SANDIA REPORT
SAND2023-09884
Printed October 2023

Sandia National Laboratories

Evaluation of Digital Twin Modeling and Simulation

Andrew S. Hahn, Jenna deCastro, Minami Tanaka, Christopher Lamb

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

A digital twin has intelligent modules that continuously monitor the condition of the individual components and the whole of a system. Digital twins can provide nuclear power plants (NPP) operators an unprecedented level of monitoring, control, supervision, and security by contributing a greater volume of data for more comprehensive data analysis and increased accuracy of insights and predictions for decision making throughout the entire NPP lifecycle. NPP operators and managers have historically relied on limited, second hand or incomplete data. With proper implementation, digital twins can provide a central hub of all intel that allows for a multidisciplinary view of an NPP. This equips operators and managers with the ability to have more information, context, and intel that can be used for greater granularity during planning and decision making. Digital twins can be used in many activities as the technology has many different concepts surrounding it. From the various definitions of a digital twin within the industry, digital twins can be differentiated by levels of integration/automation. The three main models include digital model, digital shadow, and digital twin. Digital twins offer many potential advancements to the nuclear industry that could reduce costs, improve designs, provide safer operation, and improve their overall security.

ACKNOWLEDGEMENTS

This research was funded by the U.S. Department of Energy Office of Nuclear Energy Cybersecurity research and development program under milestone M3CT-23SN1104045.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

Digital twins have a long history in industry with the concept first being introduced over fifty years ago and have long been presented as a valuable tool across industries. For the purposes of this report, digital twins are being defined as a high-fidelity digital replica of a device, process, or asset. Digital twins enable better analyses and operational predictions in addition to optimizing processes. However, for digital twins to be truly useful, they require a one-to-one correspondence with the item being modeled. The nuclear industry is interested using digital twins for the reasons stated above but is somewhat cautious to do so because of the one-to-one replication required. Digital twins are a novel advancement in modeling and simulation and are therefore attractive to high consequence industries as they provide a viable means to reduce risks. This report provides a detailed analysis of current digital twin implementations in other industries, digital twin use cases within nuclear power plants, risks arising from an expanded attack surface, and a review of the security mechanisms associated with each use case.

ACRONYMS AND TERMS

Acronym/Term	Definition
AI	Artificial Intelligence
AR	Advanced Reactor
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BP	British Petroleum
DCS	Distributed Control System
DCSA	Distributed Control System Architecture
DT	Digital twin
GE	General Electric
IAEA	International Atomic Energy Agency
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ML	Machine Learning
NASA	National Aeronautics and Space Administration
NPP	Nuclear Power Plant
O&M	Operations and Maintenance
OT	Operational Technology
PDE	Partial Differential Equation
UQ	Uncertainty Quantification
V&V	Verification and Validation

1. INTRODUCTION

Digital twins are hardly a new concept, depending on which resource is being consulted. Some publications state that digital twins were developed by the National Aeronautics and Space Administration (NASA) in the 1960s following the Apollo 13 accident [1, 2]. Others state that digital twins were created by Dr. Michael Grieves in 2002 [3, 4], or that the Defense Advanced Research Projects Agency is responsible for originally conceiving the digital twin concept [5]. Ultimately, it is fair to assume that NASA is responsible for introducing the concept of a digital twin when they built physical duplicates to match the systems they had in space. However, the recent, and rapid, development of modern technology like the Internet of Things (IoT) enabled the development of the truly digital twin which Grieves proposed [3, 6].

Initially, a digital twin was defined as a "set of virtual information constructs that fully describes a potential or actual physical manufactured product from the micro atomic level to the macro geometrical level" [3]. Put more simply, a digital twin is a high-fidelity digital replica of an asset, either a device, process, or structure [7, 8] that uses both historical and real time data [9, 10] that allows for analyses, predictions, and operation optimizations throughout the lifecycle of the asset. One group of authors identify three levels of digital twins: (1) Partial–in which the digital twin connects to limited data sources or sensors for basic devices to capture key metrics; (2) Clone–this level contains all data and measurements from multiple sources for an asset; and (3) Augmented–this digital twin enhances collected data with data from outside sources or intelligence, which is extracted through a data analytics engine and may use machine learning algorithms. Regardless of which level is being implemented, a functional digital twin requires the model of the physical object, data from that object, a one-to-one correspondence with the object, and the ability to monitor the object. The elements of control and analytics are optional depending on use case [10].

There is a common perception that digital twins have numerous benefits such as reducing costs, reducing risk and design times, reducing complexity and reconfiguration time, improving efficiency, improving maintenance decision making, improving security, improving safety and reliability, and improving processes and tools. Most importantly though, is that there are few realworld implementations that can validate these assumptions [11]. Despite this, digital twins are presented as a valuable tool for industries. The interest in their use for nuclear applications is gaining traction, but the nature of nuclear is highly conservative for good reason. Digital twins, as a technology, must be evaluated for the risks they present to the plant before any consideration can be made about the potential benefits they could produce. Furthermore, there remains a need for a better understanding of the current state of digital twin technology, understanding how regulatory guidance could relieve technical issues, and understanding of the development of the necessary infrastructure to support regulations [12].

This page left blank

2. CURRENT IMPLEMENTATIONS AND INDUSTRY USE CASES

Currently, there are few implementations of digital twins within the nuclear industry and even fewer that have been published about. Other industries, however, have been implementing digital twins in a variety of ways while many researchers have sought to understand theoretical applications that may one day become reality. For example, aircraft engine manufacturers are using digital twins to simulate engine fleets for monitoring their operation(s). By using digital twins to monitor fleet operations, manufacturers can optimize flight operations and maintenance, which ultimately lowers costs. Furthermore, the digital twins are used for automated anomaly detection to isolate and identify faults. Unfortunately, for the purposes of this report, the models that the manufacturers use are proprietary and further details have been withheld [13].

Another digital twin use case was created and used to bolster aircraft health monitoring. Traditionally, monitoring aircraft safety is done through a combination of deterministic physics models and ground inspections to track and record potential fatigue damage. In this case, the digital twin was designed to allow researchers to study the growth of cracks along the leading edge of the airplane's wing without having to waiting for a crack to develop to study. This digital twin was ultimately found to decrease the amount of time needed for a diagnosis and more effectively predict crack growth for future prognoses. At the time, the authors believed that the United States Air Force was investigating the use of their proposed digital twin model for both legacy and new aircraft to lessen maintenance related costs and aircraft downtime [14]. In the same vein, another digital twin was built to support aircraft fleet maintenance and incorporated the maintenance history, other aircraft data, and an on-board health management system to supplement the digital twin's results. Ultimately, this digital twin was able to perform incredibly accurate fault diagnosis without first initiating any form of damage to subsequently study [15].

Besides studying aircraft maintenance, the U.S. Airforce has also employed digital twins to protect the United States' critical infrastructure in space, namely to secure satellites from cyberattacks. Because satellites must be protected to the same extent as other critical assets on the ground, cybersecurity must be implemented into every level of the satellite's lifecycle, however, the remote location of the satellite necessitates the need for a digital twin to resolve complex issues. To address cybersecurity concerns, the U.S. Air Force partnered with Booz Allen to test global positioning system satellites to find vulnerabilities and craft protective measures. Booz Allen and the Air Force conducted a thorough model-based systems engineering review to construct an incredibly detailed digital twin of a Block Imaging Infrared Radiometer satellite. This digital twin was then connected to software-defined radios to emulate real radio frequency links to then simulate a control station, space vehicle, and man-in-the-middle attack. The digital twin was also used for Booz Allen to conduct penetration tests and attacks designed to gain control of radio links. Because of the digital twin, Booz Allen was able to go past the penetration tests to also recommend, and subsequently test, strategies for detecting and mitigating threats [16].

In other industries, General Electric (GE) uses digital twins to monitor, flag, and diagnose irregular engine behaviors as a means of early detection for possible engine failures. GE has also created digital twins that are enterprise scale to simulate system interactions that are complex and full-scale. These digital twins are designed for operators to test "what-if" scenarios and allow for investigations into key performance indicators and their impact on the highest probability scenarios being tested. Additionally, GE's digital twin can incorporate data such as weather, expected device performance, and other operations into scenarios to develop a robust understanding of how different elements can impact the overall enterprise [10].

Much like digital twins are being used in the aerospace industry to test "what-if" scenarios, they are being used by the oil and gas industry for the same purpose. British Petroleum (BP) uses a digital twin program called APEX, which is a simulation and surveillance system developed to test "what-if" scenarios in addition to optimizing daily operations. APEX is also used to detect irregularities within BP's wells, flow regimes, and pressures. In one situation, an APEX simulation was used to inform shutdown procedures when a pipeline required maintenance and oil flows needed to be rerouted. BP's engineers state that the use of APEX in this situation protected the flow of oil and enabled the efficient delivery despite pipeline maintenance because engineers used data gathered from the simulation to adjust flow routes and speeds [17].

Outside of the aerospace and oil and gas industries, digital twins have been used in the health industry as well. Unsurprisingly, because of the COVID-19 pandemic, researchers were prompted to find methods to safely assess patient health with the added challenge of doing so remotely. Researchers designed and tested a digital twin, based on both the IoT and internet of robotic things to enable an environment in which medical practitioners could conduct remote health monitoring of their patients. This version of a digital twin is still in its infancy but is indicative that digital twins are beneficial across many different industries [18].

3. NUCLEAR USE CASES

Simulation and modeling have been core tools for nuclear power since the advent of digital computing. It is natural for the nuclear industry to adopt novel modeling and simulation advancements; being a high consequence industry, any potential risk reduction avenue is of significant interest. Simulating processes and design elements allow designers to make informed engineering decisions before resorting to expensive physical tests. These digital models in the past were typically limited in fidelity or to a single element or system, due in part to computational limitations. As computational capacity costs decrease and simulation methods advance, the nuclear industry has been advancing more integrated simulations and models. Digital twins are the culmination of this advancing simulation capability, intending to be full-scope digital representations of physical systems.

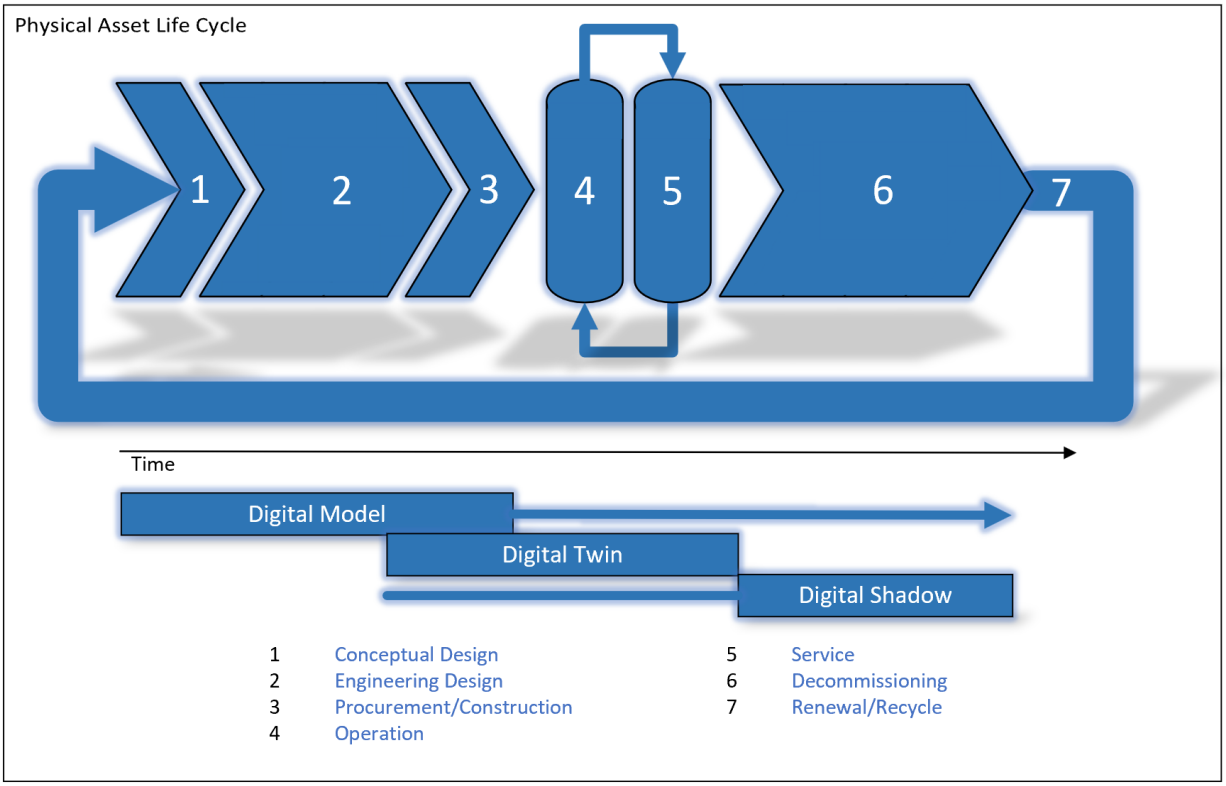

Figure 1. Physical asset life cycle phases, associated lifetimes, and activity of the digital model, twin, and shadow[1] [19]

The novelty and genericism of digital twins lend to a loose definition and plethora of use cases. It is perhaps best to describe the spectrum of digital twin applications in the context of the Nuclear Power Plant (NPP) lifecycle. Generally, this breaks down to three operational phases: design and commissioning, operation, and decommissioning. In each phase the digital twin fulfills different roles and consequently may have a different construction. Kochunas & Huan offer an interpretation of how digital twins interact with the lifecycle of a nuclear power plant and describes three distinct digital representations of the plant as shown in Figure 1. The digital model, digital shadow, and digital twin taxonomy purports that only one of these is the true digital twin, yet some in the

[1] The width of these lifetimes indicates level of interaction with the digital object.

industry would contend that each of these is a type of digital twin [20]. It is useful for the purposes of a complete understanding of digital twin use cases in the nuclear industry to use these definitions despite the debate on what constitutes a true digital twin.

Researchers from Germany had proposed a framework for cyber-physical digital twins and claims that a digital twin could be interfaced with the real world in "an elegant programming architecture" allowing simulations to to be evaluated against real world observations leading to subsequent improvements within the physical world [21]. Many design flaws can be easily rectified through the insights generated by a digital twin. Depending on the consequential concerns, system verifiability needs, availability requirements, and monetary resources of a NPP, different implementations of a digital twin representation of the physical plant are available to satisfy different needs. The needs of a physical plant must align with the level of automation provided by the selected digital twin as shown in Figure 2.

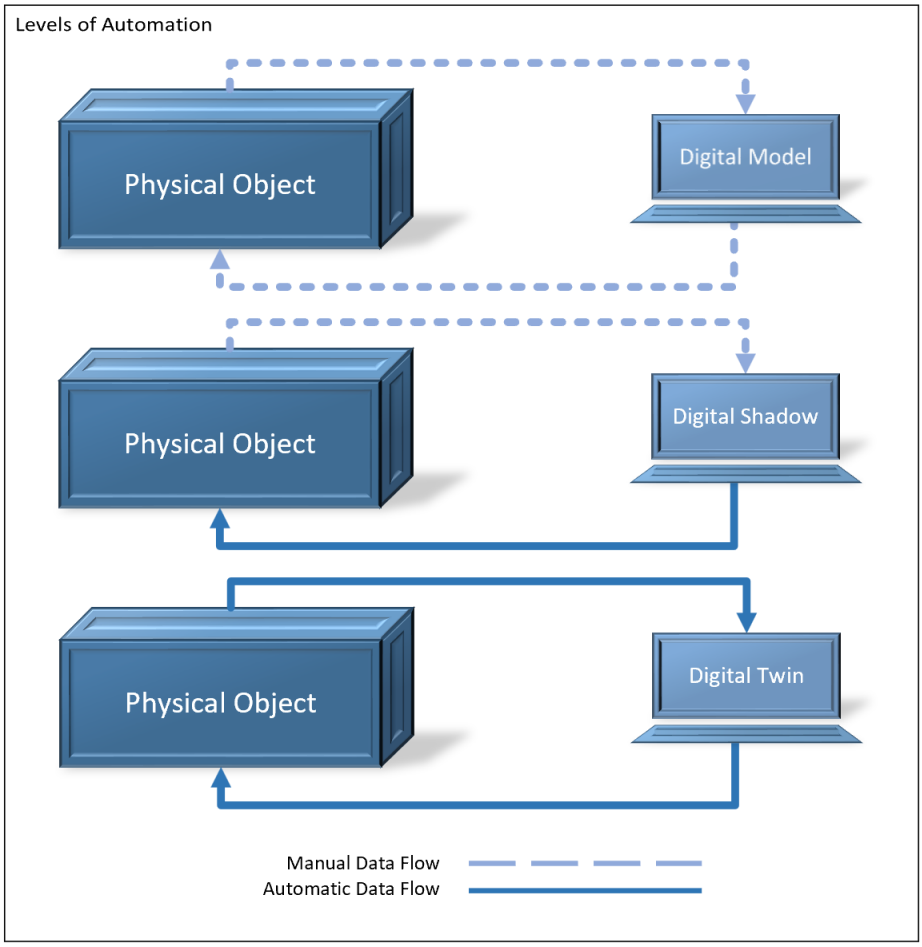

Figure 2. Digital model, shadow, and twin levels of automation [22]

Future nuclear system design can be virtually prototyped based on the actionable inputs of the virtualized digital twin and production processes can be significantly optimized to bring in as much needed efficiency. Production customization, configuration, and composition can be quickly accomplished in an agile manner with the constant inputs of the digital shadow. And the next version of the nuclear system can be improved with a greater understanding of system expectations

and operations of the digital model. Considering all challenges and advantages, effective deployment of a digital twin can be multifaceted, with a digital model being a manually configured cyber digital twin, a digital shadow used for monitoring/predictive maintenance, and a digital twin for a fully bi-directional automated deployment for NPP system advancement.

3.1. Digital Model

Nuclear designers have long been using modeling as a design aid for developing their NPP and their importance has grown with their complexity and fidelity. Neutronic, thermohydraulic, mechanical, and electrical models are conventionally independent, but integrated full-scope simulations to provide powerful insights. These are somewhat idealized models that are not necessarily based on any physical asset, which is what distinguishes this category as unique. This represents the many of the existing modeling and simulation tools in nuclear engineering, such as MCNP, RELAP, MOOSE, and MELCOR. The focus is fidelity; Monte Carlo, Computational Fluid Dynamics and Finite Element Analysis provide exceptional fidelity at the cost of computational demand. Real-time solutions are not feasible for these iterative solution methods, but the dynamics of real-time operation are highly valuable to a wide genre of design and engineering interest.

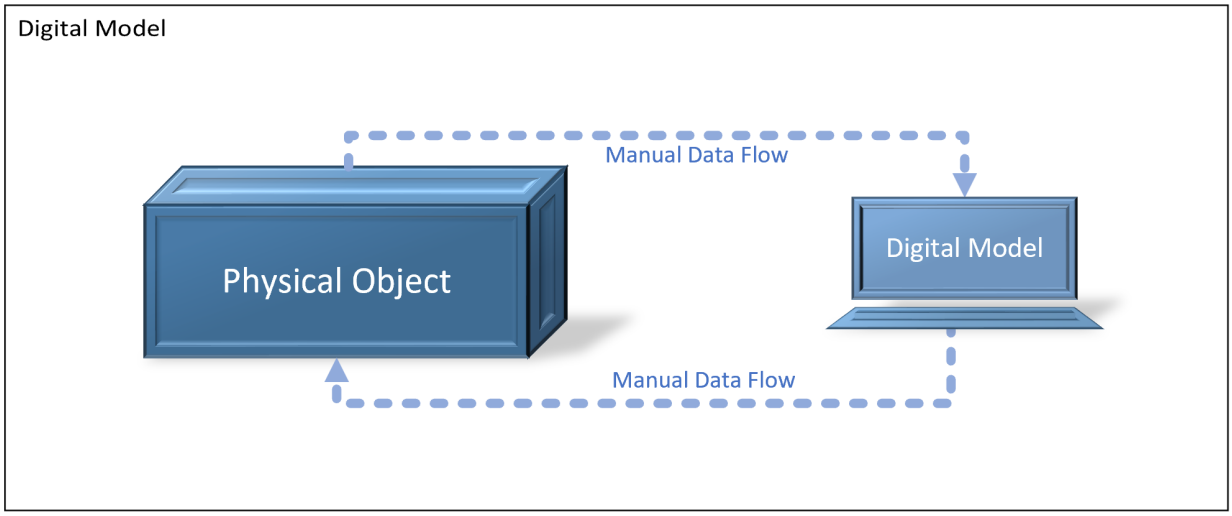

Figure 3. Digital model data flows [22]

As advanced reactor designs have become increasingly focused on multiunit Small Modular Reactor concepts and integration with renewable energy sources, the real-time control system dynamics have become more important to study [23]. Multiple heat source management, grid dynamics, load following, and combine control rooms are novel development for nuclear power and require the introspection offered by real-time dynamic models. Advanced control system design is aided by these types of simulations for Verification and Validation (V&V) and critical to cybersecurity research and design [24, 25]. Control system components are inherently real-time, so simulations must be real-time to interface with them. To reduce the computational time for each timestep to match or exceed real-time costs model fidelity but enables use cases valuable during operation of the physical plant.

Digital models of a NPP allow for system integration. Through 3D NPP visualizations on a virtualized system level, the digital model can verify constraints such as the spatial footprint and within physical connections. By connecting to a digital model, a wide range of interactions can be

simulated and manually maintained as seen in Figure 3. These interactions include data transfer, control functionality, analyzing mechanical and electrical behaviors, and simulating incident response procedural scenarios. The integration effort on-site and the associated downtime for the customer or partner is significantly reduced with a digital model. Use cases for digtial models can be found in Table 1.

Table 1. Digital model use cases

Use Case	Description
Design & Engineering	A digital model identifies complex design problems, provides a sandbox to conduct operational failure analysis, and anticipates production issues. Through experimentation using a digital twin (DT) model, innovative designs can be developed, and operations can be maximally optimized.
Verification & Validation	A digital model determines if a physical system or component satisfies its operational and system-level requirements through V&V. System requirements are established to provide adequate direction for engineers to ensure quality assurance during the developmental stage of the physical asset's life cycle.

3.2. Digital Twin

The line between a digital model and twin can be understood through the relationships they have with data flows regarding the physical system they represent as shown in Figure 4. The digital twin is a closed loop model, where information is automatically exchanged between it and the physical system allowing it to update its calculation parameters and predictions [19]. A shadow or model requires some measure of human interaction to modify its state and/or influence on the operations of the physical plant whereas the digital twin's ultimate purpose would be to automatically interact with the physical plant to perform a function. A plethora of perspective uses have been identified by academia and industry that vary in their direct influence on the plant.

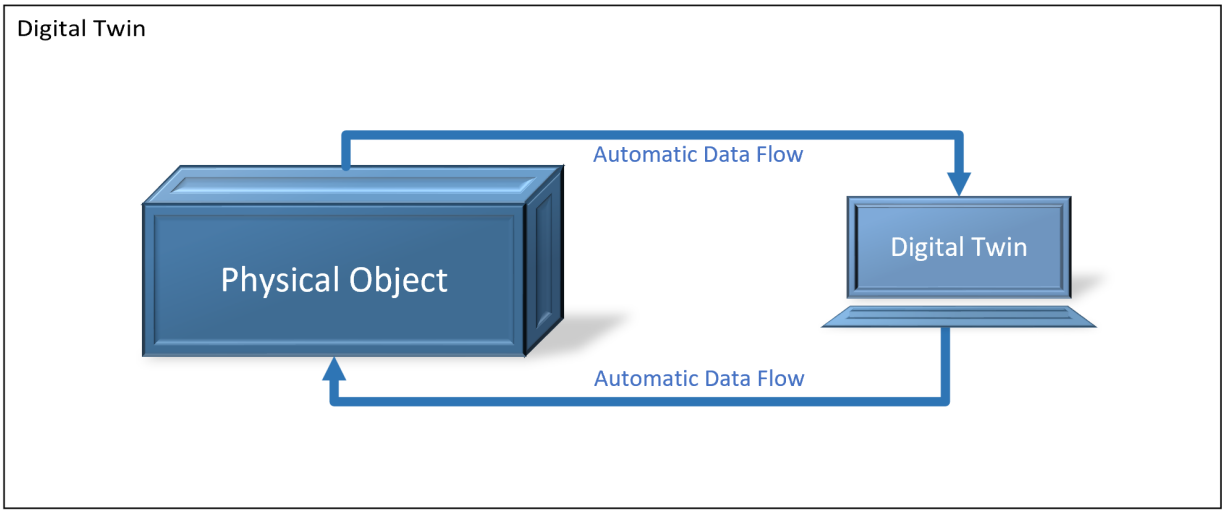

Figure 4. Digital twin data flows [22]

Sensor data, when gathered and aggregated, can give consolidated and accurate details on the prevailing state of the physical system. Additionally, the sensor and state data can be combined with

historical data to facilitate predictive analytics to extract functional as well as non-functional aspects of the physical machines. Human operators are empowered with advanced introspection to ensure the longevity and productivity of the nuclear power plant. A digital twin allows automated collection of various information across the physical asset's complete lifecycle and analyzes it to promote better system design, improve quality management, create high-performance systems, offer connected informational/operational intelligence, streamline diagnostics, provide predictive maintenance, and create opportunities for future smart control systems.

When paired with machine learning (ML) or artificial intelligence (AI), the digital twin can become a powerful control system with predictive capabilities [26]. A digital twin in association with data analytics and algorithms can generate insights that can be leveraged to produce premium and breakthrough services. With ML/AI, these devices can be self-managing, diagnosing, healing, learning, etc. Not only can the digital twin provide the training data for ML/AI, but it could also be used to by the ML/AI to determine the best control actions for optimal plant performance. This could provide a truly autonomous reactor control system and reduce or eliminate the need for an operator. This capability would be valuable for remote community deployment and integration with renewables by automatically predicting grid conditions and needs. The current perspective on these use cases is that they are immature and that their enabling technologies need further research and development to be viable from a regulatory perspective [27].

Continuous monitoring of autonomous NPP data collected from the attached IoT devices including sensors, controllers, actuators, etc. has clear advantages for quality management when compared to the standard processes of randomized system inspections. Based on the collected data, the digital twin of the physical object can mirror every aspect of the production process to proactively identify where quality issues exist and originated. The production processes can also be fine-tuned to be as optimized and organized as possible with a digital twin prototype. To further add, the digital twin contributes to the process of aggregated data analysis to ascertain whether there is potential for improved processes to enhance the systems and allow them to operate at optimal performance. Use cases for digtial twins can be found in Table 2.

Table 2. Digital twin use cases

Use Case	Description
Autonomous Control Systems	A digital twin is a model-based autonomous engineering tool that can bring, with the integration of ML/AI, autonomy to NPP systems. The bidirectional automated data flows contribute to the capability to have unmanned systems with the ability to operate without human intervention.
Cloud Control Systems	A digital twin, as a cloud-based control systems (CCS), consists of controller methods and algorithms remotely placed in the cloud far from the physical NPP systems. The remote-control system has the same capabilities as a physical DT with the additional convenience, and safety benefit, of being remote.

3.3. Digital Shadow

Most use cases that are expected to be deployed in the nuclear industry are classified closer to digital shadows. Allowing automatic influence and operational changes to a nuclear power plant without human intervention is unacceptable in the current environment. Digital twin automated control systems for nuclear power are at a low readiness level. A digital shadow automatically receives data from the physical system from which it can update its parameters and make predictions that inform

the actions of an operator. To relay the insights gained from the digital object back to the plant, a human must make the ultimate decision and manually make the operational change as shown in Figure 5. This paradigm is much more acceptable for designers, regulators, and control system vendors. The risk profile is substantially reduced and provides an opportunity to gain operational experience with digital twins.

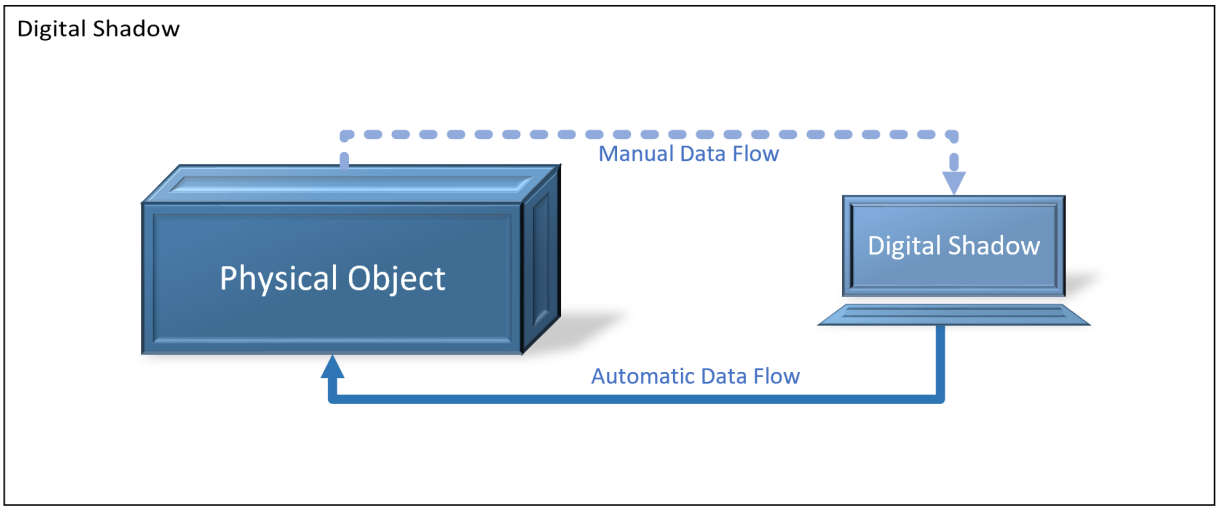

Figure 5. Digital shadow data flows [22]

Predictive maintenance stands to be the most readily deployable use for digital twins in the nuclear industry. Driving lower maintenance costs through predictive modeling makes predictive maintenance a popular use case across industry [9]. With the faster maturity and stability of machine and deep learning algorithms, predictive and prescriptive insights are being extracted in time and used for the longevity of equipment. Whether the equipment needs repair or continuous monitoring of its health condition and performance level, all the real-time and runtime information helps plan rational maintenance and reduce unplanned downtime. Digital twins can monitor connected products minutely for any threshold anomaly [13]. With the predictive analytics capability, digital twins can provide real-time alerts to move from reactive incident response to condition-based maintenance. A digital twin can analyze performance data collected over time and under different conditions. The knowledge acquired is particularly useful when maintaining any product intelligently. The combined analytics on both historical and runtime data supplies their quoted information to the administrator or operator when a component of a system needs to be repaired. Thus, data collection and deeper investigations of data heaps ultimately empower people to take a final call on the maintenance aspect. Nuclear power plants could have their maintenance costs significantly reduced by accurately predicting when components need replacing rather than relying on overly cautious maintenance schedules.

Digital twins are also being investigated for use in providing advanced anomaly detection useful for cybersecurity [28]. A digital twin is constructed to represent the network of a plant and would allow live comparisons and metrics to detect abnormal behavior. Security audits and software deployments could be done on the twin before the production equipment, reducing downtime and risk. Such a model could provide a testing ground for equipment modification and upgrades to ensure the design of the network conforms to the necessary cybersecurity requirements. Digital shadows connect ERP/MES systems to provide appropriate information toward increased operator productivity and

improved production quality. Observation of the digital shadow through a 3D nuclear system visualization can additionally provide ease in troubleshooting.

An important use case particularly valuable to the nuclear industry for the digital twin is in the opportunities presented in decommissioning. A twin or shadow that has collected operational data for the lifetime of the plant would be a valuable asset for future designs. This would be exceptionally valuable for material science digital twins to compare and validate models with destructive tests on plant components [29]. Materials science for nuclear energy is arduous, having a material digital twin that can be validated at decommissioning of the plant would provide insights on material behavior and performance in real operational environments. This could lead to operational life extensions for other plants and open a window for significant advancement of materials qualification for future plants. Digital shadows can aggregate and analyze data from different and distributed assets to provide unified real-time visibility and insight toward higher performance and quicker decision-enablement with greater confidence.

GE is implementing a variant of a digital twin as a sensor layer, similar to a digital shadow, referring to these systems as "digital ghosts." Digital ghosts can be used to secure not just the critical infrastructure but also the operational technology in an organization's data center. Like a digital shadow, the digital ghost has the capability to detect if something is not performing correctly and can identify the exact sensor that was compromised. That alone typically takes operators "days or weeks to pinpoint where the problem is. The digital ghost does that within seconds" [8] Typical OT cybersecurity is about analyzing network traffic, application security, endpoints, firewalls, etc. GE's digital ghosts focus more on how the underlying physical assets operate. GE's primary objective in creating this variant is to understand the "physics of what normal looks like, how do the controls normally operate these assets" [8]. With that knowledge and other simulated or historical data, developers "could build a really good representation of how an asset should be operating" [8]. Use cases for digtial shadows can be found in Table 3.

Table 3. Digital shadow use cases

Use Case	Description
Maintenance Prediction	A digital shadow allows for condition-based maintenance involving monitoring of equipment condition, performance, and regular baseline operations to reduce the chances of operational failure through automated unidirectional data flows.
Cyber Intrusion Detection	A digital shadow provides the ability to detect abnormal system activity through unidirectional data flow monitoring.

This page left blank

4. DIGITAL TWIN ATTACK SURFACE

Like "digital twin," "attack surface" is a somewhat contentious and evolving term useful for describing the risks of a digital system from which security measures can be distilled [30]. The concept has been developed with purely digital systems as the primary focus. The definitions offered do not account for two factors that are essential to evaluating the cyber risk of current state of digital twins: digital twins are cyber-physical systems; many are theoretical or have no example system to analyze. The unique nature, use cases, and development maturity of digital twin technology requires us to develop metrics for an attack surface that are relevant and actionable. Described below are metrics that can describe an approximate attack surface for digital twins. It is critical to note that these metrics are important, and centric, to digital twins only.

Consequence is the first dimension of the attack surface, which also implies the value of the target for adversaries. For a cyber-physical system, the risk of an attack must be measured by the consequence of system impact. The scale of this risk differs from a typical IT system, where data loss or theft may cause monetary, reputational damages, or indirect harm to human life. An attack on a cyber-physical system is a direct risk to human life or severe environmental damage. Borrowing and adapting the guidance from the International Atomic Energy Agency (IAEA) publications NSS 17-T and NSS 33-T [31, 32], we can define this in a scale of consequence in order of increasing severity:

0. **No consequence or negligible consequence**
1. **Limited consequences** – Degraded prevention, detection, and response capabilities to threats.
2. **Moderate consequences** – Causing an Anticipated Operational Occurrence, impact to plant performance.
3. **High consequences** – Design basis accidents, releases within authorized limits.
4. **Severe consequences** – Beyond design basis, unacceptable radiological consequences.

System Verifiability is a measure of how a system can be verified and the certainty to which it can reliably verified to operate in all conditions. This is beyond simply validating that the bytes have not changed, but ensuring that the system will operate as intended in and beyond the operational ranges it is expected to perform in. All systems of consequence must undergo V&V but how can advanced systems with a high degree of complexity and be properly tested? Below are four categories of verifiability listed by increasing uncertainty.

1. **Inherently verifiable –** Low complexity systems with limited functions e.g., analog system in a test configuration
2. **Verified by burn-in –** All operational conditions can be recreated in-situ or via emulation
3. **Diverse modeling and simulation –** Operational conditions cannot be replicated without modeling and simulation; extraordinary signals and data cannot produce unknown system state
4. **No verification possible –** Extraordinary signals and data can produce unknown system state

The attack surfaces of each use case for digital twins are discussed in the sections below. These require some discussion on the nuances for each. A complete understanding of the attack surface cannot yet be distilled in a series of concrete metrics, much of the information is qualitative. The

novelty of digital twin cannot be developed. With further development and standardization, a more solidified attack surface can be produced. Until a more concrete attack surface can be developed, it is difficult to determine specific tactics and techniques that facilities must defend their digital twins against. However, with the information provided in the sections below, paired with some basic operational assumptions [33], it is possible to give some examples of tactics that should be considered when assessing attack surface risks. These tactics are sourced directly from the MITRE Corporation's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. The ATT&CK framework is a knowledge base of matrices focused specifically on cyberattack behaviors that is across industries as well as by the federal government to develop robust threat models and methodologies [34]. The ATT&CK tactics listed in the sections below are some examples that must be considered but are not wholly representative of all tactics that comprise the attack surface.

4.1. Digital Model

Modeling and simulation are, currently, the most direct and current use of digital twin technology and share most of the same security issues of conventional modeling and simulation platforms. Designers rely on modeling and simulation to develop and test design decisions and safety systems. Errors and flaws in the design suites can precipitate into costly design revisions, or in the worst case, safety impacts. However, a single modeling tool does not dictate the ultimate design of safety components. Diversity of modeling is a key piece of determining these critical design decisions. These models are bounded to reality by validating them against experiments, benchmarking, and plant data [33]. This provides some inherent resilience to cyber-attacks, as single models are not trusted completely for critical safety determinations.

This regulatory guidance only applies to safety systems or systems important to safety, systems that fall outside are too numerous and would be too costly to perform this level of V&V. Digital twins present an additional potential issue in that some are not mathematically based models. Figure 6 shows a simplified process for developing and validating a simulation model of some physical phenomena that starts at developing a mathematical model. The mathematical model is a numeric quantification of a physics phenomenon that can be validated through experiment. This allows validation across all the domains of the simulation development cycle. Digital twins may use ML or AI methods that effectively bypass the mathematical modeling phase, converting sensor and actuator data directly into a simulator. This presents a major issue in quantifying the validity of such a digital twin as it breaks a critical link that bounds the simulation to a mathematically definable problem space.

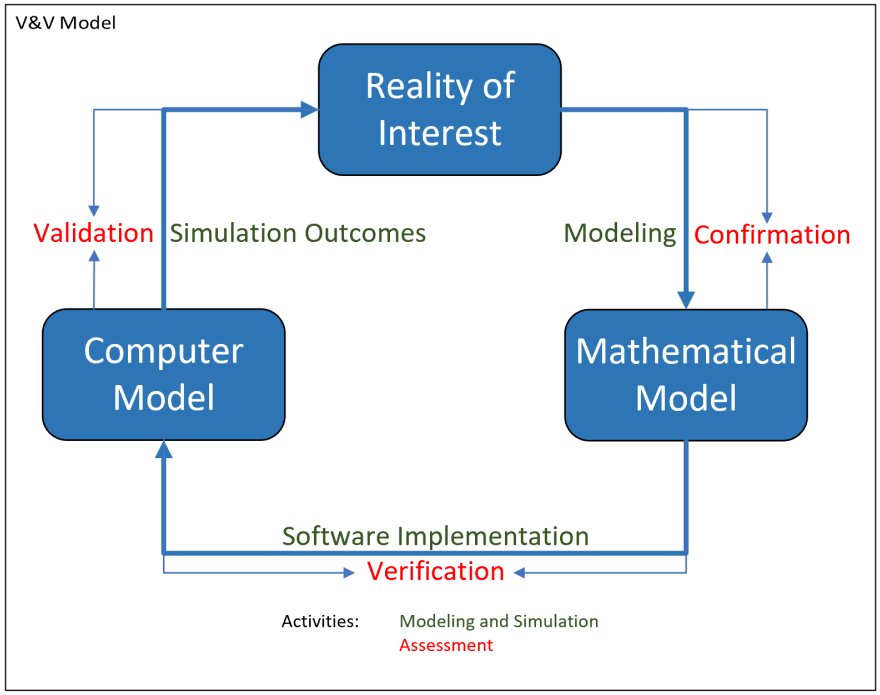

Figure 6. Simplified view of model V&V [34]

Conventional mechanistic simulation using mathematical models has known boundaries and defined behavior with any given input. An AI/ML digital twin may not have these definable boundaries and behavior. For a mathematical model, we can predict with certainty the response with each input over entire numeric fields. An AI/ML model is not necessarily deterministic and could treat each numerical value in a range differently. If we have a 32-bit float as the input to the AI/ML, there are 2^{32} possible values that may activate different solution pathways. As we increase the number of floating-point inputs the problem space exponentially increases. It becomes impossible to validate the behavior of an AI/ML model across such vast problem spaces where each combination of thousands of 32-bit or 64-bit values must be examined. Hidden attack methods that hide within this enormous problem space within AI/ML are being discovered and will continue to present serious issues to their use in safety related applications [35].

Digital twins present a major risk as sensitive information about a given plant is required and stored for the digital twin to operate properly. This is the case regardless of whether the digital twin is either a mechanistic model or an AI/ML model. Both methods produce exceedingly high-fidelity models of the plant and its systems, making it an ideal target for testing attacks and for theft of intellectual property. An adversary could use the digital twin to carefully craft an attack, either cyber or physical, to create the most significant impact with the least effort. If the digital twin contains the firmware or images of the industrial control system (ICS) components, malware could be constructed that perfects exploits against the plant equipment. If combined with a network architecture, a sophisticated cyber-attack can be developed and tested before deployment to the site.

Table 4. Digital model use case, consequence, verifiability and MITRE ATT&CK tactics

Use Case	Consequence	Verifiability
Design and Engineering	4 - Severe Consequence	3 – Mechanistic Models 4 – AI/ML
MITRE ATT&CK Tactic(s) **Execution** (TA0002) – Adversaries attempt to run malicious code using one of fourteen known techniques [36]. **Impact** (TA0105) – Adversaries use the Impact tactic to either manipulate, interrupt, or destroy industrial control systems. Any of the twelve techniques within this tactic can be used by adversaries to disrupt control processes or initiate attacks that have a long-term impact [37].		

4.2. Digital Twin

The concepts for cloud ICS and autonomous control are just beginning to gain research interest for nuclear applications. Both concepts present a similar attack surface as they will have a direct influence on the operation of the physical process. Each present a use case for digital twins; the cloud control system operates as an on-demand digital twin of a distributed control system (DCS) while autonomous control systems may use a digital twin as a reference model to predictive control. These use cases expose the control system to a direct route of influence from the digital twin. The avenues for adversary access are also greatly expanded by the implied operational cases for both. A cloud system is a highly networked system that is physically distant to the process it is controlling. Autonomous control implies remote operation or a reduced staffing requirement. Both require centralization of sensor data and actuator control [38, 39]. The risks of each are dependent on what systems are controlled and how centralized the control of the reactor is.

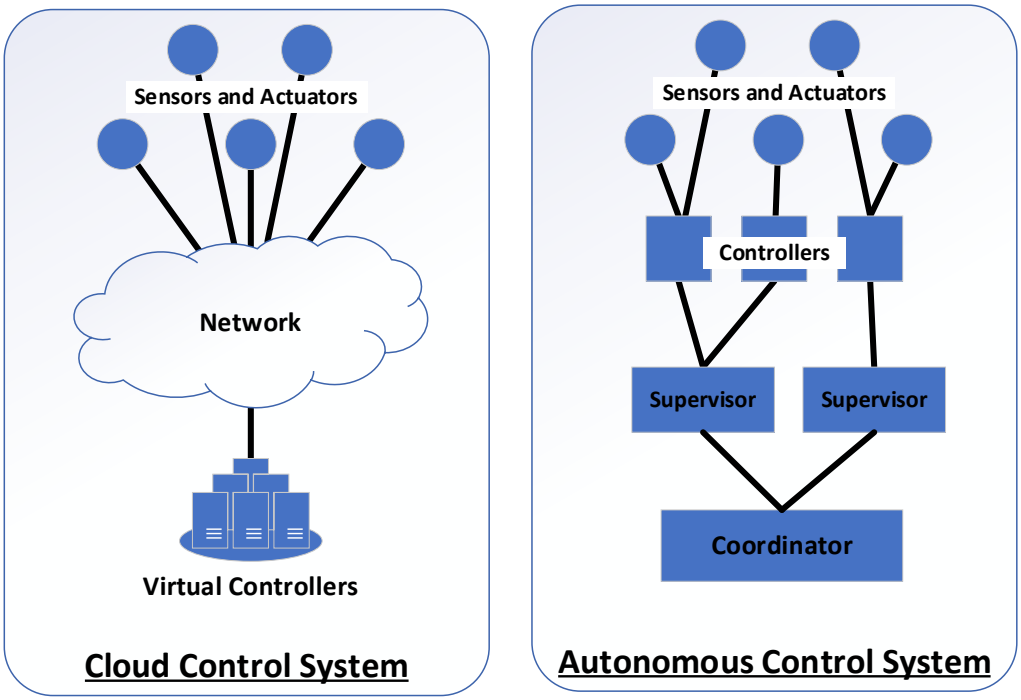

Figure 7. Comparison of Cloud and Autonomous Control Systems.

These systems interface directly with the control elements of the NPP and have a direct pathway to impact system operations. As shown in Figure 7, the control systems in these concepts become highly interconnected, which expands the potential impact an adversary can have by compromising any individual component. The supply chain risk also expands as these become complex systems demanding components and software from multiple suppliers and sources.

For a cloud control system, the potential consequence may be reduced or mitigated by allowing it to operate only those functions that cannot degrade the plants safety. For an autonomous system, separate safety systems or physical mechanism that can be assured to prevent any consequence of malicious operation may offer mitigative solutions. The consequence of malicious operation for both types of digital twin is high, but not severe assuming that they would not interact or substitute an independent safety system.

The verifiability of these systems is similar, especially for the cloud control concepts that use reference model control and AI/ML schemes. The digital twin reference model within the autonomous or cloud control system may be verifiable, but the AI/ML controllers cannot be readily verified as previously discussed. The exception to this would be cloud control systems that emulate a deterministic controller like current PLCs. This would be verifiable through in-situ testing and emulation of the process under control.

Table 5. Digital twin use case, consequence, verifiability and MITRE ATT&CK tactics

Use Case	Consequence	Verifiability
Autonomous Control Systems	3 – High Consequence	4 – AI/ML Control
Cloud Control Systems	2-3 – Moderate to High Consequence	4 – AI/ML Control 2 – Emulated PLCs
MITRE ATT&CK Tactic(s) **Command and Control** (TA0101) – Adversaries attempt to communicate with, and gain control of, compromised systems to gain access to the industrial control system environment [37].		

4.3. Digital Shadow

Maintenance prediction and operational anomaly detection are digital twin use cases that are already seen in commercial deployment. These uses can impart only a minimal risk to the safety of the plant because there is always a human in the loop. A cybersecurity network monitoring digital twin imparts a similar risk, though it is not mature enough for commercial deployment currently. These systems are diagnostic agents that provide predictions and analytics to aid the operation of an already commissioned plant. The predictions for operations and maintenance (O&M) cannot impact safety system design or operation. While the system may not be verifiable, it has no major consequence for malicious operation or failure.

The cybersecurity application may have a more serious impact if it fails, allowing malicious actors to go undetected on the network. This would constitute a degradation of the plants ability to detect and prevent cyber-attacks, thus the consequence would be in the limited category. The more serious threat would be as a pivot point for adversaries. This generally applies to all digital twin technologies as we are adding a new complex digital system to the OT environment, but this becomes more of a primary concern to the digital twin use cases that cannot directly alter or impact the plant operation.

Table 6. Digital shadow use case, consequence, verifiability and MITRE ATT&CK tactics

Use Case	Consequence	Verifiability
Maintenance Prediction	0 – Negligible Consequence	4 – AI/ML Prediction
Cyber Intrusion Detection	1 – Limited Consequence	4 – AI/ML Detection
MITRE ATT&CK Tactic(s) **Inhibit Response Function** (TA0107) – This tactic consists of fourteen techniques that adversaries can use to prevent or alter expected responses that may be initiated in the event there is a change within the ICS environment [37]. **Impact** (TA0105) – This tactic, and its associated techniques, can be used jointly with Inhibit Response Function where adversaries alter responses to provide a false sense of security to operators with the aim of obfuscating attack targets/goals [37].		

The lessons learned from the digital twin can then be applied to the real system. But if a digital model is affected by a cyberattack, any predictions are likely to be of questionable value, depending on data relevancy, interpretability, availability, and resulting data quality. The lessons learned would no longer be accurate and applying such lessons to the real system gives only a false sense of security.

5. SECURING DIGITAL TWINS

The concepts, uses, and architectures of digital twins are rapidly evolving making it exceedingly difficult to determine specific methods to secure them. The focus here will be to discuss gaps in the technology and general methods that can be used to secure the use of digital twins. It must be assumed that the software development, security, and validation guidance from the Institute of Electrical and Electronics Engineers (IEEE), the International Electrotechnical Commission, the U.S. Nuclear Regulatory Commission, and IAEA are a baseline consideration. This section will cover the gaps and methods that are unique or critical to securing Digital Twins especially the AI/ML variety. Mechanistic models do not present the same degree of opportunities and challenges to security though these recommendations will still enable greater security. Each DT technology category is linked to its greatest need for security, though each can benefit from these methods. Later these use case categories will be linked with the security methods that apply to them.

5.1. Digital Model – Verification

The core issue with digital twins across the board is verifying that they will operate correctly with expected results, most of all this critical for digital models. This plagues the mechanistic digital twin models just as much as their AI/ML counterparts. When highly coupled multi-physics problems like an NPP are modeled, coupling effects between PDE sets can cause instabilities and break downs in the solution validity [40]. How can a system as complex as a digital twin be verified to not have malicious behavior or simply dangerous unanticipated behavior? No security can be reasonably assured if we cannot distinguish between benign and malicious. AI/ML systems face greater challenges to this verification, which is an area of rapidly evolving research [41]. The fundamental frameworks for verifiable AI/ML have not yet been established. This is potentially the greatest issue that potential digital twin technology must contend with if they are to be used in safety or related to safety systems. This will likely only begin to be alleviated through standardization which will allow research resources to focus on a specific framework.

As a modeling and design tool, it will be critical to verify the accuracy of the tool especially as nuances of systems are being studied and used digital twins for them to make design decisions. The final designs will need to be verified through diverse modeling, simulation, and experimentation but that is not exceptionally different from conventional design processes. When design decisions are based on modeling that cannot be experimentally proven due to danger or expense, the validity of models becomes a safety issue. Maintenance prediction and cybersecurity may not require exceptional verification to provide useful benefits to NPPs. Even if autonomous systems have a fully verifiable DT model, it is not protective for unexpected conditions or malicious inputs. What these uses require or will benefit from is quantifying the uncertainty of the digital twin.

5.2. Digital Twin – Uncertainty Quantification

In a similar track to verification, uncertainty is an issue that needs to be quantified to allow digital twins to be valuable decision-making tools. This is critical for digital twin use cases where the twin will inform or direct action on the control system. Without knowing the uncertainty around the predictions of a digital twin, it is impossible to determine how much trust to put into its conclusions. Overconfidence in prediction can be disastrous especially when confronted with adversarial inputs [42]. Producing reliable Uncertainty Quantification (UQ) will be critical to starting to deal with adversarial actions against digital twins and all AI/ML models. Without a method to measure the real confidence of a predication from a digital twin, no derived action can be assured not to be malicious.

Uncertainty Quantification is a broad topic and area of research that will be a core piece of enabling digital twin verification. Improving the accuracy of digital twin models will require knowing how much uncertainty exist and where that uncertainty stems from [43]. When AI/ML control systems reference a digital twin for control prediction, they will also require a UQ to assess the safety or surety of a control action [44]. There exist some solutions for UQ in digital twins, but these suffer from large computational overhead and consequently struggle to meet the real-time operation necessary for most digital twin applications [19]. There are also lingering questions of uncertainty within UQ of digital twins considering the precision and accuracy of the information the digital twin was based on.

5.3. Digital Shadow – Integrity Mechanisms

The inputs to digital twins in the form of training models and real-time process data have significant influence on the system. This is most important to digital shadows that rely on data captured to inform correct predictions and recommendations. Unauthorized modification or destruction of data/operations while being processed, in transit or in storage must be prevented. The integrity of the system itself must be maintained to preserve confidence in the reliability and safety of the system operation. Preserving the system integrity is also essential to ensure non-repudiation and authenticity of commands/actions the system which are essential in its secure operation and support incident response capabilities.

Secure communication protocols are critical between the digital twin and its physical counterpart, challenging current technology deployments especially in real-time operation. An adversary affecting a digital twin, or its physical representation can introduce divergence in the behavior or state. Given the bi-directional link between the two an attacker may negatively affect both through changes in either. The challenge here is if the digital twin is used to drive system evolution and maintenance such as in Digital Shadows, it can result in malicious changes made to the digital twin being propagated to its physical counterpart. Similar concerns are present when implementing digital models, albeit in more restricted form due to their reduced integration.

Data integrity methods will be critical to all DTs as their data, training data, and historical data define their operation. Alteration of the data in a DT can result in potentially undefined behavior or if the adversary is sophisticated enough, precise malicious behavior [45]. This will be exceptionally difficult as the training data sets can be enormous, and the integrity of ever-increasing historical data will need to be maintained. The mechanisms that could detect and prevent integrity attacks are more novel and evolving than the AI/ML they are attempting to protect. For digital shadows, Zero Trust Architecture may provide the integrity mechanisms necessary to ensure reasonable protection. digital twins that may control or directly influence the physical operation of a plant may need to rely on physical safety mechanisms to ensure sufficient risk reduction.

5.4. Passive and Inherent Safety

Advanced Reactor (AR) designs were pursued with a core key interest: prevent accidents through physics rather than active systems. If staff can assure that the actions of the control system cannot cause harm to the public or environment, digital twin technology can gain significant leeway. Even if sensitive areas of a plant exist, if a digital twin implementation can prove to not have any possible impact to plant safety, the issues presented can be negated. Probabilistic risk assessment, systems theoretic process analysis, and other advanced analysis methods could define control functions of the plant where digital twins could be used for cost reduction and experience building. Implementing digital twins in practice will provide key feedback to implementing good design

elements and solid frameworks that lead to standardization, one of the critical necessities to formalizing validation schemes.

Physical and physics-based safety may be the only risk reduction technique that could allow digital twin use in the NPP environment. The exceptional risk presented by making highly accurate models of an NPP's digital and physical defenses can only be moderated if there is no reasonable pathway to consequence to the public. It cannot be expected that adversaries will never retrieve a digital twin of an NPP if one is created. If it documents a flaw in the safety or security systems and allows the adversary to experiment with methods to exploit that flaw, then the risk of NPP digital twin's existing is extreme. At the same time, digital twins will play an important role in the design of ARs and eliminating such flaws. Validating that digital twins are accurate representations of reality will be critical to eliminating design flaws that could make digital twins a significant threat in the first place.

5.5. Application to Use Cases

Each use case has a central issue in its attack surface that informs the most critical mechanisms to secure that use case, but these are not the only applicable security mechanisms. Use cases in each category of digital twin are presented below with the security mechanisms that are important to them. These security mechanisms are ordered by the greatest to least impact for the use case.

Table 7. Use cases and important security mechanisms

Use Case	Security Methods	MITRE ATT&CK Tactic
Design & Engineering	Verification Uncertainty Quantification Integrity	Execution (TA0002), Impact (TA0105) See Table 4
Validation & Verification	Verification Uncertainty Quantification Integrity	Execution (TA0002), Impact (TA0105), Command and Control (TA0101), Inhibit Response Function (TA0107), Impact (TA0105) See Table 4, Table 5, and Table 6
Autonomous Control Systems	Uncertainty Quantification Passive and Inherent Safety Integrity Verification	Command and Control (TA0101) See Table 5
Cloud Control Systems	Passive and Inherent Safety Integrity Verification	Command and Control (TA0101) See Table 5
Maintenance Prediction	Integrity Verification Uncertainty Quantification	Inhibit Response Function (TA0107), Impact (TA0105) See Table 6
Cyber Intrusion Detection	Integrity Uncertainty Quantification Verification	Inhibit Response Function (TA0107), Impact (TA0105)

Use Case	Security Methods	MITRE ATT&CK Tactic
	Passive and Inherent Safety	See Table 6

6. CONCLUSION

Digital twins have a long history as being valuable modeling and simulation tools across industries dating back to the 1960s. They are a high-fidelity digital replica of a device, process, or asset that permit better analyses and operational predictions in addition to optimizing processes; regardless of what is being replicated. They are particularly important as they continuously, and simultaneously, monitor the condition of individual components as well as the whole system. For these reasons, digital twins provide NPPs with an increased level of monitoring, control, supervision, and security across use cases from digital models to digital twins and digital shadows. They also create opportunities for operators to have more accurate insights and predictions into NPP operations throughout the entirety of the plant's lifecycle. Their implementation can reduce costs, improve designs, increase plant safety, and enhance facility security.

However, despite these inherent benefits, there are still reservations regarding fully embracing the use of digital twins within the nuclear industry because of the one-to-one digital replications that serve as attractive targets to adversaries. There are three models and their subsequent use cases that are applicable to the nuclear industry: (1) digital models, (2) digital twins, and (3) digital shadows. Each of these use cases present their own challenges to an NPPs attack surface and are attractive targets if they are not properly implemented and secured. These issues should not dissuade continued and vigorous exploration of digital twin technologies in the nuclear field but serve as goals and milestones to achieve. Nothing presented disqualifies the use of this technology in NPPs which may be one of the industries with the most to gain. Modeling a nuclear power plant in real-time and making accurate predictions of its future state is so exceptionally valuable, it demands further investment.

REFERENCES

[1] S. Ferguson, "Apollo 13: The First Digital Twin," Siemens, 14 April 2020. [Online]. Available: https://blogs.sw.siemens.com/simcenter/apollo-13-the-first-digital-twin/. [Accessed April 2023].

[2] B. D. Allen, "Digital Twins and Living Models at NASA," in *The American Society of Mechanical Engineers (ASME) Digital Twin Summit*, 2021.

[3] M. Grieves and J. Vickers, "Origins of the Digital Twin Concept," August 2016.

[4] IBM, "What is a Digital Twin," IBM, [Online]. Available: https://www.ibm.com/topics/what-is-a-digital-twin#:~:text=Michael%20Grieves%20(then%20on%20faculty,digital%20twin%E2%80%9D%E2%80%94in%202010..

[5] E. Glaessgen and D. Stargel, "The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles," in *53rd Structures, Structural Dynamics, and Materials Conference*, 2013.

[6] IEEE, *What Is a Digital Twin, Anyway?,* The Institute of Electrical and Electronics Engineers.

[7] S. Suhail, R. Jurdak, R. Hussain and D. Svetinovic, "Security Attacks and Solutions for Digital Twins," 2022.

[8] M. Korolov and A. Korolov, "The Cybersecurity Challenges and Opportunities of Digital Twins," 6 December 2022. [Online]. Available: https://www.csoonline.com/article/3682132/the-cybersecurity-challenges-and-opportunities-of-digital-twins.html#:~:text=If%20proper%20cybersecurity%20controls%20aren,and%20expose%20pre%2Dexisting%20vulnerabilities.. [Accessed February 2023].

[9] F. Tao, H. Zhang, A. Liu and A. Y. C. Nee, "Digital Twin in Industry: State-of-the-Art," *IEEE Transactions on Industrial Informatics,* pp. 2405 - 2415, April 2019.

[10] P. Raj and C. Surianarayanan, "Digital Twin: The Industry Use Cases (Chapter 12)," in *Advances in Computers, Volume 117*, P. Raj and P. Evangeline, Eds., Cambridge, MA: Academic Press, 2020, pp. 286-315.

[11] D. Jones, C. Snider, A. Nassehi, J. Yon and B. Hicks, "Characterising the Digital Twin: A Systematic Literature Review," *CIRP Journal of Manufacturing Science and Technology,* vol. 29, no. Part A, pp. 36-52, May 2020.

[12] V. Yadav, V. Agarwal, A. V. Gribok, R. D. Hays, A. J. Pluth, C. S. Ritter, H. Zhang, P. K. Jain, P. Ramuhalli, D. Eskins, J. Carlson, R. L. Gascot, C. Ulmer and R. Iyengar, "Technical Challenges and Gaps in Digital-Twin Enabling Technologies for Nuclear Reactor Applications," U.S. Nuclear Regulatory Commission, 2021.

[13] V. Zaccaria, M. Stenfelt, I. Aslanidou and K. G. Kyprianidis, "Fleet Monitoring and Diagnostics Framework Based on Digital Twin of Aero-Engines," in *ASME Turbomachinery Technical Conference and Exposition (GT2018)*, Oslow, Norway, 2018.

[14] C. Li, S. Mahadevan, Y. Ling, S. Choze and L. Wang, "Dynamic Bayesian Network for Aircraft Wing Health Monitoring Digital Twin," *American Institute of Aeronautics and Astronautics,* vol. 55, no. 3, Jan 2017.

[15] K. Reifsnider and P. Majumdar, "Multiphysics Stimulated Simulation Digital Twin Methods for Fleet Management," in *54th AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference*, Boston, Massachusetts, 2013.

[16] Booz Allen Hamilton, "Securing Space with Digital Twin Technology," Booz Allen Hamilton, [Online]. Available: https://www.boozallen.com/markets/space/securing-space-with-digital-twin-technology.html. [Accessed August 2023].

[17] BP, "Twin Win for Oil and Gas Production," BP, 3 October 2018. [Online]. Available: https://www.bp.com/en/global/corporate/news-and-insights/reimagining-energy/apex-digital-system.html.

[18] S. Khan, S. Ullah, H. U. Khan and I. U. Rehman, "Digital Twins-Based Internet of Robotic Things for Remote Health Monitoring of COVID-19 Patients," *IEEE Internet of Things Journal.*

[19] B. Kochunas and X. Huan, "Digital Twin Concepts with Uncertainty for Nuclear Power Applications," *Energies,* vol. 14, 2021.

[20] V. d. Leeuw, "Creating and Deploying Digital Twins in Process Industries," ARC Advisory Group, 2019.

[21] T. Gabor, L. Belzner, M. Kiermeier, M. Till Beck and A. Netiz, "A Simulation-Based Architecture for Smart Cyber-Physical Systems," in *2016 IEEE International Conference on Autonomic Computing (ICAC)*, Wuerzburg, Germany, 2016.

[22] A. Fuller, Z. Fan, C. Day and C. Barlow, "Digital Twin: Enabling Technologies, Challenges and Open Research," *IEEE Access,* vol. 8, pp. 108952-108971, 2020.

[23] H. Gabbar and O. Esteves, "Real-Time Simulation of a Small Modular Reactor in-the-Loop within Nuclear-Renewable Hybrid Energy Systems," *Energies,* vol. 15, 2022.

[24] D. J. Rankin and J. Jiang, "A Hardware-in-the-Loop Simulation Platform for the Verification and Validation of Safety Control Systems," *IEEE Transactions on Nuclear Science,* vol. 58, pp. 468-478, 2011.

[25] A. S. Hahn, C. Lamb, R. E. Fasano and D. Sandoval, "AUTOMATED CYBER SECURITY TESTING PLATFORM FOR INDUSTRIAL CONTROL SYSTEMS," in *12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies*, Providence, Rhode Island, 2021.

[26] A. Rashdan, J. Farber, M. Coelho, C. Primer and Y. Vaibhav, "Integration of Control Methods and Digital Twins for Advanced Nuclear Reactors," Idaho National Laboratory, 2022.

[27] V. Yadav, V. Agarwal, P. Jain, P. Ramuhalli, X. Zhao, C. Ulmer, J. Carlson, D. Eskins, C. Nellis, J. Matrachisia, J. Bass, B. Cohen and R. Iyengar, "STATE-OF-TECHNOLOGY AND TECHNICAL CHALLENGES IN ADVANCED SENSORS, INSTRUMENTATION, AND COMMUNICATION TO SUPPORT DIGITAL TWIN FOR NUCLEAR ENERGY APPLICATION," U.S. Nuclear Regulatory Commission, 2023.

[28] M. Masi, G. Sellitto, H. Aranha and T. Pavleska, "Securing critical infrastructures with a cybersecurity digital twin," *Software and Systems Modeling,* vol. 22, p. 689–707, 2023.

[29] S. R. Kalidindi, M. Buzzy, B. L. Boyce and R. Dingreville, "Digital Twins for Materials," Sandia National Laboratories, Albuquerque, NM, 2022.

[30] C. Theisen, N. Munaiah, M. Al-Zyoud, J. C. Carver, A. Meneely and L. Williams, "Attack surface definitions: A systematic literature review," *Information and Software Technology,* vol. 104, pp. 94-103, 2018.

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, "Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1)," IAEA, Vienna, 2021.

[32] IAEA, "NSS 33-T: Computer Security of Instrumentation and Control Systems at Nuclear Facilities," IAEA, Vienna, 2018.

[33] USNRC, "REGULATORY GUIDE 1.203: TRANSIENT AND ACCIDENT ANALYSIS METHODS," U.S. Nuclear Regulatory Commission, 2005.

[34] B. H. Thacker, S. W. Doebling, F. M. Hemez, M. C. Anderson, J. E. Pepin and E. A. Rodriguez, "Concepts of Model Verification and Validation," LANL, 2004.

[35] Z. Wang, C. Liu and X. Cui, "EvilModel: Hiding Malware Inside of Neural Network Models," in *IEEE Symposium on Computers and Communications*, 2021.

[36] MITRE, "MITRE ATT&CK Framework | Enterprise Matrix," [Online]. Available: https://attack.mitre.org/matrices/enterprise/. [Accessed 2023].

[37] MITRE , "MITRE ATT&CK Framwork | ICS Matrix," [Online]. Available: https://attack.mitre.org/matrices/ics/. [Accessed 2023].

[38] M. S. Mahmoud, "Cloud-Based Control Systems: Basics and Beyond," *Journal of Physics: Conference Series,* 2019.

[39] R. T. Wood, B. R. Upadhyaya and D. C. Floyd, "An autonomous control framework for advanced reactors," *Nuclear Engineering and Technology,* vol. 49, no. 5, pp. 896-904, 2017.

[40] D. E. Keyes, L. C. McInnes, C. Woodward, W. Gropp, E. Myra, M. Pernice, J. Bell, J. Brown, A. Clo, J. Connors, E. Constantinescu, D. Estep, K. Evans, C. Farhat, A. Hakim, G. Hammond, G. Hansen, J. Hill and T, "Multiphysics simulations: Challenges and opportunities," *The International Journal of High Performance Computing Applications,* vol. 27, no. 1, pp. 4-83, 2013.

[41] P. M. A. A. W. D. M. L. Weiming Xiang, N. Hamilton, X. Yang, J. Rosenfeld and T. T. Johnson, "Verification for Machine Learning, Autonomy, and Neural Networks Survey," 2018. [Online]. Available: https://arxiv.org/abs/1810.01989.

[42] D. Woodward, M. Hobbs, J. A. Gilbertson and N. Cohen, "Uncertainty Quantification for Trusted Machine Learning in Space System Cyber Security," in *IEEE 8th International Conference on Space Mission Challenges for Information Technology*, 2021.

[43] V. Singh and K. E. Willcox, "Decision-Making Under Uncertainty for a Digital Thread-Enabled Design Process," *Journal of Mechanical Design,* vol. 143, no. 9, 2021.

[44] H. B. N. D. Linyu Lin, "Uncertainty quantification and software risk analysis for digital twins in the nearly autonomous management and control systems: A review," *Annals of Nuclear Energy,* vol. 160, 2021.

[45] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu and V. C. M. Leung, "A Survey on Security Threats and Defensive Techniques of Machine Learning: A Data Driven View," *IEEE Access,* vol. 6, pp. 12103-12117, 2018.

[46] H. Hidayatullah, S. Susyadi and M. H. Subki, "Design and technology development for small modular reactors - Safety expectations, prospects and impediments of their deployment," *Progress in Nuclear Energy,* vol. 79, pp. 127-135, 2015.

[47] M. Howard, J. Pincus and J. Wing, "Measuring Relative Attack Surfaces," in *Computer Security in the 21st Century*, Boston, MA, Springer, 2005, pp. 109-136.

[48] X. Song, R. Yu, W. Mao, T. Wang, D. Wang and S. Yin, "Research Progress in Autonomous Control Strategy of Miniature nuclear reactor," in *41st Chinese Control Conference (CCC)*, 2022.

APPENDIX A. ANNOTATED BIBLIOGRAPHY

Alcaraz, C., & Lopez, J. (2022). Digital Twin: A Comprehensive Survey of Security Threats. *IEEE Communications Surveys & Tutorials, 24*(3). doi:10.1109/COMST.2022.3171465.

> Unlike many other reports that focus on digital twins, this paper goes into great detail regarding the operational requirements for a digital twin. This information is especially important because it is directly related to the threats that stem from associated attack vectors for each operational requirement. The threats that are reviewed in this paper directly impact security in terms of the confidentiality, integrity and availability triad, and numerous cyber-physical or operational technology security functions. Alcaraz and Lopez then go into great detail to list "protection measures" to reduce the security risks posed by digital twins. While the specific mitigations aren't needed for this report, what Alacaraz and Lopez detail can be directly tied back to the tactics and techniques detailed in the MITRE ATT&CK Framework.

Allen, B. D. (2021). Digital Twins and Living Models at NASA. *The American Society of Mechanical Engineers (ASME) Digital Twin Summit.* Retrieved from https://ntrs.nasa.gov/citations/20210023699

> Presentation provided by NASA that reviews the various defintions of digital twins and their use. The first digital twin was implemented by NASA in Apollo 13 to match the conditions of the spacecraft while also simulating solutions for exploration and predicting results. The presentation also reviews other areas in which the use of digital twins can be monumentally beneficial.

Gabor, T., Belzner, L., Kiermeier, M., Till Beck, M., & Netiz, A. (2016). A Simulation-Based Architecture for Smart Cyber-Physical Systems. *2016 IEEE International Conference on Autonomic Computing (ICAC)* (pp. 374 - 379). Wuerzburg, Germany: The Institute of Electrical and Electronics Engineers. Retrieved from 10.1109/ICAC.2016.29

> Proposes a framework for a cyber-physical digital twin and claims a digital twin can be interfaced with the real world in "an elegant programming architecture" which allows simulations to to be evaluated against real world obersvations which may lead to subsequent improvements within the physical world. Their framework consists of tiers 0 through 3 that represent the different levels of controls.

Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020, May). Characterising the Digital Twin: Systematic Literature Review. CIRP Journal of Manufacturing Science and Technology, 29(Part A), 36-52. doi:10.1016/j.cirpj.2020.02.002

> A thorough and systematic overview of literature on digital twins with publications ranging from 2009 to 2018. There is a common perception that digital twins have numerous benefits such as the reduction of costs, reducing risk and design times, reducing complexity and reconfiguration time, improving efficiency, improving maintenance decision making, improving security, improving safety and reliability, and improving processes and tools. Most importantly though, is that there are few realworld implementations that can validate these assumptions.

Jorgensen, J., Hodkiewicz, M., Cripps, E., & Hassan, G. M. (2023). Requirements for the application of the Digital Twin Paradigm to offshore wind turbine structures for uncertain fatigue analysis. Computers in Industry, 145. doi:10.1016/j.compind.2022.103806

This report reviews the "digital twin paradigm" and how it can provide a framework to lessen uncertainty that may be found in other analytical models using bolted joints on offshore wind turbines as a use case. While this use case is not in the nuclear industry, it is still beneficial to this report as it gives a detailed and thorough analysis of how digital twins can be used to garner additional information for important components.

Kalidindi, S. R., Buzzy, M., Boyce, B. L., & Dingreville, R. (2022). *Digital Twins for Materials.* Albuquerque, NM: Sandia National Laboratories. doi:10.3389/fmats.2022.818535

This article is specific to materials however some of the conclusions it draws are applicable to other industries. First, that the use of digital twins will allow for "unprecedented potential for consistent change management, allowing the optimization of intentional or unintentional product evolution over time." Despite this, digital twins do not adequately capture nor archive material data at the macro level.

Digital twins have thus far been used in the manufacturing and performance evaluation of complex engineered physical systems (e.g., turbine engines); Tao et al., 2018; Lim et al., 2021; Xie et al., 2021) and/or their components, where the focus has been largely on capturing accurately the macroscale geometry and the component-level performance metrics. Current digital twins do not address adequately the capture and archival of the materials data.

Korolov, M., & Korolov, A. (2022, December 6). *The Cybersecurity Challenges and Opportunities of Digial Twins.* Retrieved February 2023, from CSO Online.

In some use cases, digital twins can directly control the asset they mirrior which may double the attack surface as the asset and its digital representation can both be targeted. This is particularly concerning if the digital twin can send control commands. Some mitigations options include involving cybersecurity from the onset when building and implementing a digital twin to following NIST or TLS guidelines for encryption and access control.

However, in some instances, digital twins are being used as decoys to lure adversaries, create warning systems in the event of a cyberattack, and as a testbed to find security vulnerabilities. "One company using digital twins as a kind of highly sensitive sensor layer is GE, which is building something they call 'digital ghosts'" Digital ghosts can be used to secure both critical infrastructure and operational technology within a data center. Traditionally, OT cybersecurity focuses on network traffic, firewalls, and searching for viruses whereas GE's digital ghosts provide insight into how underlying physical assets operate so that organizations can alert to and study abnormal facility behavior. The digital ghost would detect if something's wrong and inform operators as to which device is compromised. A task which "typically takes operators days or weeks to pinpoint where the problem is. The digital ghost does that within seconds."

Raj, P., & Surianarayanan, C. (2020). Digital Twin: The Industry Use Cases (Chapter 12). In P. Raj, & P. Evangeline (Eds.), *Advances in Computers, Volume 117* (pp. 286-315). Cambridge, MA, U.S.: Academic Press.

Identifies three levels of digital twins: (1) Partial, in which the digital twin is connected to limited data sources or sensors for basic devices and captures key metrics for that device; (2) Clone, this level contains all data and measurements from multiple sources for an asset; and (3) Augmented, this digital twin enhances collected data with data from outside sources or intelligence which is extracted through a data analytics engine and may utilize machine learning algorithms.

At a bare minimum, a functional digital twin requires the model of the physical object, data from that object, and a one-to-one correspondence to the object, and the ability to monitor the object. The elements of control, analytics, are optional depending on use case.
General Electric (GE) is using "DTs in the monitoring and diagnostics space to flag any irregular behaviours that could be early signs of an emerging issue. ML workflows are also extensively leveraged to detect any deviation as early as possible."

"GE has also created enterprise-scale DTs that simulate full-scale and complex systems interactions, which simulate several 'what-if' scenarios of the future and determine optimum key performance indicators for situations with highest probability. By leveraging large data sources for weather, performance, and operations, these simulations play out possible scenarios that could impact an enterprise."

Suhail, S., Jurdak, R., Hussain, R., & Svetinovic, D. (2022). *Security Attacks and Solutions for Digital Twins.* doi:10.48550/arXiv.2202.12501

This report highlights the importance of digital twins to cyber-physical systems, industrial control systems, and operational technology. While digital twins are valuable and important tools for operators they also significantly increase an organization's attack surface. There are concerns that digital twins may provide adversaries an avenue to stealthily attack cyber-physical systems first using the digital twin as an entry point to then infiltrate the network of the physical plant. This report covers attacks using tactics and techniqes that relate back to the MITRE ATT&CK framework and then reviews potential risk mitigation options. Suhail, Jurdak, and Svetinovic provide detailed insight into attacks from the adversary's perspective and then proposes three solutions to lessen the risk that digital twins pose.

Tao, F., Zhang, H., Liu, A., & Nee, A. (2019, April). Digital Twin in Industry: State-of-the-Art. *IEEE Transactions on Industrial Informatics*, 2405 - 2415. doi:10.1109/TII.2018.2873186

This paper did an indepth review of publications on digital twins ranging from xxxx to 2018; and eventually found only fifty papers that were worth reviewing across the numerous databases that they queried. They also investigated patents for digital twins across indsutry and also touched briefely on the concept of a cyber-physical digital twin and the associated challenges. As of 2018, the cross between cyber and physical was still a new topic and therefore there was no existing framework to reference. Another concern raised by Tao et al. is that a cyber-physical digital twin would be exposed to even more threats stemming from physical threats in addition to cyber threats. And because this concept is particularly new, the authors

conclude with a recommendation that standarized connection and communication protocols should be created.

Yadav, V., Agarwal, V., Gribok, A., Hays, R., Pluth, A., Ritter, C., . . . Iyengar, R. (2021). *Technical Challenges and Gaps in Digital-Twin Enabling Technologies for Nuclear Reactor Applications.* Idaho National Laboratory. U.S. Nuclear Regulatory Commission.

There is a need for a better understanding of the current state of digital twin technology; understanding how regulatory guidance could relieve technical issues; develop the necessary infrastructure to support regulations.
Potential areas to implement DT

Zaccaria, V., Stenfelt, M., Aslanidou, I., & Kyprianidis, K. G. (2018). Fleet Monitoring and Diagnostics Framework Based on Digital Twin of Aero-Engines. ASME Turbomachinery Technical Conference and Exposition (GT2018). Oslow, Norway: American Society of Mechanical Engineers. Retrieved from https://www.diva-portal.org/smash/get/diva2:1254117/FULLTEXT01.pdf

Aircraft engine manufacturers are using digital twins to simulate engine fleets for monitoring their operation. By using digital twins to monitor fleet operations manufacturers can optimize flight operations and maintenance which ultimately lowers costs. Furthermore, the digital twins are used for automated anomaly detection to isolate and identify faults. Unfortunately for this project, the models that the manufacturers use are proprietary but it is indicative that digital twins are being used in some manner in an industry.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Ben Cipiti	8845	bbcipit@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Katya LeBlanc	katya.leblanc@inl.gov	Idaho National Laboratories

This page left blank

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.