SMART CONNECTED SYSTEMS

NIST Smart Connected Systems Newsletter – November 2021

- News Report Highlights Interoperability Approach in NIST Smart Grid Framework 4.0
- NIST, North American Electric Reliability Corporation Publish Guide for Bulk Electric System's Cybersecurity
- NIST Helps SEPA Develop Electric Vehicle Charging Use Case to Identify Interoperability Needs
- NIST Offers Guidelines for Securing Distributed Energy Resources and Proposes Research
- Publication Details NIST Tool for Forecasting Electric Loads, Enabling Potential Savings
- NIST Helps OMG Update a Simulations Standard, Improving System Engineering
- News: NIST's Pivotal Points of Interoperability Enable Smart City Standardization
- NIST, University Researchers Introduce Framework for Composing IOT Capabilities
- NIST Global City Teams Challenge (GCTC) Hosts Events, Engaging U.S. Community Stakeholders and Generating Potential New Ones in Brazil

News Report Highlights Interoperability Approach in NIST Smart Grid Framework 4.0

NIST Smart Grid Framework 4.0 helps smart grid equipment and systems work together

Smart Energy's How to improve smart grid interoperability – ISGAN reported that the International Smart Grid Action Network (ISGAN) has pointed out the suitability of a community-driven management approach to achieving interoperability, which involves users, vendors and other stakeholders. This approach is described in the ISGAN discussion paper, How to Improve the Interoperability of Digital (ICT) Systems in the Energy Sector, and cites the 'Integrating the Energy System' (IES) Austria initiative.

Smart Energy characterized Austria's IES methodology, as described in this paper, as similar to that in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. The NIST Framework proposes a manufacturer-neutral and cooperative process to define interoperability profiles and perform interoperability testing of information and communications technology systems.

Smart Energy also reported that basic elements of NIST's Interoperability Profiles include the asset description, associated physical performance specifications, communication protocol(s), and information model(s). *Smart Energy* further reported, that to better enable interoperability, the NIST Smart Grid Framework 4.0 proposes development of open-source test harnesses and expansion of formal testing and certification programs.

NIST, North American Electric Reliability Corporation Publish Guide for Bulk Electric System's Cybersecurity

A guide to help users apply both to the Bulk Electric System

In 2020, NIST and the North American Electric Reliability Corporation (NERC) mapped the NIST Cybersecurity Framework to NERC's Critical Infrastructure Protection (CIP) Standards for the Bulk Electric System. Recently, NIST and NERC jointly published the Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards. It provides the Bulk Electric System's stakeholders with guidance regarding how to apply this mapping. Specifically, it explains the mapping's three spreadsheets and their uses:

- Mapping of NIST Cybersecurity Framework to NERC’s CIP Standards: Shows the NERC standards that map to each subcategory of the NIST Cybersecurity Framework.
- Reverse Mapping of NERC’s CIP standards to NIST Cybersecurity Framework: Lists NIST Cybersecurity Framework subcategories that align with each NERC standard.
- Pivot: Shows the same information as the reverse mapping but is configurable. Users can expand or minimize each NERC standard. They can also view information from the NIST Cybersecurity Framework – such as Function, Category, and Subcategory.

Equally important, the guidance notes that the spreadsheets provide informative resources for each subcategory, like industry standards, guidelines, practices and more. These resources provide a good first step for users unsure of where to start in complying with cybersecurity requirements and the subsequent steps they can take to realize intended outcomes. Ultimately, an organization can use these resources to develop an action plan for cybersecurity.

NIST Helps SEPA Develop Electric Vehicle Charging Use Case to Identify Interoperability Needs

Image from SEPA Brief

NIST's Cuong Nguyen led the Smart Electric Power Alliance's (SEPA) Interoperability Task Force in its development of the "EV Fleet Managed Charging Use Case." The use case addresses two scenarios for managing electric vehicle (EV) charging, defining the roles of all involved and types of information exchanges that occur:

- Scenario 1 – Two-way information exchanges between an EV charging system and grid operations: In this scenario, the charging system provides grid operations with information on independently run supply equipment and near-term usage at each facility. Grid operations provide the charging system with information about historic use and future demand management events. The use case outlines how these events are communicated and how performance is verified.
- Scenario 2 – Information exchanges between EV charging stations and grid operations, via an "aggregator," which collects information from one or multiple charging systems. The charging systems have varying options for being managed. Grid operations measure performance and calculate payments.

The next step in this process is mapping requirements from the use case to applicable standards. This mapping will help reduce the number of implementation options and lead to specific configurations for implementation, to include interoperability profiles.

NIST Offers Guidelines for Securing Distributed Energy Resources and Proposes Research

NIST supports securing grid interfaces

In October 2021, NIST published Distributed Energy Resource Security: Potential Guidelines and Research Topics. This NIST Tech Note addresses an effort to validate the applicability of cybersecurity controls in NIST’s Guidelines for Smart Grid Cybersecurity (NISTIR 7628 Revision 1, published in 2014) to distributed energy resources (DER), which have new information exchanges with the grid, and which are potential points of cyberattacks.

The NIST 2021 Distributed Energy Resource Security publication reports that these interface categories can be secured based on NIST’s Guidelines for Smart Grid Cybersecurity. As examples, NIST's 2021 publication compared three new DER interface categories to cybersecurity protections for grid interface categories that existed at the time of the NIST 2014 publication, finding that the cybersecurity protections are applicable to the new DER interface categories. The 2021 publication also maps NIST's 2014 cyber controls to critical infrastructure standards set by North American Electric Reliability Corporation.

NIST’s Distributed Energy Resource Security publication points out that current cybersecurity controls for interface categories do not address the people and processes for securing high-DER environments. The publication also proposes the following research topics regarding cybersecurity for a high-DER grid environment:

- How other industries solved similar security challenges
- How updated security controls will be implemented in commercial equipment for use in high DER scenarios
- How business models will introduce independent service providers whose sole purpose is to ensure security for DER devices
- How might a framework be applied that expects 80% of cybersecurity regulatory requirements to be met and 20% of requirements to be customized, based on jurisdiction or business model
- How NIST smart grid cybersecurity documents can be harmonized to ensure their applicability in the current technology environment

Publication Details NIST Tool for Forecasting Electric Loads, Enabling Potential Savings

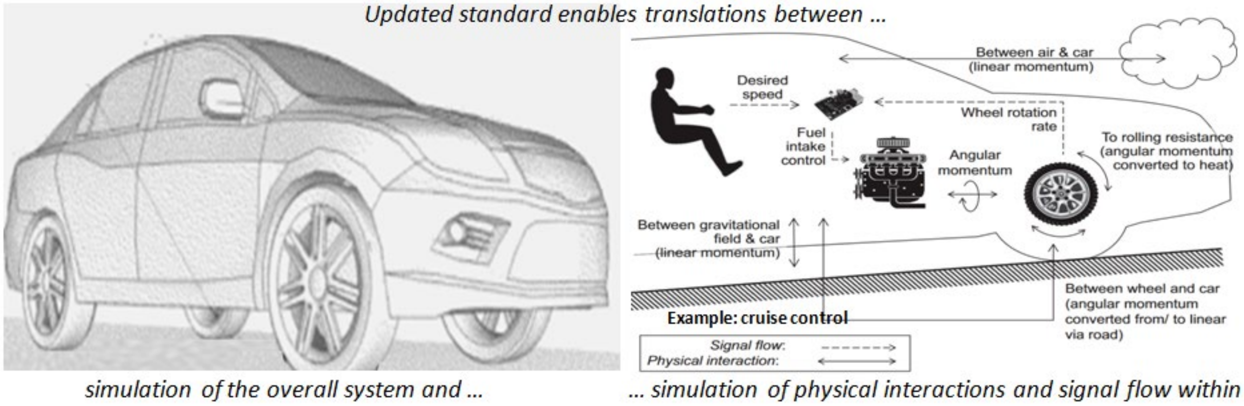
Forecasting how much power will be needed to heat and cool homes like this one

Previously, electric utilities delivered one-directional power to their customers, and balanced generation against consumption. Today, customers increasingly use renewables, such as solar panels, and electric storage, which complicates the balancing of generation and consumption. Price signals from the utility could help customers manage load and storage (thermal and electrical) so that electricity is consumed when the wind is blowing and the sun is shining. This could allow utilities to use less fossil power generation while saving customers money.

In September 2021, NIST published its Load Forecasting Tool (LFT) for NIST Transactive Energy Market. This NIST Tech Note describes a tool which can be used to estimate the next-day electrical energy consumption for a home's heating and cooling. To do this, the LFT tracks key thermal characteristics of a residential home, solar heat gain coefficient, effective window areas, and heat pump coefficient of performance from observations. With this acquired knowledge, the LFT can be used to optimize a heat pump’s operation to minimize cost while maintaining thermal comfort, accounting for heat gains and losses due to changes in the outdoor temperature.

The LFT is an integral part of the NIST Transactive Energy simulation testbed, which is a platform for conducting Transactive Energy experiments. The testbed uses the LFT to help forecast home energy consumption in order to purchase that energy in next day markets. This research supports finding effective approaches for enabling customer-owned intelligent devices, including to support more renewable energy on the electric grid.

NIST Helps OMG Update a Simulations Standard, Improving System Engineering


Updated standard enables translations between ...

simulation of the overall system and ...

... simulation of physical interactions and signal flow within

The Object Management Group® (OMG®) recently released an updated standard called [SysML Extension for Physical Interaction and Signal Flow Simulation](). A NIST [press release](), on October 28, 2021, also reported the update. The update specifies standards for translations between:

- Overall systems engineering modeling, done with Systems Modeling Language or SysML
- Simulations of physical interactions and signal flows within the system being engineered

Previously, system engineers used SysML and other modeling languages to create a model of an intended system and then described to engineers in other domains – electrical, mechanical, production, etc. – what they needed and how their products fit into the system. The other domain engineers used their own tools to specify system components and simulate their behavior. They then brought all the information together and incorporated it into a model of the overall system. However, differences between the two simulations often produced inconsistencies that were difficult for engineers to resolve.

NIST's Conrad Bock played a leading role in addressing this problem. Bock worked with stakeholders in the National Agency for Finite Element Methods and Standards to establish a need for a standard. He and other NIST researchers then conducted research underlying the standard, validated it through software, documented the standard, and shepherded it through the OMG standardization process. The resulting standard was published in May 2021. Since then, NIST researchers have interacted with industry to ensure that the standard can be implemented and used effectively, and they have identified additional needs to be addressed in future versions.

The update improves system engineering reliability. It shows how physical interactions and signals work together in a single system. It also includes a method for debugging physical interaction models, which are more difficult than signal flow models, due to bidirectional interactions between components.

News: NIST's Pivotal Points of Interoperability Enable Smart City Standardization

NIST's framework for enabling interoperability in smart cities

A recent *Propmodo* article, Middleware Needs Standardization to Hold Smart Buildings Together, points out that sensor data in smart buildings and smart cities must get to where it needs to go, so that it can be used and acted upon. That is one of the jobs of middleware software and IoT data and service platforms; they read, route and aggregate data. As the article notes, the need for "seamless collaboration has never been greater in developing the Internet of Things." Establishing interoperability between devices and systems is the key to unlocking the true potential of smart buildings and smart cities.

One challenge, however, is that standardization is needed to aid communications. The article highlights NIST's Pivotal Points of Interoperability as an important foundation for promoting such standardization, while enabling repurposing of data for innovation. The PPI concept is detailed in NIST's Internet-of-Things-Enabled Smart City Framework. It is the starting point for current efforts at NIST to relate reuse and societal benefits to Smart City data sources. The IES-City Framework calls for:

- Analyzing a smart city's existing architecture – including standards, specifications, and protocols
- Identifying overlapping concerns, such as functionality, data, timing, trustworthiness, etc.
- Determining common properties in overlapping concerns, such as in cybersecurity and time synchronization

These common properties, or solutions, reveal Pivotal Points of Interoperability with which technology developers and standards developers can focus specifications to reduce interoperability challenges and leverage to enable multiple applications.

The IoT-Enabled Smart City (IES-City) Framework was published by NIST in 2018. It was a product of the NIST-convened IES-City Public Working Group, led by Martin Burns of NIST, with representatives of government, industry and academia participating. Pivotal Points of Interoperability (PPIs) identify opportunities for consensus-developed, standardized interfaces that deal with composition of IoT without constraining innovation. PPIs provide a middle ground between two paradoxical scenarios: 1) If everything is standardized, innovation is stifled; and 2) If nothing is standardized, the result is non-interoperable clusters that are not easily integrated.

NIST, University Researchers Introduce Framework for Composing IOT Capabilities

The growing need to compose and repurpose IoT capabilities

NIST researchers and collaborators recently published the paper, A Framework for the Composition of Internet of Things (IoT) and Cyber-Physical Systems (CPS) Capabilities, in the proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). The paper resulted from a collaborative effort on the part of researchers at NIST, Grenoble Alpes University, and Johns Hopkins University.

The paper proposes an "IoT and CPS Composition Framework (ICCF)" to help stakeholders compose, model, and verify IoT capabilities for a variety of domains. It can aid open innovation and re-purposing capabilities in a world with an expected half-trillion IoT and CPS devices by 2030. The concept framework is based on previous work, including NIST's Cyber-Physical System Framework, and consists of:

- Semantics that describe capabilities, interactions, and compositions

- Languages and tools that translate semantics into specifications
- Methods of checking models and trustworthiness assessments

The paper details the methodology used to develop the IoT and CPS Composition Framework. This includes assessing the Framework's performance, using a well-being composite capability within a smart building. Researchers propose future work to address composition concerns in other domains of interest.

The NIST Global City Teams Challenge (GCTC) Hosts Events, Engaging U.S. Community Stakeholders and Generating Potential New Ones in Brazil

GCTC Webcast Provides Lessons learned from Technology Use in Smart Community Initiatives

On October 13, 2021, the GCTC Utility SuperCluster conducted a NIST co-sponsored webcast in which a panel of experts addressed the lessons from technology use in smart community initiatives. One example that was described is a windshield-mounted smart phone application that collects visual data on roads; artificial intelligence then analyzes and rates the repair needed.

Roadbotics used to collect data on road conditions

Yet, such technologies face procurement challenges in smart community initiatives. One problem is getting buy-in from all involved, stated NIST's Michael Dunaway. It is very hard work, said Metro 21's Karen Lightman, requiring an active, engaged, and thoughtful hand. Also, when procurements occur in one community, they are not always scalable and useable in another. Additionally, elected officials do not want overly extensive R&D and planning. Rather, they want results within election cycles. NIST plays an important role, as noted Bruce Walker of Analysis and Resilience Center for Systemic Risk, because NIST can accelerate initiatives by serving as an honest broker for decision makers, offering frameworks, best practices, and case studies. NIST also advocates scalable solutions for others' use, helping businesses see the possibility of greater market share, said Dunaway. The webcast is available online.

GCTC's Cybersecurity Symposium Showcases Smart Communities' "Digital Safety Nets"

Cybersecurity Symposium for Smart Cities 2021
Where the World Does Security
Lorem ipsum
October 26 -27
Digital Safety Net Secured

Symposium's vision: "Never waste a crisis. Never reinvent the wheel. Innovate a SafetyNet Together. Good, Affordable, Fast."

On October 26-27, 2021, the GCTC Secure and Safe Communities SuperCluster held the NIST co-sponsored Cybersecurity Symposium for Smart Cities 2021 focused on smart communities' "digital safety nets" – a transformation accelerated by the pandemic and growing cybersecurity needs. Videos of the Symposium are available online.

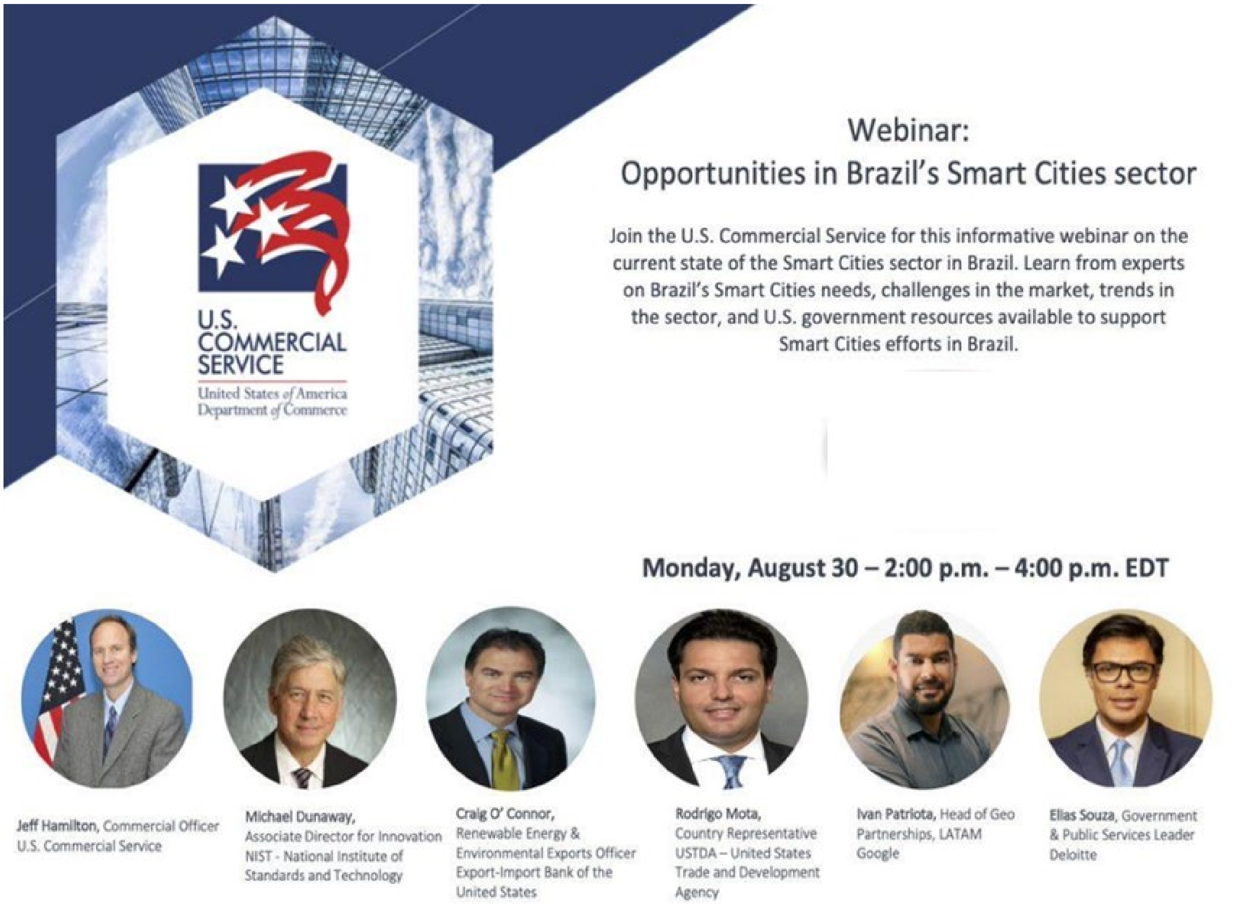
Many speakers addressed the value of these safety nets for local jurisdictions. Chappie Jones, Vice Mayor of San Jose, CA, said that when the pandemic hit, city leaders focused on helping 50,000 households, which lacked broadband access, by deploying hot spots and WiFi across the community. They also helped shop and mall-based, small business owners to transition online – including helping address language barriers.

Vince Lago, mayor of Coral Gables, FL stated his city provides digital services via a Smart City Hub public platform, that enables:

- Businesses to access traffic data in order to better plan when to open and close
- Citizens to submit digital permit requests rather than submit in person
- Drivers to find parking rather than hunt for it
- Ride sharing

Additionally, the symposium provided extensive information on resources, procedures, and agencies that communities can use to improve cybersecurity.

DoC Team including NIST's GCTC Leader Engage Brazilians on Smart City Opportunities



U.S. COMMERCIAL SERVICE
United States of America Department of Commerce

Webinar:
Opportunities in Brazil's Smart Cities sector

Join the U.S. Commercial Service for this informative webinar on the current state of the Smart Cities sector in Brazil. Learn from experts on Brazil's Smart Cities needs, challenges in the market, trends in the sector, and U.S. government resources available to support Smart Cities efforts in Brazil.

Monday, August 30 – 2:00 p.m. – 4:00 p.m. EDT

Jeff Hamilton, Commercial Officer
U.S. Commercial Service

Michael Dunaway,
Associate Director for Innovation
NIST - National Institute of Standards and Technology

Craig O' Connor,
Renewable Energy & Environmental Exports Officer
Export-Import Bank of the United States

Rodrigo Mota,
Country Representative
USTDA – United States Trade and Development Agency

Ivan Patriota, Head of Geo Partnerships, LATAM
Google

Elias Souza, Government & Public Services Leader
Deloitte

Department of Commerce organized team with GCTC Leader Michael Dunway engages Brazil on smart cities

On August 30, 2021, the Department of Commerce's U.S. Commercial Service hosted a virtual webinar on smart city opportunities for Brazilian communities and business personnel. The webinar addressed Brazil's smart city needs, particularly in the post-pandemic era, the technical challenges facing their implementation, and U.S. government resources available to aid smart city efforts in Brazil.

NIST's Global City Teams Challenge Leader, Michael Dunaway, explained the NIST Global City Teams Challenge (GCTC) and how it has helped some 200 smart city initiatives form public-private partnerships – including community residents – to produce solutions that meet communities' needs. Dunaway also explained how GCTC SuperClusters – or working groups – identify key smart cities' functions and develop improvements for transportation, data governance, public safety, and more. Ultimately, the goal is smart city solutions that are scalable and replicable for others, said Dunaway.

The webinar was the GCTC's first recent engagement with Latin America and provided an opportunity to build relationships and pursue Brazil's involvement in GCTC initiatives.