NIST Interagency Report
NIST IR 8483

Advanced Communications Technologies Standards

Report of the

Advanced Communications Technologies

Working Group

Robert B. Bohn
Christopher Greer
Jason Kahn

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8483

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8483

Advanced Communications Technologies Standards

Report of the

Advanced Communications Technologies

Working Group

Robert Bohn
Christopher Greer
Jason Kahn
Communications Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8483

September 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST IR 8483
September 2023

Publication History
Approved by the NIST Editorial Review Board on 2023-08-30

How to Cite this NIST Technical Series Publication
Bohn, R., Greer, C., Kahn, J. (2023) Advanced Communications Technologies Standards, Report of the Advanced Communications Technologies Interagency Working Group. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8483.
https://doi.org/10.6028/NIST.IR.8483

NIST Author ORCID iDs
Robert Bohn: 0000-0003-4014-0801
Christopher Greer: 0000-0002-6669-3941
Jason Kahn: 0000-0003-3798-8668

Contact Information
robert.bohn@nist.gov

Abstract

This report of the Advanced Communications Technologies Working Group of the Interagency Committee on Standards Policy (ICSP) provides an overview of Federal agency advanced communications technologies (ACT) standards activities and recommends standards priority areas for ICSP consideration. The ACT standards priorities recommendations section of the report sets out nine areas for consideration by the ICSP. The landscape review section provides an overview of each contributing agency's relevant ACT standards activities, including its mission, ACT goals, role in ACT standards, participation in standards development organizations, ACT focus areas, and examples of standards activities for each contributing Federal agency or office.

Keywords

Advanced communications technologies; international technical standards; Federal agency standards activities; standards; standards development organizations, standards priority areas.

Table of Contents

List of Tables

Executive Summary

This report of the Advanced Communications Technologies Working Group (ACTWG or Working Group) of the Interagency Committee on Standards Policy (ICSP) provides an overview of Federal agency advanced communications technologies (ACT) standards activities and recommends standards priority areas for ICSP consideration. This technical report provides an analysis of the communications technologies standards landscape based on input from the participating Federal agencies.

The primary strategy for Federal agency engagement in ACT standards development, as set out in Circular A-119 from the Office of Management and Budget (OMB) and the National Technology Transfer and Advancement Act (NTTAA), focuses on reliance on private sector leadership supplemented by Federal government contributions to discrete standardization processes.

Participation by agencies in standards activities focuses on open, consensus-based, voluntary, private sector-led, and science- and engineering-informed standards that enable:

- Innovation in products and services;
- Interoperability across systems and devices;
- Open and competitive national and global markets; and
- Efficient and effective acquisition processes.

The Advanced Communications Technologies Working Group (ACTWG) was chartered by the Interagency Committee on Standards Policy (ICSP) to enable interagency coordination on communications technologies (CT) standards efforts. Nineteen Federal agencies, departments, and offices are participating in this interagency group.

This annual report of the Working Group to the ICSP provides:

- Recommendations for ACT standards priorities areas; and an
- Overview of ACT standards activities for each of the contributing agencies or units.

The ACT standards priorities recommendations section of the report sets out nine areas for consideration by the ICSP.

- **Security and Privacy** – Standards for CT security and resilience, including compromise detection and sustained safe operation; CT systems supply chain security and reliability; and distributed ledger methods for cooperative trust and privacy protection among network entities.
- **End-to-End Services and Assurance** – CT standards for architectures, protocols, and measurement methods that support differentiated and optimized services tailored to and responsive to application requirements, including those for critical infrastructure systems.
- **Emerging Network Technologies** – Standards for AI-enabled network systems; networks supporting AI-enabled applications and distributed systems; and automated, virtual networks and services.
- **Internet of Things** – Standards for massively-scaled connectivity and interoperability in IoT environments including connected vehicles, uncrewed aerial systems (UAS),

intelligent infrastructure and smart cities, eHealth, advanced manufacturing, emergency response, smart grid, and other application areas.

- **Emerging & Future IP Networks** – Standards that promote innovation, enable broad participation, and preserve access and privacy for next-generation IP network technologies.
- **Spectrum Measurement & Management** – CT standards for maximizing spectrum resources for 5G and 6G technologies, including channel propagation models and measurement methods, wireless coexistence, antenna evaluation methods, and integrated satellite communications.
- **Open Source and De Facto Standards** – Strategic Federal role in accelerated standards processes, including interactions with industry consortia and alliances developing de facto standards.
- **Communications for Data Access and Sharing** – CT standards meeting the rate, volume, quality of service, security, and privacy needs of the expanding data universe and a global information society.
- **Quantum Communications** – CT standards for quantum technologies, including memory, interfaces, and key distribution systems, that enable advanced quantum networks and their interactions with conventional network systems.

1. Introduction and Overview

1.1. Strategy and Policy for Government Engagement in Standards Development

As described below, it is the policy of the Federal government to rely on the private sector led voluntary consensus standards whenever possible. Voluntary consensus standards development processes are those that are open, balanced, and consensus-based, with provisions for due process and appeals. Voluntary consensus standards that are informed by good science and engineering can be a powerful force for:

- Innovation in products and services development;
- Interoperability across systems and devices;
- Open and competitive national and global markets; and
- Efficient and effective acquisition processes.

Reliance on private sector leadership, supplemented by Federal government participation and contributions during the development of standards, remains the primary U.S. strategy for government engagement in standards development.

This strategy is implemented in both legislation and policy. With respect to legislation, the National Technology Transfer and Advancement Act (P.L. 104-113 or NTTAA) directs Federal agencies to use technical standards "that are developed or adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments." The Act further provides that "Federal agencies and departments shall consult with voluntary, private sector, consensus standards bodies and shall, when such participation is in the public interest and is compatible with agency and departmental missions, authorities, priorities, and budget resources, participate with such bodies in the development of technical standards." The National Institute of Standards and Technology (NIST) is charged with coordinating Federal agency implementation of NTTAA provisions.

The Trade Agreements Act of 1979 (as amended) prohibits U.S. agencies from engaging in standards-related activities that create unnecessary obstacles to trade and gives the U.S. Trade Representative (USTR) the responsibility to coordinate the consideration of international trade policy issues related to standards and conformity-assessment procedures.

With respect to policy, a central element in implementing the National strategy is Office of Management and Budget (OMB) Circular A-119 on Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity-Assessment Activities. The Circular directs agencies to use voluntary consensus standards in lieu of government-unique standards except where inconsistent with law or otherwise impractical. It also provides guidance to agencies on participation in the development of voluntary consensus standards and articulates policies relating to the use of standards by Federal agencies.

The October 2011 memorandum[1] from the Subcommittee on Standards of the National Science and Technology Council provides a high-level overview of the legal and policy framework for

[1] https://www.nist.gov/system/files/documents/standardsgov/Federal_Engagement_in_Standards_Activities_October12_final.pdf

government engagement in private-sector standards and sets out the following fundamental objectives for Federal government engagement in standards activities.

- Ensure timely availability of effective standards and efficient conformity assessment schemes critical to addressing national priorities
- Achieve cost-efficient, timely, and effective solutions to regulatory, procurement, and policy objectives
- Promote standards and standardization systems that enable innovation and foster competition
- Enhance U.S. competitiveness while ensuring national treatment
- Facilitate international trade and avoid the creation of unnecessary obstacles to trade

1.2. Interagency Committee on Standards Policy

This technical report provides an analysis of the communications technologies standards landscape based on input from the participating Federal agencies. The Interagency Committee on Standards Policy (herein after referred to as the "ICSP" or "Committee") advises federal agencies on matters related to standards policy, as required under the National Technology Transfer and Advancement Act of 1995 (NTTAA). The ICSP provides a forum for coordination on policies related to Federal participation and use of standards and conformity assessment consistent with OMB Circular A-119. It reports to the Secretary of Commerce through the Director of the National Institute of Standards and Technology (NIST) and the Director of NIST's Standards Coordination Office (SCO).

The Committee's authority is set out in Section 13 b of OMB Circular A-119 Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities of the Office of Management and Budget (OMB). The Circular establishes policy to be followed by executive agencies in participating in activities of voluntary standards organizations and in adopting and using voluntary standards. The Circular was last revised on February 10, 1998 and was published in the Federal Register (63 FR 8545) on February 19, 1998.

The purpose of the Committee is to promote effective participation by the Federal Government in domestic and international standards and conformity assessment activities and the adherence to uniform policies by Federal agencies in the development and use of standards and in conformity assessment activities. Well-considered Federal policies reflecting the public interest can expedite the development and adoption of standards that stimulate competition, promote innovation, and protect the public safety and welfare. The objective of the Committee is to promote effective and consistent standards and conformity assessment policies in furtherance of U.S. goals and to foster cooperative participation by the Federal Government, U.S. industry, and other private organizations in standards and conformity assessment activities. More information is available at: https://www.nist.gov/standardsgov/interagency-committee-standards-policy-icsp .

1.3. Advanced Communication Technologies Working Group

The Advanced Communications Technologies Working Group (herein after referred to as the "ACTWG" or "Working Group") is established under the provisions of the charter of the Interagency Committee on Standards Policy (ICSP). The objective of the ACTWG is to facilitate coordination of Federal agency advanced communications technologies (ACT) standards activities, respond to requests for information, and develop recommendations relating to ACT standards policy matters to the ICSP. The ACTWG is responsible for the following.

1. Assisting the ICSP in promoting effective and consistent Federal policies in advanced communications technologies standards.
2. Providing an annual report to the ICSP on the current ACT standards activities of participating Federal agencies and recommendations for strategic directions in Federal ACT standards efforts.
3. Responding to requests for information and advising the ICSP on effective means of coordinating advanced communications technologies standards activities with those of the private sector.
4. Sharing best practices in advanced communications technologies standards among Federal agencies.
5. Coordinating Federal advanced communications technologies standards interests across application areas such as transportation, energy, public safety, and others.

This report was developed under the provisions of item (2) above.

2. Recommendations to the ICSP for Strategic Standards Priority Areas

The ACTWG charter directs the Working Group to provide an annual report to the ICSP, including "recommendations for strategic directions in Federal Advanced Communication Technologies (CT) standards efforts." Through its monthly meeting process, the Working Group identified nine priority areas for strategic standards coordination across Federal agencies and offices. The priority areas are:

- **Security and Privacy** – Standards for CT security and resilience, including compromise detection and sustained safe operation; CT systems supply chain security and reliability; and distributed ledger methods for cooperative trust and privacy protection among network entities.
- **End-to-End Services and Assurance** – CT standards for architectures, protocols, and measurement methods that support differentiated and optimized services tailored to and responsive to application requirements, including those for critical infrastructure systems.
- **Emerging Network Technologies** – Standards for AI-enabled network systems; networks supporting AI-enabled applications and distributed systems; and automated, virtual networks and services.
- **Internet of Things** – Standards for massively-scaled connectivity and interoperability in IoT environments including connected vehicles, uncrewed aerial systems (UAS), intelligent infrastructure and smart cities, eHealth, advanced manufacturing, emergency response, smart grid, and other application areas.
- **Emerging & Future IP Networks** – Standards that promote innovation, enable broad participation, and preserve access and privacy for next-generation IP network technologies.
- **Spectrum Measurement & Management** – CT standards for maximizing spectrum resources for 5G and 6G technologies, including channel propagation models and measurement methods, wireless coexistence, antenna evaluation methods, and integrated satellite communications.
- **Open Source and De Facto Standards** – Strategic Federal role in accelerated standards processes, including interactions with industry consortia and alliances developing de facto standards.
- **Communications for Data Access and Sharing** – CT standards meeting the rate, volume, quality of service, security, and privacy needs of the expanding data universe and a global information society.
- **Quantum Communications** – CT standards for quantum technologies, including memory, interfaces, and key distribution systems, that enable advanced quantum networks and their interactions with conventional network systems.

In this section, each priority area is summarized with an introductory definition, a review of the current state of work in the priority area including trends, and future opportunities and priorities within the priority area.

2.1. Security and Privacy

2.1.1. Introduction

Future communication networks will be more immersed in every aspect of our society and hence must be more secure and resilient. At the same time, these networks will be more distributed, dynamic, complex, and hence more difficult to protect. Consequently, they will require more scalable and distributed trust management, more timely detection of compromises, reliable and resilient operation even when compromised, and risk-appropriate remote responses to incidents. Furthermore, industries are becoming increasingly connected ecosystems (e.g., interconnected producers, suppliers, brokers, delivery companies, and customers in a supply chain) that are susceptible to many security vulnerabilities, counterfeit components, and poorly designed processes. Standards and guidelines are needed for advanced cybersecurity and privacy approaches that go beyond current methods to meet the needs of future communication networks.

2.1.2. Current State

Current Standards Work

- Infrastructure Security
    - Hardware Based Platform Measurement is a means of measuring, collecting, and storing boot and firmware information to confirm the integrity of each platform in the infrastructure, which is measured and stored in a tamper resistant Hardware Security Module (HSM) such as a local Trusted Platform Module (TPM). A TPM has its own processor, RAM, ROM, and NV-RAM. It exists outside of bootloader, firmware, and OS. It is passive unless commands passed via system software. It can measure configuration and state of software on the system, among other things.
    - Hardware Based Labeling is a means of identifying or labeling an individual platform with a key value pair, which is a combination of attributes that are associated with a particular platform. The platform's key value pair will be extended onto a HSM such as a local trusted platform module (TPM).
    - Remote attestation (RA) is a central remote service that is responsible for verifying the integrity of a platform by collecting the servers' measurements and labels at boot and comparing them to the expected measurements and labels for the respective server. It can share the results of a platform’s attestation to a component in the architecture that is responsible for reporting, alerting, or enforcing rules in the environment based on given events.
    - Network Function Orchestration Enforcement: RA gives the orchestration component the ability to determine which servers are to host specific Network Functions (NFs). This determination is based on the platform measurements and

labels retrieved and attested to by the RA service. After successfully determining the servers that should host the NF, the orchestrator can deploy and migrate them.

- 5G SA Security

    - There is a focus on security capabilities that have been incorporated into 3GPP specifications as interoperable. Security capabilities include Subscriber Privacy, Radio Network Security, Authentication Enhancements, Interworking & Roaming Security, API Security, Network Slicing Security, Application Security, and Internet Security Protocol Recommended Practice.

Trends

- High Performance Systems: High Performance Systems are used in the support of high performance/mission critical use cases. This includes aspects such as ultra-reliable low latency comms, enhanced mobile broadband, massive machine-type communications, and vehicle-to-everything technology.

- Increased vSoftwarization: Increased vSoftwarization is the transition of hardware to software in the cloud. Aspects of this include software that suns on high-performance commercial off-the-shelf hardware. Increased vSoftwarization enables CI/CD, 2-edge sword for Security.

- Zero Trust (ZT): ZT assumes no implicit trust is granted to assets or users based solely on their physical or network location (i.e., local area networks versus the Internet) or asset ownership (enterprise or personally owned). This shift in philosophy is a significant change in legacy authentication and security mechanisms.

- Automation & Orchestration: Automation & Orchestration includes end-to-end service orchestration, and automation where manual operations are too complex and slow.

- Generally, the trends are moving toward more automated, virtualized, distributed, high-performance connectivity of diverse devices.

Participation in Standards Development Organizations (SDOs)

- 3GPP: RAN (Radio Access Network), SA2 (System Architecture and Services), SA3 (Security and Privacy),
- Internet Engineering Task Force (IETF): Security Area
- Internet Engineering Task Force (IETF): Secure Inter-domain Routing (SIDR)
- International Society of Automation (ISA): Industrial Automation And Control Systems Security
- SAE International (SAE): Cyber Physical Systems Security Committee

2.1.3. Future goals and priorities

Goals and priorities

- Research and develop guidelines that can be implemented in documentary standards for securing future communication networks which will be more complex, resilient, and difficult to protect.

Opportunities to make an impact

- 5G SA vs 5G non-Standalone (NSA): There are many research projects that are focused on 5G SA. But, there are still many commercial deployments of 5G non-Standalone (NSA) systems. Because of the magnitude of investments in 4G networks and 5G NSA systems, 5G NSA networks will be pervasive for many years to come. More research should be done on the security and privacy aspects of 5G NSA networks. Also, there could be vulnerabilities with communications between 5G SA and 5G NSA networks. A specific example is the N26 interface between the 5G NSA Evolved Packet Core (EPC) and the 5G SA 5G Core (5GC).

- Open RAN: There has been significant interest in the standardization of open Radio Access Networks. Security has been a large aspect of this, however there is a new component to the Open RAN architecture called the RAN Interface Controller (RIC). The RIC is a high value target for attack due to its comprehensive data about the operation of the 5G (and 4G) networks. Priority should be placed on study, remediation, and standardization of security for the RIC.

- Virtualization, Containerization and Public/Hybrid Cloud: With the deployment of 5G network infrastructure, many carriers have deployed virtualized or containerized platforms. The use of public loud providers and/or hybrid cloud deployments has increased. Studies have been done for individual sub-systems and networks layers. But, there have been limited studies and work done on the overall security of the deployments in full, particularly with respect to the implementation of zero trust standards.

2.2. End-to-End Services and Assurance

2.2.1. Introduction

Advanced communication networks, including 5G and beyond, are moving beyond one-size-fits-all connectivity to supporting differentiated and optimized services. However, assuring end-to-end (E2E) differentiated quality of service (QoS) remains a significant challenge. New approaches will be required to enable not only QoS provisions, but also quality of experience (QoE) capabilities that measure end user's experience (e.g., voice quality, speech intelligibility, message delivery success, E2E delay to access/use resources, and total system latency). Providing E2E service assurance will require new architectures, protocols, and measurement methods standards for applications such as telehealth, automated transportation, and advanced energy infrastructures.

The central terms used in this section are defined as follows:

- End-to-End: Communications performance as measured from application to application, including all system and network layers [1] [2].
- Quality of Service (QoS): A measure of the ability of a communications system to provide assured performance in metrics such as availability, latency, throughput, loss, or jitter by assigning differentiated priorities to specified applications, users, or data [3].
- Quality of Experience (QoE): A measure of communications system performance from the perspective of a user, including metrics such as interface quality (visual, aural, tactile), intelligibility, usability, timeliness, and availability of services and resources [4].

2.2.2. Current State

Current Standards Work

- The concept of QoS in communications infrastructure is not new, but the network drivers are changing and so research is ongoing on how to improve QoS across networks, especially enterprise networks. An example is that network traffic mix and characteristics are changing to where currently 90% of the traffic is now video related. There is higher bandwidth capability, advancements in standards from the IETF, new generations of wireless networks (5G), and increased security needs. Network technologies have also evolved to be packet switched and to include QoS needs in regard to differentiated packet treatments. When simple data was the primary need for networks, the traffic could be bursty and there was no sensitivity to drops and delays. But with Voice over IP (VoIP) and video, the traffic has become sensitive to drops and delays. The IETF has defined various QoS models, with 3 becoming prominent. One is Best Effort (which is no QoS) [5], [6], [7], Integrated Services or IntServ [6], and Differentiated Services or DiffServ [7], [8].

- Different types of networks have evolved to meet the QoS needs of network users, especially for time sensitive applications. Three examples of this networking are: Time Sensitive Networking (TSN) [9], [10], [11], Deterministic Networking (DetNet) [12], [13], and Optical Transport Networking (OTN) [14], [15], [16].

- TSN is a layer 2 technology that runs over Ethernet and runs in a best-effort packet network, which is important because many enterprise networks still operate best effort networks. TSN provides time synchronization (IEEE 1588) and has network use cases such as electrical power generation and distribution, industrial machine-to machine communication, and automotive and vehicle applications. TSN provides extensions to traditional Ethernet-based networks, such as synchronization, prioritization, and determinism and bounded latency. TSN converges IT, which is bandwidth-focused, and OT, which is availability-focused. But, best effort traffic will not block time-critical traffic in TSN.

- DetNet was created by the IETF to deliver end-to-end QoS over routed IP networks. DetNet operates at Layer 3 routed segments to provide IntServ and DiffServ integration, and delivers service over the lower Layer 2 bridged segments. It enables the secure exchange of information in industrial systems.

- Optical Transport Networks focus on having the highest survivability, providing protection and finding new paths if a path is broken. Open Platform Communications (OPC) Unified Architecture (OPC UA) is a platform-independent standard that enabled the secure exchange of information, primarily in industrial systems. OPC UA enhances the interoperability between devices by enriching raw data with semantic descriptions, which allows operators to use a multitude of different devices.

- Research was performed in the building of private networks for various industry verticals. Each vertical has unique use cases and has specialized QoS needs in regard to the use cases. As a proof-of-concept (POC) or to perform build pilots, a network platform for an industry vertical has been built with unique characteristics, such as: architecture including but not limited to RAN segment in network slices and Next Generation RAN; algorithms including but not limited to smart orchestration and resource control algorithms and forecasting and inference algorithms; and a framework including but not limited to a security and auditability framework. During the testing of the POCs and pilots, KPIs are typically monitored. Examples of these KPIs are: Round-trip time (RTT) latency, uplink data rate, downlink data rate, and reliability. Based on the results of the POCs and pilots, contributions have been made to open source projects such as docker, OpenStack, ONOS, and OpenSource MANO. Also, contributions have been submitted to various SDOs including the 3GPP, IETF/IRTF, IEEE, and the GSMA.

Trends

- There is growing use, or desire to use, Artificial Intelligence (AI) to analyze network data, predict and prevent network faults, and optimize network performance automatically and efficiently.

- Within optical networks, there is a growing trend of IP and Optical integration using pluggable options. Also, there are two new technologies emerging, Digital Coherent Optics (DCOs) and Multilayer software defined networking (SDN) control plane.

- Industry verticals are starting to look towards private networks to meet their specialized QoS and QoE needs.

- To aid in the build of the private network, industry verticals are using a combination of standards-based architecture, proprietary innovations, and open source solutions.

Participation in Standards Development Organizations (SDOs)

- 3GPP: SA1 (Services), SA2 (System Architecture and Services)
- IETF: Operations and Management Area (ops), Routing Area (rtg), Transport Area (tsv),

- IETF/IRTF: Internet Research Task Force Information Centric Networking Research Group (ICNRG)
- IEEE - SA: Interoperability

2.2.3. Future Goals and Priorities

Goals and priorities

- Innovate and standardize new architectures, protocols, and measurement methods to enable not only QoS provisions, but also QoE capabilities, for end-to-end services and assurances.

Opportunities to make an impact

- Standardization of Multilayer SDN control plane
- Assistance in providing missing links at the architecture level between 3GPP, ETSI NFV and IETF
    - Open source projects also leading some advanced features → work needed to get an integrated E2E solution for networks that encompass open source and traditional standardized architecture
- Participation in working groups within established standards organizations, such as the IEEE 802.1 Working Group, GSMA Internet Group and GSMA Networks Group

2.3. Emerging Network Technologies

2.3.1. Introduction

Future networks will become not just highly automated but also increasingly autonomous. Future network capabilities extend beyond automating network operations to dynamically self-learn in becoming more intelligent, capable, and adaptive. These future networks will rely heavily on Artificial Intelligence (AI), Machine Learning (ML), and other new technologies such as edge intelligence. Standards are needed that support broad implementation of new ways to explore, validate, and trouble-shoot AI/ML-powered distributed network functions and how these functions can work together to accomplish intended networking goals.

2.3.2. Current State

Current Standards Work[2]

- User Access
    - Satellites – Integrating 5G satellite and terrestrial systems, robust use cases and reference architectures, QoS user equipment to satellite access and propagation delays, antenna systems, network virtualization.

[2] Based on IEEE International Networks Generations Roadmap

  - Deployment – Access, service delivery, operations and service management, network extensions, legislative and regulatory environments (including local, regional, national, and international).
  - Connecting the Unconnected – Micro-operators, dedicated network slices, least-cost wireless front-haul and backhaul and mobile integrated access and backhaul.

- Network Components and Performance
  - Edge Services – Mobile edge architecture, edge security, edge-native services, AI/ML for edge service latency reduction and throughput optimization, service level indicators and agreements.
  - Massive MIMO – Increase capacity and improve physical layer security, deployments in varying conditions (e.g. indoor/outdoor, small cells, etc.), hardware implementation architectures (digital/analog/hybrid), optimizing beam-based wireless environments.
  - Systems Optimization – Dynamic optimization, self-organization, resource negotiation/allocation, cross-domain federation, autonomous systems models
  - Optics – Optical front/mid/backhaul networks, Co-packaged optics, optical switching, light fidelity, non-terrestrial networks, optical intersatellite links, quantum communications.
  - mmWave – Architectures, hardware capabilities, signal processing for mid-band and high-band deployment, mesh networked terminals and user equipment, testing for resiliency, quality of service, and optimization of resources; health and safety provisions.

- Systems and Standards
  - Standardization Building Blocks – Cooperation across SDOs, industry fora, and open-source communities; strategies for emerging and future technologies, pace of development, enabling innovation.
  - Testbeds – Systems optimization testbeds, 5G/6G testbeds, federation for scaling, resource utilization, complexity, and cross-domain applications
  - Energy Efficiency – Energy-efficient architectures and control, edge optimization, real-time power optimization, energy-centric network simulation, small cell migration

- Services and Enablers
  - Security and Privacy – Management and orchestration, edge security, third parties, data privacy, security monitoring and analytics, predictive/proactive security, 5G digital forensics, transmission security features and resilience
  - Applications and Services – Agriculture, education, energy, health care, public safety, transportation, water and wastewater, smart cities and regions
  - Artificial Intelligence and Machine Learning – Network automation, network slicing, digital twins, dynamic spectrum access, cloud and edge access, quantum communications

Trends

- Integration of terrestrial and satellite networks
- Mid-band and high-band mmWave deployments
- AI/ML and network virtualization

Participation in Standards Development Organizations (SDOs)

- 3GPP NTN (Non-Terrestrial Networks, Spectrum Slicing, Radio Layer 3)
- ETSI (Network Functions Virtualization, Management and Orchestration)
- IEEE (Future Networks)
- ITU SG13 (Future Networks), SG17 (Cybersecurity)
- ITU WRC-23 (Satellite Systems, Res. 172-178)

2.3.3. Future Goals and Priorities

Goals and priorities

- Advance communication networks by expanding user access, improving quality of service, enhancing security and privacy, and optimizing spectrum use.

Opportunities to make an impact

- Enable open, consensus-based standards at the pace of technology innovation
- Facilitate the emergence of quantum communications
- Explore AI/ML capabilities for enhanced network functions

2.4. Internet of Things

2.4.1. Introduction

Advanced communications technologies are the essence of the Internet of Things (IoT), especially for IoT applications with stringent latency and reliability requirements (e.g., automated driving, vehicle teleoperation, and factory automation). Challenges include connecting billions of devices, meeting stringent performance and reliability requirements, enabling interoperability, ensuring security and privacy for networked devices across different domains, and providing wireless networking capabilities in complex environments. Important application areas include connected vehicles, advanced manufacturing, and medical devices and systems. Developing a coherent strategic approach to IoT standards efforts can accelerate the adoption of effective IoT applications across all sectors of our society and economy.

2.4.2. Current State

Current Standards Work

- Industrial Wireless Environments

Increasing number of IoT devices will need innovative methods to connect to the internet or local networks. The environment of Industry 4.0. will sense everything, reliably, on-time for applications such: UAVs, robots, CNC's, analytics, materials, safety, personnel tracking, vision, safety, etc. Wireless technology offers many opportunities for increased connectivity since their installations are easier and have lower costs resulting in a simpler infrastructure [1]. Further, one will be able to install more devices for a given bandwidth on a single network are possible as bandwidth increases with RF band. Increased connectivity will have many benefits and provide lots of data which will lead to better analytics in this diverse wireless landscape.

However, a real-world situation is a non-pristine radio environment that has a series of additional issues such as interference from other networks (coexistence), blockages (attenuation), multipath, machine noise (non-communications) and intentional jamming. In addition, spectral awareness of the environment needs to be considered such as spectrum planning, continuous sensing, and control system co-design. Other concerns are transmission scheduling for QoS, TCP ACK coordination, random back-off issues, and the possible diversity options.

These concerns are addressed on 2 fronts, the creation of an industrial wireless testbed (IWT) at NIST with industry collaborators and the current development of a standard - IEEE P1451.5p - Standard for Radio Frequency Channel Specifications for Performance Assessment of Industrial Wireless Systems, currently established as IEEE 3388 [2]. NIST has published multiple guides to industry on wireless environments [3-6], measurements and testing [7-12], and sponsored international workshops. The standard is intended for applications to industrial wireless communications systems involving sensors and actuators and their monitoring and control, e.g., the IEEE Std 3388 wireless smart transducer interfaces for connecting sensors and actuators and control devices to form distributed control systems. This standard is therefore an important step towards the adoption of wireless for control systems and the assurance of the performance of wireless technology used in smart manufacturing systems.

- Cybersecurity for IoT

Advanced technologies enable digital transformation and can increase risk. The Internet of Things is wide open and will have a predominant role in Blockchain, ML, Big Data, Augmented Reality, and AI. Smarter cities will be an interconnected "system of systems" leveraging data to improve operations, energy use, efficiency, safety, quality of life, the environment, and the citizen experience. Connected healthcare will enable precision healthcare to improve insights and outcomes by leveraging big data, artificial intelligence, machine learning and quantum tools and techniques.

Cyberattacks [1][7] on healthcare devices result in attacks on device operation (insulin pumps [2], pacemakers [3]), hardware/software, data theft, data integrity, loss of privacy, compliance and ransomware pose a risk to the physical health and safety of the patient.

These specific connected healthcare concerns are addressed by TIPPSS for IoT– the New Cybersecurity Paradigm (Trust, Identity, Privacy, Protection, Safety, Security). This is on-going work as IEEE/UL P2933 – Clinical IoT Data and Device Interoperability with TIPPSS Working Group [5,6]. This standard establishes the framework with TIPPSS principles (Trust, Identity, Privacy, Protection, Safety, Security) for Clinical Internet of Things (IoT) data and device validation and interoperability. This includes wearable clinical IoT and interoperability with healthcare systems including Electronic Health Records (EHR), Electronic Medical Records (EMR), other clinical IoT devices, in hospital devices, and future devices and connected healthcare systems.

Trends

- Investigating interaction of wireless transmission/receiving with physical environment.
- Reducing latency, increasing bandwidth
- AI/ML applied to security, functionality, and energy efficiency for devices.

Participation in Standards Development Organizations (SDOs)

- 3GPP: RAN1 (Physical Layer)
- IEEE: Internet of Things
- Industrial Internet Consortium (IIC): Security Working Group https://www.iiconsortium.org/wc-security/
- ISO/IEC: JTC 1/SC41

2.4.3. Future goals and priorities

Goals and priorities

- Develop secure, reliable, and efficient communication networks that can support a wide range of devices and applications.

Opportunities to make an impact

- Explore AI/ML capabilities to enhance wireless transmission and to decrease latency.
- Lead programs in open, consensus-based standards and workshops.
- Smart cities, Industry 4.0, environmental monitoring

2.5. Emerging and Future IP Networks

2.5.1. Introduction

While the basic architecture of the public Internet has remained unchanged for several decades, a new generation of more advanced private IP networks is now providing more sophisticated services beyond best-effort packet forwarding. To address this growing divergence, several significant efforts are underway in various international standards bodies. Ensuring that these

efforts provide for openness, interoperability, reliability, and security in future IP networks that promote freedom of expression, open communication and trade, and rights for peaceful assembly and association is paramount. Developing and standardizing such future IP networks will be essential to both next-generation networks, such as 6G, and the Internet more generally.

2.5.2. Current State

Current Standards Work

- Named Data Networking (NDN) and Information Centric Networking (ICN)
    - Secure IoT – Use of NDN for secure onboarding of IoT devices, for device authentication, and establishing secure communications.
    - Secure Handhelds on Assured Resilient Networks at the Tactical Edge (SHARE) – SHARE moves management functions of multiple security levels from central locations to devices on the network edge. NDN in SHARE provides data transformation on handheld devices, group communication capabilities, the ability to run in a Disconnected Intermittent Low-bandwidth (DIL) environment, and additional security.
    - Mission-Integrated Network Control (MINC) – MINC ensures that critical data finds a path to the right user at the right time via secure control of any available communication or networking resources. NDN in MINC provides data oriented architecture suitable for Machine Learning (ML), the ability to run in a Disconnected Intermittent Low-bandwidth (DIL) environment, and additional security.
    - Information Trust – Decisions are made with the assumption that all data is inherently trustworthy, but Cyber protection techniques do not prevent data from being compromised prior to the digital signature or encryption processes. Information Trust addresses the issue of trusted data being compromised prior to the digital signature or encryption processes via blockchain and ML/AI implementations to provide data integrity. NDN in Information Trust provides data oriented architecture suitable for ML applications to identify possibly compromised data, group communication capabilities to enable highly redundant blockchain-based data log, the ability to run in a Disconnected Intermittent Low-bandwidth (DIL) environment, and additional security.
    - NDN-specific hardware – Routers and other similar hardware equipment are needed in the network infrastructure for the enhanced NDS and ICN capabilities. One example, NDN-DPDK, is a high performance NDN router (forwarder). It is the first parallel router design for the NDN architecture with a target performance of 100 Gbps. Other NDN-specific use-case hardware is also being researched.

- Open RAN
    - Network slicing – Using data-driven closed-loop control with the RAN Intelligent Controller (RIC) to automatically tune the RAN parameters for each network slice.

- Open6G End-to-End Architecture – Using open-source 4G/5G and beyond RAN with a micro-service-based architecture Core Network

Trends

- Using ICN/NDN in 5G+ wireless telecommunications networks for streamlining information and services from the closest location in both the RAN and Core Network
- Using AI in the RAN Intelligent Controller (RIC) of Open RAN technology for dynamic resource allocations

Participation in Standards Development Organizations (SDOs)

- 3GPP (Services and System Aspects (SA), Radio Access Network (RAN 1,2,3)
- IETF (Domain Name System, Internet, IPv6, Operations/Management)
- IRTF (Information-Centric Networking Research Group (ICNRG))
- ITU SG13 (Future Networks), SG17 (Cybersecurity)
- O-RAN Alliance
- Telecom Infra Project (TIP) - OpenRAN Project Group

2.5.3. Future Goals and Priorities

Goals and priorities

- Develop and standardize future IP networks to both next-generation networks, such as 6G wireless telecommunication networks, and the Internet more generally.

Opportunities to make an impact

- Standardization of the name space for NDN
- Research for NDN for Smart Cities – Multi-tenant, Mobile/dynamic resources, Un-trusted devices, Not under one orchestrator's domain
- Research for NDN for Network Edge – Unreliable network links/resources, Mobile resources, Un-trusted devices, Dynamic resources, Need for distributed orchestration
- Open-source protocol stacks and datasets for testbeds and research related to AI in the RAN

2.6. Spectrum Measurement and Management

2.6.1. Introduction

Spectrum sharing is essential to increasing the utility of scarce spectrum resources and hence an important part of advanced communication technologies. Designing effective spectrum-sharing systems requires advanced methods to, for example, measure spectrum usage and avoid potential interference among different devices. Advanced spectrum measurement and management also includes standards based on better channel propagation models for design and testing, wireless

coexistence, best practice measurement guidelines for instrumentation at gigahertz to terahertz frequencies, and effective antenna evaluation methods.

2.6.2. Current State

Current Standards Work

- Fundamental metrology - the measurement of quantities, electromagnetic shielding, and antenna pattern/performance.

  An example of a fundamental metrology standard is IEEE 1309 –Electric Field Probe Calibration. It can impact spectrum management and measurement standards at higher levels. Industry is revising the 2013 standard by adding new measurement methods (e.g., reverberation chamber) and considering modulated signals.

- Evaluation of systems –electromagnetic compatibility (EMC), wireless coexistence

  An example of evaluation is the ANSI/IEEE C63.27 -American National Standard for Evaluation of Wireless Coexistence which provides evaluation procedures, test methods, analysis options, and test report guidance. It is technology and frequency agnostic, with optional guidance for specific technologies with annexes on Wi-Fi/Bluetooth/LTE. It is currently being used by thousands of test labs globally. C63.27 provides an opportunity for disseminating research and making technical contributions in coexistence measurement methods, modeling and simulation techniques, uncertainty analysis and round-robin testing to demonstrate validity of test methods.

- Measurement campaigns for new uses of existing spectrum

  For traditional 3GPP measurement campaigns, the data collected assumed that the end user was on the ground with a device that was communicating with the network which had antennas relatively high above the ground. However, public safety users can sometimes have an end user inside a building on a higher floor communicating with a dispatch unit on the ground using device-to-device technology. Or, there may be a moving convoy of vehicles of first responders traveling to an accident using device-to-device technology. Traditional measurement campaigns do not consider important components such as directional channel characteristics. Measurement campaigns are taking place that consider channels that are important to public safety.

Trends

- Increased modeling and AI/ML are playing a large role in spectrum management to understand both coverage and interference characteristics. Separate modeling of those characteristics enables flexible analysis. Channel modeling for this purpose is different from channel modeling for system design. For other cases, modeling of basic system operation required to guide spectrum allocation.

- Most SDOs that involve wireless technology protocols, such as WiFi and 5G technology, continuously expand the use of spectrum and look for ways to use more spectrum which requires more stringent management of resources.

- Test methods are becoming more complex to cover the areas of coexistence, interoperability, electromagnetic compatibility, chamber characterization, antennas, emissions, data acquisition/collection. Also, this includes fundamental metrology in electric field probe calibration and antenna metrology.

Participation in Standards Development Organizations (SDOs)

- 3GPP: RAN1 (Physical Layer)
- ANSI/IEEE: C63.27 - American National Standard for Evaluation of Wireless Coexistence
- IEC: Electromagnetic compatibility
- IEEE: WG1309 - Working Group for Electromagnetic Field Sensors and Probes

2.6.3. Future Goals and Priorities

Goals and priorities

- Increase the utility of spectrum resources and design effective spectrum-sharing systems.

Opportunities to make an impact

- Measurement of MIMO Arrays: As the frequency increases, cellular base stations (gNB) are more likely to utilize massive antenna array (hundreds of elements), multiple beams simultaneously and time varying signals. As frequency increases, so does the far-field distance (typically the minimum distance between transmitter and receiver in a test). A base station with a 50 cm antenna array has a 25 m far field distance which is much larger than a typical anechoic chamber. NIST contributing to C63 working group developing guidance for how standards should handle the characterization of massive MIMO systems.

- Chamber (re)characterization: Many existing anechoic and reverberation chambers were built before the development of 5G. Designed and characterized for standardized testing up to 18 GHz. Systems under test with simple antennas (not arrays). Sometimes, the existing chamber characterization techniques are valid at mmWave frequencies. NIST is active in the standards working groups developing new characterization methods (C63).

- Use of Spectrum/Signal as a Tool: Existing Wi-Fi networks could be used to monitor patients in a medical setting (hospital, telehealth). NIST and FDA collaborated on research for measurement techniques to characterize this. Similar activity in IEEE 802.11bf. Goal is to enable future WiFi systems to sense features, objects and environment.

- Leveraging Artificial Intelligence (AI)/Machine Learning (ML) for Modeling and Real-time channel selection: As systems become more complex, predicting performance becomes more challenging. New models utilize measurements as inputs, ML to understand their relation, and attempts to predict the likelihood of coexistence and is a possible contribution to future C63.27. Real-time channel selection with reinforcement ML is ~5000x more efficient at selecting channels.

- Propagation Channel Measurement and Modeling for Spectrum Management : Should be double-directional. Useful for system design: because most systems use MIMO. Also for spectrum management to enable the flexible framework. Possible options for double-directional measurements are the mechanical rotation of horn antennas (popular for mmwave/THz), however it is slow and used only for static scenarios. Also in switched antenna arrays or phased arrays usually available for lower frequencies. All learning strategies require understanding of the physics of propagation.

2.7. Open Source and De Facto Standards

2.7.1. Introduction

The software industry has long been using open source to develop software systems that then may become de facto standards. More recently, the communications industry is increasingly leveraging open source to develop and implement new technologies, evidenced by the many open source implementations of 5G systems. Open source efforts form new ecosystems, not limited to traditional standards organizations, in which the communications industry develops next-generation communication technologies that inform future standards. Expanding beyond traditional approaches is needed if Federal agencies are to continue to support the private sector as it leads in this evolving communication standards landscape.

2.7.2. Current State

Current Standards Work

- Research into how de facto standards become accepted as the commercial winners.
    - Independent research has been conducted on how one technology is selected by the industry or consumer base rather than other competing solutions.
    - A de facto standard gains acceptance in the industry by achieving market share. The more entities that utilize and adopt the de facto standard, the more influence it has with industry members.
    - Through interviews and surveys, research has been done on de facto standard winners and technologies that achieved dominance over their competition. The research focuses on which factors (such as network effects, installed base, complementary goods, network externalities) lead to adoption and technology dominance. Also, strategies (such as communications, pricing of the technology, and timing of availability) are investigated on how to leverage the factors.

- Research in the Open RAN arena

    - Although some of the technical interfaces in Open RAN are standardized in 3GPP, the concept of Open RAN (as it stands today) started as a consortium of individual companies and entities with the goal of opening the 3GPP RAN into individual parts that could be supplied by different companies.
    - The wireless telecommunications industry has since adopted the concept of Open RAN as defined by the O-RAN Alliance and the Telecom Infra Project. Work continues in these organization to define the concepts of Open RAN.
    - As different parts of the RAN can now be provided by different manufacturers, interoperability is now a main focus of the industry and associated testing standards are being discussed. Other areas of focus are on security aspects and optimization.

Trends

- Focusing on increasing the compatibility and technological superiority while discounting the traditional focus of network externalities
- Working in the public collaborator domains rather than through the traditional documentary standards organizations for the creation of communications software needs
- Using consortiums of a small number of individual companies to create de facto standards rather than working through slower de jure standards organizations that are open for participation to the entire industry
- Standards Development Organizations (SDOs) are using open source as part of their overall scope. For example, a telecommunications standard may use an open source audio codec as an option in their specifications. Motivations for using open source can include, but are not limited to encourage adoption of the standard if already-popular open source material is used, to provide an option as a solution in addition to or in place of a proprietary source, to move the completion of a standard forward more quickly by using an existing open source solution rather than creating a new source

Participation in Standards Development Organizations (SDOs)

- 3GPP: RAN3 (RAN Working Group 3 - UTRAN/E-UTRAN/NG-RAN Architecture and Related Network Interfaces)
- Open Networking Foundation: SD RAN
- O-RAN Alliance
- Telecom Infra Project (TIP) - OpenRAN Project Group

2.7.3. Future Goals and Priorities

Goals and priorities

- Participate in new communications technology creation utilizing open collaboration and community-based development for free-to-use software and end-user products

Opportunities to make an impact

- Aid in the development of complementary goods, and increase compatibility and technological superiority of current communications technology.
- Expand on the concept of pre-standard efforts in organizations such as ANSI.
- Explore ways to include consumers into the standardization process or in the creation of open source technology (i.e. citizen development).
- Seek existing open source as solution in SDOs.

2.8. Communications for Data Access and Sharing

2.8.1. Introduction

A major goal of communication is to enable users – human and machine – to access and share data. Profound changes are underway in the lifecycle of data, from data generation to consumption. For example, data are becoming more diverse, dynamic, and distributed as increasing amounts are created at the network edge while users demand easier, faster, more secure, and privacy-preserving ways to access and share data. Standards-based interoperable data access and sharing (e.g., standardized web protocols) provide essential foundations for the core infrastructure underlying the information economy. Data interoperability is also essential to enabling the aggregation and analysis of data across different organizations and for enabling more seamless, accessible, and unified user experiences. Supporting such advanced data needs calls for new measurement capabilities and standards.

2.8.2. Current State

Current Standards Work

- Using the FAIR concept in data collection and storage.
    - The four FAIR principles are:
        - Findability: Data should be described with rich metadata that enables unambiguous identification and discovery.
        - Accessibility: Data should be accessible, even when it is located in distributed repositories.
        - Interoperability: Data should be represented in a way that is understandable by a wide range of software tools and systems.
        - Reusability: Data should be accompanied by clear and open licenses that permit its reuse for any purpose.
    - The “FA” is easier to implement (Findable, Accessible), but it is difficult for the data providers and researchers to find consensus on “IR” (Interoperability, Reusability).
    - FAIR Digital Objects (FDOs) are a new way of representing and managing digital data that is designed to make it more findable, accessible, interoperable, and

reusable. FDOs are based on the FAIR concept, and they are designed to address the challenges of managing large and complex datasets.

- Using a laboratory information management system (LIMS) for organizing data. laboratory information management system (LIMS). LIMS allows for automated conversion of data to open formats, and there is the ability to link systems and work areas. There is no singular solution to serve all the needs, yet shared components (and assets) provide greater economy of scale and consistent usage. However, commercial LIMS are not flexible enough for highly diverse and dynamic research situations.

- The creation of open platforms that collect data from various sources, which have different formats, and making search results on that data available for humans. The end results are easy to understand and visualize, at least that is the goal. The user of the platform does not need to consolidate the data or format it to be consistent, as the platform is designed to do that. Although using the FAIR concept while collecting data is still helpful, it is not necessarily needed because the platform will do this after the data is collected. There are numerous platforms at different levels of maturity and specializations. Some examples of platforms include Data Commons (datacommons.org) and Open Data Commons, CKAN, Datahub.io, Data.gov, Socrata, Zenodo, OpenAIRE, and Figshare. However, there are some limitations. Some data is still kept out of such platforms, such as personal and private information (patient medical records), open data that is held behind firewalls, sensitive government information, among other types.

Trends

- The increasing use of cloud computing. Cloud computing allows for easy shared access for users of the data regardless of location. Solutions can be quickly provisioned with minimal service provider interaction and costs.
- Artificial intelligence (AI) is being explored for data access and sharing.
    - Data discovery and exploration: AI can be used to automatically discover and explore data, which can help researchers to identify patterns and trends that would be difficult to find manually.
    - Data cleaning and preparation: AI can be used to clean and prepare data for analysis, which can save researchers time and effort.
    - Data analysis: AI can be used to analyze data and identify patterns and trends.
    - Data visualization: AI can be used to visualize data in a way that is easy for humans comprehend.

Participation in Standards Development Organizations (SDOs)

- IEEE: P2413: Data Science and Machine Learning for Smart Cities; P2412: Data Science and Machine Learning for Healthcare; P2411: Data Science and Machine Learning for Financial Services; P2410: Data Science and Machine Learning for Manufacturing; P2795: Sharing Analytics Across Secure and Unsecured Networks

- International Organization for Standardization (ISO): ISO/TC 302: Information and documentation — Data interchange formats
- World Wide Web Consortium (W3C): Data on the Web Working Group (DOWA)
- Open Geospatial Consortium (OGC): Data Science (DS)
- Object Management Group (OMG): Data Management Task Force (DMTF); Unified Modeling Language (UML); Data Science and Analytics Domain Task Force (DADT); Data Science and Analytics Technical Committee (DSAT)

2.8.3. Future Goals and Priorities

Goals and priorities

- Enable users to access and share data in an interoperable way by advancing communication technologies to support the diversity, dynamism, and distribution of data.

Opportunities to make an impact

- Units of Measurement – Units of measurement for humans are well-established and used globally. However, units for machines are not established on a global scale. Individual industries can and do use different units of measurements. There is a need for standardized units of measurement for machines. The interoperability of data is critically reliant on units and other aspects of metrology like uncertainty.

- Standardized web protocols for standards-based interoperable data access and sharing – there is still a need to standardize the core infrastructure underlying the information economy.

2.9. Quantum Communications

2.9.1. Introduction

Quantum communication takes advantage of the laws of quantum physics to transport and protect data. Relevant technologies include quantum repeaters, quantum memory, quantum interfaces (transferring qubit states from photons at one wavelength to another, which is necessary for connecting or scaling quantum computers), and quantum key distribution (exchanging cryptographic keys in a quantum state using qubits). Quantum networking has seen significant progress over the past decade with more fundamental breakthroughs expected in the near future. Standards and best practices for reliable and reproducible performance measurement are needed to accelerate progress and enable broad adoption.

The central terms used in this section are defined as follows:

- Quantum channels: the optical paths provided by the optical network layer to the quantum network layer to interconnect its quantum nodes/capabilities and exchange quantum information.

- Bound Quantum Channel: one qubit is assigned to each quantum channel at each end. A quantum channel with assigned qubits on each end is called a bound quantum channel.

- Quantum Link: to create a quantum link, two nodes connected by a bound quantum channel make a number of quantum entanglement attempts until successful.

- Quantum Link: When an entanglement attempt is successful, the two quantum nodes/capabilities share an entanglement pair which is represented as a quantum link. Two neighbor nodes may share multiple quantum links.

2.9.2. Current State

Current Standards Work

- Development of requirements for connectivity:

    - Connectivity should allow any 2 experimenters on the network to exchange either classical or quantum information, or both. (*connectivity*)
    - Connectivity should provide any 2 experimenters secure classical and quantum communications exchange (*security*)
    - Network nodes should have connectivity to a network management system and possibly a software-defined network controller. (*manageability/operation*)
    - Connectivity at the optical layer should have specified optical characteristics such as loss and noise (fiber characterization) (*performance*)
    - Connectivity should have bounds on latency requirements.
    - Connectivity should support some form of multiplexing.
    - Connectivity should support some form of circuit switching - fiber, core, band, or wavelength (*scalability*)
    - Connectivity should support datagram forwarding (*classical /quantum*)
    - Connectivity determinism between network nodes is desired to control the stability of the quantum layer and for certain quantum protocols (*flexibility*)
    - Connectivity between any experimenters should support scheduled/programmed connectivity.

The basis for Quantum Connectivity is the distribution of entanglement via the direct transmission of photons via fiber optics is practically impossible for large distances, because the inevitable losses in optical fibers cause an exponential decrease of the success rate with distance. Only need to distribute any one of the bell pair states.

- Development of Local Area Quantum Network Testbed, DC-QNet.

    - DC-QNet advances cooperation and enable strategic synergy among agencies in quantum network research and development. It is a non-proprietary environment for test and evaluation of quantum network concepts, components, protocols and architectures. It enables cross-cutting agency synergy in sensor development,

secure communications, distributed computing and other use case applications. Lastly, it is a dedicated resource for unique expertise and needs of the federal government.
    - Two ways for sites to connect to DC-QNet. It uses an Optical Network Layer for Classical communications and a direct or through a passive optical network layer for the quantum channel. The physical building blocks of each node contains Quantum Memory, QFC (a quantum programming language), Measurement Devices and a Quantum Node. Interfacing with a similar node, Node B occurs via quantum and classical links. Both Nodes are also connected via an entanglement generator.
    - Multiple kinds of Quantum Connectivity architectures exist and are still under development. Predominantly, there are Hub Fiber architectures, Hub wavelength architectures and a quantum datagram that contains bits, a gap and a qubit.
    - Optical Network Modeling is based on TMF 513. The TMF 513 is a TMF standard for integrated management of telecom networks.
    - The QED-C is involved in two technological projects. The interoperability project which is pursuing a multi-vendor demonstration. In addition, there is the Compatibility (Future quantum networks and Conventional networking infrastructure) Project that will help to identify potential issues early before standardization.

Trends

There are several approaches being explored to build the quantum layer connectivity:

- Make link-level entanglement generation at the Mid-point, Source and both ends. Then swap the qubits to combine link-level entanglements into end-to-end entanglements. Finally need overall management and control plane functions.
- Quantum swapping using a path - Each node builds its quantum links with some success and some failures for a configured duration. We call the result a link states (these are dynamic and probabilistic). Nodes share link states through the classical channel – sharing is limited due to decoherence.
- Quantum Network Characterization is based on a measurement suite that can do state generation and characterization, generate channel noise and loss measurement, include timing synchronization and finally provide entanglement verification/quality control. The key enablers are calibrated single-photon detectors, calibrated and deployable entangled single-photon sources and receivers and metrology methods and protocols. Other types of measurements are fiber polarization stability, fiber loss characterization, fiber connector loss characterization, quantum node synchronization, 140 km entanglement distribution and detector characterization.

Participation in Standards Development Organizations (SDOs)

- IEEE: NGFI - Next Generation Fronthaul Interface
- ISO/IEC: JTC1/WG 14 Quantum information technology

- Quantum Economic Development Consortium (QED-C): Technical Advisory Committees (TACs); Workforce Development Committee (WDC); Public Policy Committee (PPC); Communications Committee (CC); Governance Committee (GC)

2.9.3. Future Goals and Priorities

Goals and Priorities

- Accelerate the development and adoption of quantum communication technologies, standards and best practices for reliable, interoperable, and reproducible communications and performance measurement.

Opportunities to make an impact

- Research is needed to increase the entanglement rate of qubits and their stability, understand and reduce decoherence and have entanglement-aware metric for routing.

- Effort is needed for single-photon source characterization. Currently, it is based on high-efficiency superconducting single-photon detectors.

- According to the findings from the report by the Quantum Economic Development Consortium on Single-Photon Measurement Infrastructure for Quantum Applications (SPMIQA): Needs and Priorities (https://quantumconsortium.org/single-photon-report/) showed the following needs for the future:

    - Information: A common language of terms and a compendium of best metrological practices is needed along with dissemination.
    - People: An accessible training network is needed to provide appropriate best practices to the wider single-photon technology community.
    - Components: Standardized, reliable, repeatable, and widely available off-the-shelf components such as laser sources, fiber connectors, attenuators, and detectors are needed.
    - Services: Better access to calibration capabilities/services and rugged devices that do not need regular calibration, or that can be self-calibrated is needed.

3. Contributing Agency/Office ACT Standards Landscape Overview

Agencies/Offices Participating in the Advanced Communications Technologies Working Group

- Defense Information Systems Agency (DISA)
- Department of Defense, Office of the Chief Information Officer (DoD CIO)
- Department of Defense, Office of the Undersecretary of Defense R&E (OUSD/R&E)
- General Services Administration (GSA)
- National Aeronautics and Space Administration (NASA)
- National Institute of Occupational Safety and Health (NIOSH)
- National Institute of Standards and Technology (NIST)
- National Telecommunications and Information Administration (NTIA)
- United States Air Force (AFLCMC/HNAG/EZAC, AFMC)
- United States Army (STRI, DEVCOM, C5ISR, AMC, LDAC
- United States Department of State
- United States Department of Transportation (USDOT)
- United States Environmental Protection Agency (EPA)
- United States Food and Drug Administration (FDA)
- United States Navy (Navy)
- United States Nuclear Regulatory Commission (NRC)
- United States Trade Representative (USTR)

4. National Standards Strategy for Critical and Emerging Technology Strategy

Recently, the Biden-Harris Administration announced the National Standards Strategy for Critical and Emerging Technology (NSSCET) [1]. The NSSCET aims to ensure that the United States remains a leader in the global economy by promoting the development and use of standards for CET. The strategy focuses on four key objectives: investment, participation, workforce, and international engagement. The overall strategy calls for increased investment in pre-standardization research, translational research, and educational programs to promote innovation and workforce development in CET. It also calls for the promotion of participation by the private sector, academia, and other stakeholders in CET standards development activities. The strategy emphasizes priority areas such as Communication and Networking Technologies, Artificial Intelligence and Machine Learning, Quantum Information Technologies, Automated and Connected Infrastructure, Cybersecurity and Privacy, among others. There is alignment between the ACTWG and NSSCET priority areas. The following table shows the alignment:

Table 1: ACTWG and NSSCET Priority Area Alignments

ACTWG PRIORITY AREA	NSSCET PRIORITY AREA ALIGNMENT
Security and Privacy – Standards for CT security and resilience, including compromise detection and sustained safe operation; CT systems supply chain security and reliability; and distributed ledger methods for cooperative trust and privacy protection among network entities.	• **Communication and Networking Technologies** • **Cybersecurity and Privacy**
End-to-End Services and Assurance – CT standards for architectures, protocols, and measurement methods that support differentiated and optimized services tailored to and responsive to application requirements, including those for critical infrastructure systems.	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning** • **Quantum Information Technologies** • **Automated and Connected Infrastructure**
Emerging Network Technologies – Standards for AI-enabled network systems; networks supporting AI-enabled applications and distributed systems; and automated, virtual networks and services.	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning**
Internet of Things – Standards for massively-scaled connectivity and interoperability in IoT environments including connected vehicles, uncrewed aerial systems (UAS), intelligent infrastructure and smart cities, eHealth, advanced	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning** • **Automated and Connected Infrastructure**

manufacturing, emergency response, smart grid, and other application areas.	
Emerging & Future IP Networks – Standards that promote innovation, enable broad participation, and preserve access and privacy for next-generation IP network technologies.	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning** • **Quantum Information Technologies** • **Automated and Connected Infrastructure** • **Cybersecurity and Privacy**
Spectrum Measurement & Management – CT standards for maximizing spectrum resources for 5G and 6G technologies, including channel propagation models and measurement methods, wireless coexistence, antenna evaluation methods, and integrated satellite communications.	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning** • **Quantum Information Technologies**
Open Source and De Facto Standards – Strategic Federal role in accelerated standards processes, including interactions with industry consortia and alliances developing de facto standards.	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning** • **Quantum Information Technologies** • **Automated and Connected Infrastructure** • **Cybersecurity and Privacy**
Communications for Data Access and Sharing – CT standards meeting the rate, volume, quality of service, security, and privacy needs of the expanding data universe and a global information society.	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning** • **Quantum Information Technologies** • **Automated and Connected Infrastructure** • **Cybersecurity and Privacy**
Quantum Communications – CT standards for quantum technologies, including memory, interfaces, and key distribution systems, that enable advanced quantum networks and their interactions with conventional network systems.	• **Communication and Networking Technologies** • **Artificial Intelligence and Machine Learning** • **Quantum Information Technologies** • **Cybersecurity and Privacy**

5. References

5.1. References for Section 2.2 End-to-End Services and Assurance

[1] "Definition of End-to-end Encryption", https://datatracker.ietf.org/doc/draft-knodel-e2ee-definition
[2] RFC8890, "The Internet is for End Users", https://www.ietf.org/rfc/rfc8890.html
[3] Committee on National Security Systems (CNSS) Glossary (CNSSI No. 4009), https://www.cnss.gov/CNSS/openDoc.cfm?1GmdfsIBUZXQNKAlEJOUjQ==
[4] ITU-T P.10/G.100 "Vocabulary for performance, quality of service and quality of experience", https://www.itu.int/rec/T-REC-P.10-201711-I/en
[5] RFC1812 "Requirements for IP Version 4 Routers", https://www.rfc-editor.org/rfc/rfc1812
[6] RFC1633 "Integrated Services in the Internet Architecture: an Overview", https://datatracker.ietf.org/doc/html/rfc1633
[7] RFC2474 "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", https://datatracker.ietf.org/doc/rfc2474/
[8] RFC2475 "An Architecture for Differentiated Services", https://datatracker.ietf.org/doc/rfc2475/
[9] IEEE Std 802.1Qbu-2016 - IEEE Standard for Local and Metropolitan Area Networks -- Bridges and Bridged Networks -- Amendment 26: Frame Preemption
[10] IEEE Std 802.1Qbv-2015 - IEEE Standard for Local and Metropolitan Area Networks -- Bridges and Bridged Networks -- Amendment 25: Enhancements for Scheduled Traffic
[11] IEEE Std 802.1Qca-2015 - IEEE Standard for Local and Metropolitan Area Networks -- Bridges and Bridged Networks -- Amendment 24: Path Control and Reservation
[12] RFC8578 "Deterministic Networking Use Cases", https://datatracker.ietf.org/doc/rfc8578/
[13] RFC8655 "Deterministic Networking Architecture", https://datatracker.ietf.org/doc/rfc8655/
[14] Recommendation ITU-T G.872 (2001), Architecture of optical transport networks.
[15] Recommendation ITU-T G.709/Y.1331 (2009), Interfaces for the Optical Transport Network (OTN).
[16] Recommendation ITU-T G.870/Y.1352 (2004), Terms and definitions for optical transport networks (OTN).

5.2. References for Section 2.4 Internet of Things

Industrial Wireless Environments
[1] Kalsoom, T.; Ramzan, N.; Ahmed, S.; Ur-Rehman, M. Advances in Sensor Technologies in the Era of Smart Factory and Industry 4.0. Sensors 2020, 20, 6783. https://doi.org/10.3390/s20236783 of https://www.mdpi.com/1424-8220/20/23/6783
[2] IEEE-P3388, Standard for Radio Frequency Channel Specifications for Performance Assessment of Industrial Wireless Systems, https://standards.ieee.org/ieee/3388/10702/
[3] Montgomery, K. , Candell, R. , Hany, M. and Liu, Y. (2021), Wireless User Requirements for the Factory Workcell, Advanced Manufacturing Series (NIST AMS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.AMS.300-8r1/upd
[4] Guide to Industrial Wireless Deployments (AMS 300-4)
[5] Wireless User Requirements (AMS 300-8 Rev 2)
[6] Industrial Wireless Deployment Guidelines for the Navy Shipyard (AMS 300-9)
[7] IEEE 1900.2-2008: Analysis of in-band and adjacent-band interference.
[8] IEEE 802.15.2-2003: Coexistence of WPAN with other wireless networks within unlicensed bands.
[9] IEC 62657-2:2017: Industrial communication networks - Wireless communication networks - Part 2: Coexistence management
[10] FCC Part 15: The Federal Code of Regulation (CFR) FCC Part 15 is a common testing standard for most electronic equipment.
[11] MIL-STD-461G: Specifies the requirements for the electromagnetic compatibility (EMC) of devices and systems created for and used by the United States Department of Defense (DoD). Very detailed in mapping of requirements to test cases.
[12] ANSI/IEEE C63.27-2017: Test and evaluation of communications systems under basic co-channel and adjacent channel communications scenarios. Similar in our scope but only Wi-Fi, BT, and LTE are considered.

Cybersecurity for IoT:
[1] https://assets.kpmg/content/dam/kpmg/pdf/2015/12/security-and-the-iot-ecosystem.pdf
[2] Insulin Pumps Attacks. http://bit.ly/jnjinsulinpump
[3] Pacemaker attacks. https://ics-cert.us-cert.gov/advisories/ICSMA-19-080-01
[4] ”Enabling Trust and Security: TIPPSS for IoT”, IEEE IT Professional 2018; https://www.computer.org/csdl/magazine/it/2018/02/mit2018020015/13rRUxDItjT
[5] “Wearables and Medical Interoperability: The Evolving Frontier”, IEEE Computer 2018, ©2018 IEEE, https://ieeexplore.ieee.org/document/8481273
[6] IEEE/UL P2933 – Clinical IoT data and device interoperability with TIPPSS Working Group
[7] https://www.beckershospitalreview.com/finance/892-hospitals-at-risk-of-closure-state-by-state.html

5.3. References for Section 4 National Standards Strategy for Critical and Emerging Technology Strategy

[1] FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology; https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/

[2] United States Government National Standards Strategy for Critical and Emerging Technology; https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

Appendix A. Advanced Communications Technologies Working Group Charter

Establishment

The Advanced Communications Technologies Working Group (herein after referred to as the "ACTWG" or "Working Group") is established under the provisions of the charter of the Interagency Committee on Standards Policy (ICSP). The ICSP advises the Secretary of Commerce and the heads of other Federal agencies in matters relating to the implementation of OMB Circular A-119 and reports to the Secretary of Commerce through the Director of the National Institute of Standards and Technology (NIST).

Purpose

The objective of the ACTWG is to facilitate coordination of Federal agency advanced communications technologies (ACT) standards activities, respond to requests for information, and develop recommendations relating to ACT standards policy matters to the ICSP. The ACTWG reports to the Chair of the ICSP and advises the members of the ICSP on relevant issues.

Functions

The ACTWG is responsible for:

- Assisting the ICSP in promoting effective and consistent federal policies in the area of advanced communications technologies standards.
- Providing an annual report to the ICSP on the current ACT standards activities of participating Federal agencies and recommendations for strategic directions in Federal ACT standards efforts.
- Responding to requests for information and advising the ICSP on effective means of coordinating advanced communications technologies standards activities with those of the private sector.
- Sharing best practices in advanced communications technologies standards among Federal agencies.
- Coordinating Federal advanced communications technologies standards interests across application areas such as transportation, energy, public safety, and others.

Organization

Participants include Federal agency representatives with expertise relevant to standards in advanced communications technologies. Each participating Federal entity will identify one voting member to represent the entity. The ACTWG co-chairs comprise one NIST staff member designated by the ICSP Chair and serving as secretariat, along with other co-chairs as elected by majority vote of the ACTWG members present. The Working Group will follow a similar meeting schedule as the ICSP and will meet at least three times each year. Other meetings may be called at the discretion of the co-chairs.

Approval and Renewal

Approved by the ICSP 25 May 2021. This charter expires three years after the date of approval unless renewed by the ICSP.

Appendix B. Abbreviations

3GPP 3rd Generation Partnership Project

3GPP2 3rd Generation Partnership Project 2

5G 5^{th} generation mobile network

AAMI Association for Advancement of Medical Instrumentation

ANS American Nuclear Society

ANSI American National Standards Institute

APEC-TEL Asia-Pacific Economic Cooperation Telecommunications Working Group

ASCE American Society of Civil Engineers

ASME American Society of Mechanical Engineers

ASTM ASTM International, formerly American Society for Testing and Materials

ATIS Alliance for Telecommunications Industry Solutions

AWS American Welding Society

CCSDS Consultative Committee for Space Data Systems

CDC Centers for Disease Control and Prevention

CITEL Inter-American Telecommunication Commission (OAS)

CLSI Clinical and Laboratory Standards Institute

CTA Consumer Technology Association

CTIA U.S. wireless industry association, formerly Cellular Telecommunications Industry Assoc.

DHS Department of Homeland Security

DoD Department of Defense

DOE Department of Energy

DOT Department of Transportation

EM Electromagnetic

EMP Electromagnetic pulse

EPA Environmental Protection Agency

FDA Food and Drug Administration

GSA General Services Administration

G7 Group of Seven inter-governmental forum

G20 Group of Twenty intergovernmental Forum

HL7 Health Level Seven International

IAEA International Atomic Energy Agency

ICRP International Commission on Radiological Protection

ICT Information and Communications Technology

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IEEE-SA IEEE Standards Association

IETF Internet Engineering Task Force

IGF Internet Governance Forum

IHE Integrating the Healthcare Enterprise

INCITS International Committee for Information Technology Standards

INCOSE International Council on Systems Engineering

IOAG Interagency Operations Advisory Group

IoT Internet of Things

IRTF Internet Research Task Force

ISA International Society of Automation

ISO International Organization for Standardization

ISO/IEC JTC1 Joint technical committee on information technology for ISO and IEC

ITU International Telecommunication Union

ITU-R ITU Radiocommunications Sector, formerly CCIR

ITU-T ITU Telecommunications Sector, formerly CCITT

ITU-D ITU Telecom Development, formerly known as BDT

LTE Long Term Evolution, wireless communications standard

MITA Medical Imaging and Technology Alliance

NASA National Aeronautics and Space Administration

NCRP National Council on Radiation Protection and Measurements

NEI Nuclear Energy Institute

NEMA National Electrical Manufacturers Association

NIH National Institutes of Health

NIST National Institute of Standards and Technology

NITRD Networking and Information Technology Research and Development

NOAA National Oceanic and Atmospheric Administration

NSF National Science Foundation

NSTC National Science and Technology Council

NTIA National Telecommunications and Information Administration

NTTAA National Technology Transfer and Advancement Act

O&M Operations and maintenance

OECD Organisation for Economic Cooperation and Development

OEOSC Optics and Electro-Optics Standards Council

OGC Open Geospatial Consortium

OMA Open Mobile Alliance

OMB Office of Management and Budget

OMG Object Management Group

O-RAN O-RAN Alliance, operator defined open and intelligent radio access networks

OSTP Office of Science and Technology Policy

QoE Quality of Experience

QoS Quality of Service

R&D Research and development

RESNA Rehabilitative Engineering & Assistive Technology Society of North America

RTCA Radio Telecommunications Commission for Aeronautics

SA Stand Alone, combines a 5G radio access network (RAN) with a 5G core

SAE SAE International, formerly Society of Automotive Engineers

SCTE Society of CableO_RAN

Telecommunications Engineers

SDO Standards development organization

TEM transverse electromagnetic

TIA Telecommunications Industry Association

TM Forum Telemanagement Forum

UAS Uncrewed aerial system

UL Underwriters Laboratories

USAGM United States Agency for Global Media

USDOT United States Department of Transportation

V2X Vehicle to everything, vehicular communications system

W3C World Wide Web Consortium

WInnForum Wireless Innovations Forum

WRC World Radiocommunication Conference (ITU)

WTDC World Telecommunications Development Conferences (ITU)