NIST Internal Report
NISTIR 8620

Digital Twins Workshops

Summary Report

Simon Frechette
Guodong Shao
Michael Pease

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8620

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

NIST Internal Report
NISTIR 8620

Digital Twins Workshops

Summary Report

Simon Frechette*
**Former NIST employee; all work for this publication was done while at NIST.*

Guodong Shao
System Integration Division
Engineering Laboratory

Michael Pease
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8620

July 2026

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

NISTIR 8620
July 2026

Publication History
Approved by the NIST Editorial Review Board on 2026-07-16

How to Cite this NIST Technical Series Publication
Frechette S; Shao G; Pease M. (2026) Digital Twins Workshops Summary Report. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (NIST IR) NIST IR 8620. https://doi.org/10.6028/NIST.IR.8620

Author ORCID iDs
Simon Frechette: 0009-0008-4454-9659
Guodong Shao: 0000-0001-8856-3622
Michael Pease: 0000-0002-6489-2621

Abstract

This report summarizes the outcomes of a three-part NIST workshop series on digital twins for manufacturing. The workshops convened experts from industry, academia, and government to establish a shared understanding of digital twin fundamentals, identify barriers and opportunities, and prioritize future directions for research and standards development. Discussions emphasized the transformative potential of digital twins to improve design, production, and lifecycle management, while also highlighting persistent challenges in interoperability; verification, validation, and uncertainty quantification (VVUQ); cybersecurity; and workforce readiness. The report synthesizes these findings into research priorities and standards needs that will guide coordinated efforts to advance trustworthy and scalable digital twins in U.S. manufacturing.

Keywords

Cybersecurity; digital twins; interoperability; manufacturing; standards; supply chain resilience; trustworthiness; verification, validation, and uncertainty quantification (VVUQ).

Table of Contents

Executive Summary

This report presents the findings of a three-part NIST workshop series on digital twins for manufacturing. The workshops brought together stakeholders from industry, government, and academia to build a shared understanding of digital twin fundamentals, identify barriers and opportunities, and outline paths forward in research, standards, and collaboration.

Motivation

The workshop series was spurred by the increasing importance of digital twins in supporting U.S. manufacturing competitiveness, resilience, and innovation. NIST sought to provide a neutral forum to develop shared definitions, identify challenges, and chart actionable priorities for future research and standards development.

- **Advance U.S. manufacturing leadership:** Digital twins were recognized as critical tools for improving efficiency, innovation, and supply chain resilience.
- **Address uneven adoption:** Small and mid-sized manufacturers (SMM) face particular challenges in resources and expertise, requiring targeted support.
- **Enable trustworthy implementation:** Gaps in verification, validation, cybersecurity, and workforce readiness create uncertainty that must be resolved.
- **Foster coordinated collaboration:** NIST convened stakeholders to align research agendas, standards activities, and future collaborative actions.

Digital Twin Fundamentals and Definition

A key outcome of the workshops was establishing clarity on the definition and essential characteristics of digital twins. Participants emphasized that digital twins are more than advanced models or simulations. Rather, they are dynamic, data-driven representations of physical systems that enable continuous monitoring, analysis, and decision support.

- **Dynamic digital representations:** Digital twins differ from static models by being continuously updated through real-world data exchange.
- **Real-time decision support:** Digital twins enable predictive analytics, performance monitoring, and optimized operations (e.g., process control, maintenance).
- **Trustworthiness as foundational:** Verification, validation, and uncertainty quantification (VVUQ), and security were identified as essential requirements.
- **Alignment for future development:** Clear definitions provide the basis for advancing standards, research, and collaborative initiatives.

Workshop Overviews

Each of the three virtual workshops contributed unique perspectives and priorities, building toward a consolidated understanding of digital twin challenges and opportunities.

- **Workshop 1 – Fundamentals:** Established shared definitions, discussed motivations for adoption, and identified initial barriers.

- **Workshop 2 – Ecosystems:** Explored ecosystem components, pivotal interoperability points, and lifecycle considerations, with added focus on workforce readiness.
- **Workshop 3 – Trustworthiness:** Examined verification, validation, uncertainty quantification, and security in depth.

Technical Barriers

Persistent barriers were identified that hinder the scalability and trustworthiness of digital twins across manufacturing. These challenges span technical, organizational, and resource-related dimensions.

- **Interoperability gaps:** Fragmented data formats and proprietary approaches prevent seamless integration across systems.
- **Insufficient verification, validation, and uncertainty quantification (VVUQ) methods:** Existing VVUQ practices are not tailored for continuously updated models.
- **Cybersecurity vulnerabilities:** Broader connectivity expands the attack surface and exposes sensitive intellectual property.
- **Resource and workforce constraints:** Legacy systems and limited expertise, especially in small and mid-sized manufacturers, restrict adoption.

Research Priorities

The workshops emphasized the need for coordinated research agendas that directly address the identified barriers and support scalable adoption.

- **Interoperability research:** Develop methods for standardized data exchange and model integration across the digital twin lifecycle.
- **Verification, validation, and uncertainty quantification:** Create scalable approaches to ensure trustworthy outputs in real time.
- **Cybersecurity protections:** Adapt existing frameworks to account for federated data sharing and continuous synchronization.
- **Workforce development:** Build training, education, and competency frameworks aligned with emerging digital twin practices.

Standards Development Needs

Participants highlighted the importance of harmonizing and adapting standards and frameworks to support trustworthy and interoperable digital twins. Existing standards provide a baseline but must be coordinated and extended to address digital twin-specific requirements.

- **Standards for data exchange:** Enable consistency and portability across platforms and applications.
- **Model validation and lifecycle standards:** Address continuous updates, real-time synchronization, and lifecycle integration.

- **Cybersecurity frameworks:** Provide protections tailored to digital twins, including data sharing and Intellectual Property (IP) safeguards.
- **Sector-specific tailoring:** Adapt standards to reflect the unique requirements of domains such as additive manufacturing, supply chains, and critical infrastructure.

1. Introduction

1.1. Motivation

The manufacturing sector faces increasing complexity as companies seek to deliver higher-quality products at lower costs, while adapting to rapidly changing market conditions and global supply chains. Digital twins provide a means to address these challenges by offering dynamic digital representations of physical assets, processes, and systems. By linking models with real-time data, digital twins enable predictive insights, improved decision-making, and lifecycle optimization.

As manufacturers confront workforce shortages, resource constraints, and sustainability requirements, digital twins can help identify efficiencies, support training, and reduce waste. In doing so, digital twins support U.S. competitiveness in advanced manufacturing and strengthen resilience against disruptions.

NIST's convening role in this space reflects a national priority: establishing shared foundations for trustworthy and scalable digital twins. Workshops hosted by NIST between 2024 and 2025 brought together stakeholders from industry, academia, and government to identify opportunities, barriers, and research needs. Their insights form the foundation of this report and guide future directions for digital twin standards, research, and implementation.

1.2. Digital Twin Fundamentals

1.2.1. Overview

Digital twins represent a rapidly evolving class of technologies that integrate models with real-world data to support monitoring, prediction, and decision-making. They extend traditional modeling approaches by maintaining a dynamic connection to the systems they represent. In manufacturing, digital twins are applied across the lifecycle, from product design and simulation to operations, maintenance, and end-of-life management.

1.2.2. Defining Digital Twins

NIST defines a digital twin as "a set of virtual objects that are the digital representation, or twin, of corresponding physical entities. The digital twin maintains a two-way connection with its physical counterpart through data and models, enabling continuous synchronization." This definition emphasizes the twins' role as more than a static model, capturing their evolution with time and use. In addition, this perspective highlights that digital twins can exist at multiple scales and levels of abstraction, depending on the needs of their users.

1.3. Digital Twins in Manufacturing

Digital twins are central to the digital transformation of manufacturing. By providing a continuously updated digital representation of assets, processes, and systems, they enable improved productivity, flexibility, and resilience across the manufacturing lifecycle. Applications range from product design and process optimization to predictive maintenance and supply chain coordination.

In manufacturing environments, digital twins support the integration of diverse data streams from design tools, production equipment, sensors, and enterprise systems. This integration enables end-to-end visibility across the value chain, allowing companies to model, simulate, and optimize performance at multiple levels, from individual machines to entire facilities and supply networks. The ability to conduct “what-if” analyses and simulate outcomes before implementation reduces risk and enhances decision-making.

The adoption of digital twins in manufacturing is also advancing through sector-specific applications. Examples include equipment health monitoring, process control in additive manufacturing, and energy optimization in production systems. These applications demonstrate the potential of digital twins to increase efficiency while enabling sustainable practices such as reduced energy consumption and material waste.

At the same time, adoption remains uneven. Larger enterprises have led initial implementations, often through proprietary solutions, while SMMs face challenges related to cost, workforce skills, and interoperability. Trust and transparency also emerged as critical concerns, particularly when digital twins are deployed across organizational or sectoral boundaries. To fully realize the potential of digital twins, the manufacturing sector requires shared standards, reference Implementations, and open frameworks that enable solutions to scale across diverse organizations and supply chains.

1.4. Digital Twin Ecosystems

The value of digital twins increases when they are connected within ecosystems that span products, processes, systems, facilities, and supply chains. A digital twin ecosystem links multiple digital twins through interoperable data, models, and services, enabling collaboration across disciplines and organizations. Such ecosystems provide shared situational awareness, support decision-making at scale, and facilitate innovation by integrating perspectives from design, production, operations, and maintenance.

Digital twin ecosystems rely on open standards and frameworks to enable interoperability among heterogeneous systems. In practice, this means integrating equipment-level digital twins with process models, enterprise systems, and even broader supply chain representations. This interoperability allows stakeholders to exchange consistent data, run coordinated simulations, and align decision-making across the lifecycle. Without such integration, digital twins remain siloed and limited in impact.

The development of digital twin ecosystems also creates opportunities for shared platforms and marketplaces where models, components, and services can be exchanged. These collaborative environments enable manufacturers to access specialized capabilities without duplicating effort, while providing SMMs with entry points into advanced digital practices.

However, ecosystem-scale digital twins also raise new challenges. Concerns about data governance, intellectual property, and cybersecurity are magnified when information flows across organizational boundaries. Trust frameworks, including VVUQ, are essential to ensuring that models are reliable and that decisions based on them are defensible. Addressing these challenges requires coordinated standards development and testbeds that enable organizations to experiment with ecosystem-scale integration under realistic conditions.

1.5. Standards for Digital Twins

Standards and frameworks are critical to enabling the scalability, interoperability, and trustworthiness of digital twins. Without common foundations, implementations risk becoming fragmented, proprietary solutions that are difficult to integrate across organizations or sectors. Standards and frameworks provide consistency in definitions, data exchange, model validation, and cybersecurity practices, all of which are essential for digital twin ecosystems.

Several international and industry standards and frameworks already provide partial foundations for digital twin development. Examples include ISO 23247, digital twin framework for manufacturing, OPC-UA for interoperability, ASME V&V 40 for verification and validation, IEEE 1012 for software system verification, and NIST SP 800-53 and IEC 62443 for cybersecurity. These standards and frameworks offer critical building blocks but require extension and adaptation to address the unique challenges posed by continuously updating digital twins.

Harmonization across standards bodies is necessary to ensure coherence and avoid duplication. NIST's convening role allows alignment of work across ISO, IEC, IEEE, ASME, and other organizations. Coordinated development can ensure that standards and frameworks for data models, ontologies, cybersecurity, and VVUQ are compatible and can be implemented consistently across manufacturing ecosystems.

In addition, sector-specific standards and reference implementations are needed to ensure applicability for manufacturers of varying sizes and capabilities. Without tailored guidance, SMMs may struggle to adopt digital twin solutions, exacerbating digital divides within the sector. Developing pragmatic, scalable standards and frameworks is essential to ensuring that digital twin technologies can be adopted widely and equitably across the manufacturing landscape.

1.6. Trustworthy Digital Twins

1.6.1. Verification, Validation, and Uncertainty Quantification for Digital Twins

Establishing trust requires rigorous methods for VVUQ. These methods ensure that models and data-driven components are fit for purpose and that their outputs can be interpreted with confidence. While VVUQ practices are established in other domains, they require adaptation to continuously evolving digital twins that incorporate both real-time data streams and dynamic models.

1.6.2. Security for Digital Twins

Cybersecurity is equally critical to trust. Because digital twins integrate operational data, enterprise systems, and external connections, they create expanded attack surfaces that must be secured. Applying and extending cybersecurity standards and frameworks, including NIST SP 800-53, IEC 62443, and ISO/IEC 27001, is essential to safeguarding digital twin ecosystems against threats to confidentiality, integrity, and availability.

Trust also depends on transparency and governance. Stakeholders require clarity regarding how data is generated, managed, and shared within digital twin ecosystems. Frameworks for data provenance, intellectual property protection, and access control support responsible collaboration across organizational and sectoral boundaries. Testbeds and reference implementations provide environments for demonstrating trustworthy digital twins under realistic conditions, fostering confidence among manufacturers and partners.

2. Workshop Summaries

2.1. Workshop 1 – Digital Twin Standards for Manufacturing

2.1.1. Summary

NIST hosted the first of three virtual workshops on Digital Twins on October 30, 2024. This workshop convened technical professionals, industry leaders, and researchers from government and academia to explore the applications, challenges, and opportunities in developing digital twin standards for manufacturing. The discussions focused on aligning standards with industry needs, fostering cross-sector collaboration, and addressing interoperability, scalability, and cybersecurity.

Digital twins are emerging as transformative tools for manufacturing, with applications ranging from predictive maintenance and process optimization to supply chain management. However, their effective adoption is hindered by challenges such as a lack of standardized interfaces, high cost of custom implementations, and workforce skill gaps. Workshop participants emphasized the importance of accessible, harmonized frameworks to advance digital twin capabilities across varied manufacturing environments.

2.1.2. Key Conclusions

- **Applications of Digital Twins**
  - Current uses include predictive maintenance, supply chain monitoring, and energy optimization.
  - Aspirational applications envision product or system lifecycle management, digital product passports, and co-simulation environments for enhanced traceability and collaboration.
- **Challenges Identified**
  - Common Frameworks and Terminology: Lack of standardized frameworks and formalized terminology impedes the development of digital twins.
  - Interoperability and Standardization: Lack of common data models and communication protocols impedes integration across systems.
  - Cybersecurity Concerns: Securing sensitive data in connected ecosystems remains a priority.
  - Workforce Skill Gaps: Addressing the shortage of trained professionals to design and implement digital twin systems is critical.
  - Scalability and Cost: Expanding digital twin implementations across facilities requires significant investments.

- **Pathways Forward**
    - Collaborative efforts between government, industry, and academia are essential to accelerate the development of domain-specific and cross-domain standards.
    - Simplified frameworks and automated tools can reduce complexity, enabling broader adoption, particularly by SMMs.
    - Pilot programs and roadmaps can validate digital twin standards and foster confidence in their scalability and utility.
    - Robust cybersecurity frameworks and lifecycle management protocols are key to ensuring secure and reliable systems.

2.1.3. NIST Introduction

Simon Frechette (Systems Integration Division, NIST) welcomed participants, emphasizing the workshop's goal of exploring digital twin standards and the importance of cross-sector collaboration.

- **Workshop Objective:** Introduced use cases, challenges, and needs in digital twin technology as part of an initial series of workshops to advance manufacturing standards.
- **Broad View of Standards:** Emphasized that the workshop would consider a broad ecosystem of standards, including industry specifications, open Application Programming Interfaces (APIs), data models, and test beds.
- **Role of NIST:** Stressed that NIST does not mandate or create standards independently but collaborates with industry to support standards development where it can add value, particularly through testing.
- **Industry-Driven Standards:** Noted that standards should align with industry needs, complement proprietary solutions, and provide accessible pathways for small businesses.
- **Long-Term Vision:** Expressed a goal of developing sector-specific roadmaps and harmonizing existing standards, rather than creating entirely new ones, to facilitate digital twin adoption across manufacturing.

2.1.4. Keynote Presentation: “Digital Twin Evolution and Industrial Use”

Dan Isaacs, GM and CTO of the Digital Twin Consortium (DTC), delivered a presentation on the Digital Twin Consortium’s mission and the growing adoption of digital twins across industries. He emphasized the importance of integrating digital twins from edge-to-cloud and explored how recent advancements, including generative AI, are enhancing digital twin capabilities.

2.1.4.1. Key Points

- **Introduction to Digital Twin Consortium:** Dan Isaacs outlined the mission and growth of the DTC, focusing on collaborative industry efforts to develop and support digital twin standards.
- **Expanding Digital Twin Applications:** Emphasized the rapid adoption of digital twins across industries, driven by advancements in data management and real-time processing from edge to cloud.
- **Composable Frameworks:** Introduced the concept of a “composable framework” that allows digital twins to integrate various capabilities for multiple applications, enhancing adaptability and interoperability.
- **Impact of Generative AI:** Discussed the role of generative AI in advancing digital twin functionalities, noting its potential to improve predictive capabilities and support complex simulations in real-time.
- **Cross-Sector Harmonization:** Highlighted DTC’s efforts to unify standards and promote cross-sector alignment, emphasizing that harmonized standards are essential for wide-scale adoption.
- **Call for Real-World Collaboration:** Stressed the importance of aligning digital twin standards with practical use cases and engaging with end-users to ensure standards address real-world challenges effectively.

2.1.4.2. Discussion

- **Evolution of Digital Twin Applications:** Dan Isaacs addressed a question on the “periodic table” of digital twin applications, explaining that it’s an evolving framework that will expand as new use cases emerge.
- **Industry Collaboration and Standards Integration:** Isaacs discussed how DTC collaborates with multiple industries to align digital twin standards and ensure that they meet sector-specific needs.
- **Generative AI’s Role in Digital Twins:** Responding to questions on AI, Isaacs highlighted generative AI's potential to enhance digital twins by providing greater predictive capabilities and complex simulations.
- **Data Security and IP Concerns:** There was a discussion around data security and intellectual property, with Isaacs expressing the importance of frameworks that secure sensitive data while facilitating collaboration.
- **Future Roadmap and Pilot Programs:** Isaacs noted that DTC aims to create pilot programs and roadmaps that guide digital twin development across industries, leveraging real-world case studies to validate standards.

2.1.5. Breakout Session 1 – Identifying the Applications and Challenges of Digital Twins for Manufacturing

During Breakout Session 1, participants discussed the current and aspirational applications of digital twins in manufacturing, focusing on areas such as predictive maintenance, process optimization, and supply chain integration. Key challenges identified included interoperability, standardization needs, scalability issues, and workforce skill gaps, with a consensus on the importance of accessible, standardized frameworks to facilitate digital twin deployment across diverse manufacturing environments. There were four concurrent breakout rooms, each guided by a facilitator and supported by a note taker, and each session followed an identical structure, with the same set of questions and format across all rooms.

2.1.5.1. Major Takeaways

- **Current Uses of Digital Twins:** Participants discussed varied applications, including predictive maintenance, process optimization, and condition-based monitoring. Examples include machine monitoring, energy management, and tracking material properties across the production lifecycle.
- **Aspirational Applications:** Aspirational uses included supply chain digital twins, digital product passports for sustainability and lifecycle management, and the creation of secure environments for collaborative co-simulations across multiple parts and stakeholders.
- **Interoperability and Standardization Challenges:** There was a consensus on the need for interoperable systems and standardized frameworks to connect disparate machines and data sources, particularly in settings with diverse vendors and technologies.
- **Scalability and Accessibility Issues:** Participants cited challenges with scaling digital twin implementations across sites, driven by factors such as budget limitations, the complexity of managing data flows, and the need for enhanced cybersecurity in digital twins.
- **Workforce and Skill Gaps:** There was broad agreement on the need for a more skilled workforce to design, implement, and maintain digital twin systems effectively, highlighting the need for training and skill development to address these gaps.

2.1.5.2. Identifying Digital Twin Use Cases

Participants explored various current applications of digital twins, such as predictive maintenance and supply chain management, and discussed aspirational use cases including lifecycle management, co-simulation environments, and digital product passports to enhance sustainability and traceability.

Question 1: How are you currently using Digital Twins?

- **Predictive Maintenance:** Digital twins are widely used for predictive maintenance, enabling early fault detection and minimizing equipment downtime through real-time condition monitoring.

> ***Predictive Maintenance for Condition Monitoring:*** *Participants discussed how digital twins are used to predict machine failures before they occur, especially in predictive maintenance applications. For example, in semiconductor manufacturing, real-time simulations help track machine health, such as wear on computer numerical control (CNC) machines, and signal when maintenance is needed. This proactive approach reduces downtime and extends equipment life.*

- **Process Monitoring and Optimization:** Participants discussed digital twins' role in monitoring production processes and optimizing workflows, which helps companies enhance productivity and resource allocation.
- **Supply Chain Management:** Digital twins are employed to increase transparency in supply chains, allowing companies to track logistics, improve inventory control, and reduce inefficiencies throughout the supply chain.

> ***Supply Chain Optimization:*** *The integration of digital twins across the supply chain was highlighted as a powerful use case. For instance, digital twins are employed to monitor material flows and track product movements in real time, ensuring that manufacturers can optimize inventory levels and predict delays. This use case was particularly important in industries such as automotive manufacturing, where precise parts tracking and inventory control are critical*

- **Model-Based Process Control:** Digital twins are used in model-based control applications, such as virtual metrology and condition-based monitoring, to support precise, accurate manufacturing processes and maintain equipment health.

> ***Energy Management for Sustainability:*** *Energy management is another key area where digital twins are being applied. In manufacturing, digital twins simulate energy consumption across facilities, helping optimize heating, cooling, and production processes. For example, digital twins are used to track energy flows and reduce wastage in industries such as semiconductor fabrication and metal production, aligning with sustainability goals.*

- **Early Stages of Adoption:** Many companies are in the initial phases of digital twin adoption, experimenting with limited applications such as equipment monitoring and basic process optimization as they assess broader potential and scalability within their operations (including incorporating with existing simulation applications).

Question 2: Why are you interested in using Digital Twins?

- **Operational Efficiency and Process Optimization:** Participants expressed interest in digital twins as a means to improve operational efficiency and optimize manufacturing processes, such as through predictive maintenance and streamlined production flows.
- **Competitiveness and Innovation:** Digital twins are seen as essential tools to stay competitive, with their ability to drive innovation and help organizations adapt to evolving industry standards and customer demands.

Cross-Industry Digital Twin Integration: *Aspirational use cases also focused on creating digital twins that span multiple industries. For example, integrating digital twins for product design, manufacturing, and supply chain management could provide a comprehensive view from the design phase to final product delivery. Participants explored how these integrations could lead to better decision-making and resource optimization across industries such as aerospace, automotive, and energy.*

- **Data-Driven Decision-Making:** Attendees highlighted the value of digital twins in enabling data-driven decision-making, helping organizations make informed choices that enhance productivity and reduce risk.
- **Cost Savings and Quality Improvement:** Many participants noted that digital twins allow for cost savings and quality improvements by simulating processes and identifying issues before they arise, ultimately contributing to more reliable and adaptable manufacturing.
- **Empowering the Workforce:** There was a strong interest in using digital twins to empower the workforce, making tasks easier and enabling employees to work "smarter, not harder" through enhanced insights and automation.

Question 3: Where would you like to use Digital Twins, or where would you like to see them used?

- **Supply Chain Management:** Many participants expressed interest in using digital twins to enhance visibility and efficiency across supply chains, enabling end-to-end tracking and predictive management for more seamless logistics and inventory control.
- **Lifecycle Co-Optimization:** Attendees discussed the potential of digital twins to support lifecycle co-optimization, integrating design, manufacturing, and maintenance phases to improve product quality and lifecycle efficiency.

Digital Product Passports for Lifecycle Management: *Participants discussed the potential for digital twins to create digital product passports, which would store comprehensive lifecycle data for products, such as materials used, performance history, and maintenance records. For example, in the automotive industry, digital twins could track every part of a vehicle from production to end-of-life, enhancing sustainability and traceability.*

- **Manufacturing Process Simulation:** There was significant interest in applying digital twins to simulate and optimize manufacturing processes, with the aim of reducing waste, improving machine utilization, and enhancing process resilience.
- **Workforce Training and Virtual Commissioning:** Participants noted digital twins' potential for training and virtual commissioning, particularly as a safe environment for onboarding new equipment and training employees on complex systems.

Human-Centric Digital Twins for Workforce Support: *Participants highlighted the future potential of human-centric digital twins, which could simulate and optimize human interactions with machines. For example, in automotive manufacturing, digital twins could model worker-machine interactions to improve safety and process efficiency. Additionally, these models could be used for training purposes, enabling workers to practice complex tasks in a virtual environment before handling real machinery.*

- **Predictive Quality and Condition Monitoring:** Digital twins were identified as valuable tools for condition monitoring and predictive quality management, allowing manufacturers to detect potential defects early and ensure high-quality outcomes.

2.1.5.3. Identifying Challenges

Participants identified several key challenges to implementing digital twins in manufacturing, including interoperability across diverse systems, data accessibility and quality, workforce skill gaps, and cybersecurity for sensitive data and operations.

Question 4: What challenges or barriers are you facing with the implementation of Digital Twins?

- **Data Accessibility and Quality:** Participants noted challenges with obtaining high-quality, accessible data for digital twins, citing inconsistencies in data collection processes and difficulties in sharing data across systems and organizations.
- **Interoperability and Standardization:** The lack of universal standards and interoperability among diverse digital twin platforms was a significant barrier, making it difficult to integrate digital twins across different equipment, departments, and vendor solutions.

Interoperability Across Diverse Systems: *A major barrier discussed was the lack of interoperability standards among different digital twin platforms. For example, in a multi-vendor environment, a factory might use one vendor's digital twin for machine monitoring and another's for supply chain tracking. Without common data models and communication protocols, it becomes difficult to ensure seamless integration across these platforms, resulting in data silos and inefficiencies.*

- **Cybersecurity Concerns:** Ensuring data security and managing intellectual property were highlighted as key concerns, especially when sharing data between digital twin systems and external entities.
- **Scalability and Cost:** Scaling digital twin solutions across various applications and sites was viewed as costly and resource-intensive, with budget constraints limiting broader adoption and development.

High Costs and Scalability Issues: *Participants discussed the high initial costs of implementing digital twin systems, particularly in SMMs. For instance, the complexity of scaling digital twin systems to multiple factory locations, each with its own equipment and data systems, requires significant investment in infrastructure and technology. Furthermore, as digital twins grow in scope, managing data across multiple systems becomes a challenge without standardized protocols.*

- **Workforce and Skill Gaps:** Participants cited the need for specialized skills in digital twin technologies, emphasizing that workforce limitations and training gaps are hindering effective implementation and maintenance of digital twin systems.

Workforce Issues: *Many participants noted that there is a significant gap in the workforce's ability to design, implement, and manage digital twin systems. Specifically, the lack of training in areas such as AI, machine learning, and data science was highlighted as a barrier. For example, the automotive industry's use of digital twins to optimize manufacturing processes requires skilled data scientists who can manage real-time data feeds and machine learning algorithms, which are often in short supply.*

2.1.6. Expert Panel – Digital Twin Standards: Benefits for Manufacturing

The expert panel discussion addressed the role of digital twin standards in enhancing manufacturing efficiency, with an emphasis on interoperability, data security, and practical applications. Panelists highlighted the need for a collaborative approach across industry, government, and research institutions to develop standards that support scalable, cross-domain use of digital twins. Panelists:

- **Robert Brown,** Lab and Systems Development, Mitutoyo America Corporation
- **Antonio Kung,** Executive Board, Trialog
- **Suresh Rama,** Portfolio Development Executive, Siemens Digital Industries Software

2.1.6.1. Key Points

- **Interoperability as a Priority:** Panelists described the need for interoperability standards to connect diverse systems, emphasizing that compatibility across platforms is critical to realizing the full potential of digital twins.

- **Importance of Data Security:** There was a strong focus on data security, with discussions on encryption, IP protection, and the reluctance of some manufacturers to use cloud solutions due to confidentiality concerns.
- **Collaborative Standards Development:** The panel highlighted the need for government, industry, and research institutions to collaborate in creating standards that are flexible and aligned with industry needs, supporting both small and large enterprises.
- **Establishing a Digital Twin Roadmap:** A proposed roadmap would guide the development and application of digital twin standards, helping stakeholders understand where standards fit within digital twin workflows and aiding in harmonizing existing standards.

2.1.6.2. Discussion

Question 1: What are some of the most exciting current applications of digital twins in manufacturing that you or your organization are working on or planning to implement in the future, and what impact are they having or going to have?

- **Predictive Maintenance and Condition Monitoring:** Panelists highlighted predictive maintenance as a transformative use case, allowing for real-time condition monitoring of machinery and reducing unexpected downtime across manufacturing processes.
- **Process Optimization and Simulation:** Digital twins are being used to simulate and optimize manufacturing processes, enabling companies to test different scenarios, improve efficiency, and reduce waste before implementing changes on the factory floor.
- **Quality Control and Product Certification:** Digital twins support quality assurance in industries such as aerospace by monitoring material properties and helping meet certification standards, thus ensuring consistent quality across production.
- **Supply Chain and Lifecycle Management:** Panelists discussed the potential of digital twins in enhancing supply chain transparency and lifecycle management, which enables end-to-end tracking of products and components throughout their lifecycle.

Question 2: What are some technical details of standards that would most effectively reduce barriers to implementing digital twins at scale within manufacturing environments?

- **Interoperability and Common Language:** Standardized communication protocols and a common language for digital twin capabilities are essential to ensure seamless interoperability across diverse systems and enable effective integration in manufacturing environments.
- **Security and Data Privacy:** Robust security frameworks are necessary to protect sensitive data in digital twin systems while addressing cybersecurity risks and enabling real-time data sharing to foster trust in the technology.

- **Data Fidelity and Model Validation:** Establishing standards for data quality and validation processes is crucial to ensure the reliability and accuracy of digital twin models, providing trustworthy outputs for informed decision-making in manufacturing.
- **Scalability and Flexibility:** Standards that support the scalability and adaptability of digital twins are critical for manufacturers to expand and update their systems as new technologies and evolving requirements emerge.

2.1.6.3. Panel Audience Q/A

- **Use of Generative AI in Digital Twins:** Audience members inquired about the role of generative AI in advancing digital twin capabilities, with a focus on its potential to enhance predictive capabilities and improve decision-making by creating simulations and automating tasks within digital twins.
- **Validating Digital Twin Implementations:** A question was raised regarding the resources available for validating digital twin implementations, particularly around certifications and tools to demonstrate the effectiveness of digital twin standards in real-world applications, which the panel addressed by mentioning pilot programs and industry collaborations.
- **Challenges with Legacy Systems:** Audience members discussed the challenges posed by integrating legacy systems with digital twin technologies, with panelists suggesting an incremental approach, utilizing existing systems while layering digital twin technologies over time to reduce disruptions in operations.

2.1.7. Breakout Session 2 – Using Standards to Advance Digital Twins for Manufacturing

Breakout Session 2 focused on exploring solutions and needs to address the challenges discussed in Breakout Session 1, particularly around the use of standards to advance digital twins in manufacturing. Key discussions included the integration of various digital twins across the supply chain, the importance of cybersecurity and data flow, and the need for a clearer definition of digital twins, frameworks, and lifecycle management standards. Participants returned to the same breakout rooms as in Breakout Session 1, following the same structure and format.

2.1.7.1. Major Takeaways

- **Interoperability Requires Comprehensive Standards**: The integration of digital twins across multiple levels of manufacturing, from processes to factory-wide operations, requires domain-specific and cross-domain standards to address varied applications and complexities.
- **Simplification Enables Broader Adoption**: Simplifying the implementation of digital twins is critical to enable adoption across organizations with varying levels of technical expertise and resources.

- **Lifecycle Management Ensures Long-Term Reliability**: Establishing robust frameworks for lifecycle management, including revision tracking and validation processes, is essential to ensure the long-term reliability and consistency of digital twin systems.
- **Collaboration Accelerates Standards Development**: Collaborative efforts between government, industry, and research institutions are essential for accelerating the development of effective standards.
- **Training Bridges Workforce Gaps**: Workforce skill development and clear roles for digital twin architects are essential for ensuring organizational readiness and effective implementation.

2.1.7.2. Identifying Digital Twin Needs

Breakout Session 2 began with a discussion of the needs and solutions for addressing the challenges of implementing digital twins in manufacturing, focusing on how standards can play a critical role in driving successful adoption across the supply chain and organizational processes.

Question 1: What do you need to address the challenges from Breakout Session 1?

- **Interoperability Standards for Multi-Tier Supply Chains**: Developing interoperability standards that define consistent data models and communication protocols is critical for seamless integration of digital twins across supply chain tiers, especially for connecting process-level, equipment-level, and factory-level systems.

> ***Dynamic Data Models for Interoperability:*** *Participants emphasized the need to develop dynamic, real-time data exchange protocols that adapt to diverse manufacturing system requirements. They suggested leveraging standards for semantic interoperability, such as ontologies or JSON-LD, to ensure seamless communication across heterogeneous platforms.*

- **Automated Revision Tracking and Lifecycle Management**: Implementing frameworks for lifecycle management with automated revision tracking can enhance consistency and traceability, particularly when building upon existing digital twins or integrating them into broader systems.
- **Scalable Cybersecurity Solutions**: Addressing cybersecurity concerns through tiered security standards tailored to the abstraction levels of digital twins can protect sensitive data and ensure secure collaboration between organizations.

> ***Enhanced Cybersecurity for Digital Thread Protection:*** *Participants highlighted the importance of implementing multilayered cybersecurity frameworks to protect digital threads in connected manufacturing ecosystems. Proposed solutions included end-to-end encryption, zero-trust architecture, and intrusion detection systems tailored for operational technology (OT) environments.*

- **Dedicated Leadership Roles Drive Implementation**: Establishing digital twin leadership roles, such as a "digital twin champion," can drive organizational alignment, advocate for necessary resources, and oversee implementation efforts.
- **Fit-for-Purpose Abstraction Levels Simplify Implementation**: Creating digital twins at appropriate levels of abstraction based on specific organizational needs ensures practicality and reduces complexity during the implementation.

Automated Digital Twin Composition: *Participants called for the development of automated tools to aggregate and compose digital twins from modular components. They proposed leveraging AI and machine learning to dynamically link models, datasets, and operational inputs for scalable implementation.*

Question 2: How can Digital Twin standards help address those needs?

- **Domain-Specific Standards Address Unique Challenges**: Tailored standards for industries such as automotive, semiconductor manufacturing, and aerospace can address unique challenges by incorporating elements such as fidelity measurements, lifecycle management protocols, and interoperability guidelines.

Standardized Abstraction Layers for System Integration: *Participants advocated for standards defining abstraction layers to standardize how digital twins interface with systems at different hierarchical levels (e.g., factory, equipment, and product). They suggested these layers incorporate guidelines for API design, data buffering, and latency management to support real-time synchronization.*

- **Validation and Verification Build Confidence**: Standards defining methodologies for validation and verification (V&V) ensure the predictive accuracy and reliability of digital twins. These frameworks enable stakeholders to measure digital twin performance against predefined KPIs, fostering confidence and adoption.

Fidelity and Performance Metrics for Digital Twin Validation: *Participants proposed establishing benchmarks and metrics to evaluate the fidelity and performance of digital twins. They emphasized accuracy thresholds for real-world representation, processing efficiency metrics, and data fidelity validation protocols as key components of these standards.*

- **Universal Interfaces Enable Integration**: Establishing universal data models and interfaces facilitates integration and communication between disparate systems, ensuring that digital twins at different levels of the supply chain can operate within a cohesive framework.

- **Scalable Architectures Simplify Adoption**: Standards offering modular and scalable architectures simplify digital twin implementation, making the technology accessible to organizations of varying sizes and resources.

Lifecycle Standards for Predictive Maintenance: *Participants recommended the development of lifecycle standards for digital twins, focusing on calibration, degradation modeling, and predictive maintenance scheduling. They stressed the importance of integrating sensor-based feedback loops into these lifecycle updates.*

- **Collaboration Drives Standardization Success**: Partnerships among government, industry, and academia help create comprehensive, actionable standards that balance specificity and adaptability for broad adoption.
- **Simplifying Implementation for Small and Medium Enterprises**: Participants identified the need for lightweight, modular standards that SMMs could adopt without significant resource investments, such as scalable cybersecurity frameworks to secure digital threads while minimizing upfront complexity for SMMs.

Developing Use Cases from Existing Standards: *Participants pointed to standards such as ISO 23247 and Functional Mock-up Interface (FMI) as strong starting points for digital twin implementation. For example, ISO 23247 can be extended to include fidelity measurements and lifecycle management for manufacturing digital twins, ensuring alignment with existing machine tool standards.*

2.1.7.3. Partnering to Move Forward

The second portion of Breakout Session 2 addressed how government, industry, and research institutions can collaborate to accelerate the development and adoption of digital twin standards, with a focus on leveraging existing frameworks, fostering public-private partnerships, and aligning efforts across sectors.

Question 3: How can government, industry, and research institutions work together to accelerate the development and use of Digital Twin standards?

- **Industry-Driven Standards with Government Support:** Participants emphasized that while standards should be driven by industry needs, government support through strategic planning and funding is critical to help catalyze the development and application of these standards across sectors.
- **Collaboration Through Manufacturing Institutes:** The importance of utilizing existing platforms such as manufacturing institutes was highlighted, as they can serve as hubs for collaboration between government agencies, industry stakeholders, and research institutions to explore and develop digital twin standards in real-world contexts.

Building Trust Through Transparent Governance Models: *Participants recommended creating open-source repositories of digital twin patterns to foster trust and enable faster adoption. These repositories could incorporate examples from NIST's early involvement in MTConnect to provide real-world implementations for researchers and practitioners.*

- **Leveraging Research Institutions for Requirement Gathering:** Participants suggested that research institutions can play a vital role in gathering cross-sector requirements for digital twin standards, conducting research to identify gaps, and helping bridge the gap between theoretical frameworks and practical implementation.

Leveraging National Initiatives for Standards Development: *Collaborative efforts such as those facilitated by the DTC and CHIPS Act manufacturing institutes were highlighted as key platforms for aligning government, industry, and academia. Participants proposed using these initiatives to pilot digital twin applications such as semiconductor production and additive manufacturing.*

- **Public-Private Partnerships for Faster Standardization:** Several participants advocated for the establishment of public-private partnerships to fast-track the development of digital twin standards, citing examples such as NIST and other government-backed initiatives that can provide both technical expertise and regulatory alignment.

Public-Private Partnerships to Fund Standards Research and Development: *Participants discussed the need for funding programs such as USCAR grants to support innovative digital twin applications. Specific suggestions included government-backed consortia to pilot interoperability frameworks in areas such as aerospace component tracking and end-of-life recycling programs.*

- **Government Funding for Academia and Research:** It was noted that funding from government agencies is crucial to support academic research and the development of digital twin standards, ensuring that research institutions have the resources needed to contribute to the evolution of these standards.

Pilot Programs for Cross-Disciplinary Applications: *Participants suggested creating demonstration projects that combine digital twin standards with other technologies such as AI and IoT. One example discussed was integrating MTConnect with AI-driven predictive maintenance systems in smart factories to validate data interoperability and scalability across diverse manufacturing environments.*

- **Smaller Collaborative Groups to Overcome Bureaucracy:** Participants pointed out that smaller, focused working groups across government, industry, and academia are more effective for driving progress on digital twin standards than larger, more bureaucratic interagency groups, as they allow for more agility and faster decision-making.

2.1.8. Challenges and Opportunities

Digital twin adoption in manufacturing faces both challenges and opportunities, as highlighted in Workshop 1. Participants identified barriers such as the lack of common data standards, fragmented approaches to implementation, and the high cost of deployment for SMMs. Concerns were also raised about workforce readiness and the difficulty of integrating digital twins with legacy systems.

At the same time, Workshop 1 highlighted significant opportunities. Digital twins can enhance decision-making through predictive insights, enable more efficient use of resources, and support innovation across product lifecycles. Standardized approaches and collaborative platforms were seen as critical enablers for scaling adoption, while testbeds and pilot programs could demonstrate value and reduce perceived risks.

2.2. Workshop 2 – Digital Twin Ecosystems

2.2.1. Summary

NIST hosted the second of three virtual workshops on Digital Twins on January 14, 2025. This workshop convened technical professionals, industry leaders, and policymakers to explore key components of digital twin ecosystems, pivotal points of interoperability, and lifecycle considerations. The discussions focused on essential digital twin development, implementation, and lifecycle management. Participants explored how standards, frameworks, and emerging technologies can improve the scalability, trustworthiness, and interoperability of digital twins.

The event featured a keynote presentation, an expert panel discussion, and breakout sessions that addressed critical challenges and potential solutions in the digital twin landscape. Discussions emphasized the role of data governance, industry standards, human-system integration, and lifecycle sustainability in ensuring that digital twins remain effective and adaptable over time.

2.2.2. Key Conclusions

- **Advancing Digital Twin Ecosystems for Scalable Integration**
    - Defining Core Components: Digital twins rely on physical assets, virtual models, and structured data frameworks to drive real-time decision-making and operational insights.
    - Enabling Interoperability: Standardized frameworks, such as OPC-UA, ISO 23247, and ISA 95, are critical for ensuring cross-domain compatibility and scalable implementations.
    - Leveraging Digital Threads: Digital threads ensure traceability, consistency, and synchronization across the product lifecycle.

- **Overcoming Interoperability Challenges Through Standardization**
  - Need for Unified Data Exchange Protocols: Proprietary systems, fragmented standards, and inconsistent data models remain barriers to seamless interoperability.
  - Refining Existing Standards: Frameworks such as MIL-STD-3022, ASME Y14.41, and MTConnect provide foundations for digital twin integration but require enhancements for broader industry adoption.
  - Addressing Security and Data Governance Gaps: To ensure trustworthiness, digital twin ecosystems must implement stronger metadata management, cybersecurity frameworks, and verification mechanisms.
- **Ensuring Long-Term Digital Twin Sustainability**
  - Lifecycle Planning and Version Control: Organizations must implement regular updates, modular design approaches, and versioning strategies to maintain digital twin relevance over time.
  - Enterprise-Wide Asset Management: Treating digital twins as enterprise assets requires well-defined maintenance, calibration, and documentation strategies for long-term usability.
  - Lifecycle-Specific Standardization Needs: To support sustainable digital twin lifecycles, new standards should focus on data governance, decommissioning processes, and evolving technology integration.

2.2.3. NIST Introduction

Simon Frechette, representing NIST's Systems Integration Division, emphasized the importance of developing a shared understanding of digital twin ecosystems, identifying key interoperability challenges, and advancing discussions toward a strategic roadmap for digital twin standards in manufacturing.

- **Understanding Digital Twin Ecosystems:** Digital twin ecosystems consist of integrated networks of technologies, tools, applications, standards, and services that enable the design, operation, and sustainment of digital twins across industries.
- **Identifying Major Components:** Core elements of digital twin ecosystems include physical assets, virtual representations, resources, and key stakeholders, each playing a role in data-driven decision-making and interoperability.
- **Addressing Interoperability Through Standards:** Formal standards such as ISO 23247, open APIs, and reference implementations are essential for ensuring seamless integration and cross-platform functionality.
- **The Role of NIST:** NIST facilitates digital twin standardization, supporting research, industry collaboration, and cross-sector alignment rather than mandating specific frameworks.

- **Workshop Scope and Next Steps:** The workshop is intended to expand discussions beyond discrete manufacturing, contribute to a formal summary report, and set the stage for future sessions on digital twin trust and security.

2.2.4. Keynote Presentation: "An Exploration of the Digital Twin Ecosystem"

Greg Porter, Principal Solutions Architect at Sev1Tech, delivered a keynote presentation titled "*An Exploration of the Digital Twin Ecosystem.*" He emphasized that digital twins are fundamentally built on data, with their effectiveness depending on the integration of real-time and historical data. Porter explored the interplay between digital twins, digital threads, Model-Based Systems Engineering (MBSE), and Multi-Agent Generative Systems (MAGS) to illustrate how these frameworks create more robust and adaptable digital ecosystems. He also highlighted interoperability, compliance, and scalability challenges that organizations must address when implementing digital twin solutions.

2.2.4.1. Key Points

- **Digital Twins as Data-Driven Systems:** A digital twin is an integrated, virtual representation of real-world entities and processes, built on synchronized, bidirectional data interactions to drive decision-making.
- **The Role of the Digital Thread:** A digital thread provides a trustworthy and interconnected information system that links multiple dimensions, ensuring data consistency across an asset's lifecycle.
- **MBSE Enhances Digital Twin Precision:** MBSE formalizes modeling for system design, analysis, and verification, improving consistency, traceability, and cross-discipline integration.
- **MAGS Improvements:** MAGS are AI-driven systems that employ multiple intelligent agents to enhance digital twin adaptability, enabling autonomous decision-making and automated simulations.
- **Cybersecurity and Compliance Considerations:** Digital twins handle sensitive real-world data, requiring organizations to implement data security frameworks, access controls, and continuous monitoring to ensure compliance with NIST 800-171, NIST 800-53, ISO/IEC 27001, HIPAA, IEC 62443, and FERPA standards. For digital twin implementations, key considerations include data protection, access management, supply chain security, continuous monitoring, and deployment location.
- **Challenges for Implementation:** Customers face several challenges in implementing and deploying digital twins, including gaps in skills and knowledge, data complexity, real-time data processing, interoperability issues, security concerns, scalability, high costs, complex implementation processes, and integration with legacy systems.

2.2.4.2. Discussion

During the Q&A session, participants raised key questions about data trustworthiness, interoperability, and workforce challenges associated with digital twin adoption. Porter's responses emphasized the need for rigorous data validation, industry-wide education efforts, and practical strategies to scale digital twin solutions.

- **Ensuring Data Trustworthiness:** When integrating data into a digital twin, “garbage in, garbage out” remains a critical issue. Organizations must invest in data validation processes to ensure accuracy and reliability.
- **Challenges of Interoperability Between Digital Twins:** Trusting external supplier digital twins is difficult because their capabilities and data integrity are often unknown, making interoperability a persistent challenge.
- **Bridging the Digital Twin Knowledge Gap:** Many companies lack the expertise to implement digital twins, highlighting the need for education initiatives at universities, high schools, and middle schools to cultivate a knowledgeable workforce.
- **Leveraging Generative AI for Digital Twin Implementation:** Porter explained that MAGS-powered AI solutions can guide users through digital twin implementation, streamlining adoption for companies unfamiliar with the technology.
- **Adapting Legacy Infrastructure to Digital Twins:** Companies with older facilities are gradually upgrading to 5G networks and sensor-driven operations, allowing for progressive integration of digital twins into existing manufacturing environments.

2.2.5. Expert Panel – Digital Twin Ecosystem Examples

The expert panel discussion explored real-world applications of digital twins in manufacturing, demonstrating how data integration, AI-driven optimization, and system modeling are transforming industries. Panelists shared insights on convergence between physics-based and AI-driven models, optimizing semiconductor fabrication, and lifecycle-based digital twins. The discussion highlighted the need for seamless interoperability, the role of generative AI in decision-making, and strategies for integrating digital twins across complex systems. Panelists:

- **Rocco Cappiello,** Vice President, Business Development, Altair
- **Dr. Keyhoon Ko,** CEO and President, VMS Global
- **Vítor Lopes Pereira,** Regional Sales Manager, Systems & Digital Twins, Ansys
- **Dr. Gan Wang,** Vice President, Systems Engineering Ecosystem, Dassault Systèmes

2.2.5.1. Key Points

- **Convergence of Simulation, AI, and High-Performance Computing (HPC):** Digital twins benefit from integrating physics-based simulations, AI-driven data analytics, and HPC, enabling faster design iterations and optimized manufacturing processes.
- **Autonomous Digital Twin Platforms:** Digital twin ecosystems in semiconductor manufacturing include production capacity, resource layout, material handling design, and production optimization. This platform combines production optimization, factory layout modeling, and real-time decision-making to drive more autonomous, self-optimizing industrial operations.
- **Hybrid Digital Twin Approaches:** The next generation of digital twins leverages physics-based models and real-world sensor data, allowing for adaptive, high-fidelity simulations that improve accuracy over time.
- **Digital Twin Lifecycle Integration:** Digital twins extend beyond monitoring and simulation by incorporating continuous feedback loops. This ensures that models evolve with real-world system performance to enhance long-term decision-making. Their lifecycle consists of inventing, running, learning, and improving.
- **Overcoming Integration Barriers:** Bridging interoperability gaps between different vendors, legacy systems, and evolving standards, requiring harmonization of data formats and platform architectures, is a significant challenge.

2.2.5.2. Discussion

During the Q&A session, panelists addressed challenges related to standardization, trust in digital twin data, and the evolving role of AI in decision-making. The discussion emphasized the need for greater collaboration between industries, research institutions, and regulatory bodies to refine best practices for digital twin adoption.

- **Standardization and the Mapping Challenge:** Panelists highlighted the need to map existing digital twin standards across different industries, using established protocols where possible rather than reinventing new ones.
- **Trust and Verification of Supplier Digital Twins:** Companies struggle to verify the accuracy and capabilities of supplier-provided digital twins, making it difficult to integrate external models into existing workflows.
- **The Role of Generative AI in Digital Twin Adoption:** AI-driven solutions, such as MAGS, can assist users by automating digital twin setup and streamlining complex decision-making. They can also build connection layers in the digital twin context.
- **Balancing Customization and Interoperability:** Organizations must decide between highly customized digital twin solutions that fit specific needs and more standardized platforms that ensure interoperability across multiple systems.

- **Industry Collaboration to Address Complexity:** Given the multidisciplinary nature of digital twins, cross-industry collaboration is essential for developing scalable, flexible, and domain-specific best practices.

2.2.6. Breakout Session – Digital Twin Ecosystem Components and Interoperability

The breakout session allowed participants to collaboratively explore key components, challenges, and lifecycle considerations of digital twin ecosystems. The session focused on defining essential digital twin ecosystem components, addressing integration challenges, and considering long-term sustainability and lifecycle factors. Discussions highlighted the complexity of digital twin implementations across industries, emphasizing the need for structured governance models, standardization efforts, and scalable architectures to support data-driven decision-making. There were four concurrent breakout rooms, each guided by a facilitator and supported by a notetaker. Each session followed an identical structure, with the same questions and format across all rooms.

2.2.6.1. Major Takeaways

- **Interoperability Remains a Primary Challenge for Digital Twin Ecosystems:** A lack of standard data formats, communication protocols, and integration frameworks hinders seamless interoperability between digital twin systems, particularly across different industries and vendors.
- **A Standardized Digital Twin Marketplace Could Accelerate Adoption:** Participants highlighted the need for a marketplace of digital twin models and services, enabling plug-and-play tools, third-party validation, and certified components to improve compatibility and adoption.
- **Data Governance and Metadata Standardization Are Critical Needs:** The importance of metadata in digital twin evolution was emphasized, with calls for more structured data governance policies to ensure data consistency, security, and traceability over time.
- **Legacy System Integration and Lifecycle Management Require More Focus:** Many organizations struggle with incorporating digital twins into existing legacy systems, highlighting the need for strong documentation, lifecycle planning, and frameworks for managing digital twins over long operational periods.
- **Cross-Industry Collaboration Is Essential for Advancing Standards:** Participants stressed the importance of aligning digital twin standards with domain-specific expertise, ensuring that industry-led collaborations define practical guidelines for implementation, optimization, and validation.

2.2.6.2. Digital Twin Ecosystem Components

The first portion of the breakout discussions focused on digital twin ecosystem components, exploring the core elements, integration challenges, and standardization gaps within digital twin systems. Discussions emphasized the need for interoperability between physical assets, virtual models, and data frameworks, while addressing barriers such as proprietary systems, inconsistent standards, and legacy infrastructure constraints. Participants also highlighted gaps in metadata governance, semantic modeling, and security protocols, reinforcing the need for improved frameworks to support scalability and cross-industry adoption.

*Participants emphasized that a **robust digital twin ecosystem** must be built on **structured, interoperable, and secure data frameworks** to ensure reliable decision-making. A key challenge discussed was the **integration of data sources, including sensor networks, simulation models, and AI-driven analytics**, particularly when incorporating **legacy equipment and proprietary platforms**. To address these challenges, participants suggested **the adoption of standardized data formats, clear metadata governance, and scalable architectures** that support **modular system design**. Ensuring **cross-platform compatibility** requires leveraging **open communication protocols, such as OPC-UA and MTConnect**, allowing digital twins to function **seamlessly across different manufacturing and industrial environments**.*

Defining Components: What are the essential components of a robust digital twin ecosystem?

- **Data as the Foundation:** A digital twin ecosystem requires comprehensive data capabilities, including storage, transfer, validation, and interoperability via standardized APIs and data formats.
- **Physical Asset Representation:** Digital twins must accurately extract and model relevant aspects of the physical world, ensuring clear boundaries and fidelity between physical and virtual representations.
- **Purpose-Driven Design:** Digital twins should be developed with clear business objectives, considering specific industry applications, economic feasibility, and long-term value generation.
- **Human Interaction and Decision Support:** Digital twins should facilitate effective human interaction, incorporating decision-support systems, visualization tools, and intuitive user interfaces tailored to industry needs.
- **Frameworks for Interoperability and Security:** System architectures should define clear boundaries, cybersecurity mechanisms, data sharing and trustworthiness mechanisms, and infrastructure requirements, ensuring seamless integration and protection against cyber threats.

Integration Challenges: What are the primary challenges in integrating digital twin elements (e.g., physical assets, sensor data, cyber-physical systems, other digital twins) within a broader ecosystem?

- **Lack of Standardization in Sensors and IoT Devices:** Digital twin implementations suffer from inconsistent sensor specifications, calibration, and compatibility, proprietary vendor formats, and limited interoperability, complicating data exchange across systems.
- **Challenges in Incorporating Human Expertise:** Integrating human decision-making, domain knowledge, and subject matter expertise into digital twin systems remains difficult due to the limited standardization of qualitative and quantitative data.
- **Modeling and Simulation Constraints:** Many digital twin ecosystems lack robust environmental modeling, leading to incomplete representations of real-world conditions and difficulties in cross-disciplinary model integration.
- **Data Synchronization and Validation Issues:** Ensuring data accuracy, synchronization across systems, and validation mechanisms poses significant hurdles, particularly in real-time industrial applications where data sensitivity and timing are critical.
- **Network and Architecture Challenges:** Digital twin architectures face connectivity constraints, cybersecurity concerns, compatibility issues with legacy systems, and challenges with latency and throughput, making it difficult to establish reliable and secure data-sharing environments.

Where are the major gaps in existing standards that hinder digital twin adoption?

- **Human-System Integration Standards are Lacking:** Current frameworks do not adequately address the integration of human expertise, decision-making, and manual overrides within digital twin environments, necessitating new standards to formalize human roles and interactions.
- **Cross-Industry Interoperability Remains a Challenge:** While ISO 23247, OPC-UA, and MTConnect provide foundational guidelines, harmonization between different industries remains limited, requiring efforts to bridge domain-specific variations.
- **Data Exchange Protocols Lack Real-Time Synchronization:** Standards for data transmission, synchronization, and latency control between physical and digital twins are underdeveloped, limiting seamless integration across distributed systems.
- **Cybersecurity and Validation Frameworks are Incomplete:** Existing security standards do not fully address the risks of real-time digital twin data exchanges, necessitating stronger verification mechanisms, encryption models, and access controls.
- **Standardized Abstraction for Model Portability is Needed:** Many digital twin frameworks lack standardized methods for capturing, abstracting, and sharing simulation models, making it difficult to reuse or transfer models across industries and platforms.

2.2.6.3. Pivotal Points of Interoperability

The second breakout portion focused on pivotal interoperability points, examining critical areas where digital twin ecosystems require seamless data exchange, standardized communication, and cross-domain integration. Discussions focused on identifying key interoperability barriers, leveraging existing frameworks to bridge gaps, and defining the role of industry collaboration in fostering interoperability solutions. Participants emphasized that without robust interoperability frameworks, digital twins remain siloed and lack the scalability needed for widespread industry adoption.

*Interoperability remains a **critical enabler for digital twin scalability**, yet participants noted that **data inconsistencies, proprietary software constraints, and misaligned industry standards** continue to limit widespread adoption. Discussions highlighted that **fragmented sensor protocols, inconsistent simulation methodologies, and a lack of unified data exchange mechanisms** prevent seamless collaboration across **enterprise IT and real-time OT systems**. To overcome these barriers, participants emphasized the importance of **leveraging existing interoperability frameworks**, such as **ISO 23247 for manufacturing digital twins, ASME Y14.41 for model-based definitions, and OPC-UA for machine-to-machine communication**. Additionally, participants suggested that **federated architectures and open APIs** could enhance **cross-vendor and cross-industry data exchange**, ensuring that **digital twins remain adaptable and scalable across evolving technology landscapes**.*

What are the most significant barriers to achieving interoperability in digital twin ecosystems?

- **Disparate Communication Protocols Hinder Data Exchange:** Digital twins rely on various communication standards (e.g., OPC-UA, MQTT, MTConnect), but industry fragmentation prevents seamless data sharing and requires standardized interface mappings.
- **Misalignment Between IT and OT Systems:** Many digital twin architectures face challenges due to incompatibilities between Information Technology (IT) and Operational Technology (OT) systems, necessitating middleware solutions and cross-domain data synchronization. Synchronization time and requirements impact interoperability, and the absence of a central clock for synchronized data poses significant challenges.
- **Varying Levels of Model Fidelity Create Integration Challenges:** Different industries use varied levels of model fidelity (high-fidelity physics models vs. data-driven AI models), requiring interoperability mechanisms that support hybrid models and scalable accuracy adjustments.
- **Interoperability Between Digital Twin Platforms is Limited:** Proprietary software ecosystems and vendor-specific implementations create barriers to integrating digital twins across platforms, highlighting the need for open standards and plug-and-play frameworks.

- **Lack of Standardized Digital Twin Identity and Metadata Models:** There is no universal framework for assigning digital twin identities, metadata structures, and versioning protocols, making it difficult to maintain consistent data lineage across different platforms and stakeholders. Establishing a common ontology/language and understanding digital twin systems is crucial for overcoming standardization challenges.
- **Integration with Legacy Systems:** Digital twin ecosystems face significant barriers when integrating with systems of legacy equipment due to vendor and equipment differences, proprietary platforms, and the need for various data standards and streams. This requires substantial time, cost, and labor to achieve standardized interoperability.

Which existing standards or frameworks do you rely on to ensure interoperability in your digital twin ecosystem, and where do you see opportunities for new standards to improve cross-vendor or cross-industry systems?

- **A Wide Range of Standards Support Digital Twin Interoperability:** Existing frameworks such as ISO 23247 (digital twin framework for manufacturing), ISA 95 (enterprise-to-manufacturing system integration), ASME Y14.41 (digital definition), OPC-UA (machine communication), and IEC standards for industrial control systems provide essential building blocks, but harmonization across industries remains a challenge.
- **Industrial IoT and Sensor Integration Require Broader Standardization:** While wireless sensor networks (802.15), MQTT (data transport), MTConnect (device-agnostic data reporting), and Industrial IoT communication standards facilitate connectivity, expanded standards covering multi-sensor data fusion and real-time synchronization are needed.
- **Ontology and Data Structures Must be More Universally Defined:** Existing standards such as ISO 13399 (cutting tool information), STEP (information transfer), and JSON (data structure) offer applicable models, but a common semantic interoperability framework is needed to define relationships between digital twin components. Additionally, standards such as ASME Y14.41 for digital product definition and communication standards such as MT-Connect ensure device-agnostic data representation.
- **Containerization and Edge Computing Need Standardization:** New standards are needed to define containerization technologies for digital twins, ensuring consistent deployment, system portability, and interoperability between edge-native and cloud-based solutions.
- **Third-Party Validation and Open APIs Can Improve Adoption:** To increase trust and usability, digital twin standards should incorporate third-party verification mechanisms for implementation validation and call for open APIs that allow cross-platform model integration and reuse.
- **Message Brokers Facilitate Data Transport:** Standards for message brokers such as Kafka for extensive streaming data (distributed) and ZeroMQ (ZMQ) for low latency are crucial for data transport and synchronization.

Can you share examples of where standards played a key role in resolving interoperability issues or where their absence caused setbacks?

- **Smart City Digital Twin Standards Address Interoperability Challenges:** Existing smart city research and sustainability initiatives have leveraged standardized frameworks to enhance data integration, whereas the lack of standards in supply chain digital twins has led to unreliable results and incomplete datasets, highlighting the need for governing standards across digital twin ecosystems.
- **Plug-and-Play Capabilities Enable Model Reusability:** Standardized plug-and-play frameworks are critical for reusing models across different industrial contexts, such as cutting tool data exchange, ensuring that digital twin components can be easily shared and integrated across platforms.
- **Budget Constraints and Lack of Oversight Undermine Standardization:** In some cases, IT teams have bypassed standards due to budget limitations and inadequate oversight, leading to improper implementations; however, certified and verified "off-the-shelf" solutions, such as Robotics Operating System (ROS) for automation and AP242 for geometry representation, have successfully resolved interoperability challenges.
- **Simulation Model Exchange Benefits from Standardized Protocols:** When integrating models across different simulation environments, industries have leveraged FMI/FMU standards to facilitate model exchange, ensuring compatibility between various system simulation tools.
- **Interoperability Gaps Limit AI Potential in Digital Twins:** AI-driven digital twins struggle with inconsistent data formats and a lack of structured interoperability, forcing companies to rely on inefficient alternatives such as unstructured data management (e.g., LMS-based solutions). This reinforces the need for AI-specific digital twin standards.
-

2.2.6.4. Digital Twin Lifecycle Considerations

The third and final portion of the breakout session focused on digital twin lifecycle considerations, examining digital twins' long-term sustainability, adaptability, and governance throughout their operational lifespan. Discussions highlighted that digital twins must evolve alongside their physical counterparts, requiring regular updates, validation mechanisms, and security measures to maintain reliability. Participants emphasized the importance of lifecycle frameworks that consider the continuous refinement of digital twins, including version control, model retraining, and the impact of emerging technologies such as AI-driven automation and edge computing. Additionally, the session demonstrated the need for lifecycle-specific standards that define digital twin longevity, interoperability over time, and best practices for ensuring trustworthiness across industries.

*Participants emphasized that **digital twin lifecycle management must account for continuous updates, validation protocols, and long-term governance strategies** to prevent models from becoming obsolete. A recurring theme was the need for **lifecycle-specific version control, calibration procedures, and predictive analytics** to ensure that digital twins remain aligned with their physical counterparts. Several participants highlighted that **AI-driven automation and real-time data synchronization** can improve **the adaptability of digital twins**, but also raise concerns regarding **data security and validation processes**. To mitigate risks, participants suggested the **implementation of cybersecurity standards and frameworks, such as NIST 800-171 and ISO/IEC 27001, along with structured governance models** that define **data ownership, system interoperability, and the longevity of digital twin models**.*

What unique considerations should be addressed at each stage of the digital twin lifecycle: development, deployment, operation, and decommissioning?

- **Development Must Align with the Product Lifecycle:** Digital twin development should be flexible and adaptable, avoiding monolithic simulations and ensuring that verification, validation, and testing processes confirm data integrity and accuracy throughout development. Comprehensive requirements are needed during the conceptualization/pre-design stage. Cybersecurity, data security, and data quality must be prioritized alongside the creation of a common ontology and data dictionary.
- **Deployment Requires Verification, Validation, and User Engagement:** Digital twins must undergo rigorous verification and validation during deployment, involving AI and human oversight, while ensuring user engagement and buy-in to maximize adoption and effectiveness. Addressing legacy systems issues and conducting pilot testing are critical steps. System ramp-up considerations, such as the deployment rate, should be addressed, and training for all elements, including tools and workforce, is key.
- **Operation Relies on Continuous Monitoring and Maintenance:** Digital twins require ongoing validation, performance tracking using confidence intervals, and traceability of lifecycle changes, alongside routine calibration and domain-specific analytics to ensure long-term reliability.
- **Decommissioning Should Support Recursive and Future Use:** Digital twins should be archived for future reuse, while ensuring that digital decommissioning does not negatively impact physical assets, leveraging digital fingerprints for equipment replacement and documentation for quality management. Establishing nominal thresholds to determine when a digital twin no longer represents real conditions is crucial.
- **Cross-Lifecycle Data Traceability is Essential:** A structured digital thread should be established across all lifecycle stages, ensuring seamless data access, analysis, and query capabilities. This will allow organizations to extract valuable insights and optimize future implementations.

How can digital twins remain relevant and effective over time, especially in fast-evolving technological and market environments?

- **Clearly Defined Capabilities Improve Digital Twin Functionality:** Each digital twin should have a well-defined set of capabilities, such as data visualization, human modeling, or behavioral simulation, ensuring its purpose and applications remain aligned with evolving industry needs.
- **Ongoing Maintenance, Calibration, and Updates Ensure Longevity:** Digital twins should be treated as enterprise assets, requiring periodic reviews, cybersecurity updates, and modular design approaches to ensure backward compatibility and effective adaptation over time. Traceability is also essential to understand the reasons and rationale behind any changes.
- **Modular Architectures Help Digital Twins Keep Pace with Technological Changes:** A modular design approach allows incremental updates, component upgrades, and file format adaptability, while maintaining interoperability, compliance with evolving standards, and cost-effective sustainment strategies.
- **Interoperability and Information Transfer Enhance Long-Term Usability:** Digital twins should support seamless information transfer between legacy and next-generation models, ensuring that metadata, design principles, and operational insights remain accessible despite workforce changes or system transitions.
- **Agnostic and Adaptable Digital Twins Improve Scalability:** Future-proofing digital twins requires granular, changeable services that rely on metadata-driven modeling rather than static, code-dependent structures. This allows for flexibility across different platforms and industries. The core of the digital twin needs to be technology-agnostic to ensure it can be adapted and modified as the technological landscape evolves.

What standards or guidelines are you using to manage digital twins throughout their lifecycle, and are there specific points where a lack of standards or best practices is hindering progress?

- **Existing Standards Provide a Foundation for Modeling and Security:** Standards such as MIL-STD-3022 for modeling and simulation, A-Spice in the automotive sector, and various cybersecurity guidelines help ensure data integrity, security, and structured digital twin management.
- **Greater Standardization is Needed in the Development Stage:** The lack of consistent standards for digital twin development creates fragmentation across industries, highlighting the need for more structured frameworks for initial design, integration, and long-term usability.
- **Metadata and Governance Standards Need Improvement:** Data governance, metadata definitions, and lifecycle documentation remain underdeveloped, making it difficult to track changes, optimize performance, and ensure digital twin accuracy over time.

- **Maturity Models and Lifecycle Optimization Standards Must Be Addressed:** There is a lack of defined best practices for maintaining digital twins over their full lifecycle, requiring maturity models, optimization guidelines, and reusable component frameworks to support long-term sustainability and interoperability.

2.2.7. Challenges and Opportunities

Workshop 2 reinforced that while progress is being made in digital twin implementation, several systemic challenges remain. Interoperability remains a barrier, as proprietary solutions limit integration and data sharing. Participants emphasized the lack of reference frameworks for applying digital twin standards and noted that workforce skills remain unevenly distributed across the manufacturing sector. Trustworthiness was also identified as a critical issue, particularly regarding data governance and cybersecurity.

Opportunities identified in Workshop 2 included expanding collaborative testbeds to accelerate standards adoption, developing shared infrastructure to reduce costs for smaller manufacturers, and leveraging existing standards efforts as building blocks. Participants also pointed to the potential of digital twins to strengthen supply chain resilience, optimize operations, and drive sector-wide innovation.

2.3. Workshop 3 – Digital Twin Trust, Verification, and Security

2.3.1. Summary

NIST hosted the third of three virtual workshops on Digital Twins on May 27 and 28, 2025. This workshop brought together experts from industry, academia, and government to explore critical enablers of trust in digital twin systems. Building on themes from the first two workshops (e.g., definitions, architectures, and interoperability), this event focused on the attributes and mechanisms that support trustworthy digital twin behaviors across a system's lifecycle.

The workshop addressed three primary themes: (1) defining trustworthiness in digital twins, (2) applying verification, validation, and uncertainty quantification (VVUQ) methods to establish and maintain trust, and (3) identifying cybersecurity challenges and trust artifacts necessary for secure and reliable digital twin deployments. Through plenary presentations and four concurrent breakout sessions, participants discussed how these concepts intersect with existing standards, engineering practices, and the evolving digital twin ecosystem.

2.3.2. Key Conclusions

- Evolving Definitions of Trust in Digital Twin Ecosystems
    - Contextual Trust Requirements: Trust is dependent on the digital twin's purpose, operational environment, and lifecycle stage. Different levels of assurance, fidelity, and responsiveness are required depending on whether the digital twin

supports early-stage design, ongoing operations, or safety-critical decision-making.

  - Transparency as a Trust Enabler: Stakeholders need visibility into model assumptions, data inputs, processing logic, and validation history to understand and verify digital twin behavior. Reproducibility, traceability, and explainability are core enablers of trust across sectors and use cases.
  - Dynamic Trust Over Time: Digital twins must support evolving trust requirements as system conditions, use cases, and stakeholder needs change. Trust cannot be static; it must adapt with updates to data, models, and operating environments.
- Security Challenges at the Intersection of IT, OT, and Engineering
  - Organizational Misalignment: Divided responsibilities between IT, OT, cybersecurity, and modeling teams create accountability gaps and hinder risk management. These silos result in inconsistent implementation of security controls and delay the identification and resolution of vulnerabilities.
  - Expanded Threat Landscape: Increasing interconnection among digital twins introduces complex vulnerabilities, including third-party exposure and systemic trust dependencies. A compromise in one subsystem can cascade across integrated platforms, amplifying operational risk.
  - Need for Integrated Governance: Addressing security challenges requires coordinated processes across technical and organizational boundaries from design through operation. Effective governance must align policies, validation practices, and ownership of risk across all involved teams.
- Verification, Validation, and Calibration as Trust Enablers
  - Data-Aligned Validation Practices: Trustworthy digital twins rely on testable models grounded in time-synchronized, high-integrity data from physical systems. Validation must be iterative and reflect real-world operating conditions to confirm accuracy over time.
  - Rigorous Calibration Protocols: Effective calibration depends on understanding data quality, model assumptions, and performance boundaries across operational conditions. Calibration also requires clearly defined metrics and procedures to ensure consistency across use cases.
  - Documentation to Support Reuse: Validation artifacts such as test reports, simulation logs, and documented assumptions are essential for transparency, auditing, and stakeholder confidence. These records allow downstream users to assess model credibility without repeating the whole validation process.
- Adapting and Extending Standards for Digital Twin Trustworthiness

- Leveraging Existing Frameworks: Standards and guidelines such as NIST SP 800-53, ISO/IEC 27001, ASME V&V 40, and IEEE 1012 offer starting points for security and validation of digital twins. These frameworks provide structured approaches to risk management, model verification, and information assurance.
- Addressing Digital Twin Complexity: These frameworks require adaptation to account for real-time operation, multi-system control, and cyber-physical integration. Digital twins demand additional considerations such as live data synchronization, dynamic model evolution, and distributed ownership.
- Sector-Specific Alignment: Standards such as STEP (AP242) for product data exchange, Management of Change Plus by DNV for digital model lifecycle control, IEC 62443 for system protection, and Decentralized Identifiers and Verifiable Credentials by the World Wide Web Consortium for digital product passports provide domain-specific mechanisms to manage risk, traceability, and lifecycle assurance. These frameworks support trust strategies tailored to the operational realities of manufacturing, critical infrastructure, and other sectors where interoperability and system transparency are essential.

2.3.3. NIST Introduction

Simon Frechette, representing NIST's Systems Integration Division, framed the workshop by emphasizing the importance of trust in digital twin systems, highlighting the need for cross-sector collaboration to address measurement science challenges, interoperability, and validation in increasingly complex cyber-physical environments.

- **Clarifying Digital Twin Trust:** Define the essential attributes of trust in digital twins and examine how verification and validation (V&V) practices contribute to establishing and maintaining that trust.
- **Assessing and Sustaining Trustworthiness:** Explore practical methods for evaluating digital twin trustworthiness throughout the system lifecycle, including model verification and validation, performance benchmarking, and data integrity.
- **Framing Cross-Sector Challenges:** Address the complex, interdisciplinary nature of digital twin systems, including the convergence of IT, OT, modeling, and security considerations that impact trust and adoption.
- **The Role of NIST:** Support the development of trustworthy digital twin ecosystems by advancing measurement science, fostering standards development, and facilitating collaboration across government, industry, and academia.
- **Workshop Scope and Path Forward:** Gather expert insights to inform future guidance, identify research priorities, and build momentum toward a shared framework for digital twin trust.

2.3.4. Day 1 Keynote Presentation: “Verification, Validation, and Uncertainty Quantification (VVUQ) to Enable Trustworthy Digital Twins”

Sankaran Mahadevan, a professor at Vanderbilt University, delivered a keynote presentation regarding VVUQ as an enabler of trust.

2.3.4.1. Key Points

- **Digital Twin Maturity Requires a Foundation of Trust:** Establishing trust in digital twins is a prerequisite for maturity and must be built through both technical rigor and organizational alignment. Trust is not static, as it develops through sustained use, feedback, and verification and validation over time.
- **Trust Must Account for Technical, Human, and Policy Complexity:** Digital twin trustworthiness is shaped by a mix of challenges, including model limitations, changing data environments, the interpretability of outputs, and evolving regulatory expectations. Effective solutions must bridge technical systems with user and societal needs.
- **Operational Validation Reinforces Stakeholder Confidence:** Trust is reinforced as digital twins demonstrate consistent performance in real-world applications. Success depends on the ability to adapt to changing conditions and maintain reliability across operational contexts.
- **Interoperability Enables Scalable and Transferable Trust:** A major barrier to digital twin trust is the lack of interoperability across tools, platforms, and organizational boundaries. Scalable adoption depends on common interfaces, standards, and the ability to exchange trustworthy information.
- **Transparency, Traceability, and Explainability Are Essential:** Users must be able to understand and trace how a digital twin generates output (e.g., what data it uses, how it models the system, and how assumptions are encoded). These attributes are central to building confidence in decision-making contexts.

2.3.5. Day 1 Breakout Sessions

The first day of breakout sessions focused on defining trust in digital twins and identifying the role of verification and validation (V&V) methods in supporting trustworthiness. Participants were divided into four concurrent breakout rooms (A–D), where facilitators guided discussions using a shared set of questions. The sessions explored essential attributes of trustworthy digital twins, mechanisms for measuring trust, and the application of V&V practices across various domains. Participants drew on their diverse experiences to highlight practical challenges, emerging strategies, and areas where existing standards may fall short.

2.3.5.1. Major Takeaways

- **Trust Must Be Defined by Use Case and Lifecycle Phase:** Trustworthiness depends on identifying the specific trust metrics relevant to each application context, including intended outcomes, acceptable risk levels, and system function. These metrics may vary across lifecycle phases such as design, deployment, and maintenance, reflecting different requirements for model performance, reliability, and assurance.
- **Transparency and Explainability Are Central to Adoption:** Stakeholders must be able to interpret model behavior, understand embedded assumptions, and verify how inputs affect outputs in order to validate decisions/conclusions and maintain trust in complex systems. This requires access to clearly documented model structures, input parameters, and validation procedures that allow users to assess fidelity and understand the basis for system recommendations.
- **Validation Requires Iterative, Evidence-Based Methods:** Trust is reinforced through repeated validation cycles using high-quality, time-aligned data from physical systems, combined with domain-specific metrics and documented evaluation procedures. Robust validation also depends on defining acceptable performance thresholds, capturing test conditions, and continuously comparing model outputs to real-world observations across a range of scenarios.
- **Organizational Roles Must Align to Maintain Trust:** Unclear boundaries between IT, OT, cybersecurity, and engineering functions create accountability gaps that undermine confidence in both the development and deployment of digital twins. Effective risk management and model credibility require early coordination and shared governance across these roles to ensure consistent validation practices and secure operational transitions.
- **Existing Standards Provide Valuable Foundations but Require Adaptation:** A range of standards and frameworks (e.g., NASA-STD-7009, ASME V&V 40, IEEE 1012, ISO/IEC 27001, and NIST cybersecurity publications) offer guidance on model verification, validation, and security but must be extended to account for the dynamic, real-time, and federated nature of digital twin environments. Applying these standards and frameworks effectively requires interpreting them in the context of digital twin-specific challenges such as model synchronization, secure data exchange, and integration across heterogeneous systems.

2.3.5.2. Breakout Session 1: Defining Digital Twin Trustworthiness

Overall Focus Question: What attributes define trust? How do we measure it?

What are the essential attributes of a trustworthy digital twin?

- **Multidimensional Trust Characteristics:** Trustworthiness in digital twins includes attributes such as accuracy, consistency, explainability, security, and resilience across the digital twin’s lifecycle and operating context.

- **Transparency and Explainability:** A trustworthy digital twin must provide clear insight into how it functions, including the underlying assumptions, model behavior, and decision-making logic, enabling stakeholders to understand and evaluate its outputs.
- **Verification and Validation (V&V):** Ongoing V&V practices are critical to establishing and sustaining trust. They ensure that digital twin models are credible, reliable, and aligned with their intended use, even as conditions change over time.
- **Data Integrity and Provenance:** Reliable digital twins depend on high-quality, traceable data inputs. Maintaining metadata, provenance records, and version control enhances transparency and reduces the risk of model degradation.
- **Human-Centered Confidence:** Trust is influenced by human perceptions, including confidence in the system's usability, reliability, and alignment with organizational goals. Institutional reputation and prior performance also shape trust.
- **Context-Driven Trust Thresholds:** The level of assurance required for trust depends on the application domain, with mission-critical or safety-sensitive contexts demanding higher confidence and more rigorous testing.
- **Trust Artifacts and Documentation:** Formal artifacts (e.g., validation reports, traceability matrices, documented assumptions) enable trust to be communicated between developers, users, regulators, and support structured evaluation.
- **Existing Standards Offer Partial Coverage:** Frameworks and standards such as the NIST Cybersecurity Framework (CSF) and ISO/IEC 27001 provide foundational guidance on aspects of digital trust but do not fully address the complexities of digital twin systems. Domain-specific V&V standards such as NASA-STD-7009 and ASME V&V 40 serve as useful models for establishing trust in high-fidelity simulation environments but remain limited in scope for broader digital twin ecosystems.

*Participants emphasized that **defining trust in digital twins requires a nuanced understanding** of the system's lifecycle phase and operational context. For instance, a design-phase model might prioritize predictive accuracy and boundary condition coverage, while an operational model would require real-time responsiveness, fault tolerance, and strict data provenance. This framing highlighted that **trust cannot be addressed as a static property but must evolve** with the model's intended role, criticality, and exposure to change.*

How should trustworthiness be measured within a digital twin ecosystem?

- **Fit-for-Purpose Assessment:** Trust should be evaluated by whether a digital twin performs reliably and accurately for its intended use case, incorporating metrics that align with domain-specific performance expectations.
- **Verification and Validation Metrics:** Standard V&V practices (e.g., model fidelity, accuracy thresholds, error bounds, and scenario testing) can serve as measurable indicators of trust, especially when linked to defined acceptance criteria.

- **Confidence Levels and Uncertainty Quantification:** Quantitative approaches such as confidence intervals, statistical sensitivity analyses, and uncertainty bounds help convey the reliability and limitations of digital twin outputs.
- **Traceability and Provenance Indicators:** The ability to trace model inputs, data sources, assumptions, and changes over time supports reproducibility and trust evaluation by external reviewers or downstream users.
- **Operational Monitoring and Deviation Tracking:** Trustworthiness can be continuously assessed by comparing real-time digital twin outputs to observed physical system behaviors, flagging deviations for investigation or recalibration.
- **Human-Centric Trust Indicators:** Metrics related to user interaction (e.g., system usability, interpretability, or rate of operator overrides) may reflect levels of user confidence and trust in the system's performance.
- **Trust Artifacts and Documentation:** Formal documentation (e.g., validation reports, assumptions logs, V&V traceability matrices, and digital twin health indicators) serves as tangible evidence for evaluating and communicating trustworthiness.
- **Established V&V Standards Provide a Starting Point:** Standards such as IEEE 1012 (System and Software V&V), ISO/IEC 15288 (System Life Cycle Processes), and ASME V&V 10 and V&V 40 offer foundational approaches for defining measurable indicators of trust. However, these standards require extension or adaptation to account for the dynamic, real-time, and cyber-physical attributes that distinguish digital twin systems from conventional software or modeling environments.

What does the industry need to know to trust and use digital twins in their environments?

- **Ongoing Verification and Validation:** Continuously applying V&V techniques throughout a digital twin's lifecycle is required to maintain alignment with physical systems and evolving operational contexts, reinforcing trust over time.
- **Improved Transparency and Documentation:** Clear communication of model assumptions, data provenance, limitations, and updates builds user confidence and supports regulatory or stakeholder evaluation.
- **Establishment of Trust Artifacts:** Creating structured trust artifacts (e.g., audit trails, validation summaries, or traceability matrices) enables consistent and repeatable assessment of trustworthiness across use cases.
- **User Engagement and Feedback Loops:** Involving end users in digital twin design, testing, and validation promotes ownership, improves usability, and surfaces context-specific trust concerns early in the process.
- **Credentialing and Certification Pathways:** Third-party validation, certifications, or standardized evaluation frameworks were proposed as mechanisms to increase trust across organizations and sectors.

- **Community Standards and Shared Practices:** Developing common taxonomies, documentation formats, and performance benchmarks fosters consistency and comparability, helping users interpret and rely on digital twin outputs.
- **Adapted Frameworks Can Support Digital Twin Trust:** Established guidance, such as the NIST AI Risk Management Framework, ISO/IEC 17025, and sector-specific V&V protocols, can serve as foundational starting points for building trust infrastructure in digital twin environments, though adaptation is necessary to reflect the unique characteristics of these systems.

*Across sessions, participants described the **need for auditable model validation processes** that allow others to understand not only how a model was tested but under what assumptions, data conditions, and constraints. Especially in regulated sectors or multi-stakeholder environments, validation artifacts, such as **test case coverage reports, simulation logs, and dependency maps were seen as necessary tools** to support reuse and ensure trust beyond the original development team.*

2.3.5.3. Breakout Session 2: Verification & Validation (V&V) as a Trust Enabler

Overall Focus Question: How can V&V methodologies strengthen trust?

How do we benchmark a digital twin's performance against real-world systems?

- **Quantitative Alignment with Physical Data:** Benchmarking should compare digital twin outputs with data collected from the corresponding physical system across key variables such as time, frequency, accuracy, and event response.
- **Use of Time-Synchronized Data Streams:** Validation requires high-resolution, timestamped datasets from both the digital twin and the physical system to assess real-time fidelity and alignment.
- **Scenario-Based Testing for Edge Cases:** Digital twins should be evaluated against known failure modes or abnormal operating conditions to determine robustness and predictive accuracy under stress.
- **Domain-Specific Metrics and Tolerances:** Performance benchmarks should be tailored to the operational domain, such as manufacturing throughput, thermal stability, or energy efficiency, with clear tolerances for acceptable deviation.
- **Iterative Validation Across System Lifecycle:** Benchmarking is not a one-time activity but an ongoing process across development, deployment, and operation phases to ensure the model remains accurate as systems evolve.
- **Traceability of Assumptions and Modeling Parameters:** Benchmarking must account for assumptions made in the modeling process, including fidelity limits, parameter estimates, and simplifications that may affect real-world alignment.

- **Established V&V Standards Support Model Benchmarking:** Standards such as NASA-STD-7009 and ASME V&V 40 provide structured approaches for validating model fidelity, documenting test procedures, and supporting benchmarking efforts in complex digital twin environments.

What are the best practices for calibrating digital twin models to reflect real-world conditions?

- **Calibration Requires Access to High-Fidelity Sensor Data:** Reliable calibration depends on the availability of accurate, time-synchronized data from physical systems to align digital model parameters with real-world behaviors.
- **Feedback Loops Enable Ongoing Calibration:** Implementing automated or semi-automated feedback mechanisms allows the digital twin to self-correct or refine parameters based on observed discrepancies over time.
- **Model Parameters Must Be Contextually Tuned:** Calibration processes should account for system context, such as operating conditions, physical constraints, and environmental variability, rather than relying on static or generalized inputs.
- **Physical and Virtual Tests Should Be Iteratively Integrated:** Calibration benefits from a cycle of simulation and real-world testing, allowing deviations between predicted and actual performance to guide model refinement.
- **Transparent Documentation of Calibration Procedures Builds Trust:** Clearly recording the data sources, assumptions, and parameter adjustments involved in calibration supports reproducibility and stakeholder confidence in the model.
- **Cross-Disciplinary Collaboration Enhances Calibration Accuracy:** Coordination among domain experts, data scientists, and engineers improves the quality of parameter selection, boundary condition modeling, and validation strategies.
- **Established V&V and Calibration Standards Guide Model Alignment:** Standards such as ASME V&V 40, ISO/IEC 17025, and IEEE 1012 provide structured approaches for calibrating models through controlled testing, uncertainty analysis, and verification of measurement systems.
- **Industry Standards Support Calibration in Specific Domains:** Standards such as MTConnect provide a standardized data interface that can be used to collect operational data for manufacturing equipment calibration and support continuous near-real-time feeds into digital twins, while ASTM standards for additive manufacturing support model validation in workflows sensitive to material behavior and build variability. Frameworks such as QIF (Quality Information Framework), STEP (AP242), and MOC+ by DNV offer structured approaches for managing quality data, integrating lifecycle models, and overseeing change management, each contributing to calibration integrity in domain-specific digital twin applications.

Participants noted that best practices for calibration are undermined when sensor data lacks synchronization, context, or clear lineage. ***In dynamic environments****, even* ***minor inconsistencies*** *in data timestamps or source assumptions* ***can lead to significant drift between the physical and virtual systems****.* ***Effective calibration requires*** *not only* ***precise instrumentation but also transparent data pipelines and governance structures*** *that maintain data quality and accessibility.*

2.3.6. Day 2 Keynote Presentation: "Trust but Verify: Cybersecurity Challenges for Digital Twins"

Steve Lu, CEO of Stealth Software, delivered a keynote presentation regarding the challenges of cybersecurity for digital twins.

2.3.6.1. Key Points

- **Digital Twins Reshape Security Boundaries:** Unlike traditional IT or SCADA (Supervisory Control and Data Acquisition) systems, digital twins combine real-time data exchange, dynamic system modeling, and physical control, creating a unique and evolving security landscape that spans both cyber and physical domains.
- **Cybersecurity Challenges:** Five major digital twin security issues include (1) massive instrumentation and untrusted sensor data, (2) centralized data aggregation as a point of failure, (3) deceptive visual representations, (4) remote control risks, and (5) interoperability and trust gaps in current standards.
- **Comparison with Other Ecosystems Highlights Gaps:** While enterprise IT and SCADA systems offer partial parallels, digital twins introduce deeper integration with IoT, identity, and autonomous systems that complicate traditional security models and controls.
- **Zero Trust as a Starting Point, not a Solution:** Zero Trust architectures (e.g., micro-segmentation, continuous verification) offer a partial mitigation strategy but fall short of addressing deeper trust questions tied to model fidelity, output accuracy, and secure multiparty use.
- **Modern Cryptography Enables New Trust Models:** Privacy-enhancing technologies such as secure multiparty computation, verifiable computation, and encrypted analytics can support trust in sensitive, distributed, and federated digital twin environments by ensuring confidentiality, integrity, and accountability without exposing raw data.

2.3.7. Day 2 Breakout Sessions

The second day of breakout sessions focused on cybersecurity, trust artifacts, and assurance mechanisms to support trustworthy digital twin deployment. Participants reconvened in the same four breakout rooms to explore how existing cybersecurity frameworks apply to digital twins, what types of artifacts can serve as evidence of trust, and how standards might evolve to address these needs. Discussions drew on a broad range of perspectives, including those from operational technology, software assurance, policy, and systems engineering. Key themes emerging from the sessions emphasized the complexity of defining trust across interconnected systems, the growing need for verifiable evidence in digital engineering workflows, and opportunities to build on existing security and risk management guidance.

2.3.7.1. Major Takeaways

- **Cybersecurity Responsibilities Are Diffuse and Fragmented:** Similar to the Day 1 discussions on organizational role misalignment, cybersecurity accountability is often divided among IT, OT, and engineering teams without clear ownership. This fragmentation creates gaps in protective coverage, limits coordination on risk mitigation, and weakens the overall cybersecurity posture of digital twin environments.
- **Interconnected Digital Twins Amplify Risk and Complexity:** As digital twins become more integrated across systems and organizations, new vulnerabilities emerge, including expanded attack surfaces, third-party exposure, and cascading trust dependencies. A compromise in one node can propagate throughout a connected ecosystem, increasing the difficulty of containment and attribution in federated digital twin system architectures.
- **Trust Infrastructure Must Be Built into Digital Twin Architectures:** Establishing trust at scale will require embedded technical mechanisms such as cryptographic credentials, auditable logs, and model validation artifacts alongside processes for lifecycle assurance and risk governance. Effective trust infrastructure includes verification documentation, model lineage records, and transparent integration protocols to support secure reuse and handoffs between systems.
- **Sector-Specific Risks Demand Tailored Mitigations:** The unique characteristics of domains such as critical infrastructure, manufacturing, and healthcare require customized approaches to digital twin security that reflect operational realities and regulatory constraints. Risk mitigation strategies must be aligned with the system's function, safety profile, and compliance requirements to ensure protections are contextually appropriate and enforceable.
- **Security-Relevant Standards Must Be Interpreted Through a Digital Twin Lens:** Standards and frameworks such as NIST SP 800-53, 800-82, 800-160 Vol. 2, and ISO/IEC 27001 should be adapted to address the specific demands of digital twin environments, including continuous model evolution, integration of real-time data streams, and secure coordination across multiple interconnected systems.

Applying these standards and guidelines effectively requires interpreting them in the context of dynamic, data-driven operations and complex system interactions.

2.3.7.2. Breakout Session 3: Cybersecurity Challenges & Trust Artifacts

Overall Focus Question: What Security Measures and Trust Artifacts Should be Required?

What specific cyber threats pose the most significant risk to digital twin implementations?

- **Data Integrity Attacks on Models and Inputs:** Malicious tampering with model inputs or training data can degrade system performance or produce misleading outputs, undermining trust in operational decisions.
- **Exploitation of Interfaces and Integration Points:** API endpoints, data connectors, and third-party integrations represent vulnerable surfaces where attackers can inject malicious code or extract sensitive information.
- **Unauthorized Access to Real-Time Control Functions:** In systems where digital twins influence physical operations, compromised credentials or misconfigured access controls can enable adversaries to manipulate actuators or override safeguards.
- **Insider Threats Within Multi-Disciplinary Teams:** The convergence of IT, OT, and engineering roles introduces complexity in access management, increasing the risk of accidental or intentional misuse by trusted insiders.
- **Lack of Visibility Across Distributed Components:** Without unified monitoring, it becomes difficult to detect anomalies or lateral movement across interconnected components of a digital twin ecosystem.
- **Firmware and Embedded Device Vulnerabilities:** Legacy industrial devices that interface with digital twins often lack modern security protections, making them attractive targets for exploitation or pivot attacks.
- **Inadequate Segmentation Between Virtual and Physical Systems:** Poorly isolated digital environments increase the risk that cyber intrusions will affect physical assets or critical infrastructure operations.

What are the security implications of interconnected digital twins in critical infrastructure?

- **Expanded Attack Surface Across Connected Systems:** Interconnecting digital twins increases the number of entry points for malicious actors, especially when systems span enterprise, operational, and third-party domains.
- **Dependency and Cascade Risks:** A compromise in one component or node can propagate through the broader digital twin ecosystem, amplifying impact across physical and digital assets.
- **Unclear Governance in Federated Environments:** When digital twins are distributed across multiple organizations or tiers of ownership, security roles and responsibilities become harder to define and enforce.

- **Complex Identity and Access Management Requirements**: Interconnected systems must support fine-grained access control and credentialing mechanisms that can operate reliably across diverse platforms and trust boundaries.
- **Integrity of Shared Models and Data Streams:** The security of shared data flows and models is critical to maintaining trust, especially when models influence physical processes or decision-making in real time.
- **Verification and Validation Transparency:** Documentation that describes model testing procedures, limitations, and assumptions helps ensure that integrated components can be evaluated and trusted within critical infrastructure contexts.
- **Cryptographic Assurance of Provenance:** Applying digital signatures, secure hashing, or credentialing to models and workflows supports traceability and confidence in the authenticity of shared components.

*Breakout room discussions repeatedly pointed to **friction between IT, OT, cybersecurity, and modeling teams**. These gaps often lead to **unclear ownership of risk**, with **security threats going unmitigated due to fragmented responsibilities**. Addressing this issue requires **governance models that define shared accountability, integrate cybersecurity into early model development stages, and establish protocols** for coordination during both deployment and incident response.*

2.3.7.3. Breakout Session 4: Evidence-Based Trust

Overall Focus Question: What Standards Should Govern Digital Twin Trustworthiness?

What existing cybersecurity frameworks apply to digital twin security?

- **NIST Cybersecurity Framework (CSF):** The CSF offers a baseline for managing cybersecurity risk across digital twin environments, supporting role clarity, governance structures, and adaptive protection strategies.
- **NIST 800-Series Controls:** Publications in the 800-series deliver detailed guidance for implementing risk-based security, system engineering, and zero trust principles tailored to cyber-physical systems (e.g., SP 800-53 for security and privacy controls, SP 800-160 for system security engineering, and SP 800-207 for zero trust architecture).
- **NIST Cybersecurity for IoT:** The IoT framework helps secure digital twins that rely on distributed sensing, embedded systems, or cloud-to-edge connectivity through lifecycle management and device-level safeguards.
- **NIST Privacy Framework:** The Privacy Framework enables digital twin implementations to manage risks related to personal and sensitive data, especially in systems involving surveillance, biometrics, or consumer interactions.

- **UK NCSC Operational Technology Guidance:** UK National Cyber Security Centre publications offer structured practices for securing industrial control systems and digital twins operating in critical infrastructure environments.
- **IEC 62443 Standards:** The IEC 62443 series provides international security standards for industrial automation and control systems, applicable to digital twin deployments in manufacturing and infrastructure sectors.
- **ISO/IEC 27001 Information Security Management:** ISO/IEC 27001 provides a recognized framework for managing information security risks and aligning cybersecurity practices across digital twin environments.
- **ITU Digital Trust and AI Security Guidance:** The International Telecommunication Union's work on digital trust, including AI-related cybersecurity, informs cross-border policy development and harmonized standards for secure digital twin ecosystems.

What are the gaps in existing digital twin trustworthiness guidance?

- **Lack of Context-Specific Definitions of Trustworthiness:** Current frameworks provide general concepts but do not define trust in ways that reflect the unique priorities of different sectors, applications, or operational contexts.
- **Insufficient Support for Real-Time and Autonomous Systems:** Most existing standards are not designed for systems that operate in real time or autonomously, limiting their usefulness for operational digital twins.
- **Limited Emphasis on Socio-Technical Dimensions of Trust:** Key human-centered elements of trust, such as transparency, explainability, and stakeholder confidence, are often overlooked in technical guidance.
- **Missing Criteria for Model Lifecycle Management:** There is little guidance on how to manage digital twin models over time, including updates, retraining, validation after deployment, and version control.
- **Inadequate Integration of Cyber-Physical Risk Considerations:** Current standards often treat cyber and physical system risks separately, failing to address the blended nature of threats in digital twin ecosystems.
- **Lack of Assurance Mechanisms for Federated Systems:** Guidance is limited when it comes to establishing trust across distributed or federated digital twins that span organizational or system boundaries.
- **Gaps in Verification of Data Provenance and Model Integrity:** Existing frameworks do not fully address the need for traceability and verification of data sources, transformations, and model authenticity.

Do we need to develop a cybersecurity framework specific to digital twins?

- **Existing Frameworks Do Not Fully Address Digital Twin-Specific Risks:** Current cybersecurity frameworks were not designed for systems that mirror and interact with physical assets in real time, leaving gaps in areas like model tampering, fidelity assurance, and bidirectional data flows.
- **Digital Twin Architectures Involve Unique Attack Surfaces:** The combination of modeling systems, real-time control, third-party integrations, and cloud-edge connectivity creates novel vulnerabilities that existing frameworks do not fully anticipate.
- **Dynamic and Evolving Models Require Adaptive Security Controls:** Digital twins undergo frequent updates, retraining, and contextual reconfiguration, which demands security frameworks capable of managing evolving risk states and dependencies.
- **No Standard for Securing the Virtual-Physical Interface:** Interactions between the digital model and physical asset introduce trust and safety challenges that are not addressed by traditional IT or OT cybersecurity practices.
- **Cross-Disciplinary Complexity Requires Tailored Guidance:** Security responsibilities span IT, OT, systems engineering, and modeling teams, making it difficult to apply conventional frameworks that assume clear domain boundaries.
- **Sector-Specific Needs May Require Customizable Modules:** A unified framework for digital twins would need to be modular or adaptable to suit the varying cybersecurity needs of sectors such as manufacturing, energy, healthcare, and defense.

Rather than calling for entirely new frameworks, many contributors advocated ***for adapting existing standards such as NIST 800-53 for controls, ASME V&V 40 for validation, and ISO/IEC 27001 for security management*** *to the specific challenges of digital twin environments. This includes interpreting how these standards apply to real-time data flows, system-of-systems architectures, and the joint modeling of physical, software, and organizational components.*

2.3.8. Challenges and Opportunities

The discussions in Workshop 3 highlighted the maturity of digital twin advances but emphasized persistent challenges. Uncertainty quantification and validation remain underdeveloped, particularly for complex and dynamic systems. Cybersecurity risks were described as expanding with increased connectivity, and participants reiterated concerns about scaling adoption across organizations with varying resources. Integration across the digital twin lifecycle also requires clearer standards and reference implementations.

Opportunities from Workshop 3 focused on aligning research and standards development to support trustworthy digital twins. Participants discussed the potential for digital twins to improve decision-making across product lifecycles, enhance competitiveness through innovation, and enable new models of collaboration between industry, government, and academia. Contributions from multiple sectors and use cases were seen as strengthening the foundation for a shared ecosystem.

3. Research Opportunities and Priorities

3.1. Overview

Research is central to advancing the development, deployment, and trustworthiness of digital twins in manufacturing. The NIST workshops suggested that while digital twins are already being applied across design, production, and supply chain management, significant gaps remain in the scientific, technical, and organizational foundations that support their use. Addressing these gaps requires coordinated research efforts that extend beyond individual implementations and align with broader national priorities in manufacturing and innovation.

The research priorities identified in this report reflect input from stakeholders across industry, academia, and government. These priorities build on common themes from the workshops, including the need for improved interoperability, rigorous verification and validation practices, and robust approaches to cybersecurity and governance. Stakeholders also emphasized the importance of advancing reference implementations and testbeds, developing a skilled workforce, and enabling sector-specific applications that demonstrate measurable value.

Taken together, these priorities provide a roadmap for guiding collaborative research and development activities. They highlight where standards and frameworks must evolve, where testbeds and experimentation environments are needed, and where new methods and tools can strengthen the confidence of manufacturers in adopting digital twins. By advancing these priorities, stakeholders can help ensure that digital twins deliver on their promise of improving productivity, resilience, and competitiveness in U.S. manufacturing.

3.2. Interoperability and Integration

A central research priority is advancing interoperability so that digital twins can exchange data and models across platforms, organizations, and lifecycle stages. Current implementations are often proprietary and siloed, limiting integration across design, manufacturing, and operations. Research is needed to define methods for enabling interoperability across heterogeneous systems while preserving fidelity and context.

One research direction is the development of common data models, ontologies, and semantic frameworks that allow digital twins to represent information consistently. These approaches support alignment across disciplines and facilitate the reuse of models and data. Additional research is needed to evaluate how standards and frameworks such as ISO 23247 and OPC-UA can be extended or harmonized to meet the requirements of dynamic, evolving digital twins.

Integration across the product lifecycle presents another research challenge. Manufacturers require methods for linking digital twins of products, processes, and systems into cohesive ecosystems. Research on reference implementations and case studies can provide guidance on integrating digital twins across lifecycle phases, from product design to end-of-life management.

Finally, supply chain integration highlights the need for research on secure, controlled data exchange across organizational boundaries. This includes methods for protecting intellectual property while enabling trusted collaboration. Advancing these research directions will provide a foundation for scaling digital twins from isolated use cases to interoperable ecosystems that deliver enterprise and sector-wide value.

3.3. Verification, Validation, and Uncertainty Quantification

Establishing trust in digital twins requires rigorous methods for verification, validation, and uncertainty quantification. While VVUQ practices are well-established in some other domains, they are not yet adapted for continuously evolving digital twins that integrate real-time data streams with dynamic models. Research is needed to define methodologies that account for the changing fidelity, scale, and purpose of digital twins in manufacturing contexts.

A priority research direction is the development of domain-specific VVUQ frameworks that can be applied across manufacturing applications. These frameworks should enable manufacturers to assess the accuracy and reliability of digital twin predictions under varying conditions, including rapidly changing operating environments. Research is also needed to establish benchmarks, test cases, and performance metrics that allow consistent evaluation across organizations and sectors.

Another area of research opportunity is the integration of uncertainty quantification into lifecycle decision-making. Manufacturers require methods for capturing and communicating uncertainty to inform design, production, and maintenance choices. This includes developing techniques for propagating uncertainty across interconnected digital twins in larger ecosystems. Incorporating these research directions into reference implementations and testbeds will provide manufacturers with practical methods for ensuring that digital twins are both accurate and trustworthy.

3.4. Cybersecurity and Data Governance

Cybersecurity emerged as a consistent research priority across all three workshops. As digital twins connect operational technologies, enterprise systems, and supply chains, they expand the potential attack surface. Without clear cybersecurity and governance practices, manufacturers risk exposing sensitive operational data and intellectual property to adversaries. Research is needed to adapt and extend cybersecurity standards and frameworks to the unique challenges posed by continuously updating highly interconnected digital twins.

One priority research area is the application of existing cybersecurity frameworks, including NIST SP 800-53, IEC 62443, and ISO/IEC 27001, to digital twin environments. Workshops highlighted the need to evaluate where these frameworks are sufficient and where new approaches are required to address real-time synchronization, federated data sharing, and dynamic access control. Research on threat modeling for digital twins, including attacks on data integrity, model manipulation, and denial of service, can inform appropriate security controls.

Data governance was also identified as a critical need. Manufacturers require mechanisms to ensure data provenance, protect intellectual property, and manage access rights within and across organizations. Research is needed on frameworks for establishing trust agreements that define responsibilities for data sharing, accountability, and transparency in multi-party ecosystems. This includes policies and technical methods for balancing openness with confidentiality.

3.5. Reference Implementations and Testbeds

Reference implementations and testbeds are critical research priorities for accelerating digital twin adoption in manufacturing. Manufacturers often lack practical examples and implementation models that demonstrate how digital twins can be deployed at scale. Reference implementations can provide shared blueprints for integrating digital twins across lifecycle phases, while testbeds create environments where methods, standards, and frameworks can be evaluated under realistic conditions.

Developing reference implementations will help clarify how digital twins of products, processes, and systems can interoperate within larger ecosystems. These implementations can define roles, interfaces, and integration points, reducing the need for manufacturers to build one-off solutions. They also provide a foundation for aligning digital twin implementations with existing standards and frameworks, ensuring consistency across sectors and organizations.

Testbeds serve as another essential enabler. By providing controlled environments for experimentation, testbeds allow stakeholders to test interoperability, validate performance, and assess cybersecurity measures before deploying digital twins in production settings. They also support workforce development by providing practitioners with opportunities to engage in hands-on demonstrations. Collaborative testbeds can further accelerate innovation by bringing together manufacturers, technology providers, and researchers to solve shared challenges.

Advancing research in these areas will support the development of scalable and trustworthy digital twins. Reference implementations will provide the structural guidance needed for adoption, while testbeds will supply the evidence and confidence required for implementation in diverse manufacturing environments.

3.6. Workforce and Skills Development

Advancing digital twin adoption requires a workforce equipped with the skills to develop, implement, and maintain these technologies. Workforce readiness is a significant barrier, particularly for SMMs that often lack specialized expertise. Research is needed to identify the skills most critical for digital twin deployment and to design educational pathways that address gaps across engineering, computer science, data science, and manufacturing disciplines.

One area of research involves developing curricula and training programs that integrate digital twin concepts into higher education and vocational training. This includes embedding digital twin practices into engineering design courses, manufacturing systems education, and cybersecurity training.

Partnerships between academia, industry, and government can ensure that educational content aligns with emerging needs and provides hands-on opportunities to engage with digital twin tools and testbeds.

Another research direction is exploring workforce models that enable broader participation in digital twin ecosystems. SMMs may require shared resources, such as regional training centers or collaborative platforms, to access expertise without having to maintain it in-house. Research can examine how such shared infrastructure supports equitable access and reduces digital divides within the sector.

Finally, workforce development must address organizational change management. Manufacturers require guidance on integrating digital twin capabilities into existing workflows, job roles, and decision-making processes. Research into effective change management strategies, including workforce adoption of new standards and frameworks, will support smoother transitions and sustained implementation.

3.7. Sector-Specific Applications

Sector-specific applications represent an important research frontier for digital twins in manufacturing. While general frameworks and methods are essential, adoption depends on demonstrating clear value in particular industrial contexts. Research is needed to identify and evaluate applications in which digital twins can address sector-specific challenges, such as process optimization, quality assurance, and supply chain resilience.

One priority is advancing applications in additive manufacturing. Digital twins can support real-time monitoring and validation of builds, addressing challenges related to material variability and process control. Research can focus on methods for integrating sensor data with simulation models to improve quality and reduce waste.

Another opportunity is in predictive maintenance for critical equipment. Digital twins that monitor machine health and anticipate failures can reduce downtime and extend equipment life. Research is required to refine these models, validate their accuracy across different equipment types, and establish best practices for integration into production systems.

Supply chain applications also warrant further investigation. Research can examine how digital twins can provide end-to-end visibility across supply networks, allowing manufacturers to anticipate disruptions, optimize logistics, and improve resilience. This includes methods for securely sharing data across organizations while protecting proprietary information.

By advancing research into these sector-specific applications, stakeholders can demonstrate tangible benefits of digital twins. These applications can serve as exemplars that build confidence, guide standards development, and accelerate broader adoption across manufacturing.

4. Standards Needs

4.1. Overview

Standards and frameworks are essential for enabling digital twins to operate across organizational boundaries and throughout the product lifecycle. The workshops highlighted that while many relevant standards exist in domains such as data exchange, modeling, and cybersecurity, there is currently no coordinated framework that integrates all of them into a cohesive foundation for digital twins. The absence of such integration creates barriers to interoperability, validation, and trustworthiness.

Participants emphasized that advancing digital twin adoption requires identifying gaps in existing standards, clarifying how current efforts can be harmonized, and defining new standards or frameworks where needed. This includes not only technical specifications but also governance models, implementation guidelines, and reference frameworks that help manufacturers apply standards in practice.

The workshops also revealed the importance of balancing flexibility with standardization. Overly rigid requirements could limit innovation, while insufficient guidance may lead to fragmented and proprietary approaches. Research and collaboration are needed to determine the appropriate scope, structure, and level of prescriptiveness for digital twin standards and frameworks.

4.2. Interoperability

Interoperability was consistently identified as one of the most pressing standards needs for digital twins. Current implementations often rely on proprietary formats and interfaces, preventing digital twins from exchanging data or integrating across systems. Standards and frameworks are needed to define common approaches for data representation, model exchange, and system integration.

Participants noted that existing standards and frameworks, such as ISO 23247 (Digital Twin Framework for Manufacturing) and OPC UA, provide important starting points but do not yet fully address the complexity of multi-domain, multi-organization digital twin ecosystems. Research and standards development should focus on extending and harmonizing these efforts to support semantic interoperability, real-time data synchronization, and lifecycle integration.

Interoperability standards are also critical for scaling digital twins from individual applications to enterprise and sector-wide ecosystems. Manufacturers require reference implementations and profiles that demonstrate how standards can be applied consistently across diverse contexts. Clear conformance criteria and test methods will further ensure that systems claiming compliance can reliably interoperate.

Without such standards, digital twin adoption risks becoming fragmented and proprietary, limiting manufacturers' ability to collaborate, share data, and build trustworthy systems. Addressing interoperability through coordinated standards efforts will create the foundation for scalable, connected, and resilient digital twin ecosystems.

4.3. Verification, Validation, and Uncertainty Quantification

Establishing trust in digital twins depends on clear and consistent approaches for verification, validation, and uncertainty quantification (VVUQ). While many standards exist for model validation and simulation, they are not fully adapted to the dynamic and evolving nature of digital twins, which continuously integrate real-time data streams with models that change over the product lifecycle.

The workshops emphasized that standards and frameworks are needed to define methods for verifying that digital twin implementations meet intended requirements, validating predictions against experimental or operational data, and quantifying uncertainty in meaningful ways for decision-making. Without such guidance, manufacturers may struggle to assess whether digital twins are reliable and fit for purpose.

Existing efforts such as ASME V&V 40, IEEE 1012, and related modeling and simulation standards provide valuable foundations. However, these must be extended to account for real-time updates, federated systems-of-systems, and cross-domain interactions. Standards should also define benchmarks, reference use cases, and performance metrics to ensure comparability and consistency across implementations.

Developing VVUQ standards will not only enhance trust in digital twins but also support regulatory acceptance and sector-wide adoption. By aligning on shared approaches, stakeholders can reduce duplication of effort, accelerate validation processes, and improve confidence in using digital twins for critical manufacturing decisions.

4.4. Cybersecurity and Data Governance

Cybersecurity and data governance emerged as critical areas across the workshops where standards and frameworks are urgently needed. As digital twins increasingly connect operational technology, enterprise systems, and supply chains, they expand the potential attack surface and expose sensitive data. Without consistent approaches to cybersecurity and governance, manufacturers risk undermining trust and limiting adoption.

Participants highlighted that existing standards and frameworks, such as NIST SP 800-53, IEC 62443, and ISO/IEC 27001, provide strong starting points, but they are not tailored to the specific needs of digital twins. Standards must address real-time synchronization of data, federated sharing across organizations, and dynamic access controls for continuously evolving systems. Threat modeling approaches specific to digital twins are also needed to guide the implementation of appropriate protections.

Data governance is equally essential. Manufacturers require clear frameworks to ensure data provenance, maintain intellectual property protections, and manage access rights across organizational boundaries. Standards should establish mechanisms for accountability, transparency, and trust agreements that enable data sharing while protecting confidentiality.

By developing cybersecurity and data governance standards, stakeholders can strengthen trustworthiness and resilience in digital twin ecosystems. Such standards will not only safeguard data and systems but also provide the confidence needed for scaling digital twins into enterprise and sector-wide applications.

4.5. Reference Implementations and Testbeds

Reference implementations and testbeds are essential for translating standards into practice and demonstrating their applicability in real-world contexts. The workshops emphasized that while many standards exist in isolation, manufacturers often lack guidance on implementing them cohesively within digital twin ecosystems. Reference implementations can provide structured blueprints that illustrate how standards and frameworks align across different layers of digital twin systems, from data collection to enterprise integration.

Testbeds play a complementary role by creating controlled environments where standards can be applied, tested, and refined. These environments allow stakeholders to evaluate interoperability, cybersecurity, and performance under realistic conditions, while also identifying gaps in existing standards. Testbeds can further accelerate adoption by serving as collaborative platforms where industry, academia, and government can experiment with emerging technologies and share lessons learned.

Standards development organizations can leverage insights from reference implementations and testbeds to ensure that standards remain practical, implementable, and aligned with industry needs. Conversely, reference implementations guided by standards will provide manufacturers with confidence that their digital twin solutions are both compliant and interoperable.

Advancing standards based on reference implementations and testbeds will help bridge the gap between high-level frameworks and operational use, ensuring that digital twin implementations are consistent, scalable, and trustworthy.

4.6. Workforce and Skills Development

The successful adoption of digital twins depends not only on technology but also on the availability of a skilled workforce capable of applying standards and frameworks in practice. The workshops emphasized that workforce readiness is uneven across the manufacturing sector, with SMMs in particular, lacking the resources and expertise to implement digital twin technologies effectively.

Standards and frameworks can play an important role in addressing these gaps by defining competencies, training requirements, and reference materials that support workforce development. Clear guidelines can help align curricula in higher education, vocational training, and professional development programs with the skills needed to design, deploy, and maintain digital twins.

Participants also noted that standards can provide a foundation for certification programs, enabling organizations to validate workforce competencies and ensure consistency across industries. Workforce-related standards should also address organizational practices, including change management and integration of digital twin methods into existing roles and processes.

By linking workforce development directly to standards, stakeholders can ensure that training and education programs are aligned with industry needs and that workers are equipped to implement digital twins in a way that is consistent, interoperable, and trustworthy.

This report has also identified AI and machine learning as technologies to be leveraged for automated digital twin composition. This will also have a profound impact on the skills industries need to develop and maintain digital twins. Workers will rely on AI tools to automatically organize, collect, and compose data for building and updating digital twins. This will result in reduced need for advanced programming skills since workers will have the ability to translate data associated with different scenarios into actionable recommendations on the shop floor

5. Conclusions

5.1. Overview

Digital twins are increasingly recognized as a transformative technology for U.S. manufacturing, offering the potential to improve competitiveness, efficiency, and resilience. Across the three workshops, participants emphasized the ability of digital twins to enable predictive insights, optimize resource use, and foster innovation across product lifecycles. These benefits were consistently framed not as abstract possibilities but as practical drivers for adoption, highlighting the technology's potential to reshape how manufacturers design, operate, and sustain complex systems.

Despite clear momentum, the workshops also highlighted persistent barriers to broad deployment. Challenges related to interoperability, VVUQ, cybersecurity, and workforce readiness remain unresolved, creating risks of fragmentation and uneven adoption. Participants stressed that addressing these issues requires not only technical solutions but also coordinated research, harmonized standards and frameworks, and new models of collaboration. The conclusions presented in this chapter synthesize the most significant shared findings and outline future directions to advance trustworthy digital twins across the manufacturing ecosystem.

5.2. Common Challenges Across Workshops

A central conclusion from the three workshops is that digital twin adoption is constrained by persistent challenges that cut across technical, organizational, and strategic dimensions. Chief among these is the lack of interoperability and integration across systems. Manufacturers face fragmented approaches, proprietary data formats, and limited alignment of existing standards, all of which hinder the seamless exchange of information needed to support digital twins. Without common approaches, digital twin ecosystems risk remaining siloed and difficult to scale.

VVUQ capabilities also remain underdeveloped. While standards for validation of models and simulations exist, they are not tailored to the continuous, real-time updating that defines digital twins. The inability to consistently assess the reliability of digital twins limits trust in their outputs, particularly in high-stakes decision-making in manufacturing and supply chains.

Cybersecurity and data governance present further obstacles. As digital twins connect to more data sources and external partners, the potential attack surface expands, increasing risks of intrusion and data misuse. Participants highlighted that existing frameworks must be adapted to address real-time synchronization, federated sharing across organizations, and intellectual property protection. Absent clear frameworks, manufacturers may hesitate to adopt digital twins at scale.

Finally, workforce readiness and uneven resource availability present practical challenges. SMMs often lack the expertise or infrastructure to implement digital twins effectively, creating disparities in adoption. Integration with legacy systems adds further complexity, as many organizations struggle to align new digital twin technologies with established production environments. These common barriers show that realizing the potential of digital twins will require coordinated progress on technical, organizational, and human factors.

5.3. Cross-Cutting Opportunities

While the workshops highlighted significant barriers to digital twin adoption, they also revealed clear opportunities for advancing the technology in ways that strengthen U.S. manufacturing. A recurring theme was the potential of digital twins to deliver predictive insights that improve decision-making. By simulating outcomes and monitoring systems in real time, digital twins can help manufacturers anticipate failures, optimize processes, and reduce downtime, resulting in more efficient and resilient operations.

Another cross-cutting opportunity lies in lifecycle efficiency. Digital twins enable manufacturers to link design, production, and maintenance in a continuous feedback loop. This integration supports faster innovation, improves quality control, and reduces costs across product lifecycles. Participants emphasized that lifecycle integration is not only a technical advantage but also a competitive differentiator that can position U.S. manufacturers at the forefront of global markets.

Collaboration also emerged as a critical opportunity. Digital twins open pathways for new business models, where manufacturers, suppliers, and customers can engage through shared data and co-developed processes. Testbeds and pilot projects were highlighted as enablers, providing practical environments for demonstrating value, validating standards, and reducing uncertainty about return on investment. These collaborative efforts can accelerate adoption while ensuring that solutions remain aligned with industry needs.

Finally, digital twins offer the opportunity to strengthen resilience across supply chains. By providing real-time visibility into operations and external dependencies, digital twins can support adaptive responses to disruptions. This capability is particularly important given the increasing complexity of global supply chains and the need for greater agility in manufacturing. Collectively, these opportunities point toward a future where digital twins enhance competitiveness, resilience, and innovation across the sector.

5.4. Path Forward for Research and Standards

The workshops made clear that advancing digital twins requires coordinated progress in both research and standards. Research priorities must address technical gaps in interoperability, VVUQ, cybersecurity, and workforce development. Participants consistently noted that fragmented or uncoordinated research risks producing isolated solutions that cannot be scaled across manufacturing. Aligning research agendas across government, industry, and academia is therefore essential to accelerate progress and maximize impact.

Standards and frameworks were described as equally critical to ensuring that digital twins are trustworthy and interoperable. Participants stressed that while many relevant standards already exist, they are not harmonized into a cohesive framework that addresses the unique demands of digital twins. Participants stressed that while many relevant standards exist, they lack a cohesive framework tailored to the unique demands of digital twins. Consequently, current implementations that rely on existing solutions remain fragmented, leading to vendor lock-in and high integration costs. To meet real-time and lifecycle requirements, areas such as data exchange, model validation, and cybersecurity need new development or specialized standard extensions. Without these efforts, manufacturers risk encountering fragmented, proprietary solutions that undermine collaboration and trust.

Reference implementations and test beds were repeatedly identified as mechanisms to bridge research and standards. These environments provide platforms for evaluating new methods, validating interoperability, and refining standards in practice. By demonstrating how digital twins can be implemented consistently across different contexts, testbeds can reduce uncertainty and accelerate adoption. Participants also highlighted the need for sector-specific tailoring of standards and research to reflect the unique requirements of domains such as additive manufacturing, supply chains, and critical infrastructure.

Taken together, the path forward calls for coordinated investment in research, harmonization of standards and frameworks, and expansion of collaborative platforms that link the two. This approach will help ensure that digital twins evolve into scalable, trustworthy, and widely adopted tools for advancing U.S. manufacturing.

5.5. Collaborative Actions and Future Outlook

The workshops concluded that achieving the full potential of digital twins will require sustained collaboration across government, industry, and academia. Public–private partnerships were repeatedly cited as essential for pooling resources, aligning priorities, and creating shared platforms that reduce duplication of effort. Such partnerships can accelerate the development of testbeds, reference implementations, and workforce programs while ensuring that outcomes reflect the needs of diverse stakeholders.

Workforce development was another recurring theme. Participants emphasized that digital twin adoption cannot succeed without manufacturers trained to apply standards and frameworks in practice. Aligning education and training programs with emerging standards will ensure that the workforce is prepared to design, deploy, and maintain digital twins. Certification programs, competency frameworks, and integration of digital twin concepts into engineering and vocational curricula were identified as important mechanisms for advancing readiness.

Trust and transparency were also identified as critical factors for widespread adoption. Conformance testing, shared benchmarks, and reference implementations can provide manufacturers with confidence that digital twins will perform reliably and interoperate effectively. Establishing clear mechanisms for accountability and intellectual property protection will further support collaboration while safeguarding sensitive data.

Looking forward, participants envisioned digital twins becoming integral to manufacturing ecosystems, enabling scalable, interoperable, and trustworthy operations. By building on the progress already underway in research, standards, and collaborative platforms, the United States has the opportunity to lead in shaping digital twin technologies that strengthen competitiveness and resilience across sectors.

Appendix A. Workshop Agendas

Workshop 1

NIST Workshop on Digital Twin Standards for Manufacturing

Virtual Zoom Meeting
October 30, 2024

Time	Purpose	Presenter
11:00 AM	**Welcome and Administrative Notes**	Energetics
11:05 AM	**Introduction to NIST and Workshop Origins**	NIST
11:15 AM	**Keynote Address** ***Digital Twin Evolution and Industrial Use*** *Q/A to follow*	Dan Isaacs GM & CTO: Digital Twin Consortium, Chief Strategy Officer, Object Management Group
12:00 PM	**Lunch Break**	
12:30 PM	**Breakout Session Logistics**	Energetics
12:35 PM	**Breakout Session 1** ***Identifying the Applications and Challenges of Digital Twins for Manufacturing***	*Breakout Rooms A, B, C, D*
1:35 PM	**Expert Panel** ***Digital Twin Standards: Benefits for Manufacturing*** *Q/A to follow*	Robert Brown, Lab and Systems Development, Mitutoyo America Corporation Antonio Kung, Executive Board, Trialog Suresh Rama, Portfolio Development Executive, Siemens Digital Industries Software *Reconvene in Main Room*
2:10 PM	**Break**	
2:20 PM	**Breakout Session 2** ***Using Standards to Advance Digital Twins for Manufacturing***	*Breakout Rooms A, B, C, D*
3:20 PM	**Workshop Summary and Next Steps**	Energetics *Reconvene in Main Room*
3:25 PM	**Closing Remarks**	NIST
3:30 PM	**Adjourn**	

Workshop 2

NIST Workshop on Digital Twin Ecosystems

Virtual Zoom Meeting
January 14, 2025

Time	Purpose	Presenter
11:00 AM	**Welcome and Administrative Notes**	Energetics
11:05 AM	**NIST Introduction**	NIST
11:15 AM	**Keynote Address** ***An Exploration of the Digital Twin Ecosystem*** *Q/A to follow*	**Greg Porter** Principal Solutions Architect, Sev1Tech
12:05 PM	**Expert Panel** ***Digital Twin Ecosystem Examples*** *Q/A to follow*	**Rocco Cappiello**, Vice President, Business Development, Altair **Dr. Keyhoon Ko**, CEO and President, VMS Global **Vítor Lopes Pereira**, Regional Sales Manager, Systems & Digital Twins, Ansys **Dr. Gan Wang**, Vice President, Systems Engineering Ecosystem, Dassault Systèmes
1:30 PM	**Breakout Session Logistics**	Energetics
1:35 PM	**Breakout Session** ***Digital Twin Ecosystem Components and Interoperability***	*Breakout Rooms A, B, C, D*
3:05 PM	**Workshop Summary**	Energetics *Reconvene in Main Room*
3:20 PM	**Next Steps**	NIST
3:25 PM	**Closing Remarks**	NIST
3:30 PM	**Adjourn**	
11:00 AM	**Welcome and Administrative Notes**	Energetics
11:05 AM	**NIST Introduction**	NIST

Workshop 3

NIST Workshop on Digital Twin Trust, Verification, and Security

Virtual Zoom Meetings

May 27, 2025

Day 1: Verification, Validation, and Trustworthiness Foundations

Time	Purpose	Presenter
11:00 AM	**Welcome and Administrative Notes**	Energetics
11:05 AM	**Opening Remarks:** The Importance of Trust in Digital Twins	NIST
11:15 AM	**Keynote Address** Verification, Validation, and Uncertainty Quantification (VVUQ) to Enable Trustworthy Digital Twins	**Sankaran Mahadevan** Vanderbilt University Professor
11:45 AM	**Breakout Session 1: Defining Digital Twin Trustworthiness** *(What attributes define trust? How do we measure it?)*	Facilitated Discussion
12:30 PM	**Breakout Session 2: Verification & Validation (V&V) as a Trust Enabler** *(How can V&V methodologies strengthen trust?)*	Facilitated Discussion
1:00 PM	**Thank You and Adjourn**	NIST

May 28, 2025

Day 2: Cybersecurity & Trust Assurance for Digital Twins

Time	Purpose	Presenter
11:00 AM	**Welcome and Administrative Notes**	Energetics
11:05 AM	**Opening Remarks:** Cybersecurity & Digital Twin Risk Management	NIST
11:15 AM	**Keynote Address** Trust but Verify: Cybersecurity Challenges for Digital Twins	**Steve Lu** CEO of Stealth Software
11:45 AM	**Breakout Session 3: Cybersecurity Challenges & Trust Artifacts** *(What security measures and trust artifacts should be required?*	Facilitated Discussion
12:30 PM	**Breakout Session 4: Evidence-Based Trust** *(What Standards Should Govern Digital Twin Trustworthiness?)*	Facilitated Discussion
1:00 PM	**Thank You and Adjourn**	NIST

Appendix B. List Abbreviations and Acronyms

AI
Artificial Intelligence

API
Application Programming Interface

ASME
American Society of Mechanical Engineers

ASTM
ASTM International (formerly American Society for Testing and Materials)

CEO
Chief Executive Officer

CSF
Cybersecurity Framework (NIST)

CTO
Chief Technology Officer

DNV
Det Norske Veritas (assurance/standards body)

DTC
Digital Twin Consortium

FERPA
Family Educational Rights and Privacy Act

FMI
Functional Mock-up Interface

FMU
Functional Mock-up Unit

GM
General Manager

HIPAA
Health Insurance Portability and Accountability Act

HPC
High Performance Computing

IEC
International Electrotechnical Commission

IEEE
Institute of Electrical and Electronics Engineers

IP
Intellectual Property

ISA
International Society of Automation

ISO
International Organization for Standardization

IT
Information Technology

ITU
International Telecommunication Union

JSON
JavaScript Object Notation

LMS
Learning Management System

MAGS
Multi-Agent Generative Systems

MBSE
Model-Based Systems Engineering

MOC
Management of Change

MQTT
Message Queuing Telemetry Transport

NCSC
National Cyber Security Centre (UK)

NIST
National Institute of Standards and Technology

OPC-UA
Open Platform Communications Unified Architecture

OT
Operational Technology

QIF
Quality Information Framework

ROS
Robotics Operating System

SCADA
Supervisory Control and Data Acquisition

SMM
Small and mid-sized manufacturers

STEP
Standard for the Exchange of Product Model Data

VVUQ
Verification, Validation, and Uncertainty Quantification

ZMQ
ZeroMQ (universal messaging library)