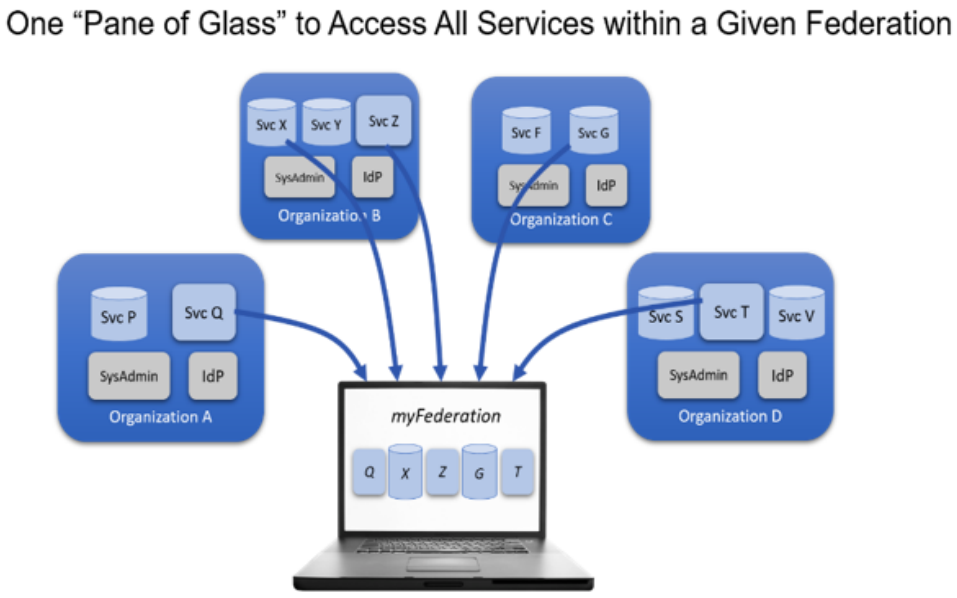
NIST Smart Connected Systems Newsletter – December 2021

IEEE Approves Cloud Computing Standard, Aided by NIST



A user creates their own federation from different clouds and organizations

On December 8, 2021, the IEEE Standards Association Standards Board approved the IEEE 2302-2021 Standard for Intercloud Interoperability and Federation produced by IEEE's P2302 Working Group (chaired by NIST's Robert Bohn), following the IEEE's Standards Review Committee recommended approval. The standard is also based on the NIST Special Publication 500-332 The NIST Cloud Federation Reference Architecture and NIST research.

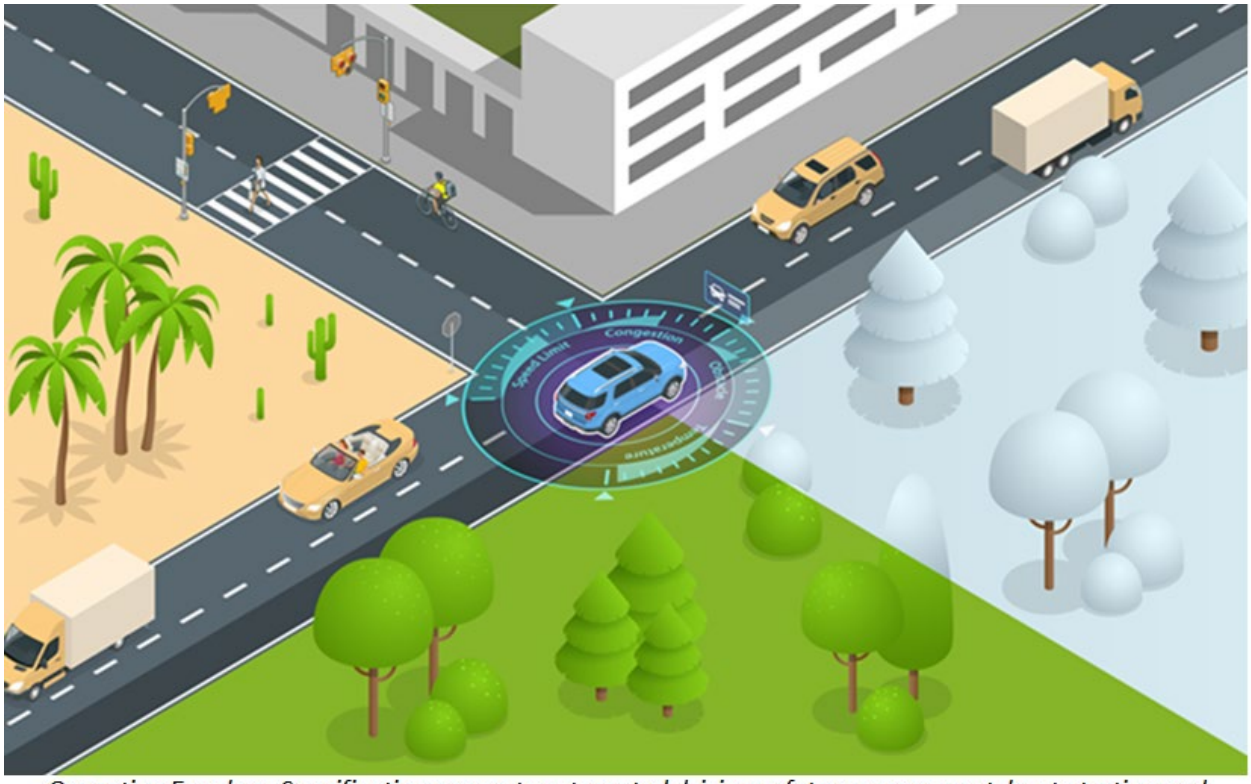
To date, the interoperability of cloud services has been a challenge for providers and customers. Consequently, cloud services were limited in geographic coverage, functionality, and scalability. Cloud computing incompatibilities are analogous to the early days of the telephone and the Internet.

The IEEE standard represents a major advance for cloud computing – or computing on demand – enabling greater interoperability. It defines a functional model for a cloud federation and addresses the following:

- Topology, which defines its clouds, exchanges, and gateways
- Functional elements, which include messaging, resource ontologies, and trust infrastructure
- Governance elements – its registration, geo-independence, trust anchor, compliance, and audit

The intended technical benefit of the standard is to enable a dynamic infrastructure that can support evolving business models, and ultimately facilitate the growth of cloud computing.

NIST Proposes Operating Envelope Specification Concept to Support Automated Driving Safety

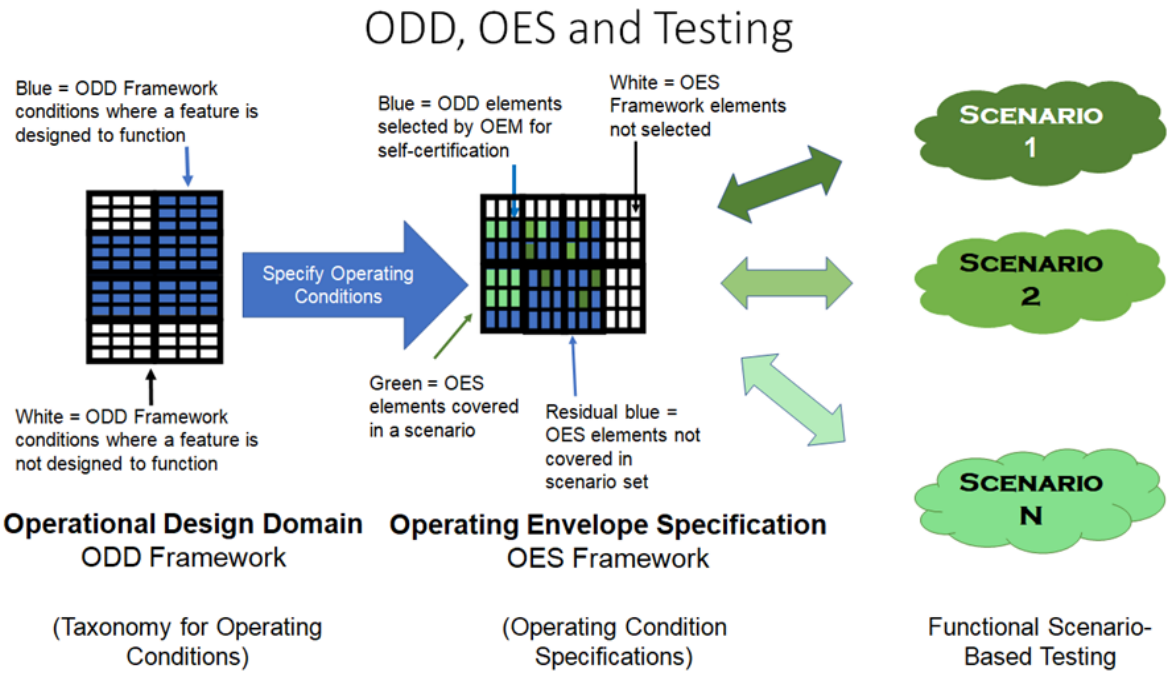


Operating Envelope Specification supports automated driving safety measurement, key to testing and public acceptance of automated vehicles

NIST released its Special Publication 1900-301, Automated Driving System Safety Measurement Part I: Operating Envelope Specification. It presents a novel approach to automated driving systems (ADS) safety measurement.

SAE International defines an automated vehicle as being a vehicle equipped with an ADS. The NIST approach to measuring automated vehicle safety builds on the *operational design domain* (ODD), or operating conditions for which ADS is designed to function. The ODD for an automated vehicle was originally proposed by the Crash Avoidance Metrics Partnership. The ODD is now broadly accepted by industry and government as a taxonomy for original equipment manufacturers to express the design intent for vehicle automation.

NIST introduces the concept of an *operating envelope specification* (OES), a structured description of the operating environment for driving. The OES supports calculation-based reasoning for vehicle performance in that environment, with testing and certification applications and in real-time driving.



NIST approach to measuring automated driving safety

A diverse group of stakeholders can benefit from OES, including developers, technology suppliers, and safety assessors. Infrastructure designers, as well as owners and operators of ADS-equipped vehicles, also can use OES to determine whether operating conditions are suitable for safe automated vehicle operation. Additionally, teleoperators can use OES data to support remote driving or remote assistance. Finally, the automated vehicle itself will need access to OES information to understand and respond safely to its environment. Reliable safety assessment methods can contribute to public acceptance of automated vehicles.

The NIST approach resulted from an open stakeholder engagement process in the NIST ADS Safety Measurement Technical Working Group, which was initiated based on stakeholder input at the NIST workshop on Consensus Safety Measurement Methodologies for Automated Driving System-Equipped Vehicles and open to all interested parties, including manufacturing, transportation, research and development, government, and roadway design participants. The approach also leverages the NIST

Cyber-Physical System Framework, which describes the engineering concerns of system stakeholders, including trustworthiness, and how they are addressed in component, subsystem and full system development.

Ongoing work at NIST, with its industry, government, and academic partners, will build on OES to characterize safety metrics for automated vehicle maneuvers and overall performance.

NIST Supports Teleoperation Forum on Concepts and Standardization

NIST's Tao Zhang provides insights on standardization in teleoperations forum

On December 2, 2021, over 180 experts from around the world participated in the first 5G-Blueprint Forum on Teleoperation, organized by 5G-Blueprint Project, the Teleoperation Consortium, and NIST. The Forum addressed approaches and concepts for remotely operating different types of vehicles.

NIST's Tao Zhang contributed to the panel on legal, regulatory, and standardization aspects of teleoperation, along with Scott McCormack (Teleoperation Consortium); Michael Fernandez-Ferri (Greggo Networks); Mathijs Klepper (KPN); Gino Ducheyne (Belgian Institute for Postal Service and Telecommunication); and Yunpeng Zang (Ericsson).

A key issue identified in the Forum was the relationship between autonomous vehicles and teleoperated mobility. Zhang stated that the two are intrinsically integrated. Today, human teleoperators can help self-driving vehicles navigate situations the vehicles cannot handle on their own. Over time, increasingly automated teleoperation can provide additional ways to achieve driving automation beyond putting all driving intelligence on the vehicle. Zhang also noted several teleoperation topics of industry interest that could benefit from standardization, including:

- Taxonomy for teleoperation

- Matrix characterizing the safety of teleoperation
- Operational design domains for teleoperation
- Interfaces for the teleoperation system and the vehicle
- Interfaces for vehicle passengers interacting with the teleoperation system

Zhang emphasized the need to examine teleoperation applications. They should be considered along with network requirements. No matter how well a wireless network is designed, its performance can fluctuate due to many factors such as physical environments and network congestion. Therefore, it is important to consider what teleoperation applications can do to enable the safety of remotely operated vehicles under poor network conditions. The more the applications can do, the less stringent requirements they will require the network to meet.

NIST-led IEEE Working Group Pursues Radio Channel Standard for Wireless Industry

A standard enabling wireless networks for these systems and more

On November 16, 2021, IEEE initiated the IEEE P1451.5p working group, chaired by NIST's Rick Candell and assisted by NIST's Kang Lee and Karl Montgomery. The working group seeks to produce a standard that specifies the radio frequency environment characteristics and configuration for performance evaluation of industrial wireless network designs, before commissioned deployment in industrial and mission-critical settings. This standard will include a model that represents the radio frequency environment and will account for factors (aggressors) degrading the performance of radio channels, such as jamming and interference, competing for traffic overlays, and multi-path. The standard will include profiles that address levels of severity and the unique radio channel challenges of different industries and application scenarios.

Research and standardization to be conducted under this working group were requested by industry at the Workshop on Performance of Industrial Wireless Mechatronics Systems on June 8, 2021, at the IEEE Industrial Electronics Society's International Conference on Factory Communication Systems.

The IEEE P1451.5p standard is seen as significantly benefiting industry by advancing confidence in the use of wireless technologies for applications in the Industrial Internet of Things, from sensing and actuating to automation and real-time control. This standard also would enable important concepts of smart manufacturing such as mobility of actors, factory agility, flexibility of factory configuration and deployment, and simplicity of maintenance. Smart manufacturing is seen as more efficient than present-day manufacturing practices. Additionally, the use of wireless technologies would reduce cabling and thus cut costs, as well as allow more mobile and reconfigurable networks. Verification of wireless network performance on the factory floor is an essential part of the industrial wireless deployment lifecycle (See NIST AMS 300-4 Guide to Industrial Wireless Systems Deployments) for which standardization in test configuration plays a crucial part.

NIST and University Researchers Offer Future 6G Network Concept

The "Mailbox Theory" for 6G – an intelligent network

In 6G Cognitive Information Theory: A Mailbox Perspective, published in *MDPI*, October 16, 2021, NIST and international researchers propose a "cognitive" 6G network – significantly enhancing the 5G network which encodes and transmits data with their meaning or semantics.

With commercial 5G rapidly deploying, researchers have begun to look at 6G. Its key technologies for mobile communication networks are expected to become available as early as 2023, with 6G networks emerging in 2030, according to Saad et al. Compared to 5G, the 6G network will increase data rates by over 100 times, to one TeraByte per second or more, enabling the inclusion of edge intelligent devices and computing. To move large amounts of data to where and when it is needed, 6G networks will need to customize services to meet demands, transmit valued data, and interact with users.

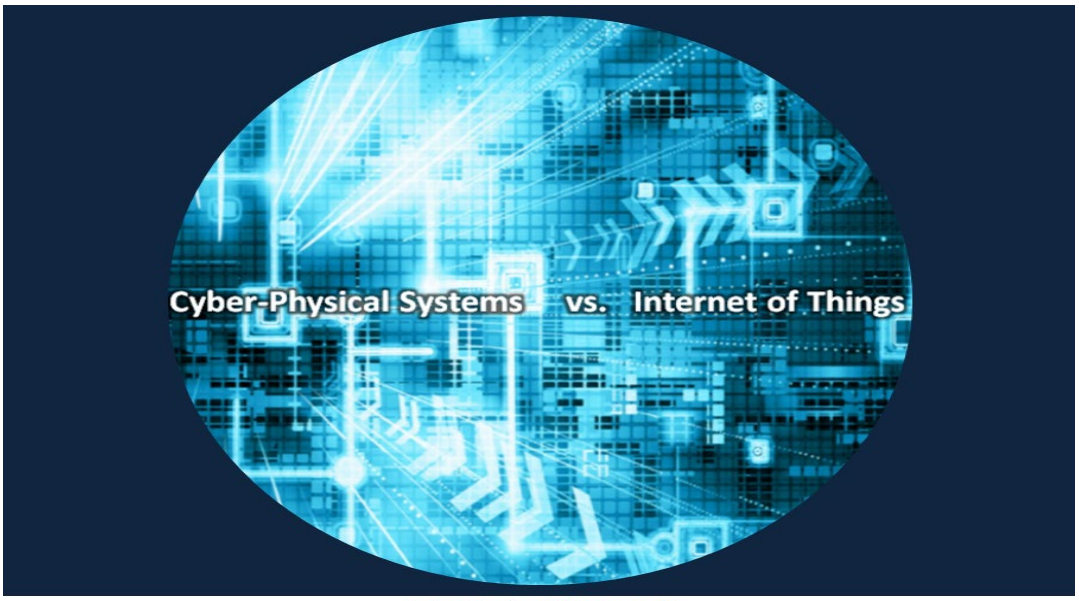
To meet these requirements, the paper offers a "mailbox theory" which envisions a 6G network characterized as a:

- Distributed Intelligent Network: This would have intelligent applications embedded throughout the network and be intelligent, managed and controlled. The network would be capable of transmission, storage, analysis of large-scale data, and providing personalized access at any time and place.

- Proactive Interactive Network: This would be a personalized, demand-centered network. Users would define network functions for on-demand resource scheduling. Moreover, the network would adjust in real time according to changes in user demand. Such a design requires artificial intelligence to adjust the network as well as protection for personal data.

- Cognitive Information Transmission: Compared to traditional communications, the 6G network would significantly reduce redundant transmissions and better ensure semantic meanings are mined, extracted, and sent.

University Researchers Use NIST Report to Pursue Clearer CPS and IOT Definitions



What's the difference?

In The 12 Flavors of Cyberphysical Systems in the December 2021 issue of IEEE's *Computer*, Pennsylvania State University's Joanna F. DeFranco and University of Patras' Dimitrios Serpanos seek to define cyber-physical systems (CPS) and the Internet of Things (IoT). They build on NIST's Special Publication 1900-202 on Cyber-Physical Systems and Internet of Things, which addresses the implications of a unified CPS/IoT perspective. The pursuit of definitions is intended to eliminate confusion regarding the subjects and focus future research.

The researchers evaluated 12 definitions of CPS from Department of Homeland Security, Department of Transportation, Cyber-Physical Systems Virtual Organization, IEEE, National Science Foundation, and

NASA. The researchers then compared these definitions to six characteristics of CPS, as described by the NIST publication. Overall, researchers found many CPS definitions addressed NIST's CPS characteristics, but still missed one or more.

The researchers said that CPS and IoT technologies are related but that there continues to be a lack of consensus among other researchers regarding similarities, differences and relationships, and a lack of consistency in their respective definitions. Their finding is similar to that of the NIST publication, which, based on an analysis of the literature, found four schools of thought regarding CPS versus IoT: equivalency, partial overlap, CPS as a subset of IoT, and IoT as a subset of CPS. The article seeks to provoke discussions regarding these concepts, leading to clear definitions.

NIST Researchers Collaborate Internationally on Time Synchronization Approach for IoT

Time synchronization of sensor networks is critical to the Internet of Things (IoT). These sensor networks must provide real-time data in monitoring and controlling physical infrastructures. This entails forwarding sensor data and data fusion results to the cloud and sharing data with IoT applications – and all of the IoT devices should be synchronized based on a common time base. However, most IoT devices, such as IoT wireless sensors and actuators using microcontrollers, do not have real-time clock modules.

NIST researchers (Eugene Song, Kang Lee) and other IEEE members recently presented and published Time Synchronization of IEEE P1451.0 and P1451.1.6 Standard-based Sensor Networks as part of the IECON 2021 conference. It introduces time synchronization approaches for IoT sensor networks, which are based on the IEEE P1451.0 standard. The proposed architecture consists of two-level time-synchronization systems for:

- Wide-area networks (WANs), based on IEEE P1451.0 and P1451.1.X standards
- Wireless local area networks (LANs), based on IEEE P1451.0 and P1451.5.X standards

The paper focuses on the time synchronization of WANs based on IEEE P1451.0 and P1451.1.6 standards. The paper also provides the implementation of time-synchronization for wireline and wireless networks adhering to IEEE P1451.0 and P1451.1.6 standards, along with preliminary results from verifying the approach.