SMART CONNECTED SYSTEMS

NIST Smart Connected Systems Newsletter – March 2022

NIST International Collaboration Develops New Framework for Smart Cities and Communities

Smart City Holistic Key Performance Indicators support community benefits

Have you ever wondered what it is about a smart city or community that makes it 'smart?' In an international collaboration with Dr. Martin Serrano of the National University of Ireland Galway, NIST researchers have answered that question.

Smart cities and communities commonly use metrics, or Key Performance Indicators (KPI), for evaluating or measuring their smart city ecosystems. However, many KPI approaches are limited by their technology- or sector-specific focus and their inability to measure benefits essential to assessing community impact and return on investment. To overcome this limitation, a Holistic Key Performance Indicators (H-KPI) Framework has been developed that builds on conventional KPI methods and accounts for unique characteristics such as varying districts and neighborhoods, differences in population and economic scale, the reuse of previously deployed technologies, and other factors relevant to a city or community. In this work, the term 'smart' in 'smart cities' is defined as the efficient use of digital technologies to provide prioritized services and benefits to meet community goals, such as economic vitality, equity, resilience, sustainability, or quality of life.

The H-KPI Framework is described in the recently published NIST Special Publication 1900-206 Smart Cities and Communities: A Key Performance Indicators Framework. The Framework provides the basis for developing measurement methods and tools that allow for integration, adaptability, and extensibility at three interacting levels of analysis: technologies, infrastructure services, and community benefits. The publication describes a H-KPI method which provides a structured representation of smart city and community information flows and enables computational methods for systems design, analysis, operations, and assurance. The five core metrics of the method are:

- alignment of KPIs with community priorities across districts and neighborhoods;
- investment alignment with community priorities;
- investment efficiency;
- information flow density; and
- quality of infrastructure services and community benefits.

Applications of the H-KPI methodology include strategic planning, systems design and assurance, and operations management. The approach will benefit future efforts in the NIST smart cities and communities program including the NIST Global City Teams Challenge.

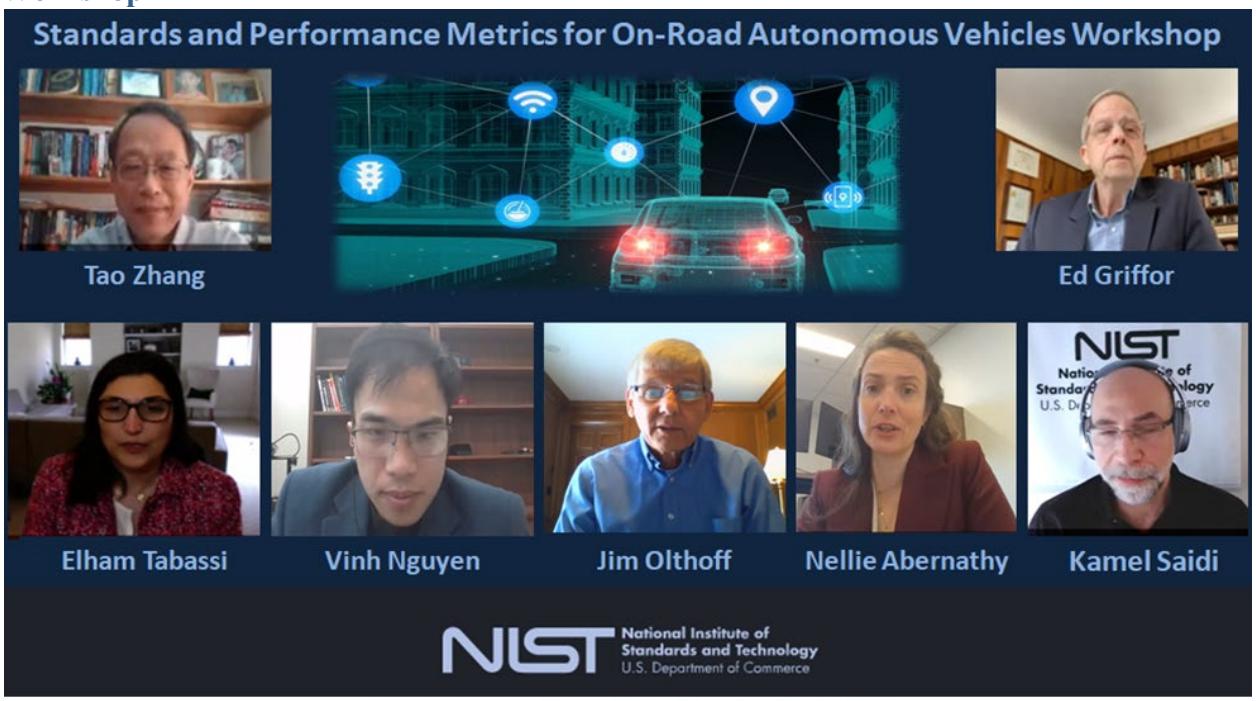
In this collaboration, Dr. Serrano (Senior Research Fellow in the Insight Centre for Data Analytics at the National University of Ireland Galway) was supported by the NGI Explorers Program under the EC Horizons 2020 framework.

Equipped with tools to measure progress, cities and communities can now navigate their course to a smarter future for their residents and businesses.

Media reporting on NIST's H-KPI Framework for smart cities and communities includes the following:

- *Smart Cities Connect,* NIST Holistic Key Performance Indicators Framework Expands Evaluation Criteria for Smart Cities, March 18, 2022
- *IEC,* Evaluating smart cities, March 16, 2022
- *Smart Cities Dive*, How smart is your city? NIST provides a framework to measure, March 14, 2022
- *OpenGov Asia,* NIST, U.S. Publishes Indicators for Smart Cities, March 7, 2022
- *GCN*, How smart is your city? NIST can help you find out. March 4, 2022

Stakeholders Provide Input on Automated Vehicle Performance Metrics in NIST Workshop



Listening to stakeholders – it's what NIST does

NIST hosted the Standards and Performance Metrics for On-Road Autonomous Vehicles Workshop, March 7-8, 2022, with nearly 800 attendees from industry, academia, and government. The goal was to discuss the needs for standards, test methods, and performance metrics for autonomous vehicles, noted acting NIST Director, Jim Olthoff, who kicked off the workshop. Stakeholder collaboration is also required to help automated vehicles transform industries, mitigate vehicle accidents, cut carbon and more, stated Nellie Abernathy, acting Director, Office of Policy and Strategic Planning, Department of Commerce.

Panels of experts addressed key areas for autonomous vehicles, which were safety, communications, artificial intelligence, cybersecurity and privacy, and sensor perception. Attendees further discussed these key areas in breakout sessions, with designated spokespersons summarizing their sessions' findings in the concluding meeting with all workshop attendees. NIST plans to publish a report on the workshop. Workshop videos are available on the workshop webpage.

.

NIST Releases Cybersecurity Guide for Manufacturing Control Systems

Protecting control systems against cyberattacks

(NIST image)

The recently published IBM X-Force Threat Intelligence Index 2022 stated "For the first time in five years, manufacturing outpaced finance and insurance in the number of cyberattacks levied against these industries…" To help meet these growing cyber threats, NIST published Special Publication 1800-10 Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector, developed in collaboration with cybersecurity providers. Its goal is to help manufacturers protect Industrial Control Systems which enable management of machinery, production lines, and other physical processes that produce goods. Specifically, the guide seeks to help manufacturers:

- Secure historical system data
- Prevent execution or installation of unapproved software
- Detect anomalous behavior on a network
- Identify hardware, software, or firmware modifications
- Enable secure remote access
- Authenticate and authorize users

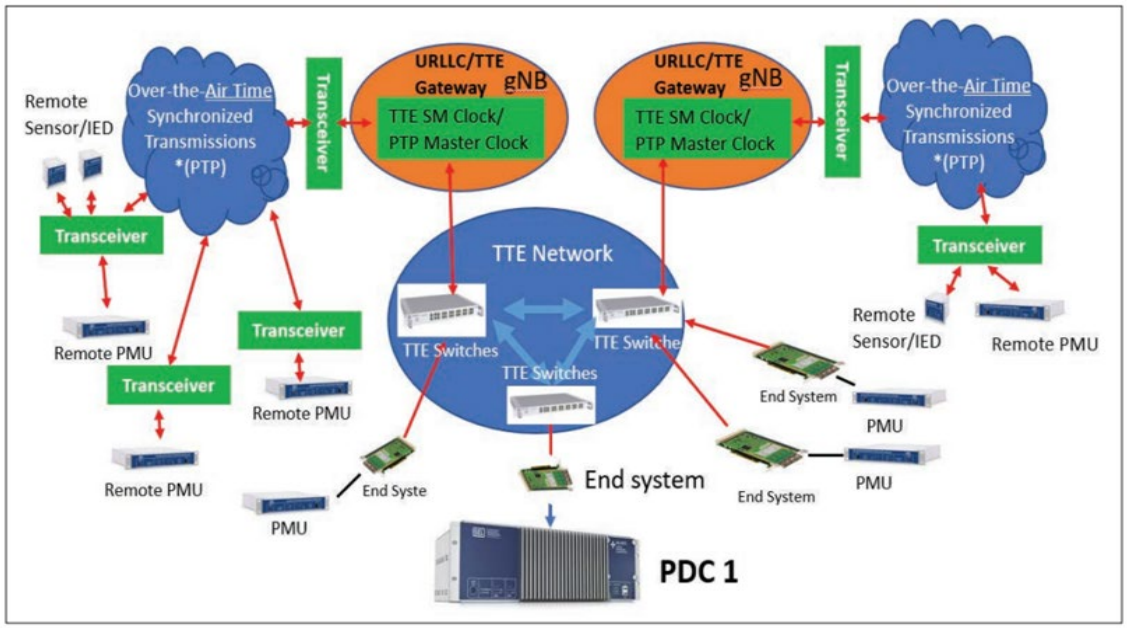
The guide offers four examples of practical solutions which manufacturers may adapt to their unique environments and needs. Each scenario is mapped to relevant NIST Cybersecurity Framework functions and subcategories and details security capabilities provided by proposed products. The solutions are consistent with other relevant practices and guidance, which the Guide lists.

The Guide also points out the intended audiences – manufacturing's chief information officers, program managers, and information technology professionals in other sectors – and proposes how they may use the

Guide. Additionally, NIST solicits feedback on the Guide, which can be provided at manufacturing_nccoe@nist.gov.

Security Week reported on the publication in NIST Releases ICS Cybersecurity Guidance for Manufacturers, March 17, 2022.

NIST Researchers Investigate a Hybrid Wired/Wireless Deterministic Network for the Smart Grid



A hybrid deterministic network for smart grid

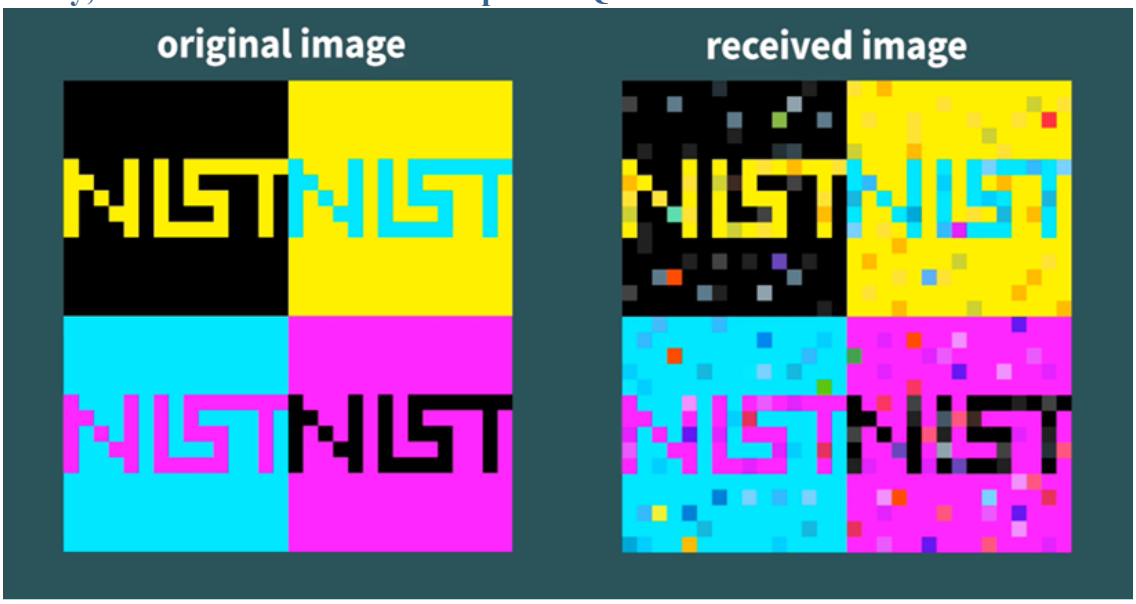
NIST researchers have published a technical paper in *IEEE Wireless Communication*: A Hybrid Wired/Wireless Deterministic Network for Smart Grid, to examine opportunities for new technologies to improve communications in certain power system domains. A key motivation is to address the low-latency, low-jitter, and high-reliability requirements of time-critical applications, such as smart grid synchrophasor communications.

In this publication, the authors consider a time synchronized network that uses a combination of Time Triggered Ethernet and 5G for high speed, ultra-reliable, and low-latency communications. In this example, the network distributes universal time and synchronizes grid devices to a common time source. NIST researchers point out that this hybrid network must have high reliability and low delay wireless communications capability to complement traditional wired communication attributes for application sensors and data streams to be most useful, wherever wired access is not available. Such a network would be able to reliably connect large numbers of Phasor Measurement Units which monitor the health of the power grid.

NIST researchers also address the challenges of implementing such a network. Specifically, they point out that the main challenge will be achieving interoperability between Time Triggered Ethernet and 5G ultra-reliable, low-latency communications. Another technical challenge will be integrating wired and wireless networks in order to coordinate and synchronize timing.

Researchers simulated a hybrid network, including solutions for these challenges, for synchrophasor applications. Researchers reported the simulation showed that the proposed, fully synchronized hybrid wired/wireless network could achieve high reliability and low jitter, which are essential for synchrophasor communications.

University, NIST Researchers Offer Improved Quantum Measurement



Visualization of experimental shot-by-shot (pixel-by-pixel, in image) quantum measurement confidence estimation, outperforming classical measurement.

Quantum mechanics involves the study at the subatomic scale, where photons, electrons and other elementary particles can become the building blocks for future innovations. This research has led to better clocks, computers, and communications networks. The challenge is measuring the quantum state, which is needed to relate the quantum world to our "classical" macroscopic world.

University of Maryland and NIST researchers experimentally developed a way to improve such measurements, which is described in Experimental Shot-by-Shot Estimation of Quantum Measurement Confidence in *Physical Review Letters*. Essentially, researchers obtained confidence estimates for quantum state measurements and then verified estimates by matching them to observed success probabilities, averaged over a large number of measurements. Here, confidence is a quantum analog of accuracy and it is estimated separately for each laser pulse under measurement. This method was demonstrated by continuously counting photons in a single laser pulse over its duration; these were then compared to the averaged fidelity of measured outcomes. These verified estimates proved more accurate than ideal classical measurements which were found by simulations.

This research makes single-shot confidence estimation available to others for use. The single-shot confidence estimation vector can be used to discard low confidence quantum measurements and can help correct measurement errors. This result can potentially improve optical classical networks by reducing the energy requirements at the receiver.

Sign up for NIST's Public Safety Broadband Stakeholder Meeting

Registration is open

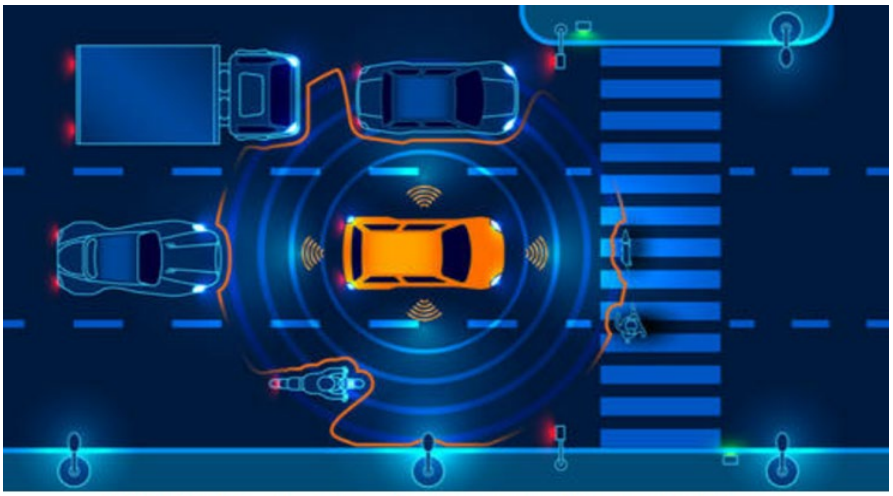
NIST's Annual Public Safety Broadband Stakeholder Meeting will bring together representatives from public safety, federal agencies, industry, and academia, in its first in-person gathering in three years. The 2022 meeting is hosted by NIST's Public Safety Communications Research (PSCR) Division, which seeks to drive research, advancing communications technologies for the public safety community, in partnership with its stakeholders. These annual stakeholder meetings provide PSCR with direct input, guidance, and feedback from this diverse stakeholder community.

The 2022 meeting will emphasize opportunities for PSCR staff, partners, and stakeholders to reconnect. Industry leaders and public safety partners will address cutting-edge technology findings, features, and functionalities. NIST's PSCR engineers and researchers also will provide testing updates, upcoming R&D, and opportunities for involvement. The 2022 meeting offers:

- Over 50 research presentations, available on-demand, prior to the meeting
- Five plenary sessions
- Over 15 breakout sessions
- Over 25 technology demonstrations
- Scheduled informal networking

Registration is open and online. A block of hotel rooms has been set aside for meeting participants at the Westin San Diego Gaslamp Quarter, and rooms can be reserved online.

Virginia Tech Daily, *Roanoke Star* Report on VTTI-NIST Tool for Developing Automated Driving



VTTI, NIST tool aiding development of automated driving

Virginia Tech Daily reported Virginia Tech Transportation Institute researchers develop an open-access interactive tool to advance automated driving systems across the country, on March 3, 2022. The report identified that NIST-funded development of the tool, termed "Operational Design Domain Element Quantification Element," provides developers with critical information needed to safely and effectively deploy automated driving systems. The report quotes NIST's Ed Griffor, “The ability to determine whether the capabilities of automated driving systems are sufficiently exercised in the testing environment is critical to understanding their safety, and this tool aims to show it is feasible.” The report also provides a link to a video demonstrating the tool. The *Roanoke Star* also reported on this work, on March 4, 2022.

Media Reports Credit NIST with Advancing an Understanding of Cyber-Physical Systems

Guiding the way for Cyber-Physical Systems

"Innovative cyber-physical systems are already ushering in the next Automation Age," reported *The ST Blog* in How New Cyber-Physical Systems are Making a Positive Difference, March 1, 2022. *The ST Blog* further reported that this is a new type of automation, largely due to the confluence of these cyber and physical systems, and that the rate of automation will increase significantly in the coming years. The ST Blog article also was published in *ELE Times* and *Electronics Online*, both on March 28, 2022.

The ST Blog credited NIST with formalizing the term, "cyber-physical systems" in its Special Publication 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview, which describes CPS as "smart systems that include engineered interacting networks of physical and computational components." *The ST Blog* also said that many have asked about the difference between CPS and the Internet of Things (IoT) and that NIST again helped clarify through its Special Publication 1900-202 Cyber-Physical Systems and Internet of Things. *The ST Blog* ST adopted the interpretation that CPS is a superset that includes IoT and that CPS provide control systems, mostly absent in traditional IoT.

In COVID's Silver Lining: The Acceleration of the Extended IoT, February 16, 2022, *Security Week* also cited NIST's Cyber-Physical Systems website which defines CPS as "comprising interacting digital, analog, physical, and human components engineered for function through integrated physics and logic." The article reported that the COVID-19 pandemic forced many organizations to rapidly adopt the use of CPS/IoT based on the value it delivers, enabling them to move forward faster, securely, and with no turning back.

Additionally, *Forbes* reported on The Security Challenge Of Protecting Smart Cities (which use CPS), October 10, 2021. It pointed out that NIST's Smart Cities and Communities Framework applies best practices in providing cities and communities with technical guidelines for planning, developing, and implementing smart solutions.