transmission, or storage of a quantum state, while BSM operations are required in protocols such as quantum teleportation, entanglement swapping, and measurement-device-independent QKD [23]–[26]. In entanglement swapping, for example, a joint measurement on photons from independent entangled pairs can establish entanglement between distant systems that have not directly interacted, thereby extending entanglement across a network [9], [25]. In quantum repeater architectures, these detection-based operations support strategies designed to overcome the loss limitations that otherwise constrain long-distance quantum connectivity [24], [25].

This greater dependence on detector performance arises because many quantum-network operations depend on coincident or joint detection events. In a simplified network-budget representation, the success probability of a joint-detection operation can be expressed as

$$P_{\mathrm{succ}} \simeq p_{\mathrm{BSM}} \prod_{i=1}^{n} \left(\eta_{\mathrm{ch},i} \cdot \eta_{\mathrm{det},i}\right), \tag{5}$$

where p_{BSM} represents an effective, protocol-dependent success factor associated with the BSM or joint-measurement stage, $\eta_{\mathrm{ch},i}$ is the transmittance of the i-th optical path, $\eta_{\mathrm{det},i}$ is the efficiency of the corresponding detector, and n is the number of photons that must be successfully transmitted and detected for the operation to be accepted. In the idealized case of identical channels and detectors, Eq. (5) reduces to $P_{\mathrm{succ}} \simeq p_{\mathrm{BSM}}(\eta_{\mathrm{ch}} \cdot \eta_{\mathrm{det}})^n$.

Although simplified and protocol-dependent, this expression captures the main scaling problem in quantum networks: transmission losses and detector inefficiencies enter multiplicatively. As a result, a moderate reduction in detector efficiency may have a larger effect in a multi-photon network operation than in a single final detection event. Dark counts, timing jitter, and imperfect interference are not explicitly included in Eq. (5); rather, they enter through false heralding, reduced coincidence visibility, and lower fidelity of the generated or swapped entangled state [9], [24], [25].

These functions can impose additional, and in some cases stricter, requirements on SPDs than those encountered in point-to-point communication. False detections may produce incorrect heralding or coincidence events, while limited efficiency reduces the success probability of entanglement-generation, entanglement-swapping, and entanglement-distribution protocols. Timing jitter also affects network operation because many protocols depend on identifying coincidences between photons arriving from independent paths and on synchronizing operations across different nodes [16]–[18]. Operational stability, wavelength compatibility, and integration with sources, memories, photonic circuits, and classical control systems therefore become key requirements for scalable quantum-network implementations.

As network architectures become more complex, these detector limitations accumulate across several stages. In multi-link operations, losses and inefficiencies reduce success probabilities multiplicatively, while dark counts and timing uncertainty can produce false heralding or reduce the visibility of coincidence measurements. Detector performance therefore enters the network budget through entanglement-generation rate, swapping success probability, synchronization accuracy, and the number of attempts required to establish end-to-end connectivity [9], [24], [25]. This is the point at which improvements in SNSPDs, integrated photonic detectors, and optimized avalanche platforms become relevant to network scalability rather than only to device performance.

V. Challenges and Perspectives

The development and selection of SPDs involve coupled trade-offs that prevent a single platform from being ideal for all quantum communication and quantum-network applications. In operational systems, detector choice depends not only on efficiency or noise, but on the combined effect of detection efficiency, dark count rate, timing jitter, maximum count rate, recovery time, wavelength compatibility, operating temperature, cost, stability, and integration potential [16]–[19]. These quantities should be treated as part of a system-level design problem, since improving one metric may increase complexity, cost, or infrastructure requirements associated with another.

Detector selection is therefore architecture-dependent. A laboratory experiment may prioritize efficiency and timing

resolution even at the cost of cryogenic complexity, whereas a field-deployed QKD system may require compactness, stability, reduced maintenance, and compatibility with existing fiber or free-space infrastructure. Satellite or free-space links impose additional constraints related to background light, pointing stability, mass, power consumption, and environmental robustness [27]. Integrated photonic platforms may instead prioritize footprint, scalability, coupling efficiency, and compatibility with on-chip sources and circuits. Consequently, the most suitable SPD platform is not determined by a single figure of merit, but by the balance among performance, integration, and deployability [11]–[13], [19].

Fig. 4 summarizes this design space by grouping the main selection criteria into three system-level dimensions. Performance includes detection efficiency, dark count rate, timing jitter, and maximum count rate. Integration concerns compatibility with telecommunication wavelengths, photonic circuits, detector arrays, sources, memories, and control electronics. Deployability includes operating temperature, cost, long-term stability, maintenance burden, and environmental robustness.

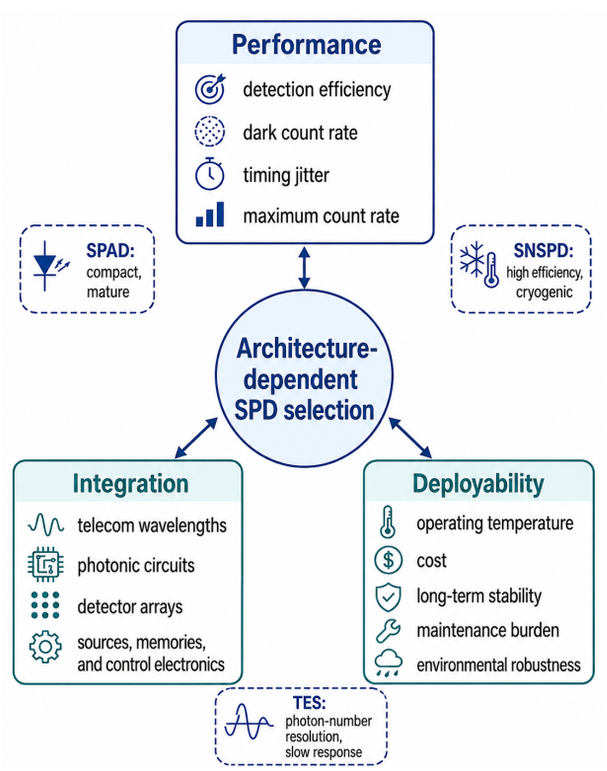

Fig. 4. Architecture-dependent trade-off in SPD selection, balancing performance, integration, and deployability.

The same trade-off appears in the selection of detector platforms. SPADs are mature, compact, and compatible with photon-counting receivers, which makes them attractive for fieldable and integrated systems. Silicon SPADs are effective in the visible and near-infrared regions, whereas InGaAs/InP SPADs are commonly used at telecommunication wavelengths. Their limitations include dark counts, afterpulsing, wavelength-dependent efficiency, and dead-time constraints, especially in high-rate or long-distance links [16], [17], [20], [28]. SNSPDs, in contrast, provide high detection efficiency, low dark count rates, low timing jitter, and broad spectral sensitivity, making them attractive for long-distance fiber links, free-space quantum communication, high-rate QKD, entanglement-distribution protocols, and quantum-network operations [18], [19]. Their main limitation is the requirement for cryogenic operation, which increases infrastructure complexity. TESs occupy a more specialized niche because they can provide high efficiency, photon-number resolution, and energy-resolving detection. These features make them useful for metrology, source characterization, and precision experiments, although their low operating temperatures and slower response make them less suitable for high-speed communication links [17], [29].

TABLE I

SYSTEM-LEVEL COMPARISON OF REPRESENTATIVE SINGLE-PHOTON DETECTOR PLATFORMS.

Platform	Main contribution	Main deployment constraint	Representative role
SPAD	Compactness, maturity, fast response, and compatibility with photon-counting receivers	Dark counts, afterpulsing, dead time, and wavelength-dependent efficiency	Fieldable QKD receivers and compact links
SNSPD	High efficiency, low noise, low timing jitter, and telecom-wavelength compatibility	Cryogenic operation, packaging, and infrastructure complexity	Long-distance links, high-rate QKD, and quantum networks
TES	Photon-number resolution and high detection efficiency	Very low operating temperature and slower response	Metrology, source characterization, and precision experiments

Beyond the platform comparison in Table I, a central engineering task is to translate detector-level improvements into scalable architectures. This includes operation at telecommunication wavelengths, coupling to photonic circuits, development of detector arrays, reduction of cryogenic complexity, long-term stability, calibration procedures, and compatibility with sources, memories, repeaters, and classical control electronics [9], [19]. In quantum networks, where operations may depend on several sequential or simultaneous detection events, gains in efficiency, timing resolution, or noise suppression can improve entanglement-distribution rates, heralding probabilities, and network reliability [9], [24], [25].

This integration problem also has direct implications for the development of defense and dual-use technological capabilities. For countries developing autonomous capabilities in quantum technologies, including Brazil, quantum communication and quantum networking require more than the acquisition of complete systems. They depend on expertise in enabling components and qualification procedures, including detector characterization, photonic coupling, materials and fabrication routes, cryogenic or thermal interfaces, calibration, environmental testing, electronic control, and system-level validation. In this context, expertise in single-photon detection becomes part of the technological base required to evaluate, adapt, certify, maintain, and develop secure quantum infrastructures under national operational constraints [2], [5], [6].

Consequently, progress in SPD technologies should be assessed simultaneously at the material, device, and architecture levels. Low-dimensional materials, integrated superconducting detectors, improved semiconductor avalanche platforms, detector arrays, and hybrid photonic architectures may contribute to more efficient, compact, stable, and scalable

photon-counting systems [18], [19]. For fieldable quantum communication links and future multi-node networks, however, these advances must be coupled to packaging, long-term stability, calibration protocols, supply-chain resilience, and compatibility with classical communication and control infrastructure.

VI. Conclusion

This review analyzed SPDs as functional components of optical quantum communication and quantum-network systems. By converting weak optical quantum states into discrete classical records, detectors connect the physical layer of photon transmission to protocol-level operations such as key generation, coincidence analysis, heralding, and entanglement-based networking.

In point-to-point links, detector efficiency, noise, temporal response, recovery time, and wavelength compatibility condition the link budget, QBER, usable event rate, and transmission range. In networked architectures, the same parameters acquire additional weight because several operations depend on joint or sequential detections. The selection of SPADs, SNSPDs, TESs, or emerging integrated platforms should therefore be guided by the requirements of the target architecture rather than by a single detector metric.

From a defense and dual-use perspective, detector performance is part of the reliability chain required for future quantum communication links and quantum networks supporting secure information exchange, distributed sensing, clock synchronization, satellite and free-space optical links, and command-and-control infrastructures. For countries seeking autonomous capabilities in quantum technologies, with Brazil among them, competence in single-photon detection should be understood as part of a broader technological base involving photonics, materials, characterization, calibration, integration, qualification, and long-term system maintenance. Progress in these areas strengthens national capacity to evaluate, adapt, certify, and develop secure quantum infrastructures aligned with operational and strategic requirements.

References

[1] J. P. Dowling and G. J. Milburn, "Quantum technology: the second quantum revolution," *Phil. Trans. R. Soc. A*, vol. 361, no. 1809, pp. 1655–1674, 2003.

[2] M. Krelina, "Quantum technology for military applications," *EPJ Quantum Technol.*, vol. 8, no. 1, p. 24, 2021.

[3] A. Acín *et al.*, "The quantum technologies roadmap: a European community view," *New J. Phys.*, vol. 20, no. 8, p. 080201, 2018.

[4] Quantum Flagship. (2016) Quantum manifesto: A new era of technology. Accessed: Jun. 14, 2026. [Online]. Available: https://qt.eu/media/pdf/93056_Quantum-Manifesto_WEB.pdf

[5] E. P. Maldonado *et al.*, "Initiative in quantum networks and their applications at the Aeronautics Institute of Technology (ITA)," *Spectrum*, vol. 25, no. 1, pp. 31–35, 2024.

[6] A. J. C. Chaves, D. D. C. Brito, R. P. Ferreira, and V. G. M. Duarte, "Tecnologias quânticas: prospecto atual, desafios e oportunidades para as Forças Armadas Brasileiras," in *Proc. Simpósio de Aplicações Operacionais em Áreas de Defesa*, São José dos Campos, Brasil, 2023, accessed: Jun. 14, 2026. [Online]. Available: https://www.sige.ita.br/edicoes-anteriores/2023/st/235536_1.pdf

[7] J. Lino da Silva and I. Brosso, "Quantum remote sensing applied to national defense," *Spectrum*, vol. 26, no. 1, pp. 78–83, 2025.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[9] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: a vision for the road ahead," *Science*, vol. 362, no. 6412, p. eaam9288, 2018.

[10] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[11] M. Krelina, "The prospect of quantum technologies in space for defence and security," *Space Policy*, vol. 65, p. 101563, 2023.

[12] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, p. 16025, 2016.

[13] J. S. Sidhu *et al.*, "Advances in space quantum communications," *IET Quantum Commun.*, vol. 2, no. 4, pp. 182–217, 2021.

[14] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, 2014.

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[16] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nat. Photon.*, vol. 3, no. 12, pp. 696–705, 2009.

[17] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, 2011.

[18] L. You, "Superconducting nanowire single-photon detectors for quantum information," *Nanophotonics*, vol. 9, no. 9, pp. 2673–2692, 2020.

[19] T. H. Dao *et al.*, "Single-photon detectors for quantum integrated photonics," *Photonics*, vol. 12, no. 1, p. 8, 2025.

[20] M. Rahmanpour, A. Erfanian, A. Afifi, M. Khaje, and M. H. Fahimifar, "Implementable methods for characterizing single photon avalanche diode parameters," *Results Opt.*, vol. 16, p. 100709, 2024.

[21] A. Lee, A. Tello Castillo, C. Whitehill, and R. J. Donaldson, "The impact of spot-size on single-photon avalanche diode timing-jitter and quantum key distribution," *IET Quantum Commun.*, vol. 5, no. 4, pp. 443–449, 2024.

[22] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[23] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, 1993.

[24] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5932–5935, 1998.

[25] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Rev. Mod. Phys.*, vol. 83, no. 1, pp. 33–80, 2011.

[26] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, 2012.

[27] G. Tsochev, E. Gieva, and M. Nenova, "Single-photon detectors for satellite and CubeSat quantum key distribution: a systematic evidence map," *Entropy*, vol. 28, no. 3, p. 295, 2026.

[28] M. Abrari, S. T. Sajjadian, P. Nedaei, and M. Ghanaatshoar, "Recent developments in single-photon avalanche diode (SPAD) technologies: from device engineering to optimized photonic performance in quantum communication," *Photonics*, vol. 13, no. 7, p. 650, 2026.

[29] A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," *Opt. Express*, vol. 16, no. 5, pp. 3032–3040, 2008.