INL/RPT-23-75113
Revision 000

Attack Surface Analysis of the Digital Twin and Advanced Sensor and Instrumentation Interfaces

Cyber Threat Assessment and Attack Demonstration for Digital Twins in Advanced Reactor Architectures

September 2023

M3CT-23IN1105033

Idaho National Laboratory
Chris Spirito

Lofty Perch
Jeff Ly
Michael Veretennikov

INL is a U.S. Department of Energy National Laboratory operated by Batelle Energy Alliance, LLC

INL/RPT-23-75113
Revision 000

Attack Surface Analysis of the Digital Twin and Advanced Sensor and Instrumentation Interfaces

M3CT-23IN1105033

Idaho National Laboratory
Chris Spirito

Lofty Perch
Jeff Ly
Michael Veretennikov

September 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Engineering
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

Page intentionally left blank.

CONTENTS

FIGURES

Page intentionally left blank.

ACRONYMS

AI	Artificial intelligence
API	Application Programming Interface
ASI	Advanced Sensor and Instrumentation
BWR	Boiling water reactor
CLI	Command line interface
DCS	Distributed Control System
DT	Digital Twin
DTDL	Digital Twin Definition Language
HMI	Human-Machine Interface
IAEA	International Atomic Energy Agency
IIoT	Industrial Internet of Things
I&C	Instrumentation and Control
JADE	Java application and developer environment
JSON	Javascript object notation
MCO	Moisture Carryover
ML	Machine learning
OT	Operational Technology
PWR	Pressurized water reactor
RBAC	Role-based access control
RDF	Resource Description Framework
REST	Representational state transfer
SDK	Software Development Kit
SLA	Service Level Agreement
SMR	Small Modular Reactor
XML	Extensible markup language

Page intentionally left blank.

1. DT-ASI Applications in Nuclear

A digital twin is a virtual representation of a physical system or object using real-time data that can predict and analyze how the system or object performs. This relatively new technology can be applied to the field of nuclear power generation, to aid in the design and development of new nuclear power plants and reduce operation costs using predictive maintenance and other data analytical methods. While there are already companies utilizing simulation software to train operators and technicians in the nuclear industry, some are now transitioning to utilizing their existing technology, software, and methods to develop digital twin solutions for the next generation of nuclear power plants, offering their services to utilities and government organizations around the world.

Digital twins have a combination of unique requirements that must be satisfied to maximize their full capabilities when applied to advanced small modular reactors within the nuclear power industry. Advancements in instrumentation and sensors allow measurements to be continuously and accurately transmitted with low latency rate thresholds to maintain state concurrence [1] of the digital twin. This enables a virtual representation of the physical system to be created and maintained in real-time. The potential applications of digital twins are far reaching; the integration of artificial intelligence and machine learning for state cognizance [1] has the potential to provide novel insight and constant improvements to streamline operations, maintenance, and management of physical processes rather than just simply applying pre-existing methods.

While deep discussion of physical specifications for advanced sensors and instrumentation technology is required for successful integration of a digital twin, such topics are out of the scope of this report. Rather, this report will explore possibilities of communication and data transfer interfacing between ASI and DT components, the protocols and specifications needed to support them, and a deep dive into security concerns regarding digital twin deployment. A baseline of recommended best practices to ensure digital twins are deployed in alignment with industry safety standards and a proof-of-concept with documentation of methodology, simulations, and tests will further provide evidence of real-life use cases and the potential impact threat actors can have on digital twins, and by extension, the physical systems, and operations.

DT-ASI Interfaces, Specifications, Protocols

Advanced sensors and instrumentation have progressed significantly for expansion of functionality within harsh nuclear environments and enhanced control capabilities for applications that require additional measurements to be gathered. For instance, innovations like high-temperature sensors and radiation-resistant cameras have enhanced the ability to monitor and control nuclear reactors in real-time, ensuring optimal performance and safety. In order to support the capabilities of digital twins, these components must address certain specifications and protocols to enable smooth operation, such as adherence to the Digital Twin Definition Language (DTDL) which provides a unified language for describing models and interfaces. Future-state technology suggests a trend towards a hybrid combination of wired and wireless networking technology for data transfer between the traditional operational technology (OT) systems and the digital twin. The advancement in Mesh networking technology, for instance, allows devices to communicate in harsh or remote environments where traditional networking systems might fail. Depending on industry requirements, stakeholders have multiple options to utilize digital twin

interfacing infrastructure including on-premises, cloud-based, or vendor-supported digital twin applications. A real-world example of this flexibility might include an energy provider utilizing an on-premises digital twin model to ensure data security while a smart city initiative might employ a cloud-based model for scalable, collaborative urban planning. There are also several influencing factors, such as data privacy, integration complexity, and cost, that must be considered, especially in critical infrastructure sectors like nuclear energy where regulatory compliance and safety are paramount:

- Potential communication protocols [3]:
  - Wireless: 5G, NB-IOT, LoRaWAN**,** SigFox, WirelessHART, XBee
  - Wired: MQTT, OPC UA, CoAP
- Security standards (encryption, access control)
- Data heterogeneity (e.g. data formats – JSON/XML)
- Resilience and redundancy
- Regulatory standards and compliance

1.1 On-Premises Solutions

An on-premises digital twin solution has the potential to expedite the deployment process and simplify management operations. Stakeholders will have familiarity with the in-house physical system and its underlying infrastructure, contributing to a smooth deployment of the digital twin with the ability to address unique site characteristics and requirements. Communication streams, data transfer/storage, and privacy designed around organizational standards, policies, and procedures allow for security controls to be aligned with business needs. Solutions designed and operated on-premises allow stakeholders greater control over resource allocation, maintenance, and updates required for both the physical and digital twin. Deployment and operation of digital twins within the nuclear industry is in continuous research and development to further understand concerns such as communication security between ASI and DT interfaces. As these concerns are adequately addressed as the solution evolves over time, digital twins could reach a level of maturity suitable for live integration into small modular reactors.

1.1.1 MAGNET

In July 2022, Idaho National Laboratory conducted their initial testing for a digital twin of the Microreactor Agile Non-Nuclear Experimental Testbed (MAGNET). It was designed with a combination of technology including Digital Engineering techniques, the INL DeepLynx data warehouse and MOOSE Multiphysics framework [14]. MAGNET utilized a Data Acquisition System, or DAQ, integrated with sensor data gathering, Multiphysics simulation, machine learning forecasting, and asset control. The digital twin was successfully able to predict future process conditions, calculate undesirable system states, and autonomously adjust system controls, leading the system back to a favorable steady state. Although designed for non-nuclear applications, this digital twin prototype demonstrated functionality that can be enhanced for the application of digital twins in advanced nuclear reactor environments.

1.2 Cloud Solutions

When discussing cloud-based digital twins, the Industrial Internet of Things (IIoT) is an umbrella term that commonly refers to components with wireless networking capabilities that connect to the Internet and upload information to a centralized database. In the context of this discussion, common devices associated with IIoT will be referred to as smart sensors or internet-connected devices; components that measure, record, and aggregate data on various processes and transmit them to the digital twin for analysis. Many of the advanced sensor and instrumentation devices being developed for future digital twin integration include the functionality of these smart devices.

From an operational standpoint, cloud-based digital twins require a unique approach compared to the on-premises and third-party counterparts. In many critical infrastructure environments, particularly in the nuclear industry, any unplanned downtime may be unacceptable and could compromise the safety of on-site operators. While operator safety is the primary concern, thousands of households could be affected by a single outage based on the daily average production output of a single SMR. Although cloud-based solutions include significant benefits such as convenient accessibility through the cloud and scalability for future-state expansion due to the platform-as-a-service model, this option also requires a set of security engineering decisions that may be more approachable with an on-premises solution. Due to increased complexity related to the logistics for data transmission, platform configuration, and application integration of a cloud-based digital twin, organizations may need to dedicate more resources towards the implementation of the twin in conjunction with the physical system. The application of security controls must be consistent with operating standards and compliance not only within the organization, but within the residing country as well.

Should an organization choose to use a cloud-based digital twin deployment, procurement of a vendor would require due diligence in ensuring vendor and organization policies and procedures are aligned. A thorough analysis will be conducted on a common cloud-based digital twin provider: Microsoft's Azure Digital Twin.

1.2.1 Azure Digital Twin

Microsoft's cloud-based Azure Digital Twin is operated through a platform-as-a-service model to replicate physical processes, environments, and systems in a digital domain. It enables the creation of twin graphs used to analyze operating conditions and performance, providing insight leading to the direct improvement of system functions. The solution typically relies on integration with other Azure products for increased functionality, including Azure Digital Twins Explorer, Azure Data Explorer, and Azure SignalR Service [15]. Figure 1 below showcases the integration of the Azure Digital Twin within an Azure IoT solution.

The twin graph is the heart of Azure Digital Twins representation of the physical system. It connects all the individual digital twin components through relationships, allowing operators to view, manage, and interact with individual processes or the entire system-of-systems. Management operations are interfaced through Azure Digital Twins APIs and SDKs, Azure Digital Twins Explorer, REST API calls, and Azure CLI commands. In Azure Digital Twins Explorer, twins and relationships can be created through either JSON or Excel format graph files. Azure Data Explorer is Microsoft's machine language solution for high volume, near real-time data analyzation. It allows for historical queries into twin graph updates and

lifecycle events as well as insights on system behavior for predictive performance output, maintenance, and operations. Information processed by the twin graph is queried through Azure Digital Twins Query API using Azure Digital Twins query language, a custom SQL-like query language.

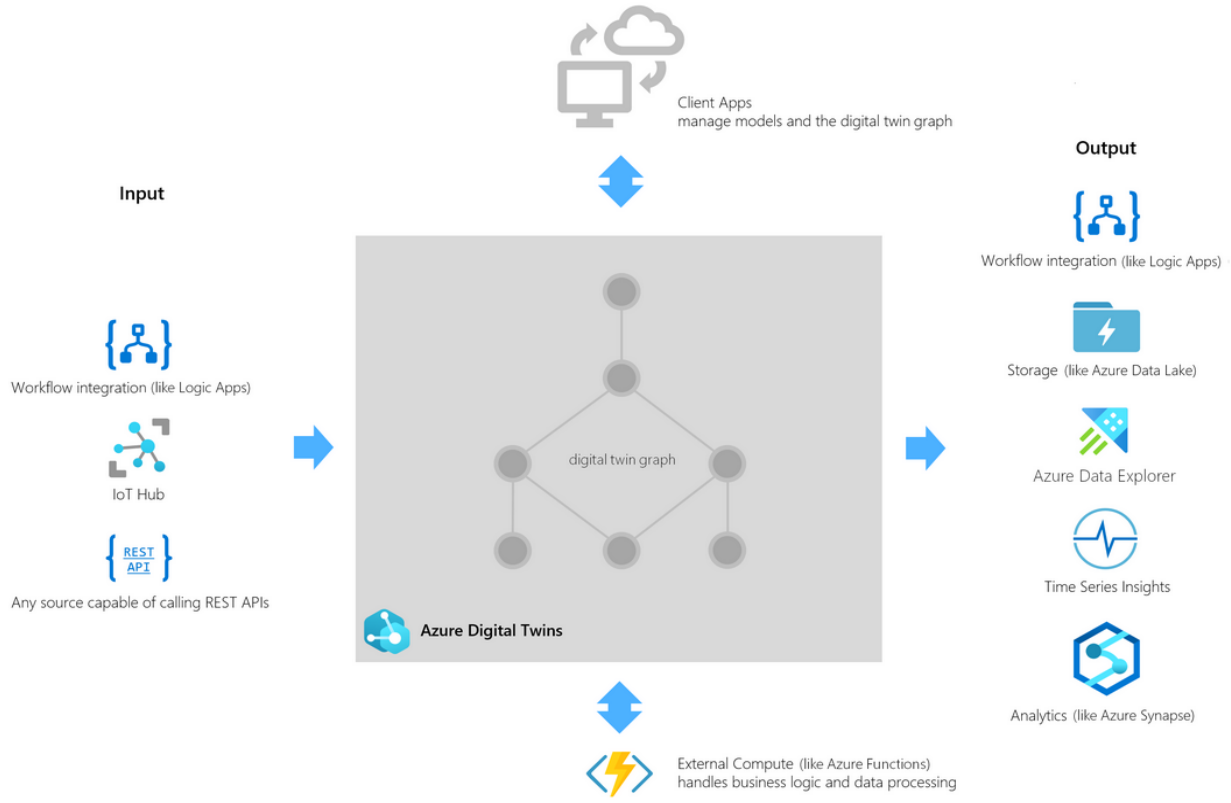


Figure 1: Azure Digital Twins within an Azure IoT Solution [15]

Within Azure Digital Twins, users have the ability to define their own models with customizable definitions and behavior using their digital twin definition language (DTDL). DTDL is derived from JSON-LD, providing compatibility for both JSON directly or in resource description framework (RDF) systems [17]. In DTDL, metamodel classes form a foundational structure to facilitate attribution of information within the digital twin models. The primary metamodel classes are [18]:

- Interface
- Command
- Component
- Property
- Relationship
- Telemetry.

Utilization of these metamodel classes introduces a standardized language and structure for interoperability between multiple digital twins and systems. Figure 2 represents a basic DTDL model describing a Home and its relationship to a Floor model.

Figure 2: A basic DTDL model[a]

When observing data ingress from sensors to the digital twin, an Azure function can be written to update the digital twin based on IoT telemetry events that are ingested in the IoT Hub [20], as shown in Figure 3. It allows for telemetry from virtually any source with event-driven triggers to receive data. Functions provide native support for scripts and code in C#, Java, JavaScript, PowerShell, and Python. There are two options for data egress; if the destination is to Azure Data Explorer, data history can be used to automatically send updates to a cluster as historical data. If the destination is another Azure service, it must be attached to an endpoint consisting of an Event Hub, Event Grid, or Service bus instance.

The usage of cloud-based applications provides organizations with enhanced accessibility and convenience to store, access, and process data that resides in the cloud and can significantly reduce hardware costs. While this is very attractive to many organizations, implementing cloud solutions without performing a comprehensive assessment may expand the attack surface and reduce the security posture of an organization and its assets. Azure Digital Twin has taken a number of cyber security concerns into consideration, namely authentication and authorization of users, integrity of information, and availability of the platform. Integration of Azure Digital Twins with Azure Active Directory (Azure AD) allows the management of roles and permissions for digital twin instances through Azure role-based access control (Azure RBAC). Data at rest and in transit within the Azure ecosystem is encrypted through a Microsoft-managed encryption key [21]. Lastly, Azure Digital Twins are covered under the Microsoft Azure service SLA, providing redundancies for high availability services. In the event of an outage in the region, Microsoft-initiated failover is exercised to replicate data stored in Azure Digital Twins to a corresponding

[a] https://learn.microsoft.com/en-us/azure/digital-twins/concepts-models

paired region [22]. The process is monitored using the Azure Service Health tool and provides high-availability and redundancy to the digital twin to ensure that data is not lost in the event of a failure.

```
using System;
using System.Text;
using System.Threading.Tasks;
using Microsoft.Azure.Devices;
using Microsoft.Azure.WebJobs;
using Microsoft.Extensions.Logging;
using Azure.Identity;
using Azure.DigitalTwins.Core;
using Azure;
using Newtonsoft.Json.Linq;

public static class IoTHubTriggeredFunction
{
    private static readonly string iotHubConnectionString = Environment.GetEnvironmentVariable("IoTHubConnectionString");
    private static readonly string adtInstanceUrl = Environment.GetEnvironmentVariable("ADTServiceUrl");
    private static readonly DigitalTwinsClient digitalTwinsClient = new DigitalTwinsClient(new Uri(adtInstanceUrl), new DefaultAzureCredential());

    [FunctionName("UpdateDigitalTwinFunction")]
    public static async Task Run(
        [EventHubTrigger("messages/events", Connection = "IoTHubConnectionString")]EventData message,
        ILogger log)
    {
        log.LogInformation($"C# IoT Hub trigger function processed a message: {Encoding.UTF8.GetString(message.Body.Array)}");

        // Deserialize the message body
        var telemetryData = JObject.Parse(Encoding.UTF8.GetString(message.Body.Array));

        // Extract device ID and telemetry information from the incoming message
        string deviceId = telemetryData["deviceId"].ToString();
        string temperature = telemetryData["temperature"].ToString();

        try
        {
            // Construct the digital twin update patch
            var updateOperations = new UpdateOperationsUtility()
                .AppendReplaceOp("/Temperature", temperature)
                .Serialize();

            // Update the digital twin using its ID (assuming the device ID corresponds to a digital twin ID)
            await digitalTwinsClient.UpdateDigitalTwinAsync(deviceId, updateOperations);

            log.LogInformation($"Updated digital twin {deviceId} with new temperature value: {temperature}");
        }
        catch (RequestFailedException e)
        {
            log.LogError($"Failed to update digital twin {deviceId}. Error: {e.Message}");
        }
    }
}
```

Figure 3: Notional code for Azure Function[b]

The exploration of Azure Digital Twin has illuminated the multi-faceted nature of implementing a cloud-based digital twin, revealing considerations from data integrity to user accessibility in a comprehensive digital twin architecture. The encapsulation of various metamodel classes through the digital twin definition language (DTDL), coupled with the meticulous orchestration of IoT components, offers a rich, intricate representation of physical processes, further bridging the gap between actual operations and their digital counterparts. Notwithstanding, it also underscores the intricate layers of complexity that organizations must navigate—striking a balance between operational agility, data security, and regulatory compliance. As we pivot to a discussion on third-party vendors in the ensuing section, the delicate equilibrium between technological capability and operational security becomes paramount. Especially within critical infrastructures, such as those found in the nuclear industry, the imperatives of aligning vendor solutions, like those provided by Azure, with organizational, regulatory, and operational needs necessitate a critical lens. Moving forward, the discussion will unravel the nuances of vendor selection, spotlighting the crucial areas such as cybersecurity, compliance adherence, and robustness of solution, thereby leading organizations to make informed decisions in their digital twin and IIoT journey, fortifying not just operational capability but also safeguarding the intricate web of digital and physical operations.

[b] Generated by Chat GTP 4.0

1.3 Third-Party Vendors

1.3.1 Notable Companies and Vendors

There are several companies that provide digital twin solutions for the nuclear power industry. The following list contains some major and notable vendors that have worked on or are currently working on developing a digital twin solution for nuclear power purposes.

- **L3Harris**
- **GSE Systems**
- Framatome
- Siemens
- GE & GE Hitachi
- Westinghouse

The companies that are in bold will have their digital twin platforms analyzed more in depth as they offer digital twin and simulation platforms which are designed to be applicable to the entire nuclear industry rather than customized for a specific nuclear power plant and/or process. Analyzing these solutions will provide insights into security controls that may be applicable to any vendor solution.

1.3.2 L3Harris - *Orchid*^{tm} Platform

Utilizing their Orchid^{tm} platform, L3Harris has been providing customers with simulation technology for both nuclear operators and engineers for the last fifty years. Their platform was used to simulate various third generation nuclear power plants around the world and is now being used to develop advanced fourth generation nuclear power plants. Given their industry prominence, their platform is a good candidate to examine for potential cybersecurity issues and concerns.

The Orchid platform is a Java-based platform that utilizes a client-server architecture model comprised of several different software components that perform specified tasks. A security analysis is required on key software components that will be utilized to create and operate a digital twin of a nuclear power plant [25]. The three main programs that are used for the design and modification of the digital nuclear facility are the Orchid Core Builder, Orchid Modelling Environment, and Orchid Control System. These programs must be installed on a central server or engineering workstation to create or make modifications to the digital twin. The Orchid Simulator Executive and Configuration Manager software packages must be installed on the server or computer that performs simulation and modeling. These programs manage the runtime of the simulation and store all necessary configuration files for the source code of the individual applications and the digital twin simulations.

It is important to note that the Configuration Manager software will be connected to a database to store and retrieve configuration data for the simulation. Finally, the Orchid Network Loader and Orchid Input Output applications may be the most significant programs to analyze as they manage the digital twin over the network and its connections to the physical plant and/or ASI data. There are additional applications included for graphical design and multimedia purposes including audio and video, however, these are more geared towards operator training rather than digital twin simulation. Regardless, all Orchid applications that are used for the creation and operation of a nuclear power plant digital twin are required to be analyzed for any potential vulnerabilities and source code concerns prior to implementation.

L3Harris utilizes three separate techniques for creating a digitized representation of a plant DCS as shown on Figure 4, and IAEA publication IAEA-TECDOC-1500 is used as a template for implementing these techniques. In all cases, the process models will be generated and established via the Orchid platform utilizing various physics and engineering calculations and figures. This will require a database to store all generated data from the digital twin. The specific data ingested by the simulation model and how this data is transmitted is configured on a case-by-case basis as desired by the customer.

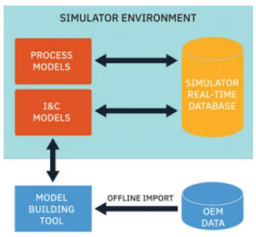
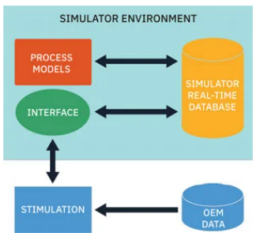
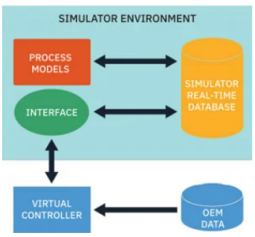
Stimulation	Emulation	Simulation
		
Implementation of a replica of the reference plant DCS on the simulator using actual DCS hardware and application software as installed on the reference plant.	Implementation of the reference plant DCS on the simulator using the same application software installed on the reference plant but running on the lower cost simulator hardware and operating system. In the case of DCS controls, emulation is sometimes referred to as “virtual machine,” “virtual stimulation” or “virtual controllers.”	Implementation of the reference plant DCS by simulating the DCS functionality using simulator vendor tools.

Figure 4: Techniques for Incorporating DCS on L3Harris Simulators [26]

The first technique is to create a replica control system made from the exact same hardware and software licenses that will be utilized to receive the process data from the plant. This provides highly accurate responses from the model to be used in the simulation environment. The second technique is similar; however, lower cost hardware and software are utilized to simulate physical process responses. The third technique utilizes virtual controllers instead of the physical controllers in the plant to simulate physical process responses in its digital twin. The use case for each scenario is based on the requirements and resources of the customer themselves but each technique does pose cyber risks to the customer if not implemented securely.

A major concern for each of the implementations above, is how the ASI data is transferred from the physical system to the digital twin being used to simulate responses. There are several possibilities for data integration between the physical system and the digital twin based on where the digital twin is hosted. The first technique will host the vendor solution on-prem and therefore be connected directly to the physical plant itself. The second option hosts the solution off-prem and the ASI data will be accessed via cloud service integration or other data-sharing services. The third option is to manually upload plant data offline. Each approach comes with its own security concerns. If the digital twin solution is hosted on site and connected to the physical plant for ASI data ingestion, then it will need to be assessed with the same scrutiny as the physical system. Should the digital twin be hosted in the cloud, the security controls for the cloud/data-sharing service access and management must be analyzed as the digital twin will be accessing the plant data using this interface. For the third option of manual offline data transfer, security

controls would have to be in place to ensure the integrity and validity of the uploaded ASI data and establishing requirements for the storage and encryption of the offline data. These same concerns are also applicable regarding access to the generated simulation data.

The simulator environment that is hosting the digital twin will have different security concerns depending on what configuration is chosen. If the simulator environment consists of the identical industrial hardware and controllers used in the physical system, it may be susceptible to the same vulnerabilities and therefore require an equal level of security controls and countermeasures. It is also worth noting that the possibility exists for an adversary to indirectly disrupt the physical process by exploiting the autonomous capabilities of the digital twin. With regards to the use case that utilizes similar but downscaled versions of the hardware to control the digital plant, it is expected that this would lead to similar security countermeasures regarding data formatting and processing. Potential conflicts may arise if data from the more advanced sensors and instrumentation cannot be reliably processed by the downscaled digital twin controller. The third configuration consists of completely virtual industrial controllers to simulate the plant. In addition to the security concerns from the previous configuration regarding appropriate data formatting and processing, this configuration may suffer from incompatibility issues in the communication process itself. Further considerations (e.g. where the virtualized components are hosted within the network; how advanced sensor data must be processed) surrounding integration within the DT must also be addressed.

Considering scalability in terms of cost, the technique of utilizing the exact same control infrastructure in the digital twin would be least scalable as it requires the same physical hardware as the physical plant itself which will lead to high equipment costs. The second technique of utilizing downscaled control hardware to simulate the plant is the compromise between simulation accuracy and equipment cost. Utilizing virtual control hardware would be the most scalable in terms of equipment but at the potential loss of accuracy for the digital twin simulation. In terms of scalability from a security perspective however, the order is reversed. The first technique of utilizing the same control hardware in the DT as the physical plant would mean that most of the security controls and countermeasures developed for the physical plant can be applied to the DT architecture. In the second method of utilizing downscaled control hardware, minor adjustments would be made to the security controls of the plant to be applied to the hardware of the DT to account for the differences. These changes mostly concern data formatting and processing, to ensure the integrity of the data being transitioned. For the technique of utilizing virtualized control hardware, it would be the least scalable in terms of security. As new components are added to the ASI of the physical plant, the data from the ASI would have to be formatted appropriately for the virtual controller of the DT to process. This could also entail communication protocol differences creating the need for additional security analysis.

1.3.3 GSE Solutions - *JADE*^{tm}

Like L3Harris, GSE System also develops simulation software for engineering and training purposes. However, GSE is focused on power systems only and have extensive experience in the nuclear power industry across the world with claims to be the first company to make a commercial simulator for nuclear power operations, making them a good candidate to explore. The company offers multiple applications that serve various purposes for simulation and training, all of which can be tailored specifically for digital twins of nuclear power generation facilities.

The central platform or software suite that GSE uses to simulate power plant operations is called JADEtm, an acronym for Java Application & Developer Environment [27]. The platform is a Java-based platform which is mainly designed for a Windows desktop or server environment although there is compatibility with UNIX based environments as well [28]. The software suite consists of programs including JTopmeret, Jelectric, Jlogic, Jcontrol, and Jdesigner, each of which are used to generate various aspects of a virtualized process such as those in a digital twin of a nuclear power plant. The key program to analyze from GSE is SimExec as it manages the runtime of the simulations and facilitates the interfaces for the various JADE programs. Unlike the L3Harris platform, GSE's simulation platform does not have any dedicated programs for managing its network and interfaces, instead it utilizes "built-in Windows server-client protocols" [28]. While this does allow for more flexibility, potential misconfigurations could result in significant security issues, especially if the only security controls and countermeasures in place are dependent on the OS of the server it is hosted on.

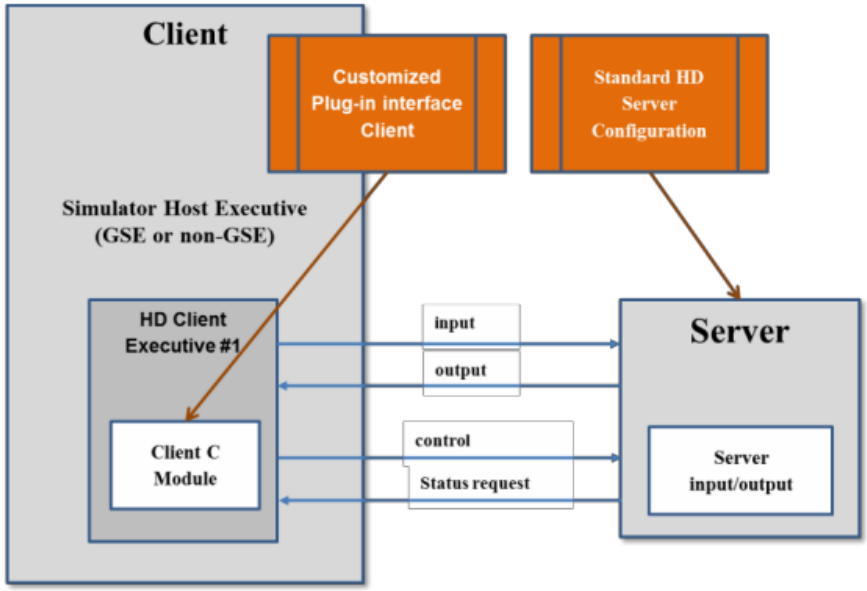


Figure 5: Client and Server Control Diagram [30]

GSE Systems has used its general JADE software suite to collaborate with researchers and build simulation solutions for specific nuclear operation purposes. The PSA-HD platform utilizes JADE software and the MAAP5 program developed by the Electric Power Research Institute to simulate PWR, BWR, fuel containment, turbine, and emergency operations of nuclear generation facilities [28]. The platform follows a server-client architecture where the simulation software will reside on a client device and request various parameters and data from a server, as illustrated in Figure 5. Adapting this to the case of a digital twin for a nuclear power plant, the server will have to contain data from the physical plant's ASI system. Each server will have to correlate to various aspects of the plant's infrastructure subsystems such as its reactors, fuel containment, and other sub-units as necessary (see Figure 6).

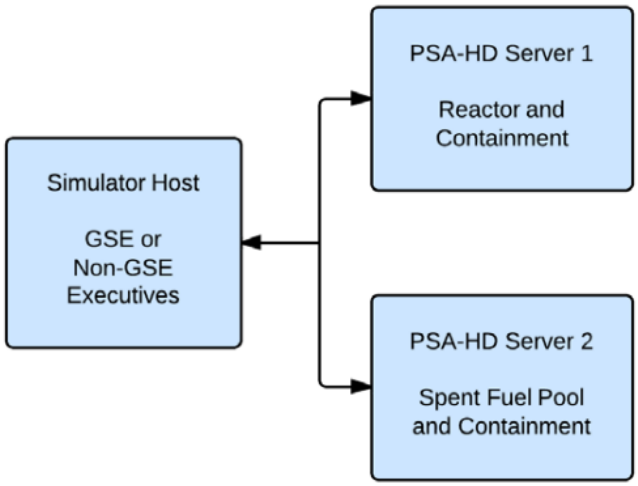


Figure 6: Sample PSA-HD Layout for a Plant with One Reactor Unit and a Spent Fuel Pool.[30]

This network model leads to security concerns related to data integrity and validity, access controls, location of servers on the network, and the communication requirements for the simulation clients that request the required ASI parameters from the servers. This infrastructure configuration creates the same issues as the L3Harris platform regarding ASI data storage and processing for DT simulations. It is also important to note that the type of hardware used to host the DT process and control is not included in this analysis, but likely has similar requirements to what is outlined in the L3Harris platform. The GSE systems main page has indicated a preference towards I&C system products made by companies such as Beckhoff, Wago, and Weidmuller for its nuclear simulation solutions.

1.3.4 Custom Vendor Solutions

While the two vendors analyzed above offer a tailored platform based on their previous experiences of simulating nuclear processes to build a digital twin for nuclear facilities, there are other vendors with considerable experience in the nuclear power industry that have designed and/or developed custom digital twin solutions for a nuclear power generation facility. These companies utilize their proprietary hardware and software to interface directly with industrial controllers, data historians/databases, HMI devices, and physical process components to create a digital twin or simulation environment. An example of this is the Westinghouse Electric Company's simulation and training environment for their AP1000 PWR (Figure 7) as its underlying design and technical components could be adapted to develop a full-function digital twin.

While there are components in this architecture that were specifically designed with training nuclear operators in mind such as the instructor station system, the overarching architecture is likely very similar to what a nuclear digital twin would require. The Ovation Highwaytm at the bottom of the diagram represents real-time data (including ASI data) from a nuclear power plant control center which feeds unidirectional data into several components. The DT architecture would need to be capable of bidirectional traffic to have the capability to send data back to a nuclear control room if it is designed with the intention of performing tasks such as preventative maintenance and sensor data adjustments. As

previously stated, the requirement for transitive trust between the physical system and the DT are key security concerns as the integrity of the data being transmitted from the ASI is a critical success factor. Other components in this infrastructure are those of a typical I&C system (excluding the simulation environment which can be viewed as the SimStationTM and its connected components) and would require appropriate security analysis, controls, and countermeasures that would be commensurate for these systems.

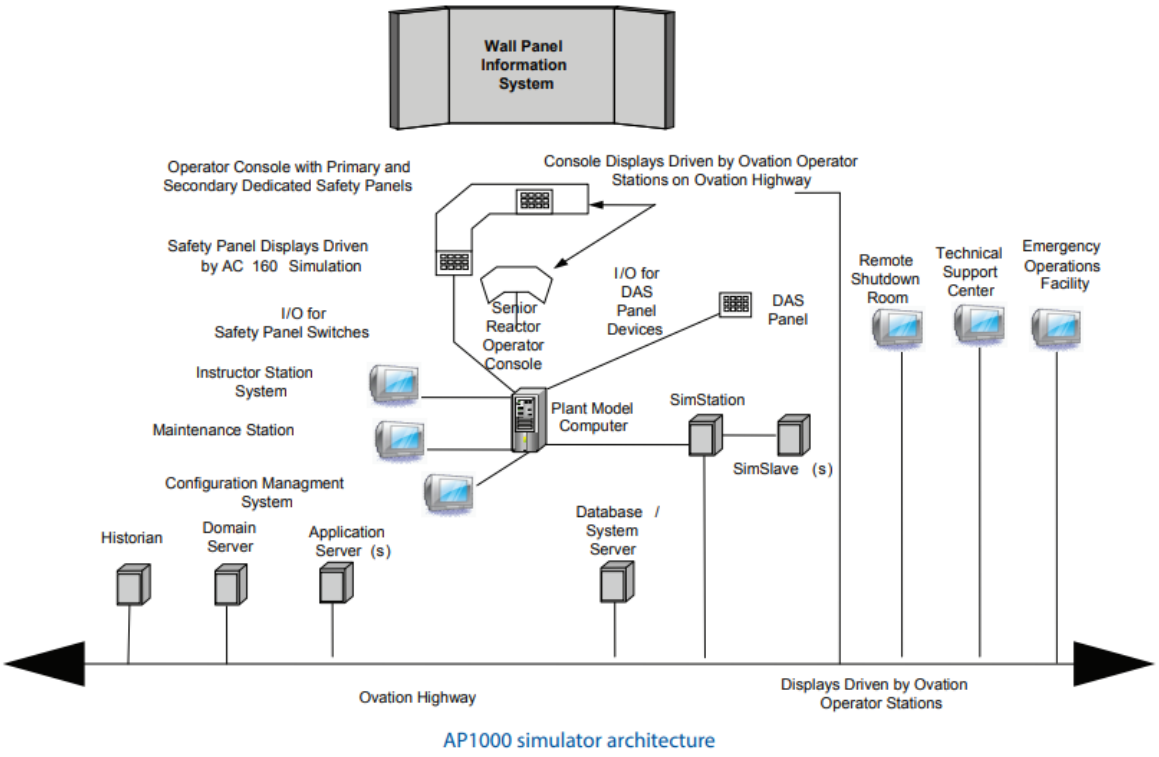


Figure 7: AP1000 Simulator Architecture [33]

The DT simulation environment architecture and its required components including plant models, I&C interface, and analytical output database will differ based on what DT solution the customer decides to implement. When considering a custom DT solution, especially a vendor managed solution, it will be important to keep scalability in mind. It is likely that any additions or modifications made will have to utilize the same hardware and software from the vendor which may cause licensing to be a limiting factor. Furthermore, as the entire solution and its components are provided by the same vendor as the physical system, both the DT and physical system would be as susceptible to supply-chain attacks. This should be taken into consideration when considering an identical vendor managed solution as any underlying security vulnerabilities with the vendor's software and equipment may negatively impact the security posture of the DT.

1.3.5 Vendor Solution Summary

Choosing to utilize a vendor solution rather than a custom in-house solution to create a digital twin for a nuclear facility provides many significant benefits. Most vendor engineering modelling software that simulates physical processes utilizing ASI data from a nuclear power plant are proven to be effective and perform their desired functionality. Furthermore, if the existing instrumentation and control

infrastructure was made by the same vendor or a vendor with experience in the nuclear sector, then interfacing a digital twin using the ASI of the plant should be within their domain of expertise. This will lead to a higher likelihood of successful and effective implementation of the digital twin. However, if a vendor solution is chosen for implementation of the DT, then various security requirements, controls, and countermeasures must be put in place to reduce cyber risk. There will be many interfaces between the vendor solution and nuclear plant ASI, including but not limited to:

- servers that host the vendor physical simulation models,
- servers that store plant ASI data,
- servers that store data generated by the DT,
- control systems utilized by the DT for simulation,
- various other interfaces regarding configurations and auxiliary functions.

All DT vendor solution software must be thoroughly analyzed for any inherent vulnerabilities, especially if they are publicly known. Concerning security issues that are common among all DT vendor solutions include the amount of trust and control the DT would have over the actual plant ASI system, how nuclear process and model generated data would be managed between the ASI of the plant system and the vendor solution components, and the security of the communication protocols between the physical and digital systems. Furthermore, hardware components of the vendor solution may or may not be provided as part of that solution on a case-by-case basis. This introduces the requirement for additional security analysis regarding the forms of hardware infrastructure acquired to create the DT network infrastructure.

2. Nuclear Power Generation Digital Twin Attack Scenarios

Utilizing digital twins for operation of nuclear power facilities can bring many benefits including more safe and effective power plant designs, better understanding of emerging nuclear technology, reduced operation and maintenance costs, and improved viability of nuclear energy overall. However, it is important to note that like any other emerging digital technology, there will be cyber risks related to adversaries utilizing security vulnerabilities to create potential attacks against these new forms of technology. By examining various attack scenarios on digital twins, stakeholders can reduce cyber risk by incorporating the appropriate countermeasures. Prior to examining specific attack scenarios, attacks will be classified based on a variety of factors pertaining to the intended target of the digital twin.

2.1 Intended Target of Digital Twins

A digital twin (DT) is a virtualized representation of a physical system with physical processes for a nuclear power generation facility. This would be accomplished by interfacing the plant's existing ASI infrastructure with the network infrastructure of the DT to provide data and parameters for the physics and engineering process models of the DT.

A digital twin system can be broadly classified into three different sections. The physical section, which is comprised of the actual physical process assets, which includes components such as instrumentation and sensors including thermistors and radiation detectors; controllers such as PLCs and RTUs; and process equipment such as heat exchangers, turbines, etc. There will be a digital section comprised of assets such as servers, workstations, and its own I&C devices that host and run the digital models and virtual simulations of the DT. Finally, there will be a communications section which is made up of network assets

such as routers, switches, servers, wiring, etc. which will provide the interface between the physical and digital components to allow for bidirectional data transfer. For nuclear power facilities, an adversary is likely to be a state-sponsored actor who will have significant capabilities and may target the physical section of a DT, disrupting physical nuclear process equipment. The adversary may utilize techniques such as ransomware to suspend nuclear operations or attempt to cause damage to the physical systems. While the physical components are certainly an interesting target, the adversary may primarily target one or both of the digital section or communications section instead. Should the physical section be dependent on the operation of digital section (e.g. The digital twin ML and AI models are used to collect and calibrate sensor readings for radioactivity) then compromising the digital section assets will achieve a similar effect as compromising a physical asset. It is also possible that the adversary will target multiple sections at once and with the intent of launching an attack that disrupts many subsystems simultaneously for a crippling and/or devasting effect. This type of attack would require significant resources that are commensurate with a nation-state actor to accomplish.

Depending on the adversarial goals and objectives, a compromised asset in any of these sections does not necessarily mean that section is the intended target. An adversary may target one or multiple sections of a DT and may utilize those resources to attack its intended target. For the purposes of this scenario, the adversary will utilize a compromised asset in the digital section or communication section of the DT to transition into the physical section of the plant. A study from the University of Malaga defined a four-layer model for digital twins (Figure 8) to visualize the relationships between various components of the DT and organize attack scenarios for each layer which will used to assist in visualization and understanding of attack scenarios for this report regarding the DT-ASI interfaces.

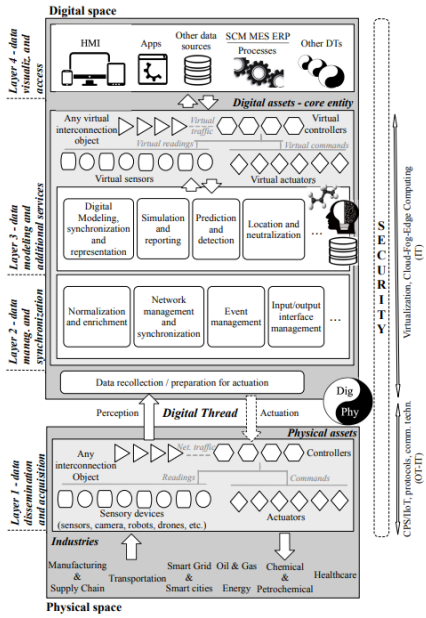


Figure 8: A four layer-based digital twin [34] (See Annex for full image)

- **Layer 1:** Represents the physical process and the data collected from it. (Physical Section)
- **Layer 2:** Represents the communication and information processing equipment required for information to be processed bidirectionally between the plant and DT. (Communication Section)
- **Layer 3:** Represents the engineering and physics models, simulations and other processes required to virtualize the physical processes. (Digital Section)
- **Layer 4:** Represents the end users and technologies that utilize the data generated by the digital twin. (Communication Section)

The following segment explores possible vectors adversaries could leverage to create attack scenarios within digital twins and ASI technology of advanced nuclear reactors. While the scenarios being discussed are theoretical in nature, they are plausible elements which may potentially materialize in the form of a high consequence event. This discussion is in no way exhaustive of every possible outcome; rather, it

serves as a mechanism for conversation on insights into the intrinsic risk areas in this emerging technology.

Each scenario presents unique challenges and requires a tailored approach to mitigate and reduce the impacts of an attack. Understanding the fundamental factors within these scenarios is instrumental in building out appropriate security controls that are adaptable, sustainable, and repeatable in addressing the multifaceted nature of modern cyber threats. This study will examine attacks on the three layers of concern: the physical system, the digital twin, and the communication interface between them.

2.2 The Physical Section

In the nuclear industry, operational functionality and safety of the system is the main focus and can outweigh requirements for the implementation of cybersecurity. System designs that focus specifically on safety, or designs that are based on an improper balance between safety and security, may create opportunities for adversaries to identify and exploit system weakness. Additionally, with the introduction of internet connected IIoT devices (sensors, edge gateways, etc.), adversaries are presented with a broad range of attack vectors to exploit.

Traditionally, in the physical system, consideration of data integrity and validation in field devices such as sensors was neglected and there was an implicit trust of data to be precise, accurate, and reliable. Through exploitation of this trust in combination with supply chain compromise, adversaries may potentially manipulate the data being collected and transmitted. In addition to manipulating the data from sensors, adversaries can exploit vulnerabilities in the supply chain to compromise physical assets either by counterfeit hardware or modifying the firmware or software of the devices. This can result in severe safety issues for operators and other personnel. For example, in 2019, Yokogawa issued an announcement alerting its customers of counterfeit process sensors being sold by unauthorized sellers.c Adversaries were able to counterfeit process sensors and sell them to unsuspecting customers. Yokogawa stated that the counterfeits pose a serious safety risk and that customers must purchase from authorized sellers.

Sensors are calibrated and recalibrated periodically as a preventative safety measure to ensure accuracy of data collection. Proper calibrations and recalibrations of sensors in the nuclear industry are crucial to operations and safety. Interference and manipulation of the process data by an adversary may result in compromised safety, operational disruptions, and unintended consequences.

2.2.1 Attack Scenario – Physical Section

A case study based on a hypothetical scenario was conducted involving supply chain compromise of IIoT pressure sensors used in nuclear reactor applications. The attack was funded by a competent, nation-state adversary with the intent to cause a disruption and impact energy production output in nuclear reactor systems in the targeted region. The threat actor was able to infiltrate the supply manufacturer as an employee on the production floor level and insert malware affecting the firmware of each device intended for the target facility. As the vendor maintained an established relationship with the target organization, the sensors did not undergo further validation between departure from the production

[c] https://doeopexshare.doe.gov/lesson/28014

facility and installation in the target system. Consequently, the infected devices were installed in the physical system of the nuclear reactor unhindered. The attack exploited the inherent trust of sensor measurements to be accurate, and for the digital twin to apply autonomous change to the system in response to those values. Over time, the modified process values transmitted to the digital twin were normalized to be considered within safe operating range, although they deviated beyond recommended component specifications. The system operated in a prolonged state beyond the safe operating conditions, causing accelerated deterioration of components. Maintenance shutdown of the plant was required, far in advance of the anticipated maintenance timeframe for the product life cycle. The threat actors successfully completed their objectives to disrupt operations and decrease energy production of the target.

Preparations for the attack initiated through infiltration of the supply chain vendor. The threat actor possessed sufficient ability to secure a role within the manufacturing organization in a position that provided direct access to the devices targeted for infection. In addition, the adversary was able to leverage opportunities to conduct inside reconnaissance of device functionality to tailor strategies specific for the capabilities of the compromised devices.

The malware consisted of malicious code in a multi-layered approach; it was designed to detect operational network connectivity and send modified packets carrying incorrect sensor data to the digital twin. The machine learning and artificial intelligence algorithms would then use the incorrect data to create an artificial baseline for autonomous control within the digital twin. Based on predefined values using engineering knowledge of nuclear energy production, if the physical system reached a critical state, the sensors would simultaneously trigger a denial of service through packet flooding to prevent the digital twin from responding and restoring the physical system to a stable state.

As the exclusive supplier of the IIoT pressure sensors for the victim, there was an implicit trust relationship between the vendor and the target organization. Although infected sensors were pre-calibrated and verified prior to leaving the production facility, the malware was coded to activate only when IP-specific conditions matching the production network were met. The threat remained undetected until investigations were conducted following identification of the underlying issue.

The malware was successful in increasing the upper pressure limit within the nuclear reactor through minute modifications of sensor data sent to the digital twin over time. Ultimately, the compounded alteration of acceptable operating conditions in conjunction with the digital twin's autonomous closed-loop feedback resulted in the physical system reaching a critical state. Simultaneously, a denial-of-service packet flooding from all infected sensors was triggered due to a predefined pressure value threshold condition being breached. At that point, stakeholders were notified and determined an emergency shut down of the reactor was required to minimize damage and preserve the safety of on-site personnel.

The full impact of the plant shutdown was considerable; significant downtime and resources were exhausted to restore operations to their intended state. A full investigative analysis was conducted to identify the issue, determining it was a cyber incident stemming from a supply chain compromise. The IIoT sensors were required to be redeveloped with increased scrutiny and verification factors at each step of the production process before being re-deployed in the production environment.

Various mitigative actions could be applied in a layered approach to prevent or reduce impact to operations across the duration of the attack. Complacency due to trust relationships in vendor-client relations, reliance on sensor and instrumentation accuracy, and a lack of monitoring for digital twin

autonomous logic provided the means for the attack to be successfully executed. Verification of components would mitigate any of the subsequent events from occurring. A holistic check of sensor hardware, firmware, and software components both prior to leaving the manufacturer and upon arrival in the nuclear facility before installation would ensure intended operation. Additionally, provided there are no environmental constraints, secondary trust sensors could be used for primary sensor validation and measurement verification. These sensors could provide an additional layer of heterogenous information to increase reliability of compromised sensor detection from cyber attacks. Since secondary sensors do not directly measure the primary values, they are not directly related to the process and do not affect operation process loops. Various human-in-the-loop measures could be introduced, such as periodic comparison of component operating specifications against real-time process measurements, as well as comprehensive operator training on acceptable conditions for manual monitoring and identifying problematic situations.

2.3 The Digital Section

In theory, an attack on a digital twin should produce the same results as an attack on the physical system itself, provided there is a dependency on feedback loops and autonomous capabilities. Digital twins commonly function as an anomaly detection tool; the required information for application includes relationships among processes, defined and learned baseline measurements, and libraries of knowledge-based or behavior-based patterns. Exploitation of this deep data and system configuration data can allow an adversary to manipulate the system and force it into an undesirable state.

A digital twin contains the entire inventory of assets found throughout the physical system. They provide an increase in visibility into the physical system and allow operators to view internal components that are not easily accessible. Also, digital twins contain data of component logic and operation input from machine learning algorithms and artificial intelligence. Adversaries can leverage this by exfiltrating the data within the digital twin and replicate the digital twin offline. Once the adversary has a fully operational copy of the digital twin, the adversary can practice exploits and carry out dry-run attacks to determine the best ways to attack the system, whether they are against the physical system itself or the digital twin, undetected and inflict maximum damage.

In the event an adversary has access to the digital twin, there are two modes of attack [35]:

1. **Replication mode** – the digital twin is synchronized with the physical system through sensor measurements, network communication, or log files. It maintains a constant connection with the physical system and may initiate cyclic updates. For an effective attack, the adversary may need to maintain an active connection due to the time-dependent state synchronization and consistency of information between the systems.
2. **Simulation mode** – the digital twin is operated in an isolated environment and requires user-specified settings and parameters as input. It is repeatable with a broad range of trial-and-error learning mechanisms. Attackers may attack the theme of simulation mode – security by design by reverse engineering the defined configurations of the system. The attacker can learn the system passively but cannot trigger automated attacks within the system due to absence of a direct feedback loop.

2.3.1 Attack Scenario – Digital Section

In an additional case study referencing a hypothetical scenario (unrelated to the previous example), the effects of a cyber attack directed at the digital twin component of a nuclear energy facility are examined. This attack consisted of a nation-state threat actor leveraging a server-side request forgery (SSRF) vulnerability [36][37] to exploit an Azure Digital Twin instance in the cloud. The adversary was able to reproduce an offline version of the digital twin in simulation mode to test varying degrees of attack with the intent to maximize system damage and compromise safety systems. The adversary was successful in orchestrating a situation fulfilling the necessary conditions to trigger a high consequence event, forcing an emergency shut down of the facility.

The SSRF vulnerability in the Azure Digital Twins Explorer service was discovered and sold to an unknown nation state to be utilized in an attack. Their objective was to cause damage and impact safety critical systems. Initialization with the cloud-based digital twin did not require authentication and permitted the adversary to identify endpoints, services, and open ports, allowing for initial entry into the cloud environment and facilitate lateral movement. Once inside, the adversary was able to pivot to the host's Cloud Instance Metadata Service (IDMS), exposing detailed information on the target's cloud instances. The adversary then exfiltrated the data and generated an offline duplicate of the digital twin. The vulnerability was a perfect opportunity for the attacker to capitalize on the simulation mode of the digital twin replica to conduct extensive analysis and test a wide variety of attack methodologies.

The threat actors examined various attack vectors within the digital twin with the knowledge that it was an exact replica of the target physical system. First, they investigated the extent of control the digital twin could exert on the reactor. The digital twin was at a mature state, providing autonomous control of many processes within the reactor and operators were dependent on its capabilities to address interdependencies and maintain efficiency of the system. Identifying the relationship between changes in the digital twin and their response on the production environment was critical for the adversary to determine which subsystems to focus their attack on. As their primary objective was to inflict maximum damage on the system, they deployed engineering-based analysis and utilized the physics-based model of the digital twin to simulate attack outcomes.

The adversarial group determined that compromising the primary and secondary power supplies for the cooling systems was the optimal approach. The digital twin capabilities included regulating power to the cooling systems based on sensor feedback. By modifying the data received by the digital twin, it was deceived into throttling the output from the power supplies. In doing so, the cooling systems would be unable to sustain their processes and increase the temperature and pressure within the reactor, causing an explosion that damaged the reactor pressure vessel.

The impact of the attack was substantial; first and foremost, the primary concern was the safety of the operators, which was compromised due to the crippling effect the attack had on the safety mechanisms of the system. As a collateral consequence, the alarm system alerting personnel of the danger was compromised with the disabling of the primary and redundant power supplies. However, while all on-site staff were able to evacuate without serious injury, the potential for a devastating outcome was still present. Secondly, there was critical damage to key components of the reactor, namely the reactor pressure vessel. The time, cost and human resources required for replacement was not insignificant. Technical complexity and plant downtime further stressed recovery of the reactor. Radioactive vapors

were released into the atmosphere and the effects were far-reaching; requirements addressing environmental contamination concerns were adhered to for regulatory compliance and disaster recovery for a period following the incident, including sampling, and monitoring of the surrounding environment in proximity to the facility. Lastly, the misappropriated digital twin technology was still in possession of the adversary. The likelihood of future threats leveraging newly discovered vulnerabilities through exploitation of the digital twin was notable and stakeholder discussion for subsequent course of action was required.

Following the attack, the Azure Digital Twin SSRF vulnerabilities were swiftly addressed by Microsoft. To prevent unauthorized access of the IMDS endpoint, requests were required to contain the "Metadata:true" header and not contain the "X-Forwarded-For" header. Additionally, an "Identity Header" for the Azure service added features for token retrieval in REST endpoints using a managed identity. To do so, two environment variables were defined: IDENTITY_ENDPOINT containing the URL to the local token service, and IDENTITY_HEADER with a rotating value by the platform used to mitigate SSRF attacks.

In this case, risk associated with the digital twin was transferred to the Microsoft Azure provider. Proper cyber hygiene, account protection policies, and logging was exercised, and robust security measures were present from an organizational IT perspective. However, from an OT approach, engineering principles could be used to further increase the security posture of the system. Passive safety features such as analog interlocks not dependent on active systems or external power sources are strongly recommended. Continued training and awareness on security, incident response, and disaster recovery protocols in conjunction with the comprehensive security features enacted by the digital twin would contribute greatly to enhance the security posture of the facility. The digital twin is a powerful tool that can be utilized to optimize operational efficiency and provides an additional analysis capability.

2.4 The Communication Section

With the integration of cloud computing in industrial control systems, companies have the ability to host their digital twins off-site, in the cloud. The digital twins themselves and the data storages that accompany them are prime targets for adversaries. When a digital twin is hosted in the cloud, the physical system must be connected to the internet to allow for bidirectional traffic between the physical system and the digital twin. This allows adversaries to conduct various types of attacks to hijack or interrupt the traffic between both sections. Adversaries can intercept internet traffic between the physical system and the digital twin (a man in the middle attack) and manipulate the data being displayed to the operator or manipulate the data to cause the physical system to react in ways that are undesirable.

Due to the latency requirements, application of cryptographic countermeasures may not be possible, resulting in adversarial access to communications between the ASI and DT. Whether the digital twins are hosted in the cloud or on-premises, the absence of encrypted communication protocols allow adversaries to conduct reconnaissance activities, design attacks, and exploit vulnerabilities within either the physical systems or the digital twins. The absence of encrypted communication protocols allows for adversaries to collect valuable information such as credentials used by administrators providing the adversaries access to systems and components without the need for phishing attacks or social engineering to obtain credentials.

2.4.1 Attack Scenario - Communication Section

This attack scenario highlighted the communications interface between the physical and digital sections as the primary attack vector. Threat actors aimed to disrupt a nuclear power plant using insider knowledge of the communication protocols used at the facility. The adversary deliberately targeted components dependent on wireless communications with a single point of failure to cause a short denial of service within certain devices, resulting in the digital twin being deprived of real-time process data. Operators were required to manage operations manually until services were restored.

Although execution of the attack was straightforward, it demanded meticulous understanding of the facility network infrastructure. Reconnaissance was a pivotal step in determining the specific targets within the nuclear operations. The adversary utilized techniques such as spear phishing, social engineering, and open-source intelligence gathering to obtain a list of system components vulnerable to the attack method. Employees, supply manufacturers, and contractors involved in the installation of the private 5G network were targeted to gain information on the communication frequency bands. The information was used to acquire signal jammers with long range capabilities on the dark web black market.

Once preparations were complete, the threat actors configured the jammers strategically placed outside the facility perimeter to simultaneously disrupt all applicable sensors during peak energy production periods. Facility operators were immediately alerted of the disruption and transitioned to a fallback manual operation mode as the digital twin could no longer function autonomously without real-time data input. In accordance with incident response policies and procedures at the facility, processes and systems were required to be manually monitored until investigation of the incident had concluded. Although no considerable damage was done, operations were partially disrupted, and energy production was reduced during the transient phase between the digital twin control and manual mode. In addition, the facility operations were assessed, and security was on high alert for an extended period.

The usage of multiple frequency bands through band hopping and switching with randomized intervals may have prevented, or at a minimum, minimized the disruptions from the frequency jamming. However, this strategy would require a larger allocation of 5G bandwidth to accommodate multiple subchannels or frequencies to switch to., Frequency interference and source identification technologies would allow stakeholders to quickly detect and intercept incidents as soon as they occur.

3. Recommendations for Countermeasures

Effective mitigation of risks associated with vulnerabilities, attack vectors, and the attack surface is possible by identifying opportunities to introduce additional countermeasures that increase the cybersecurity posture of the system. While no unified framework for digital twin-based security currently exists [38], it is advisable to implement countermeasures in accordance with organizational risk tolerance. The implementation of additional countermeasures can also position the overarching cybersecurity strategy to further align with anticipated future regulations. A multifaceted cybersecurity approach addressing both traditional cybersecurity implications and kinetic impacts allows for a holistic framework to be developed, ensuring long term sustainability and resilience in both the physical system and digital twins.

3.1 A Resilient Framework for Sensor-Based Attacks

To address concerns of primary sensor compromise, a framework for recovery of control was developed by the U.S. Naval Academy and the University of Maryland. It includes three concepts [39]:

1. Secondary sensors to provide an assessment of the primary sensors' trust status.
2. A trust-weighted consensus algorithm that fuses estimates from observers of interconnected processors with information from the secondary sensors to accurately reconstruct the state of the attacked process.
3. Communication-aware self-triggered control protocols that regulate the attacked process using the consented estimate in the absence of reliable data from its primary sensor.

Secondary, non-intrusive sensors are proposed to validate the trust status of primary sensors deemed essential to operations. These auxiliary sensors typically have lower fidelity and are utilized for verification of trust through measurement of quantities that are independent, yet related to the primary sensor measurements, and therefore do not demand stringent real-time latency requirements. Secondary sensors utilize different technology or physical principles than primary sensors to minimize the likelihood of common-mode failures. However, they may leverage interdependencies to extrapolate data to determine the trust status of primary sensors.

The strategic utilization of heterogenous sources of data in anomaly detection aims to enhance the speed and reliability of detecting compromised sensors resulting from cyber-attacks. Validation through secondary sensors effectively increases detection of sensor failure, maintains the high fidelity of sensor data, and increases the system's resilience to sensor failures. In the event of an attack, extrapolation of data from secondary sensors may provide sufficient information to reconstruct affected system processes, facilitating continuous operations without significant disruptions, offer insight for post-attack analysis, and expedite the process of recovery efforts.

A trust-weighted consensus scheme using data from secondary sensors is employed to determine primary sensor trustworthiness and identify compromised sensors. The trustworthiness data is then subsequently fed into a trust-weighted consensus algorithm and integrated with process state estimates to mitigate attacks. The integration leverages a direct correlation between the trust of a sensor and the weight of their measurements for control of processes within the system. As the consensus feedback signal is continuously updated, sensors that no longer transmit false information regain trust and weighting within consensus values to autonomously stabilize conditions for intended operating behavior.

Self-triggered control is an effective control strategy to reduce strain on communication resources while preserving system stability and operational integrity should sensor-based attacks occur. The self-triggered control scheme initiates a consensus event based on global trust-weighted state estimates that trigger actions utilizing predefined conditions that are necessary to maintain the operating state and preserve plant stability. The state estimate then provides adaptive response for the continuous operation of the system until the system returns to a predictable, safe state.

Utilizing these three concepts to mitigate risks and minimize potential impacts on operational processes allows stakeholders to proactively address vulnerabilities and reinforce the capability to respond effectively to sensor compromises. This provides a heightened level of resilience within the

system to withstand attacks attempting to disrupt processes, damage components, and cause harm within nuclear operations. By integrating these principles, robust defensive countermeasures are applied, enhancing not only the system's ability to resist adversarial threats but also its capacity to swiftly recover and continue operations.

3.2 Data-Driven and Physics-Based Modeling for Digital Twins

Both data-driven and physics-based modeling for digital twins can be applied to determine the underlying indicators of a cyber-attack. Each model possesses distinct advantages and disadvantages, and this section explores how these models can be applied simultaneously to minimize their respective limitations within the framework of a sustainable digital twin deployment. By employing a synergistic integration of data-driven and physics-based approaches, a more comprehensive understanding of cyber-attacks can be achieved. This approach empowers digital twins to not only detect and respond to known attack patterns but also adapt to emerging threats and anomalies, ultimately enhancing the resilience and security of nuclear systems.

CAPABILITY	DD	PB
Immune to operating point change?	N	Y
Diagnosis resolved to specific fault?	N	Y
Rank ordering of likelihood of faults?	N	Y
Applicable to engineering systems?	—	Y
Free of need for library of fault signatures?	N	Y
Generates virtual sensors?	N	Y
Adapts upon dropped sensor?	—	Y
Yields component performance index?	N	Y
Supports design of optimal sensor set?	N	Y

Figure 9: Advantages of a Physics-based Model vs. Data-driven Model [41]

Machine learning and big data processing have significantly enhanced the capability of data-driven models in the detection of anomalies through the analysis of heterogeneous, real-time data streams. These models exhibit scalability and adaptability, allowing them to continuously monitor and analyze varying data volumes while adjusting for changes in operational conditions and status. Empirical data is leveraged to provide a realistic representation of system behavior, offering immediate insights into cybersecurity threats. This does raise a significant concern regarding the balance of sensitivity and false-positive alarms, which may lead to issues related to reliable reporting. Furthermore, data-driven models are susceptible to data poisoning, including sensor data manipulation, which can result in misguided autonomous actions.

To address the limitations of data-driven models (Figure 9), the incorporation of a physics-based model offers a means to identify specific faults, provided the available sensor data is sufficient. This approach facilitates a deep understanding of the underlying physical processes, enabling identification of potential cyber threats and vulnerabilities derived from system scenario simulations through analysis of critical parameters within the calculation process. Physics-based models require minimal dependency on data, instead relying on established scientific principles and equations, providing stability under a wide range of conditions. In addition, the capability to estimate unmeasured process variables provides an increased heightened understanding of the current system state. However, physics-based modeling also presents its own set of challenges. Calculations required for the model are resource-intensive and often time consuming and may not be suitable for rapidly changing conditions. As well, physics-based models rely on computational simulations leveraging fundamental physical principles and laws, resulting in limitations to account for nuances in complex system components and infrastructure.

Unifying data-driven and physics-based models within a digital twin strategically offsets each model's respective limitations, enabling the implementation of robust security measures for protecting the

operational integrity of the system. By cross-referencing data-driven insights from real-time sensor measurements with the foundational understanding of the physical characteristics of nuclear processes, digital twins can not only detect abnormalities but also identify the exact source of the anomaly to facilitate immediate incident response and recovery. As these models continuously adapt and learn from real-time data and account for underlying physical principles, they can dynamically evolve to anticipate and mitigate emerging vulnerabilities and attack vectors. This integration allows for validation of sensor data through quantitative analysis and capitalizes on the inherent strengths of each model to provide a comprehensive understanding of the system's behavior [42].

3.3 Mitigative Tools

In the age of digitization and advanced technology application across various industries, software solutions like the PRO-AID and General Electric's Digital Ghost represent notable advancements in implementing robust, real-time monitoring and cybersecurity defense systems for industrial assets and critical infrastructure. The PRO-AID software package, developed by Argonne National Laboratory, utilizes automated reasoning and a physics-based digital twin, meticulously crafted from piping and instrumentation diagrams supplemented by a component library, to ensure accurate real-time monitoring and diagnostic procedures within predefined sensor measurement parameters. On the other hand, GE's Digital Ghost, as an amalgamation of digital twin technology and edge computing, employs a comprehensive defense mechanism against cyber threats through machine learning and AI, offering not only detection, localization, and neutralization of abnormalities but also predictive capabilities and heightened situational awareness within the system's operational sphere. These innovative approaches not only stand testament to the strides in digital twin technology and cybersecurity in the industrial realm but also pave the way towards a discussion on their application, integration, and future developments in securing critical infrastructural environments.

3.3.1 Pro-AID

The PRO-AID software package, conceived and developed by Argonne National Laboratory, epitomizes the confluence of digital twin technology and automated reasoning, deploying them astutely to navigate the intricacies of real-time monitoring and diagnostics in various systems. Through the meticulous creation of a physics-based digital twin—utilizing detailed piping and instrumentation diagrams and enriched by a comprehensive library of plant components—PRO-AID achieves a nuanced and precise overlay of the physical system in a digital realm. This approach is not only academically fascinating but also practically essential in arenas such as nuclear power plants or chemical processing facilities, where accurate diagnostics and monitoring are paramount to both efficiency and safety. For instance, consider a scenario involving a nuclear reactor cooling system, where any discrepancies or failures could result in catastrophic outcomes. In such a scenario, PRO-AID, through its digital twin, would actively engage in real-time monitoring of parameters such as coolant flow rate, temperature, and pressure, ensuring that they align precisely with the predefined and accepted physical models. If a sensor indicates a sudden spike in temperature—an anomaly not corroborated by the majority and potentially indicative of a sensor fault rather than a genuine system failure—the software is engineered to minimize false alarms by correlating this data against the expected physical phenomena within the digital twin. This sensor data is systematically validated against the stringent parameters defined within the system's digital

replica, thereby mitigating the risk of erroneous alarm triggers, and ensuring that any diagnostic actions or alarms are substantiated by accurate, verifiable data, which is crucial in maintaining both the reliability and safety of the monitored system. Illustrative examples and a deeper dive into the PRO-AID software application might be depicted in Figure 10, shedding light on its operational nuance and reliability in a tangible, industrial context.

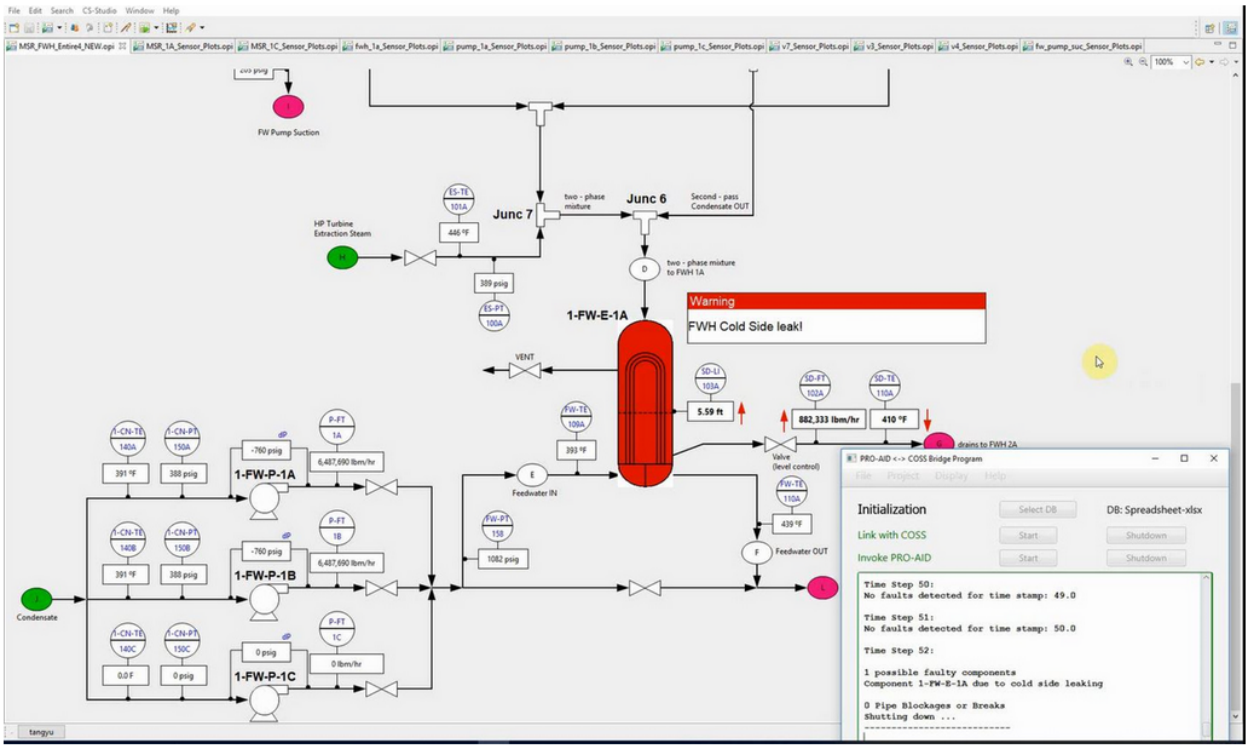


Figure 10: PRO-AID Software [43]

Argonne National Laboratory is also developing a software package for maintenance optimization integrating PRO-AID diagnostic information in conjunction with underlying knowledge of component deterioration mechanisms.

3.3.2 Digital Ghost

General Electric's Digital Ghost is a real-time, active cyber defense system for securing industrial assets and critical infrastructure [45][46]. As a combination of GE's digital twin and edge computing technologies, it leverages machine learning and artificial intelligence driven by high-performance algorithms. Its multifaceted functionality encompasses the detection, localization, and neutralization of abnormalities, in addition to capabilities to predict deviations in system processes, heighten situational awareness on irregular events, and provide early warning for unintended behavior. While the digital twin represents the precise operating conditions and state of a system, the Digital Ghost possesses abilities to not only detect anomalous activity but to also identify the compromised sensor accurately. The Digital Ghost offers a sophisticated solution to combine digital twin functionality, machine learning, and predictive algorithms for robust countermeasures in response to the rapidly evolving threat landscape.

4. Cyber-Informed Engineering Strategies

4.1 Cyber-Informed Engineering

Cyber-Informed Engineering (CIE) is a methodology or approach that can be used by engineers to characterize the risks presented by the implementation of digital assets in control system environments and provides a strategy to apply engineering risk processes to mitigate those risks [47]. CIE is applied throughout the entire systems engineering lifecycle, from conceptual design to decommissioning. Cyber risks are considered at the earliest design stages (the most optimal time to introduce cybersecurity approaches effectively) and are continually reanalyzed throughout the entire lifecycle. Not only are digital failures and unintentional cyber incidents included in cyber risk, but the possibility that an adversary may purposefully disrupt, deter, deny, degrade, or compromise digital systems in such a manner to cause harm to the organization and its personnel [48].

4.1.1 Engineering Process

The most commonly used engineering process model is the DOT Vee or Engineering Vee Department of Transportation Systems Engineering process. This model is used to illustrate the relationships between all phases of the development lifecycle. The model emphasizes the importance of testing and validation are continually performed throughout the development lifecycle of the system [49]. As shown in Figure 11, the left side of the "V" indicates a top-down approach starting with the system as a whole moving down to the subsystem(s) and lastly to the components within the system. As the lifecycle of the system progresses, the right side of the "V" indicates a bottom-up approach through the implementation and testing of each layer from the component layer to the subsystem to the system layer [49].

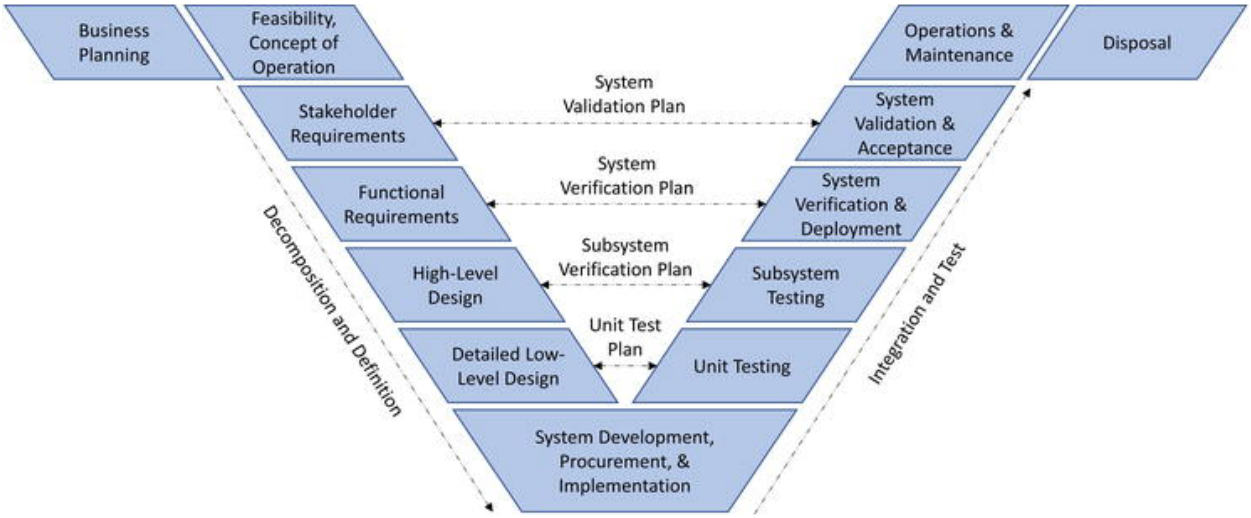


Figure 11: DOT Vee or the Engineering Vee Department of Transportation Systems Engineering Process [50]

In scrutinizing Figure 11, the meticulous structuring and systematic progression of the DOT Vee model become palpably apparent, offering viewers a tangible visual representation of an engineering paradigm. The figure illustrates the cascade from a holistic system viewpoint down through its constituent subsystems and components, embodying a decomposition that ensures every minute detail is considered, scrutinized, and validated in the developmental phase. Concurrently, the ascending right side of the "V"

depicts the reintegration of these validated components, culminating in a cohesive system. This visual representation underscores the quintessential balance between detailed analysis and holistic synthesis that is pivotal in navigating the complexity and multi-faceted challenges encountered in systems engineering. The DOT Vee model, thus, not only serves as a blueprint for engineering projects but also as a symbolic reminder of the necessity for a disciplined, systematic approach in navigating the convoluted journey from conceptualization through to realization in engineering endeavors.

4.1.2 CIE Principles

There are two groups of principles within the Cyber-Informed Engineering methodology that must be considered throughout the development lifecycle. These groups are Design and Operational Principles and Organizational Principles. Each group has its own set of elements that make up an ICS engineering risk management process [51].

Design and Operational Principles

Consequence-Focused Design – CIE strategies should be applied to the critical functions where cyber manipulation could result in undesirable or unacceptable consequences at the very beginning. Organizations must identify where cyber-attacks may result in high-consequence events and examine how to prevent and avoid such consequences through secure design, implementation, and operation.

Engineered Controls – To minimize cyber risk, organizations should integrate engineering changes and process controls early in the system design phase, reducing the subsequent need for added IT cybersecurity controls. This involves the collective use of controls and processes to prevent high-consequence events and necessitates a collaborative effort between engineers and cybersecurity specialists to incorporate cybersecurity into system design, engineering, and modification phases.

Secure Information Architecture – Design information pathways to ensure that data only flows in desired ways and enforce the designed information flows using proper architectural controls. This will limit an adversary's ability to use the system or the information within the system in undesirable ways to the organization.

Design simplification – simplify the system, subsystem, components, or architecture design to limit high-consequence events and unnecessary complexity within digital functions. This reduces the opportunity for adversaries to misuse the digital component of the system.

Resilient Layered Defenses – Employ a defense-in-depth strategy that reduces the opportunity for a single point of failure to impact the system's critical functions or create a domino effect of cascading failures. Defense-in-depth includes building in redundancy, system hardening, and cybersecurity appliances as various levels of the system architecture.

Active Defense – utilize dynamic elements throughout the design of the system that can detect and defend against cyber threats. This enabled the system to continuously operate in the event an intruder is detected, isolating, or removing the threat without compromising critical operations.

Organizational Principles

Interdependency Evaluation – Consider input from multiple disciplines and operational departments within the organization to understand how the misuse of the digital component could affect their area of operation. This ensures that engineers plan for cyber risks that are introduced by system interdependencies that may be outside of the engineer's purview.

Digital Asset Awareness – Maintain an accurate and up-to-date digital asset inventory that allows engineers to track hardware, software, and firmware of assets over time. This enables engineers to detect, evaluate, and analyze vulnerabilities that reside in digital assets.

Cyber-Secure Supply Chain Controls – Use procurement language and contract requirements to ensure that vendors, integrators, and third-party contractors adhere to organizational policies and procedures, processes, and controls that support cybersecurity. Also, use procurement language and contract requirements to ensure products meet design specifications upon delivery.

Planned Resilience with No Assumed Security – Expect that any digital asset can be compromised at any point during its lifecycle. Plan for continuous operation during all cyber-attack lifecycle phases that may degrade digital controls. Develop and exercise an incident response and contingency plan.

Engineering Information Control – Ensure the protection of sensitive engineering records that may provide an adversary with critical information that puts the system at greater risk. This includes requirements, specifications, designs, configurations, testing, etc.

Cybersecurity Culture – Ensure that cybersecurity is built into the organizational culture by leveraging a cross-functional and cross-disciplinary team to take into consideration cyber-related concerns in the system design and implementation. Enforce continuous cybersecurity training across the entire organization to empower employees to actively participate in cybersecurity.

4.1.3 CIE Pillars

The National Cyber-Informed Engineering Strategy developed by the U.S. Department of Energy is built on five integrated pillars. These five pillars offer a set of recommendations on how to apply CIE to the energy infrastructure, and to incorporate CIE as a common practice in future energy systems to reduce or eliminate the opportunity for a cyber-attack to generate a significant impact [51][52].

Awareness – Raise awareness of the CIE approach, the gaps it addresses, its potential when implemented, and the major benefits among decision makers in the engineering community.

Education – Develop a pipeline of CIE practitioners through education, training, and certification of CIE knowledge and skills.

Development – Mature CIE approaches and promotes broad application by building a repository of tools, practices, methods, and other enrichments that practitioners can draw upon to apply CIE to existing and new infrastructure and validate CIE applications.

Current Infrastructure – Use a consequence-driven approach to identify and apply CIE principles to the nation's systemically important critical infrastructure already commissioned and in service today.

Future Infrastructure – Nurture and sustain an Energy Sector Industrial Base that enables manufacturers and asset owners to apply CIE principles into the full lifecycle of newly commissioned critical infrastructure systems.

4.2 Attack Impacts - Small Modular Reactors and Wind Turbines

In the nuclear industry, small modular reactors are an emerging technology generating sustainable, efficient, and clean energy. The core principle underlying the operation of SMRs is the controlled fission of radioactive materials within the reactor's fuel rods. This fission process releases an enormous amount energy in the form of heat that must be efficiently converted into electricity. One of the fundamental methods employed within SMRs for conversion of thermal energy into electricity is the integration of

steam turbines, as illustrated in **Error! Reference source not found.**. This section will explore the impact of an attack targeting the underlying engineering relationship between the SMRs and wind turbines and apply cyber-informed engineering strategies to mitigate these consequences using autonomous control within digital twins.

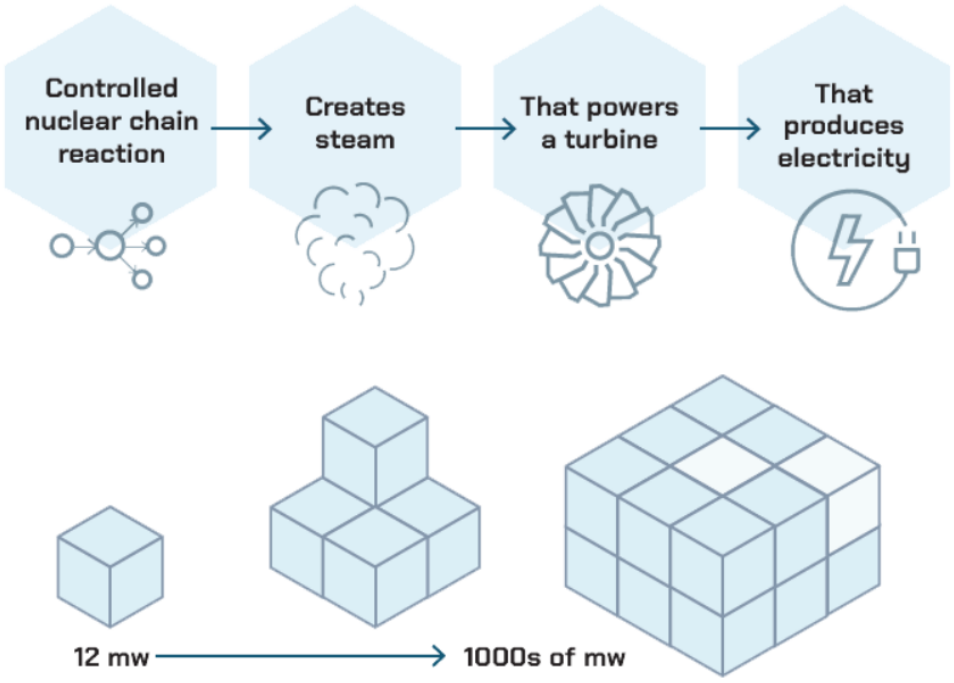


Figure 12: Stages of nuclear energy production in small modular reactors [53]

In contrast to traditional nuclear reactors, SMRs are characterized by their simplified designs and capabilities for diverse configurations adaptable for a variety of environments. The key factor distinguishing them in security lies in safety features that rely on physical phenomena [54] (e.g., natural circulation, self-pressurization, gravity) during abnormal process states, resulting in a reduction in scenarios requiring the need for human intervention to cool or shut down the system. This automatic response enhances safety and resilience within system operations in the event of an emergency whether they originate from a system fault or cyber-attack.

4.2.1 Water Induction and Moisture Carryover

Water induction is an inadvertent introduction of liquid water or vapor into the steam turbine during operation. It is a critical risk with consequences ranging from accelerated deterioration of components within the turbine to catastrophic failure [55]. It can have detrimental effects on operation such as erosion, corrosion, and the formation of droplets, all of which can reduce turbine efficiency, increase maintenance costs, and shorten the equipment's lifespan. Understanding and preventing water induction is crucial to the safety and continued operations of nuclear energy generation. In recent years, advancements in technology and research have provided insights into the complex mechanisms underlying water induction in steam turbines.

Moisture carryover represents a distinct form of water induction, as it directly corresponds to the unintended presence of liquid within a mixture intended to consist exclusively of dry steam. Originally, the steam drying system was designed to limit MCO to within acceptable levels through engineered design

features [57]. Recent enhancements in other areas of the system have reduced quality of steam and increased velocity of steam through moisture separators, resulting in the prevalence of excessive MCO levels. The impact of moisture carryover relies on a variety of factors (e.g., temperature differential between the water and components, duration of the unintended state, etc.) However, the severity of the impacts can be quantified through analysis of process performance, continued real-time sensor measurements, and insight through digital twin machine learning. Ultimately, the primary concerns are elevated dose exposure to on-site personnel [57], and failure of components due to physical degradation, such as warping of turbine blades. If such a situation materializes, it is highly likely a reduction in efficiency will occur. In addition, affected components may require further maintenance and inspection leading to additional maintenance costs.

A proficient threat actor, versed in engineering principles and systems operation, could exploit vulnerabilities in the nuclear operational technology by manipulating sensor readings, spoofing control commands, or instigating water induction scenarios. This could be achieved through an array of sophisticated methods like utilizing advanced persistent threats (APTs) to infiltrate and linger within the network, deploying malware to disrupt data integrity, or exploiting cybersecurity vulnerabilities in IoT devices and control systems to induce malfunctions. Such a malefactor might seek to manipulate moisture carryover, escalating the risk of component failures or perhaps even orchestrating a catastrophic event by leveraging their understanding of system dynamics and exploiting cybersecurity weaknesses.

Utilizing cyber-informed engineering (CIE) strategies can thwart such nuanced attacks by enforcing multidimensional security protocols and real-time anomaly detection through the digital twins. The digital twins, reflecting the optimal operational parameters and conditions, would instantaneously detect discrepancies stemming from malicious tampering, such as alterations in moisture carryover metrics or abnormal shifts in turbine performance indicators. Concurrently, robust cybersecurity measures, informed by the CIE, ensure that counteractive actions are promptly deployed to safeguard the physical systems. This could include automatically isolating compromised systems, triggering fail-safes, or initiating immediate remedial actions, thus preserving system integrity, and ensuring continuous, secure operations amidst the cyber-physical threat landscape. This multi-faceted approach, intertwining astute engineering principles with vigorous cybersecurity practices, offers a resilient defense mechanism against adept adversaries aiming to compromise critical nuclear infrastructure.

4.3 Cyber-Informed Engineering Leveraging Digital Twins

Cyber-informed engineering is a significant influence that enhances design, operation, and security of complex nuclear systems. When combined with the capabilities of digital twins, there are a host of benefits that promote the development of highly resilient and secure systems.

Digital twins provide a realistic environment to simulate and test various scenarios and configurations, enabling engineers to identify weaknesses and vulnerabilities prior to deployment on live systems. A combination of data-driven and physics-based modeling discussed in previous sections further cultivate machine learning algorithms for early detection of deviations and anomalies that may potentially lead to adverse effects within a system. Cyber-informed engineering incorporated into the digital twin allows for an increased level of security by assisting in the process of identifying interdependencies in the system, providing insight for visualizing the system design, and testing the impact of cybersecurity measures against threat simulations. This allows stakeholders to refine safeguards while preserving system

performance, ultimately fostering a more secure and resilient environment. Such an approach facilitates a feed loop for continuous improvement, with real-time data being fed to the digital twin, which in turn provides insights for guiding engineering decisions and improvements to the physical process, reflected in improvement of operational flow.

Configuration of the digital twin's autonomous control on the physical system requires a cyber-informed engineering approach to ensure the safety, reliability, and security of the physical and digital systems. Mitigation of cyber risk surrounding the digital twin involves validation and verification of control actions; a combination of artificial intelligence algorithms and operator insight into the nuances and intricacies of the underlying engineering factors provides multiple layers of defense against cyber-attacks.

In relation to the moisture carryover issues discussed above, a cyber-informed engineering approach can utilize the autonomous capabilities of the digital twin to address those concerns. Employing the hybrid data-driven and physics-based modeling allows for real-time tracking and adaptation of primary sensor data directly correlated with moisture carryover, while at the same time validating those changes through calculation of variables using principles of physical laws that govern the behavior of the system. Identifying the necessary processes to ensure the minimization of moisture carryover through interdependencies within the system allow the digital twin machine learning algorithms to recognize patterns associated with potential moisture carryover and limit it through corrective action at an early stage (e.g. near instantaneous response to decrease steam flow or temperature for optimal steam quality). The digital visualization of these autonomous process changes and their effects allow engineers to effectively optimize systems to reduce the moisture carryover for future design.

5. Recommended Pathways

The hypothetical attack scenarios have outlined that the possibility of altering the baseline utilized by the digital twin for autonomous control of a nuclear reactor exists. Based on the potential impact of modifying the parameters associated with advanced sensor data to cause significant damage to nuclear reactor operations, several pathways exist to further understanding with these risks. Considering the impact of an attack on both the physical section and the digital section of the digital twin infrastructure could cause the system to operate outside of normal operational parameters, additional compensating controls must be analyzed. A number of pathways exist to further analyze the effectiveness of additional compensating controls.

The potential for false data to be processed by the autonomous control system allows an adversary to alter the functionality of the system gradually over time and potentially cause damage to system components as well as affect the safety of operators. The implementation of additional security controls to validate the integrity of the data may sufficiently reduce this risk, however, the machine learning algorithms may still be susceptible to the alteration of baseline data. This risk can be further analyzed to give a greater understanding of how the machine learning algorithm itself may be utilized as an attack vector by an adversary. Should an adversary be able to modify the algorithm itself, this may present an opportunity to alter the functionality of the autonomous system without compromising the integrity of sensor data.

Given further allocation of time for research, a reasonable pathway would provide simulations of the various attack scenarios described. Results could be analyzed and validated against attack outcomes to

gauge plausibility of each scenario and the realistic impact each mitigation control would provide, contributing to the overall maturation of the digital twin.

6. Summary

This report outlined several considerations for evaluating cyber threats and vulnerabilities associated with digital twins and advanced sensors and instrumentation. On-premises, cloud-based, and third-party implementation modes for digital twins were explored and analyzed for sustainability, reliability, and safety in response to evolving threats within the nuclear industry. A comprehensive assessment was conducted surrounding interfaces and communications within advanced reactor architecture, noting key factors for risk mitigation and impact reduction. Investigation into possible attack scenarios and techniques for exploitation of vulnerabilities against physical, digital, and communication sections of digital twin implementations resulted in countermeasures developed for general applicability to small modular reactors. The integration of cyber-informed engineering methodology to digital twins with regards to autonomous control proved valuable in enhancing the security of nuclear energy generation operations.

Moving forward, this report establishes a baseline for guidance in securing advanced nuclear facilities while maintaining optimal system performance and ensuring operational efficiency. However, further research is required to address challenges associated with system intricacies on a case-by-case basis to develop targeted solutions specific to the facility in question.

References

[1] United States N.R.C, 2023. “Digital Twins.” https://www.nrc.gov/reactors/power/digital-twins.html

[2] Nakoogar, F., 2022. “Integration of Wireless Sensor Networks and Battery-Free RFID for Advanced Reactors”. U.S. DOE 16-50050-16_R0. https://www.energy.gov/ne/articles/advanced-sensors-and-instrumentation-newsletter-issue-16-march-2022

[3] Ala-Laurinaho, R., 2019. “Sensor Data Transmission from a Physical Twin to a Digital Twin.” Aalto University. https://core.ac.uk/download/pdf/199295333.pdf

[4] Kochunas, B. and Huan, X., 2021. “Digital Twin Concepts With Uncertainty for Nuclear Power Applications.” Energies 2021, 14, 4235. https://www.mdpi.com/1996-1073/14/14/4235

[5] Al Rashdan, A.Y., Farber, J.A., Montezzo Coelho, M.E., Primer, C.A., Yadav, V. 2022. “Integration of Control Methods and Digital Twins for Advanced Nuclear Reactors.” INL/RPT-22-69937-Rev.0, Idaho National Laboratory. https://www.osti.gov/biblio/1924292

[6] Yadav, V., Zhang, H., Chwasz, C.P., Gribok, A.V., Ritter, C., Lybeck, N.J., Hays, R.D., Trask, T.C., Jain, P.K., Badalassi, V., Ramuhalli, P., Eskins, D., Gascot, R.L., Ju, D., Iyengar, R. 2021. “The State of Technology of Application of Digital Twins.” TLR/RES-DE-REB-2021-01. U.S. NRC. https://www.nrc.gov/docs/ML2116/ML21160A074.pdf

[7] Primer, C.A., Calderoni, P., Agarwal, V., Ramahaulli, P. Vilim, R. 2020. “Nuclear Energy Enabling Technologies (NEET): Advanced Sensors and Instrumentation (ASI) Program Plan.” INL/EXT-20-57280. Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_22022.pdf

[8] Bhuyan, A. 2022. “Idaho National Laboratory (INL) Wireless Test Beds for Over the Air (OTA) Experimentation.” INL/CON-22-67504-Revision-0. Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_63140.pdf

[9] IAEA. 2023. “International Workshop on Instrumentation and Control, and Computer Security for Small Modular Reactors, Chair Report.” IAEA.

[10] IAEA. 2023. “International Workshop on Instrumentation and Control, and Computer Security for Small Modular Reactors, Appendix 2 – Working Group Reports.” IAEA.

[11] IAEA. 2023. “Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors, Appendix 7 – Technical Meeting Report.” IAEA.

[12] Laikari, A., Backman, J. 2021. “Industrial Internet of Things in Nuclear: Feasibility Study.” ISBN 978-91-7673-726-2, Energiforsk. https://energiforsk.se/media/29219/industrial-internet-of-things-in-nuclear-energiforskrapport-2021-726.pdf

[13] Preston, J., Bertolli, M., Eggers, S., McKenzie, P.L., Thorsen, D., Haack, J., Thomas, K., Burke, L.M., Rosa De Jesus, D.A. 2022. “Emerging Threats and Technology Investigation: Industrial Internet of Things – Risk and Mitigation for Nuclear Infrastructure.” IROS65120. Office of International Nuclear Security. https://doi.org/10.2172/1893157

[14] Office of Nuclear Energy. 2022. “Idaho National Laboratory Demonstrates First Digital Twin of a Simulated Microreactor.” https://www.energy.gov/ne/articles/idaho-national-laboratory-demonstrates-first-digital-twin-simulated-microreactor

[15] Microsoft. “What is Azure Digital Twins?”. Accessed 2023. https://learn.microsoft.com/en-us/azure/digital-twins/

[16] Microsoft. “Digital twins and their twin graph.” Accessed 2023. https://learn.microsoft.com/en-us/azure/digital-twins/concepts-twins-graph

[17] Microsoft. “DTDL Models.” Accessed 2023. https://learn.microsoft.com/en-us/azure/digital-twins/concepts-models

[18] Github. “Digital Twins Definition Language (DTDL). Accessed 2023. https://github.com/Azure/opendigitaltwins-dtdl/blob/master/DTDL/v3/DTDL.v3.md

[19] Microsoft. “Azure Digital Twins data history (with Azure Data Explorer).” Accessed 2023. https://learn.microsoft.com/en-us/azure/digital-twins/concepts-data-history

[20] Microsoft. “Data ingress and egress for Azure Digital Twins.” Accessed 2023. https://learn.microsoft.com/en-us/azure/digital-twins/concepts-data-ingress-egress

[21] Microsoft. “Secure Azure Digital Twins. Accessed 2023. https://learn.microsoft.com/en-us/azure/digital-twins/concepts-security

[22] Microsoft. “Azure Digital Twins high availability and disaster recovery. Accessed 2023. https://learn.microsoft.com/en-us/azure/digital-twins/concepts-high-availability-disaster-recovery

[23] Yadav, V., Zhang, H., Chwasz, C.P., Gribok, A.V., Ritter, C., Lybeck, N.J., Hays, R.D., Trask, T.C., Jain, P.K., Badalassi, V., Ramuhalli, P., Eskins, D., Gascot, R.L., Ju, D., Iyengar, R. 2021. “The State of Technology of Application of Digital Twins”. TLR/RES-DE-REB-2021-01. Idaho National Laboratory. https://www.nrc.gov/docs/ML2116/ML21160A074.pdf

[24] L3Harris™. 2022. “High Realism Simulation & Training.” L3Harris™.

[25] L3Harris™. “Orchid Total Development & Simulation Environment”. Accessed 2023, https://www.l3harris.com/all-capabilities/orchid-total-development-simulation-environment

[26] L3Harris™. “Simulator DCS Solutions”. Accessed 2023, https://www.l3harris.com/all-capabilities/simulator-dcs-solutions

[27] GSE Systems™. 2012. “SimExec™ & JADE Installation Guide Version 4.1.” GSE Systems, Inc.

[28] GSE Systems™. 2015. “PSAHD Product Overview.” GSE Systems, Inc.

[29] GSE Systems™. 2013. “SimExec™ Simulation Executive and JDashboard™ Graphical User Interface. GSE Systems Inc.

[30] GSE Systems™. 2012. “SimExec™ Product Overview.” GSE Systems, Inc.

[31] GSE Systems™. “Which I/O System is right for your simulator?” Accessed 2023, https://www.gses.com/2023/06/22/simulator-io/

[32] Boring, R., Agarwal, V., Fitzgerald, K., Huge, J., Hallbert, B. 2013. “Digital Full-Scope Simulation of a Conventional Nuclear Power Plant Control Room, Phase 2: Installation of a Reconfigurable Simulator to Support Nuclear Plant Sustainability.” INL/EXT-13-28432. Idaho National Laboratory.

[33] Westinghouse. 2011. “Nuclear Automation: AP1000® Full-Scope Simulator.” Westinghouse Electric Company.

[34] Alcaraz C and J. Lopez. 2022. “Digital Twin: A Comprehensive Survey of Security Threats.” IEEE Communications Surveys & Tutorials, vol. 24, pp. 1475 – 1503. https://doi.org/10.1109/COMST.2022.3171465

[35] Suhail, S., Jurdak, R., Hussain, R. 2023. “Security Attacks and Solutions for Digital Twins.” Computers in Industry, Volume 151. doi:10.1016/j.compind.2023.103961

[36] Shitrit, L.B. 2023. "How Orca Found Server-Side Request Forgery (SSRF) Vulnerabilities in Four Different Azure Services." Orca Security. https://orca.security/resources/blog/ssrf-vulnerabilities-in-four-azure-services/

[37] Shitrit, L.B. 2023. "Unauthenticated SSRF Vulnerability on Azure Digital Twins Explorer." Orca Security. https://orca.security/resources/blog/ssrf-vulnerabilities-azure-digital-twins/

[38] Tsiknas, K., Taketzis, D., Demertzis, K., Skianis, C. 2021. "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures." Special Issue Cyber Security and Privacy in IoT. https://doi.org/10.3390/iot2010009

[39] Severson, T.A., Croteau, B., Rodríguez-Seda, E.J., Kiriakidis, K., Robucci, R., Patel, C. 2020. "A Resilient Framework for Sensor-Based Attacks on Cyber-Physical Systems Using Trust-Based Consensus and Self-Triggered Control." https://doi.org/10.1016/j.conengprac.2020.104509

[40] Argonne National Laboratory. "Digital Twin." Accessed 2023. https://www.anl.gov/nse/ai-ml/digital-twin

[41] Argonne National Laboratory. "Maintenance." Accessed 2023. https://www.anl.gov/nse/ai-ml/maintenance

[42] Blackseth, S.S., Rasheed, A., Kvamsdal, T., San, O. 2022. "Combining Physics-Based and Data-Driven Techniques for Reliable Hybrid Analysis and Modeling Using the Corrective Source Term Approach." Applied Soft Computing, Volume 128. https://doi.org/10.1016/j.asoc.2022.109533

[43] Argonne National Laboratory. "PRO-AID." Accessed 2023. https://www.anl.gov/nse/ai-ml/proaid

[44] Argonne National Laboratory. "AI/ML Automated Reasoning." Accessed 2023. https://www.anl.gov/nse/ai-ml/automated-reasoning

[45] GE Research. "GE Digital Ghost: Real-Time, Active Cyber Defense." Accessed 2023. https://www.ge.com/research/offering/digital-ghost-real-time-active-cyber-defense

[46] GE Research. "GE Research Unveils Cyber-Defense Solution, Digital Ghost." Accessed 2023. https://www.ge.com/research/newsroom/ge-unveils-real-time-active-cyber-defense-solution-industrial-control-systems-called

[47] Anderson, R.S., Benjamin, J., Wright, V.L., Quinones, L., Paz, J. 2017. "Cyber-Informed Engineering." INL/EXT-16-40099. Idaho National Laboratory. https://www.osti.gov/biblio/1369373

[48] Eggers, S., Anderson, R. 2021. "Cyber-Informed Engineering for Nuclear Reactor Digital Instrumentation and Control." DOI: 10.5772/intechopen.101807. Nuclear Reactors. https://www.intechopen.com/chapters/81013

[49] Turner, T. "Cyber Informed Engineering – Engineering Basics." Accessed 2023. https://www.cyberinformedengineering.com/en/engineering-basics

[50] Eggers, S.L., Le Blanc, K.L., Youngblood III, R.W., McJunkin, T.R., Frick, K.L., Wendt, D.S., Anderson, R.S. 2021. "Cyber-Informed Engineering Case Study of an Integrated Hydrogen Generation Plant." INL/CON-21-61671-Rev001. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_46017.pdf

[51] Department of Energy. 2022. "The U.S. Department of Energy's (DOE) National Cyber-Informed Engineering (CIE) Strategy Document." DOE. https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document

[52] Wright, V.L. 2023. "Cyber-Informed Engineering." INL/MIS-23-71048-Revision-0. Idaho National Laboratory. https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_65032.pdf

[53] Idaho National Laboratory. "Advanced Small Modular Reactors." Accessed 2023. https://inl.gov/trending-topics/small-modular-reactors/

[54] Liou, J. 2021. “What are Small Modular Reactors (SMRs)?.” IAEA. https://www.iaea.org/newscenter/news/what-are-small-modular-reactors-smrs

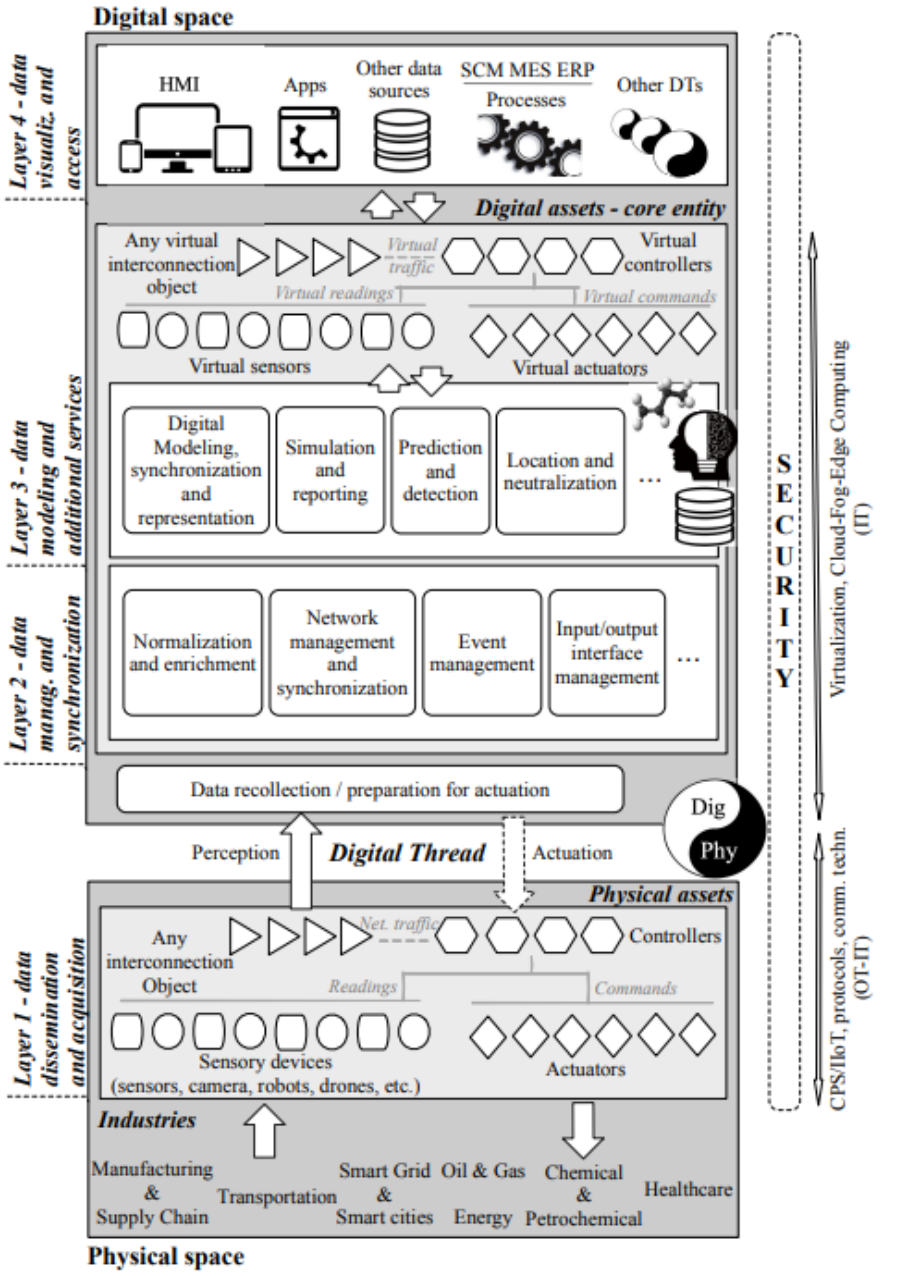
[55] EPRI. 2020. “Water Induction in Steam Turbines for Power Generation: Understanding and Preventing Water Damage.” EPRI Technical Brief 3002019316. https://www.epri.com/research/programs/113173/results/3002019316

[56] Wang, H., Gruenwald, J.T., Tusar, J., Vilim, R. 2021 “Moisture-Carryover Performance Optimization Using Physics-Constrained Machine Learning.” Elsevier, Progress in Nuclear Energy Volume 135. https://doi.org/10.1016/j.pnucene.2021.103691

[57] Morgan, D., Dunphy, W. 2010. “Scoping Study of Moisture Carryover in Boiling Water Reactors.” EPRI 1021185. https://www.epri.com/research/products/1021185

Annex I: Full Size Images

A four layer-based digital twin from Section 2.1 Intended Target of Digital Twins



Page intentionally left blank.