# NIST Smart Connected Systems Newsletter – February 2022



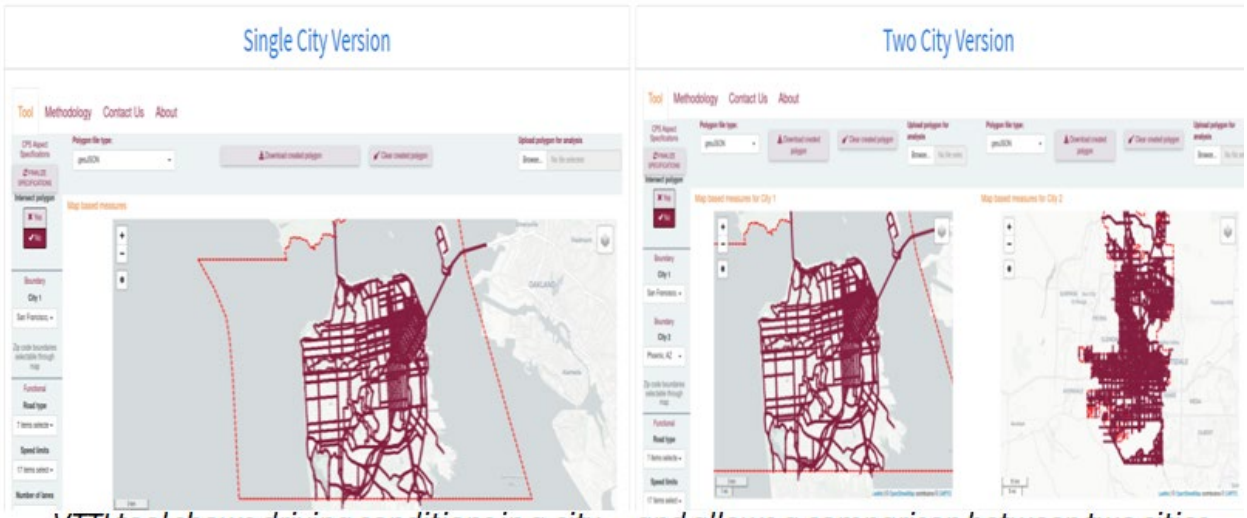
## VTTI, NIST Provide Tool for Quantifying Automated Driving Conditions

*Quantifying environmental conditions and more in the design of automated driving systems*

A new online tool, the Operational Design Domain Element Quantification Prototype, was developed and made available for use by Virginia Tech Transportation Institute (VTTI). NIST funded the tool's development through a cooperative agreement with VTTI and collaborated on its research.

The tool helps researchers and industry practitioners to understand and quantify automated driving operating conditions in a city, community, or region. These conditions are described in the Operational

Design Domain (ODD) in which an automated vehicle is designed to operate. The ODD of an automated vehicle provides a description of its environmental, geographical, and other restrictions, as well as applicable constraints, such as permissible speeds, geographic areas, road types, and environmental conditions. The ODD is used in the design, build, and test of Automated Driving Systems (ADS). Ultimately, the tool helps to provide a foundation for assessing the safety of an ADS-equipped vehicle.




*VTTI tool shows driving conditions in a city … and allows a comparison between two cities*

The VTTI tool, supported by NIST, offers a data-driven approach for choosing where to test an automated vehicle, based on its ODD, and is intended for users in government, industry, and academia. The tool makes use of NIST's Cyber-Physical Systems Framework and is designed to show the ODD elements' interconnectedness. The tool provides users with access to a set of key ODD elements in 30 major U.S. cities. For example, the tool shows ODD elements such as monthly weather conditions, route types, crash data, and more. Users can use the tool to:

- Develop ODD definitions suitable for a market or region
- Quantify conditions facing ADS-equipped vehicles in any of 30 major U.S. cities
- Explore how changing ADS challenges impact ODD specifications
- Demonstrate extensions of ODD specifications using NIST's CPS Framework

## NIST Smart Grid Framework 4.0 Aids Gap Analysis of Southeast Asian Grid Standards


*"The main reference document used in this study was the National Institute of Standards and Technology's (NIST) Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0"*

The Department of Commerce's International Trade Administration, with the support of the Electric Power Research Institute (EPRI), recently released the report, Smart Grid Interoperability Standards Adoption in Southeast Asia, which involved a gap analysis of existing standards in Indonesia, Malaysia, Philippines, Thailand, and Vietnam. NIST staff helped to guide ITA's assessment of smart grid standards adoption in this region, including using the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. The study noted that, "The Framework provides a useful conceptual model for smart grid applications by categorizing functions within various domains and subdomains." In addition, NIST staff engaged with the study team to help identify which standards would be the most meaningful to assess, and to guide the metrics used to evaluate gaps.

As part of the gap analysis, the study team explored the impact that different approaches to establishing requirements can have on standards adoption. The results inform policymakers and private industry about the adoption of smart grid interoperability standards within targeted markets, and the impact that different governance strategies can have on standards adoption. The study team also identified five important smart grid standards and developed case studies to examine the benefits that enhanced adoption could bring to governments, utilities, and customers in the five Southeast Asian markets.

The study informs Southeast Asian policy makers at a time when their nations are evaluating electricity generation for mitigating and adapting to the worst impacts of climate change. The study also said these nations expect to add over 50 gigawatts of generation capacity and spend nearly $100 billion on upgrades, power transmission, and distribution networks by 2030. This modernization enables U.S. standards development organizations and the U.S. Government to share best practices and creates opportunities for U.S. exporters and service providers.

## NIST Researchers Receive Award for Manufacturing Cybersecurity Guidelines, Achieving Wider Use

*Enabling cybersecurity for small and medium manufacturers*

On January 12, 2022, NIST presented the Department of Commerce Bronze Medal to Keith Stouffer, Timothy Zimmerman, CheeYee Tang, Michael Pease, and Jeffrey Cichonski for developing and disseminating the first, detailed cybersecurity guidelines for small and medium-sized manufacturers.

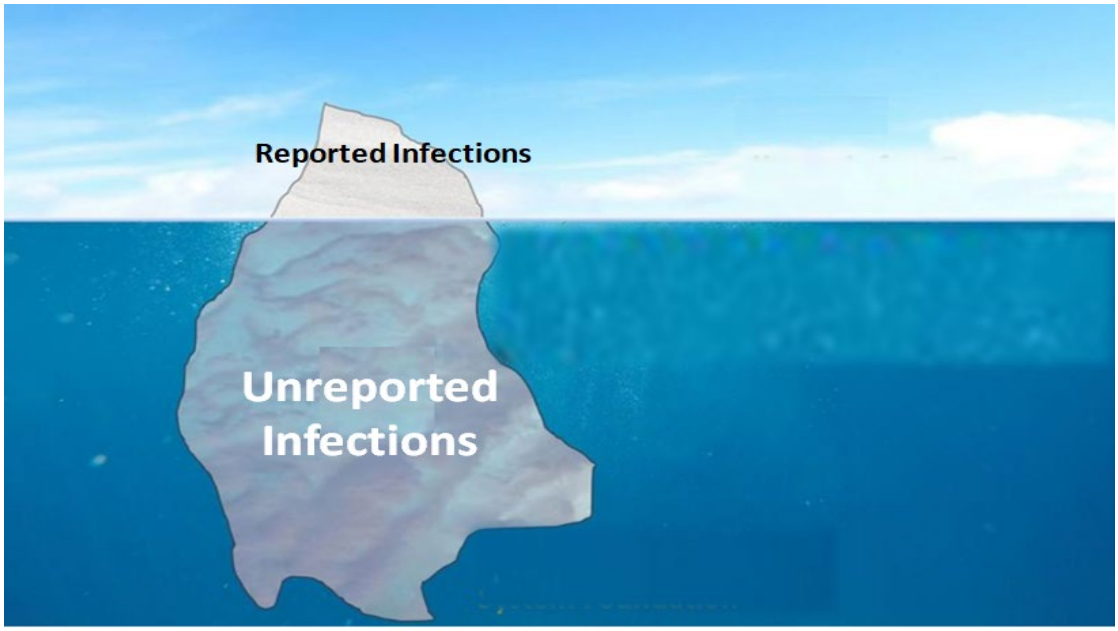
In 2018, an assessment by the DOC Bureau of Industry and Security documented that fewer than half of small and medium-sized manufacturers had any cybersecurity measures in place. Yet, growing automation and Internet connectivity made systems more vulnerable to attack and hackers were increasingly targeting them.

These NIST researchers recognized the need to secure these systems. They developed NISTIR 8183 Cybersecurity Framework (CSF) Manufacturing Profile (subsequently updated to Version 1.1) and corresponding NISTIR 8183A Implementations Guide, Volumes 1, 2, and 3 to help small and medium-sized manufacturers manage cybersecurity risk, while also optimizing their operations. These publications are tailored to manufacturing business goals and industry best practices. They provide small and medium-sized manufacturers with an easy-to-understand process to efficiently select and deploy cybersecurity tools and techniques that best fit their needs, making cybersecurity no longer a "black art."

Researchers based the NIST guidelines on quantitative network and operational performance impact measurements of cybersecurity technologies (e.g., industrial firewalls, intrusion detection systems, anti-virus software, etc.). Researchers made these measurements in a testbed representative of manufacturing environments. Researchers also helped to develop industry consensus for the guidelines and promoted their adoption.

The Manufacturing Extension Partnership (MEP) selected the guidelines as the basis for cybersecurity implementation guidance for small and medium-sized Department of Defense (DoD) suppliers, as well as for piloting cybersecurity program implementations at two MEP member companies that supply to DoD. Results from the pilot are being used to provide cybersecurity implementation guidance to small and medium-sized manufacturers across the U.S. via the national network of MEP centers. In addition, the Department of Homeland Security's Critical Manufacturing Sector Cybersecurity Working Group expressed its thanks to "NIST and its other contributors for developing and updating this outstanding and valuable manufacturing profile for our sector."

## How Many Infections Are in Networks (or Society)? NIST Researchers Offer a Way to Find Out




*Just the tip of the Iceberg*

When infections spread, like malware in networks or diseases in society, not all individual cases are known. Networks may lack the latest detection means and, in society, infected individuals may be asymptomatic. Thus, the true number of infections in an epidemic could be much larger–a key point made by NIST researchers in Story of Two Populations in Epidemics: Is Every Infection Counted? recently published in *Complex Networks & Their Applications X.*

NIST researchers address the need to quickly determine the presence of undetected infections in a network, so that they can be contained and treated. Their approach involves modeling populations' detected and undetected infections and their approximate transmission times, which vary (undetected cases transmit for longer times). The approach also calls for modeling a population with only detected infections and their approximate transmission times. The two modeling results are then compared to determine how significant the number of undetected cases might be.

NIST researchers applied this approach using publicly available COVID-19 data from France, Spain, the United Kingdom, and the United States, reported in each country at the beginning of the pandemic.

Their findings suggest that there were significantly more infections than reported in all four countries. The U.S. Center for Disease Control estimated that only 1 in 4.2 cases, or roughly 23.8% of COVID-19 infections were reported in the U.S. – close to the NIST researchers' estimate of 22.1%.

## NIST, University Researchers Offer Model for Minimizing Large Networks' Cybersecurity Costs

*Getting the most cybersecurity for large networks with a minimum investment*

Large networks are often comprised of interdependent subsystems, such as information, communication, and power systems, which may make them vulnerable to cyberattacks. A virus/malware infection in one system can spread internally, attacking other systems, potentially impacting the overall system. Researchers noted that the problem is similar to that of the spread of diseases in social networks.

NIST and university researchers have developed a model for minimizing large networks' cybersecurity costs that was described in Optimal Cybersecurity Investments in Large Networks Using SIS Model: Algorithm Design, recently published in *IEEE/ACM Transactions on Networking*. The researchers sought a way to determine optimum investments needed to minimize the costs of securing these networks, providing recovery from infections and repairing their damage.

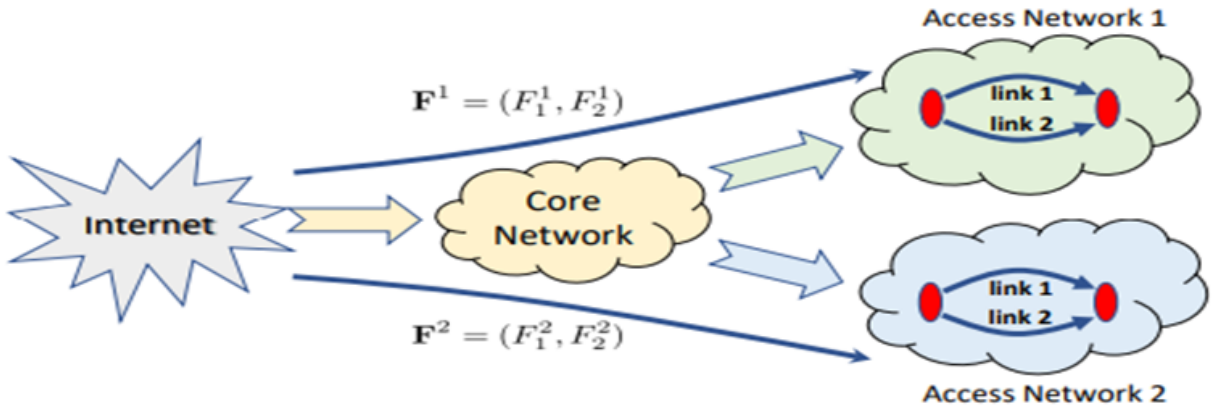
Unlike previous studies that involved optimum vaccination strategies for quickly reducing infection rates in epidemics, researchers used a time-averaged, aggregate security cost, based on a network's long-term behavior analysis as a key performance metric for determining security investments. The researchers then developed a model which assessed investments for security measures, such as monitoring, diagnostics, and more, against the following:

- Probabilities of virus/malware breaching systems;
- Rates of spread within systems; and

- Rates of recovery and repair.

Based on modeling results, a set of efficient algorithms was developed for determining optimum investments that would minimize security costs for given conditions.

## NIST Researchers Develop Algorithm for Assuring Quality-of-Service in 5G/6G Networks




*NIST's proposed algorithm enables 5G/6G's core and access networks to coordinate data needs*

5G and 6G networks will differ greatly in composition and services, compared to one-size-fits-all 4G networks. 5G and 6G networks must provide varying services for such Internet of Things applications as automated manufacturing, vehicle-to-vehicle communications, and remote drone operations – all having differing requirements for data amounts and flow rates. Some of these applications will be very sensitive to data delays.

A significant challenge will be assuring quality of service for user systems at the ends of these networks. NIST researchers have proposed a way to do that in End-to-End Quality-of-Service Assurance with Autonomous Systems: 5G/6G Case Study, recently published by the IEEE Consumer Communications & Networking Conference.

The paper addresses the problem of managing a 5G/6G network's required data flows to multiple user systems, which can be adversely impacted by random events, such as network congestion. This management is challenged by the limited coordination regarding data flows between the 5G/6G network's subordinate networks which autonomously manage themselves. These are:

- Access networks, which wirelessly connect user systems; and
- Core networks, which coordinate some parts of the access network and connects to the Internet.

NIST researchers have developed a framework, which allows these autonomous, subordinate networks to achieve greater coordination among themselves. Specifically, the framework involves an algorithm that allows the networks to negotiate local, needed data amounts. This algorithm also enables these subordinate networks to exchange their estimates regarding overall, global constraint functions. NIST researchers demonstrated the algorithms using numerical studies.

## NIST-led Panel Assesses Test and Evaluation of Industrial AI, Risk Awareness, and Barriers to Use


*NIST-led panel at 2021 INFORMS meeting*

At its 2021 meeting, the Institute for Operations Research and the Management Sciences held a panel on Testing and Evaluating Industrial AI and Risk Management, chaired by NIST's Michael Sharp and moderated by NIST's Mehdi Dadfarnia. The panel included experts in industrial AI and sought the knowns and unknowns in this fast-changing field. The following are some key points.

*Need for Testing and Evaluating industrial AI:* Many AI systems are producing good results, but some are not. Determining the good and bad depends on testing and evaluating AI systems, which some do not know how to do, or do not have the resources to accomplish. In some cases, the testing does not exist.

*Determining Risks in Industrial AI:* There are risks in applying an AI to an industrial system, as well as risks within the AI and industrial system separately. These standalone risks along with their possible interactions must be considered in testing and evaluation.

*Test Scenarios for AI Must Reflect Real World Uses:* In practice, this is hard to do, as not everything can be tested. Testing requires controlled and bounded scenarios. However, even with bounded limits, it is infeasible to predict and evaluate every possibility for many systems. This is particularly true in systems where the most pertinent scenarios are rare by design, such as predicting failures in safety critical machines.

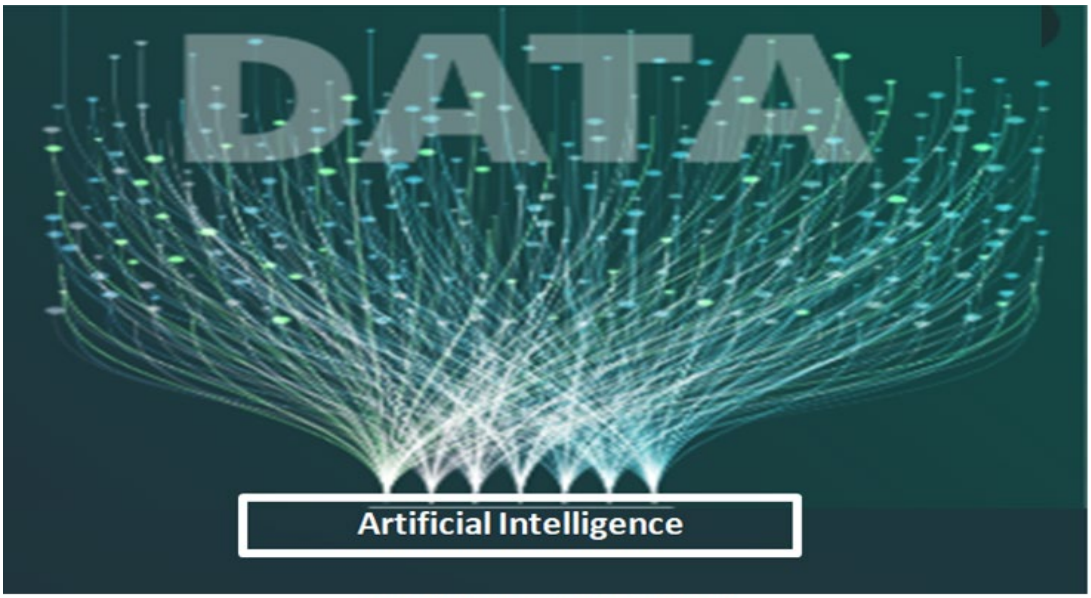
*Determining an AI system's Acceptable and Unacceptable Risks:* These come from bounding test scenarios. Scenarios determined to be acceptable in their risks and consequences may not need to be

tested. Conversely, identified, unacceptable risks should be in testing scenarios and evaluated for mitigation. The level of acceptable risk will vary with an AI system's needed reliability.

*Determining How Much Testing and Evaluation Is Worth It:* This depends on a business case, showing that an AI system will bring so much money by decreasing a degree of risk with low level testing, then matching the resources put into testing to what is justified by the investment and expected return. This balance of testing versus return should qualify relevant metrics and scenarios to the point where the users trust that anything unaccounted for falls within their acceptable risk threshold.

*Barriers to Industrial AI Adoption:* Many industry stakeholders are resistant to invest in AI applications where there is a lack of trust or an unclear return from using the technology. However, those are not the only concerns. Many companies are hesitant to invest in AI tools that could be negated by changes in regulations, or even by rapid changes in the technology itself.

## NIST-led Panel Addresses Qualifying Data for AI Use




*Making data useable for AI*

At its 2021 Conference, the Prognostics and Health Management Society held a panel on Qualifying Data and Data Use Assuring Data Capability for Intelligent Systems and Beyond, organized and chaired by NIST's Michael Sharp and moderated by NIST's Vincenzo Ferrero. The panel sought to identify concerns regarding data use for artificial intelligence. While data may seem correct, it must be functionally useable for AI. This requires qualifying data for given applications, which includes:

- Identifying the data's source and its collection methodology, so as to be aware of any bias
- Ensuring data adequately covers what it is supposed to, like test scenarios
- Knowing any variances related to data
- Storing data without distortion or corruption, which can occur with certain data
- Avoiding the collection of too much data, which can be difficult to store as well as use

- Preventing data from being subverted – intentionally modifying it for personal interests
- Ensuring intellectual property and personal identifiable information are protected or absent

Identifying these concerns helps build consensus regarding how to address them. It also helps pursue mechanisms for measuring the quality of collection, use, and return on investment.

## Are Industrial AI Tools Worth it? NIST Researchers Offer An Evaluation Procedure

*How do you know your getting your money's worth from industrial AI?*

Industry is increasingly using artificial intelligence to aid analysis and decision-making. It is also recognizing the need to evaluate these tools with respect to their utility and value. Are these tools doing what they are supposed to, and, moreover, are they worth it? To help answer such questions and more, NIST researchers recently published a Procedural Guide for System-Level Impact Evaluation of Industrial Artificial Intelligence-Driven Technologies: Application to Risk-Based Investment Analysis for Condition Monitoring Systems in Manufacturing in the *Journal of Manufacturing Science and Engineering.*

The procedure focuses on evaluating condition monitoring systems, used to identify problems – faults, defects – in a system/process, and thus reduce their risks. This case study is intended to serve as a basis for evaluating other industrial artificial intelligence tools.

The procedure begins with assessing the viability of a condition monitoring. It calls for determining if a system/process will benefit from monitoring – not all systems/processes do, notes the paper. The procedure involves determining if condition monitoring will detect problems associated with risks, assessing whether risks can be mitigated, and quantifying risks in terms of frequency and severity.

The results help to evaluate if condition monitoring is worth it, and the paper proposes steps for this evaluation:

- Determine a system's/process's baseline risk without condition monitoring
- Determine a condition monitoring system's installation and operating costs

- Assess the risks of operating condition monitoring system
- Estimate the value of condition monitoring for a given system/process
- Conduct a risk-based investment analysis with metrics used by businesses

The paper also shows how these procedures could be used to evaluate condition monitoring systems in paper mill cutting and multistage laser-engraving operations.

## NIST Researchers Propose Method for Modeling Smart Sensor Interoperability in Smart Grids

*The smart grid depends on these systems and others sending and receiving messages and data*

Smart sensors play a critical role in smart grids, supporting bidirectional flows of energy. Such sensors are needed for real-time monitoring of energy flow; controlling power generation, transmission, and distribution to customers; and protecting the overall power systems. However, the interoperability of smart sensors is an issue, due to the number of different manufacturers employing various interface protocols in their products.

To help address the interoperability issue, NIST researchers propose A Methodology for Modeling Interoperability of Smart Sensors in Smart Grids, recently published in *IEEE Transactions on Smart Grid.* The modeling methodology is based on interactions, using labeled transition systems and finite state processes techniques to quantitatively and automatically measure and assess smart sensors' interoperability. Any interoperability issues can be identified based on the assessment results and ultimately resolved to improve sensor data interoperability in smart grids.

The methodology is used to build an interoperability model of synchronous message passing from a sender to a receiver. This model can be used to assess interoperability between the sender and receiver. The paper also provides a use case study, showing that this methodology and interoperability model work with the IEEE C37.118 phasor measurement unit-based smart sensors and phasor data concentrators. This methodology can also be applied to modeling interoperability of smart sensors, based on other standard communication protocols.

The interoperability model, built based on the methodology, is intended to help manufacturers, developers, and test laboratories assess the interoperability of smart sensors.

## Plan to Virtually Attend NIST's Autonomous Vehicle Workshop, March 8-9, 2022

*Help NIST help the automated vehicle domain*

NIST will host the Standards and Performance Metrics for On Road Autonomous Vehicles Workshop, March 8-9, 2022. The virtual workshop will solicit stakeholder input regarding key areas in which NIST can apply its technical expertise to advance on-road, autonomous vehicles. Attendance is free and open to the public. Registration is required and can be done online.