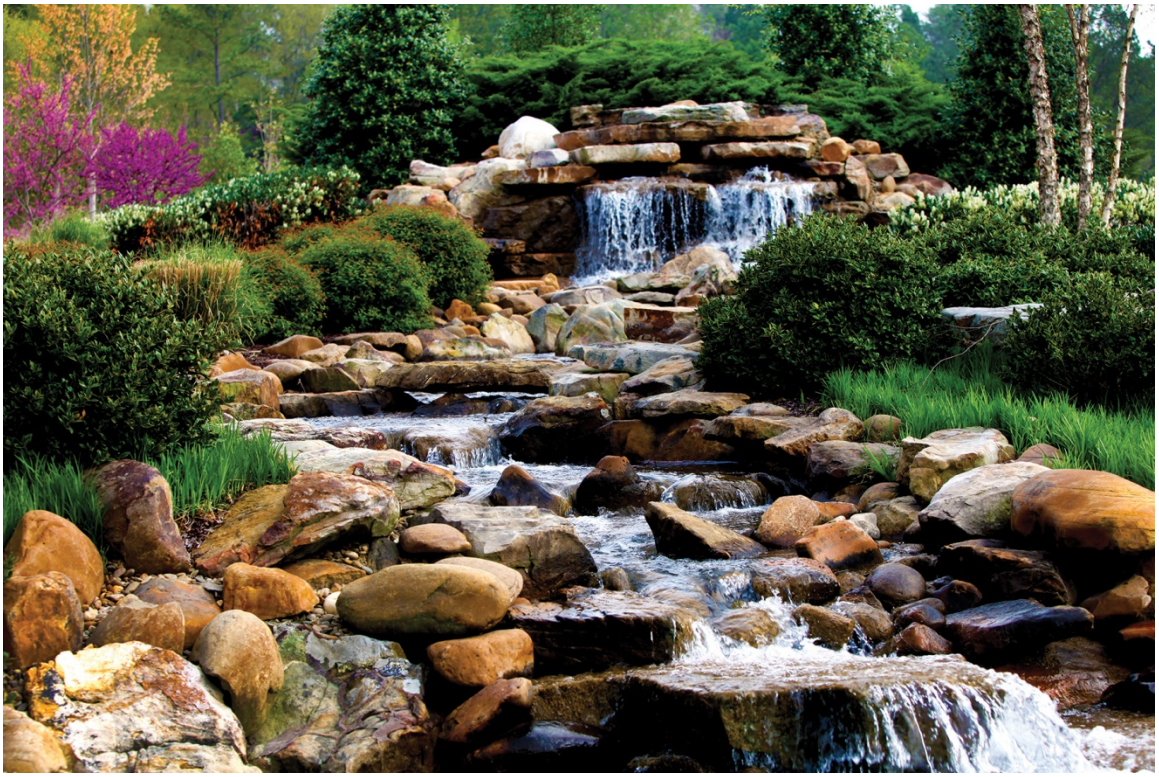
ORNL/SPR-2022/2493

Status Report on Regulatory Criteria Applicable to the Use of Digital Twins



M. D. Muhlheim
P. Ramuhalli
A. Huning
A. Guler
R. Wood
A. Saxena

June 2022

OAK RIDGE National Laboratory

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

ORNL/SPR-2022/2493

Nuclear Energy and Fuel Cycle Division

STATUS REPORT ON REGULATORY CRITERIA APPLICABLE TO THE USE OF DIGITAL TWINS

M. D. Muhlheim
P. Ramuhalli
A. Huning
A. Guler
R. Wood
A. Saxena

June 2022

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

ç

ABSTRACT

Although the interest in the use of Digital Twins (DTs) in nuclear energy is increasing rapidly, at present their implementation is limited. This rapid increase in interest is not surprising considering that implementing DT technology would allow for continuous monitoring, facilitate the implementation of predictive maintenance with optimized staffing plans, enable the automation and autonomy opportunities that can drastically reduce the fixed operation and maintenance costs, and provide training for operations and maintenance. Other industries are using DTs for construction and in the nuclear arena DTs can provide great benefit in decommission activities. Their ability to operate in real time vastly increases their potential impact.

It has been recognized that before a DT can be used in design, operations, or as a regulatory tool, the specifics on the regulations applicable to the use of DTs need to be established. The difficulty is that the specific use cases will dictate the applicability of regulations. For example, even within the application domain associated with operations, the regulations may vary if the DT is used to create a virtual reference for plant operations, be used for training, optimization of maintenance intervals, prioritize of maintenance activities, etc. Different still is if the DT is to be used for design. A DT that is integrated into the design or design process can facilitate improved decision making and greater operational flexibilities and its use to support the selection of technical specifications will introduce other requirements.

This report describes the research results to date to identify regulatory implications of DT technologies and their uses. Specifically, this report reviews current regulatory guidance relevant to the application of predictive maintenance DTs, artificial intelligence (AI), and automation. The focus of this review included determination of constraints on the application of DT technology, identification of any regulatory gaps or uncertainties, and clarification of anticipated technical basis information likely to be important for regulatory acceptance of these technologies. The research included review of topical reports and other submissions to the US Nuclear Regulatory Commission (NRC) on technologies relevant to using DTs for predictive maintenance, NRC safety evaluation (SE) reports, and other relevant literature to identify specific regulatory concerns.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

The information, data, or work presented herein was funded in part by the Advanced Research Projects Agency-Energy (ARPA-E), US Department of Energy, under Award Number DE-AR0001290. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

ABBREVIATIONS

AEA	Atomic Energy Act
AI	artificial intelligence
ALWR	advanced light-water reactor
AOO	anticipated operational occurrence
AR	advanced reactor
AR	augmented reality
ASIC	application-specific integrated circuits
BEACON	Best Estimate Analysis of Core Operations - Nuclear
BNL	Brookhaven National Laboratory
BTP	branch technical position
BWR	boiling water reactor
CCF	common cause failure
CFD	computational fluid dynamics
CFR	US Code of Federal Regulations
CLW	co-located worker
COL	combined license
CPLD	complex programmable logic device
CPU	central processing units
CRT	cathode-ray tube
CT	completion time
DC	design certification
DEG	digital engineering guide
DI&C	digital instrumentation and controls
DL	deep learning
DNBR	departure from nucleate boiling ratio
DoD	US Department of Defense
DOE	US Department of Energy
DT	digital twin
ECCS	emergency core cooling system
EMI	electromagnetic interference
ENIQ	European Network for Inspection Qualification
EPRI	Electric Power Research Institute
ESF	engineering safety feature
ESFAS	engineered safety features actuation system
FEA	finite element analysis
FMEA	failure modes and effects analysis
FPGA	field programmable gate array
FSAR	final safety analysis report
FW	facility worker
GDC	General Design Criterion
GE	General Electric
GPS	glass panel simulator
HFE	human factors engineering
HMI	human–machine interface
HIS	human interface system
HIS	human–system interface
IAEA	International Atomic Energy Agency

I&C	instrumentation and control
ICS	industrial control system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
I/O	input/output
IT	information technology
ITAAC	inspection, test, analysis, and acceptance criteria
JAD	joint application development
LAR	license amendment request
LCO	limiting conditions for operation
LLWR	large light-water reactor
LOCA	loss-of-coolant accident
LWR	light-water reactor
MAAP	Modular Accident Analysis Program
ML	machine learning
NDE	nondestructive examination
NEI	Nuclear Energy Institute
NRC	US Nuclear Regulatory Commission
NUREG	NRC publication
NUREG/CR	NUREG prepared by a contractor
OEM	original equipment manufacturer
O&M	operation and maintenance
ORNL	Oak Ridge National Laboratory,
OS	operating system
PAL	programmable array logic
PE	programmable electronic
PHM	prognostic health management
PLA	programmable logic array
PLC	programmable logic controller
PLD	programmable logic device
PMDT	predictive maintenance digital twin
PMx	preventive and corrective maintenance
PNNL	Pacific Northwest National Laboratory
PRA	probabilistic risk assessment
QA	quality assurance
QHO	quantitative health objective
RAD	rapid application development
RCS	reactor coolant system
RES	Office of Nuclear Regulatory Research
RG	regulatory guide
RIS	regulatory issue summary
RISC	risk-informed safety class
RPS	reactor protection system
RTS	reactor trip system
RUL	remaining useful life
RUP	rational unified process
SAR	safety analysis report
SCADA	supervisory control and data acquisition
SCS	supervisory control system
SE	safety evaluation

SF	surveillance frequency
SIL	safety integrity level
SMR	small modular reactor
SNL	Sandia National Laboratories
SPLD	simple programmable logic devices
SRP	standard review plan
SSC	structures, systems, and components
STS	standard technical specification
TCP/IP	transmission control protocol and the internet protocol
TCR	Transformational Challenge Reactor
TECDOC	technical document (IAEA)
TEDE	total effective dose equivalent
TRISO	tristructural isotropic
TS	technical specification
TSTF	Technical Specifications Task Force
URC	unacceptable radiological consequence
V&V	validation and verification
VR	virtual reality

1. INTRODUCTION

This report provides an update on the progress made on Milestone 5.1, "Assessment of current regulatory guidance applicable to PMx [preventative and corrective maintenance]." The objective of Milestone 5.1 is to identify the potential regulatory pathways and associated requirements for incorporation of preventative maintenance of digital twin (PMDT) technology for operations and maintenance (O&M) of an advanced reactor (AR). The review is being completed in two parts. The first part (this report) provides a review of the current regulatory guidance relevant to application of PMx, artificial intelligence (AI), and automation. The outcomes of this review include determination of constraints on the application of such technology, identification of any regulatory gaps or uncertainties, and clarification of anticipated technical basis information likely to be important for regulatory acceptance of PMx, AI, and automation. Gaps in uses and regulatory requirements will be addressed in the next phase of this task under Milestone 5.2.

1.1 NEED

Design concepts begin with a recognized need and an analysis of requirements and regulations. Although predictive modeling and simulation can be used to support conceptual design efforts,[1] models with the higher fidelity provided by digital twins (DTs) can have an even greater impact on maintenance scheduling, operations, and technical specifications (TSs). Furthermore, their ability to operate in real time vastly increases their potential impact. These capabilities motivate the development of higher fidelity models that can operate in real time. The conceptual features of DTs are varied. However, the identification of the regulations applicable to the specific uses of DTs have not been established. Regulations must be identified so that the next essential step to develop DTs can be taken. The regulations will differ if the DT has a safety, important-to-safety, or nonsafety function. Moreover, it may be possible to identify if existing regulations are sufficient and could be adapted or considered to accommodate DTs for advanced reactors (ARs) or if new regulations and guidance are needed. However, changes to existing or the creation of new regulations may not be needed; the solution could be developing guidance documents that include DTs and AI.

1.2 OVERVIEW

DT technology allows for continuous monitoring, facilitates implementation of predictive maintenance with optimized staffing plans, and enables automation and autonomy opportunities that can drastically reduce the fixed operation and maintenance (O&M) costs in advanced nuclear power systems. However, technology development and demonstration must incorporate regulatory considerations such as built-in safeguards and objectives that must be achieved for compliance. It is equally important to understand the safety and security drivers for these policies, the data needs for satisfying them, and where appropriate, the defining technical bases that will inform future regulatory policy decisions.

The current regulatory framework for nuclear energy in the United States is focused on the use of defense-in-depth measures that provide a reasonable assurance of safety. Generally, such measures include periodic inspection and testing of safety-significant components, with preventive maintenance performed on a time-based schedule to ensure component operability. DTs can be used to maintain the same level of safety while optimizing preventive maintenance schedules.

[1] Examples include the General Electric (GE) Predix that provides predictive assessments of key power plant components, Westinghouse's Modular Accident Analysis Program (MAAP) that simulates light-water reactor (LWR) system response to a severe core accident, and plant simulators that feature a physical replica of a plant control room and interfaces via an input/output (I/O) system with a plant simulation.

The deployment of DT technology may require additional considerations and requirements such as specific documentary evidence of performance and specific forms of technical data prior to acceptance of safety-significant components. Deployment of DT technologies on balance-of-plant components or on components that are not considered to be safety significant likely will have little or no regulatory restrictions or necessary approvals.

This report describes the research results to date to identify regulatory implications of DT technologies. Specifically, this report reviews current regulatory guidance relevant to the application of predictive maintenance DTs (PMDTs), AI, and automation for a nuclear power plant. The focus of this review included determination of constraints on the application of such technology, identification of any regulatory gaps or uncertainties, and clarification of anticipated technical basis information likely to be important for regulatory acceptance of these technologies. The research included review of topical reports and other submissions to the US Nuclear Regulatory Commission (NRC) on technologies relevant to PMDT, NRC safety evaluation (SE) reports, and other relevant literature to identify specific regulatory concerns.

1.3 CHALLENGES

Challenges in developing and implementing the use of DTs include real-time reduced order or surrogate models, data production and integration, virtual prototyping, autonomous control, and sensor requirements. Validating the DT is another challenge.

The second NRC Office of Nuclear Regulatory Research (RES)-sponsored workshop on DTs identified the following regulatory challenges and opportunities [1]

- The three main categories of potential DT use [1] are (1) use by industry for inherent benefits (e.g., improved design, construction, operations and maintenance), (2) use by industry as a tool for regulatory compliance (e.g., licensing submittals, safety analysis), and (3) use as an NRC regulatory tool (e.g., shared source of plant information, enabler of iterative design approvals and just-in-time regulation).

- Industry and regulators must develop agreed-upon guidance and frameworks for acceptance of DT applications that are consistent, explicit, and that enable the use of DTs as an additional avenue to meet the intent of existing regulations.

- One approach to building confidence in DT technology—an important aspect for acceptance and adoption of DTs—is to pioneer DT applications with nonsafety components or systems and to demonstrate acceptable performance prior to safety-related applications.

- DTs can enhance NRC inspection activities, including automated regulatory compliance testing and on-demand access to high-fidelity plant information.

EPRI's collaborative investigation entitled "Digital Twin Applications to Advanced Reactors," determined the following common challenges to maturing DT technologies:

- Lack of common language / taxonomy / conceptual framework
- Standard processes for review of technology readiness
- Quantitative assessments of the cost of DT implementation vs. benefits to AR analyses
- Identification and evaluation of potential use cases for ARs

2. POTENTIAL APPLICATIONS OF DTs

Implementation of DT technology in nuclear power plants is currently limited. How a DT will be used will determine the regulatory criteria. To minimize requirements, the data connection between the physical asset and the digital model are currently exclusively one-directional, and it is not always in real time [2]. In the broader scope, data connections are to support the interconnection of all components of the DT, including the connection between physical entities and virtual models, the connection between physical entities and data, connection between physical entities and services, connection between virtual models and data, connection between virtual models and services, and the connection between services and data.

DTs are built using software tools and are only now beginning to be used in the design, monitoring, and control in nuclear plants. However, this technology is already being explored or in use in process industries, unmanned aerial vehicles (drones), ocean-going supertankers, oil derricks and ocean drilling platforms, telemedicine and remote patient monitoring, and robotic surgery.

Future DT applications will be used to form a unified system or plant DT to provide for increased communication and control capabilities and for supporting scheduling maintenance activities. DT implementation will require that gaps for licensing be identified, and licensees will require assurance of a DT regulatory infrastructure. The state-of-the-art assessment was broadly aimed at finding answers to the following questions [2]:

1. What are DTs?

2. What are the applications of DTs in nonnuclear industries?

3. What are the applications of DTs or associated technologies in the current fleet of nuclear reactors?

4. What are the current efforts and future vision for applying DTs in the next generation of nuclear reactors?

The answers to these questions are discussed in this report as follows. This section presents a discussion about the current definition, understanding, and perception of what is a DT. Section 3 highlights the current efforts undertaken by global DT technology companies and presents some notable applications of DTs in nonnuclear industries. Section 4 is a two-part comprehensive discussion of DTs in nuclear reactor applications for the current fleet and for next-generation reactors. Section 5 presents an assessment of data analytics, machine learning (ML), AI, and advanced modeling, which are the enabling technologies of DTs. As part of the milestone for reviewing regulatory requirements on the use of DTs, a literature search was performed to assess any potential aspects of DTs that may require greater regulatory scrutiny. Document types reviewed include:

- NUREG and NUREG/CR series reports documenting criteria for digital instrumentation and control (I&C) system review and licensing

- Technical letter reports (Oak Ridge National Laboratory [ORNL], Idaho National Laboratory [INL], Pacific Northwest National Laboratory [PNNL], Brookhaven National Laboratory [BNL], Sandia National Laboratories [SNL]) and topical reports (Electric Power Research Institute [EPRI], Technical Specifications Task Force [TSTF], etc.) on surveillance frequency extension, monitoring, digital I&C system and software reliability, and DTs and AI in commercial nuclear power

- NRC workshops on DTs and NRC public meetings

- International Atomic Energy Agency (IAEA) workshop reports and technical documents (TECDOCs)

Some of the focus areas where DTs will be applied in the nuclear industry are design and licensing, plant construction, training simulators, predictive O&M, autonomous operation and control, failure and degradation prediction, obtaining insights from historical plant data, and safety and reliability analysis.

The purpose of this status report is to:

1. Identify the NRC requirements that would be applicable for the use of DTs
    a. Regulatory requirements will be based on how the DT will be used.
    b. This review is based primarily on the use of DTs in the operations phase.
2. Determine the suitability of existing regulations:
    a. Do existing regulations and guidance suitably address DT issues for existing and small light-water reactors (LWRs) and ARs?
    b. What modifications of the regulations and guidance might be needed for existing and future plants?
    c. Will new guidance be needed to support licensing reviews for existing and future reactors?
3. Identify the NRC's general expectations for the use of DTs.
    a. Participants in the closing plenary session at a workshop evaluating the applicability of DTs identified the following challenges [3]:
        - Implementation of DTs in the nuclear setting is increasingly complex because nuclear power plant (NPP) operational models are difficult to change.
        - Real-time data management to support DT implementation is a challenge.
        - It is a challenge to identify the areas in which DTs can contribute to optimizing regulatory oversight.
    b. Participants in this session identified the following key takeaways for the workshop:
        - DT technology may be able to reduce the scope and cost of regulatory oversight.
        - DTs can be used to identify which components are most important for safety.
        - It will be helpful for organizations to turn over DTs to the NRC to increase shared information and system knowledge. Sharing models directly with the NRC staff has already been fruitful. It has saved hundreds of hours by providing a platform for direct interactions with the DT finite-element models, allowing for quick responses to questions.
        - The IAEA is working on a plant taxonomy that may eventually support DTs.
        - It is important to learn from organizations in other regulated industries using DTs, such as self-driving car manufacturers and the Federal Aviation Administration. For example, the Food and Drug Administration uses risk-based information to determine how extensively a new drug should be tested.

Implementation of digital twin (DT) technology in the nuclear arena is currently limited, and how it is used and its interfaces with plant systems will determine the regulatory criteria. Industry and regulators must develop agreed-upon guidance and frameworks for acceptance of DT applications that are consistent, explicit, and that enable the use of DTs.

There are as many (slightly varying) definitions of DTs as there are people developing and using them. A recent survey by VanDerHorn and Mahadevan found 46 different definitions for a DT [4]. The different complexities and solutions result in the different definitions of DTs. The complexity of DTs increases in

line with the nature of the physical system, the purpose for which the twin is used, and the number and kinds of participants involved in developing, using, and maintaining the solution [5]. For this report, the DT refers to a digital model (or a collection of models) that encode phenomena tied to specific outcomes for the physical entity. For instance, these DTs could be modeling system/process performance, system health, or even planning/scheduling scenarios. DTs can provide insights equivalent to Modeling and Simulation (M&S) but need to learn and provide those insights much faster than the development and uses of M&S. DTs are tightly coupled with operation with the ability to assimilate and adapt to real-time information from the operating environment through continuous learning.

The DT for nuclear systems has existed for decades in the form of on-line core monitoring systems [6]. What has changed are the advances in modeling, sensors, calibration techniques, and machine learning-based predictive analytics to enable a step change in decision-making capabilities for reactor operation.

Recently, EPRI has been leading a collaborative investigation entitled "Digital Twin Applications to Advanced Reactors." The goal of this effort is to explore benefits, challenges, capabilities, and possible applications of DTs in design, construction, commissioning, operations, maintenance, and decommissioning to demonstrate best practices and to establish recommendations for leveraging DT technologies to optimize ARs. The first phase of the project was dedicated to identifying and screening potential DT use cases for AR applications with feedback from both AR developers and potential AR owners/operators (i.e., utilities).

Applications of DTs can be mapped to two distinct lifecycle phases: (1) AR design, construction, and commissioning (2), and O&M. Several use cases were identified as described below:

1. Design
2. Construction
3. Commissioning
4. Operations
5. Maintenance
6. Decommissioning
7. Regulatory tool

Although this list is not exhaustive, it does provide a wide variety of DT definitions and use cases currently being pursued across the nuclear industry. Based on perceived importance from original equipment manufacturers (OEMs) and utility operators, the most highly ranked use cases were determined to be (1) construction sequence simulation, (2) real-time construction sequence optimization, and (3) predictive maintenance. Predictive maintenance use cases were identified as the most important in terms of new value added for sustainable low-cost O&M and for maximizing component life.

2.1 DESIGN

DTs can be used to maximize the speed of design iteration; to support regulatory intents to protect personnel and the environment; to provide the information necessary to dynamically assess risk and make risk-informed decisions; to act as a common source of information for both regulators and developers; and to standardize internal documentation, provide visualizations, and automate analysis [7].

Many AR developers are designing plants with DTs integrated throughout their lifecycles to facilitate improved decision making and greater operational flexibilities such as a potential dynamic operating envelope. DTs give multi-dimensional views into the design and how it's performing. A DT offers a means to test "what-if" scenarios, including the impact of design changes and security events. As an added benefit, a DT can collect substantial data under one environment.

A DT used in design combines the design, sensor, and operating data with intelligent multidimensional digital models. A true DT possesses the operational and behavioral awareness necessary to simulate, predict, and inform decisions based on actual operational conditions.

When used during design, DTs can be used for

- Automated design updates via integrated design platforms
- Construction sequence simulation
- Site selection optimization
- Sensor layout optimization

2.2 CONSTRUCTION / DECOMMISSIONING

Prohibitively large and unforeseen increases in construction cost are one of the greatest challenges for future nuclear reactors. DTs have produced significant performance improvements and schedule reduction in the aerospace, automotive, and construction industries [3]. This integrated modeling approach has not been fully applied to nuclear safeguards programs in the past. DTs combined with AI technologies can lead to innovations in process monitoring detection, particularly in event classification and data tampering.

Recent advances in virtual reality (VR) and augmented reality (AR) have enabled inexpensive visual viewing of digital twin representations. During construction, DTs could be used to construct 2D or 3D static views or VR/AR views of the plant. Such VR or AR views would enable architects, designers, engineers, and maintenance crews to "see" the plant as if they were physically walking through it.

DTs can be used in the decommissioning of power plants to reduce data loss from human error.

When used during construction, DTs can be used for

- Supply chain modeling, simulation, and tracking
- Real-time construction sequence optimization and front-running simulations
- Automated construction quality assurance (QA)
- Quality control and qualification of off-site manufactured components

When used during decommissioning, DTs can be used for

- Deconstruction sequence simulation
- Chain of custody management for irradiated waste

2.3 OPERATIONS

Multiphysics simulations for DTs include plant control and protection systems. A DT can create a virtual reference for plant operations, identify abnormal operations early before the integrity of structures, systems, and components (SSCs) is challenged, increase the reliability of nonsafety-related control

systems, and reduce the frequency of safety-related system actuations and operation (

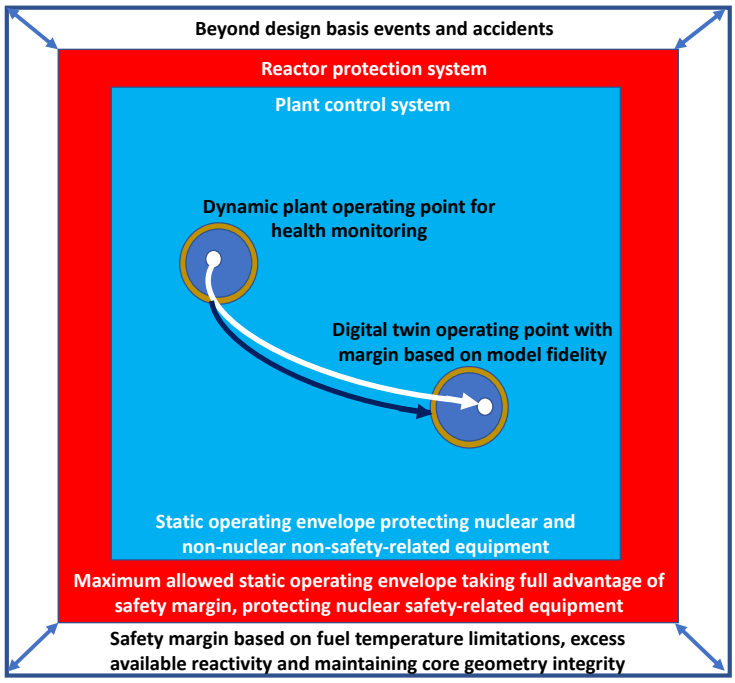


Figure 1) [8]. Thus, during operations, DTs would enable operators to monitor every aspect of the plant, possibly precluding the need for certain physical monitoring and inspection. Actionable insights, simulations, and a connected view of all online and offline data enable quick and better decisions to optimize performance and efficiency.

The result could be an increased safety margin.

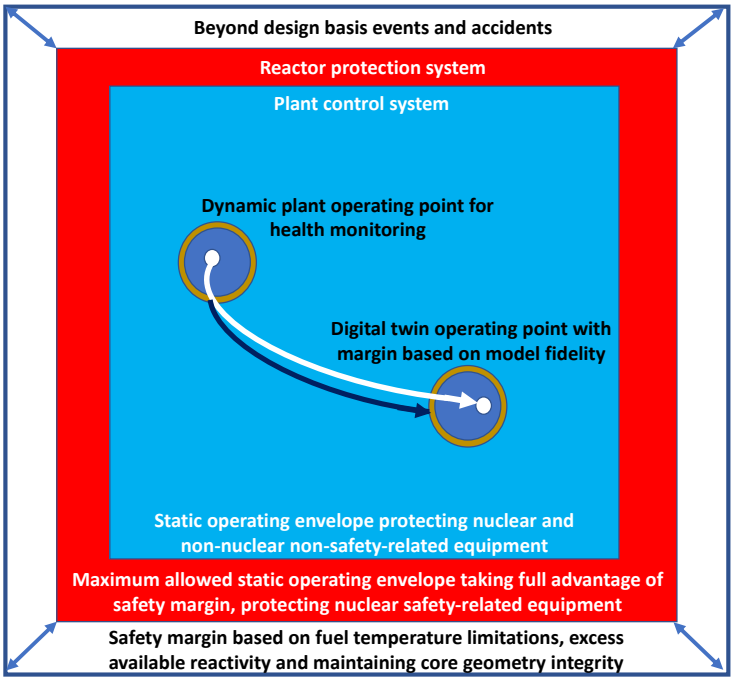


Figure 1. Health monitoring using a DT.

When used during operations, DTs can be used for

- 3D mapping and augmented reality visualization of radiation levels
- Smart chemistry monitoring and control
- Smoke and fire detection and response system
- Narrow-band dynamic operating envelope
- Personnel tracking and authorized access enforcement
- Automated quality control and yield optimization of tristructural isotropic (TRISO) pebble production
- Fleet-level performance optimization
- Mobile access to digital configuration management information
- Monitoring and active management if thermal stresses in high temperature coolant lines
- Simulated stress testing of NPP's cybersecurity framework

2.4 TRAINING

Plant simulators can be used for training for operations or by virtually performing maintenance in high radiation areas. Training and education, and its use in dose reduction for plant workers are two of the main applications of VR in the nuclear industry. A VR model of the actual physical plant when complimented with a digital twin is likely to provide an even better environment for increased operational efficiency and safety of NPPs.

When used during training, DTs can be used for

- Virtual plant simulator for operations training and optimization

- Virtual commissioning

2.5 MAINTENANCE

DT technology allows for continuous monitoring, implementation of predictive maintenance with optimized staffing plans, and enables automation and autonomy opportunities that can drastically reduce the fixed O&M costs. Preventive maintenance is typically performed on a time-based schedule to ensure component operability. DTs can be used to maintain the same level of safety while optimizing preventive maintenance schedules. With a complete collection of all the data, the DT, with real-time sensor data and predictive recommendations through ML and AI, can greatly improve maintenance and operations. Thus, maintenance activities could be predictive rather than reactive.

When used during maintenance, DTs can be used for

- Robotic maintenance
- Virtual walk-down and inspection
- Integrated dynamic probabilistic risk assessments (PRAs)
- Sensor fault detection
- Predictive maintenance
- Structural health monitoring

2.6 REGULATORY TOOL

DTs can be used to maximize the speed of design iterations [9]. If information on the DT and model variables are shared, DTs can provide a common source of information between regulators and developers. For the regulator, DTs provide parameters and documentation sources, validation and verification (V&V), and high-fidelity modeling and simulation of operations. For the developer, DTs provide control systems / real-time modeling and simulation, anomaly response modeling, performance assessment, and ML applications. If the regulator and developer share the DT and its output, then significant benefits include automation of explicit analysis flows and a common interface between regulators and developers.

3. REGULATORY REQUIREMENTS FOR A DT

The conceptual features of DTs are varied. However, the identification of the regulations applicable to the specific uses of DTs have not been established. Regulations must be identified so that the next essential step to develop DTs can be taken. The regulations will differ if the DT has a safety, important-to-safety, or nonsafety function. For example, if the DT is used as a construction tool and is not part of the licensing basis it would not be subject to regulatory requirements. By identifying those regulations that may apply to a DT (which will be based on its application), it may be possible to identify if existing regulations are sufficient and could be adapted or considered to accommodate DTs for advanced reactors (ARs) or if new regulations and guidance are needed. However, changes to existing or the creation of new regulations may not be needed; the solution could be developing guidance documents that include DTs and AI.

An NRC-sponsored workshop on DTs concluded that industry and regulators must develop agreed-upon guidance and frameworks for acceptance of DT applications that are consistent, explicit, and that enable the use of DTs as an additional avenue to meet the intent of existing regulations [1]. This report describes potential common frameworks and DT applications as a starting point for meeting that objective. Regulatory requirements for DTs begin with the Atomic Energy Act (AEA) as amended (Figure 2), which licensees must meet. The AEA remains the primary authority for the NRC's implementing regulations.

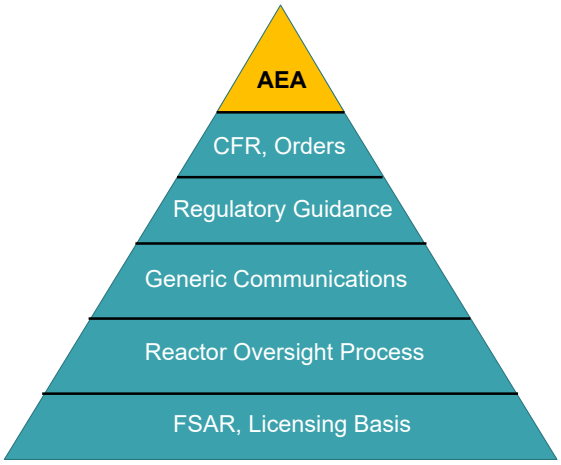


Figure 2. Hierarchy of regulations for a DT.

The AEA remains the primary authority for the NRC's implementing regulations. Title 10 of the US Code of Federal Regulations (CFR) and commission orders are rules for NRC staff to follow to implement the law. 10 CFR Parts 50 and 52 provide the current rules for plant licensing; Part 53 is under development, as detailed below.

Part 50, "Domestic Licensing of Production and Utilization Facilities," is a two-step licensing process including: (1) issuance of licenses and construction permits, and (2) issuance of an operating license. Part 50 is for the licensing of production and utilization facilities.

Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," governs the issuance of early site permits, standard design certifications, combined licenses, standard design approvals, and manufacturing licenses for nuclear power facilities. This is a *combined operating license* (COL) that provides for approval of a combined construction permit and operating license. Many sections of Part 52 require compliance with sections of Part 50, including compliance with all Appendices in 10 CFR 50, including the General Design Criterion (GDC) in Appendix A.

Part 53, "Risk Informed, Technology Inclusive Regulatory Framework for Advanced Reactors," is under development.

Guidance on satisfying the rules is provided in the Standard Review Plan (SRP) (NUREG-0800) and in NRC regulatory guides (RGs). Once a design is approved, a plant's licensing basis is the plant's legal authorization for design, construction, maintenance, and operation.

3.1 GENERAL REQUIREMENTS FOR I&C

At the highest conceptual level, I&C systems in an NPP can be categorized by safety (protection) and nonsafety (control) systems. The reactor protection system (RPS) includes the reactor trip system (RTS) and the engineered safety features (ESFs). The RTS is designed to initiate the reactivity control system (control rods) automatically to ensure that specified acceptable fuel design limits are not exceeded. Because the safety systems are important to protecting public health and safety, they have strict requirements on their design, construction, and operation, and they receive the NRC's most stringent review.

If the DT is to provide a protection system function, then it must meet the requirements of a safety system. Relevant acceptance criteria are based on meeting the relevant requirements for an I&C *protection system*.

The NRC's mission is to ensure the safe use of radioactive materials for beneficial civilian purposes while protecting people and the environment. The NRC regulates commercial NPPs and other uses of nuclear materials through licensing, inspection, and enforcement of its requirements. At a high level, a malfunction or failure of any system cannot prevent/block a safety action or initiate a challenge to that system.[2] The fundamental design principles for an I&C system at an NPP are as follows:

- Redundancy (single failure criteria)
- Quality (especially software QA)
- System integrity (determinism)
- Independence (physical, electrical, communication)
- Diversity and defense-in-depth
- Environmental qualification
- Reliability
- Simplicity
- Control of access

In addition to the fundamental design principles listed above, operators must have a diverse means of seeing current and reliable values of essential reactor operating parameters. That is, operators must be able to trust the information provided and to understand the current state of the plant.

The objectives of the control systems are to maintain the controlled variables within prescribed operating ranges, and the effects of operation or failure of these control systems are bounded by the accident analyses in Chapter 15 of the safety analysis report (SAR).

Relevant acceptance criteria based on meeting the requirements for an I&C control system include the following:

1. 10 CFR 50.34 requires the licensee to include information describing the facility, to present the design bases and the limits on operation, and to present a safety analysis of the SSCs and of the facility as a whole.

2. 10 CFR 50.49 requires each licensee to establish a program for qualifying all "electric equipment important to safety."

[2] This is an example of a control system failure that, although it did not prevent/block a safety action, resulted in a challenge to a safety system and a reactor scram. On May 10, 1996, Browns Ferry Unit 2 experienced an automatic reactor scram on low reactor water level from full power (LER 260-96-005-00). When software parameter changes were made active (saved) in the control system, a reinitialization sequence occurred within the control software block which drove the feed pump speed demand signal to zero for a few seconds. Plant personnel were unaware that entering these new software parameters would cause the feedwater control system to reinitialize. The cause of the event was attributed to inadequate design of the control system software. A design weakness existed in the installed system, in that making software parameter changes in certain software blocks would cause the control system to automatically reinitialize to zero output. This characteristic of the software design was not known to plant personnel.

3. 10 CFR 50.54(jj) and 50.55(i) require that SSCs subject to the codes and standards in 10 CFR 50.55a must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

4. 10 CFR 50.55a(h) requires compliance with Institute of Electrical and Electronics Engineers (IEEE) 603-1991 and the correction sheet dated January 30, 1995.

5. 10 CFR Part 50, Appendix A, General Design Criterion (GDC)
   GDC 1, "Quality Standards and Records"
   GDC 10, "Reactor Design"
   GDC 13, "Instrumentation and Control"
   GDC 15, "Reactor Coolant System Design"
   GDC 19, "Control Room"
   GDC 24, "Separation of Protection and Control Systems"
   GDC 28, "Reactivity Limits"
   GDC 29, "Protection against Anticipated Operational Occurrences"
   GDC 44, "Cooling Water"

6. 10 CFR 50, Appendix B, "Quality Assurance Criteria"

10 CFR 52.47(b)(1) requires that a design certification (DC) application contain the proposed inspection, test, analysis, and acceptance criteria (ITAAC) that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria are met, then a plant that incorporates the design certification is built and will operate in accordance with the design certification, the provisions of the AEA, and NRC's regulations.

10 CFR 52.80(a) requires that a COL application contain the proposed inspections, tests, and analyses, including those applicable to emergency planning, that the licensee shall perform, and the acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria are met, then the facility has been constructed and will operate in conformity with the combined license, the provisions of the AEA, and the NRC's regulations.

3.2 REQUIREMENTS FOR A DT

Any DT must be assessed against licensing requirements. Presentations at the various workshops recognize that the licensing requirements for DTs must be met but do not provide any specifics rather than to indicate that software, cybersecurity, and requirements in general are needed. In summarizing the working group's work to participants [10] Roland and Guerra stated that the "IAEA in collaboration with other organizations should develop SMR [small modular reactor] design roadmap to safety/security requirements with respect to regulatory requirements. This should include differences in requirements, such as dose thresholds (e.g., variations of URC [unacceptable radiological consequence] between countries)."

The requirements outlined below are not applicable to all potential uses of DTs and will depend upon its use as a control system, a protection system, or input to determining safety system settings. For example, if the DT is used during the design phase to provide insights into TS limits, then it could be subject to 10 CFR 50.36.

The hardware and development of the software for the DT, regardless of its functionality, must be of sufficient quality commensurate with the importance of the function(s) to be performed. QA become more critical for DTs that use AI and ML. It is important that this is applied throughout the software lifecycle.

The applicability of the regulations below will depend on how the DT is to be used.

10 CFR 50.36 and 52(ii)(30) – Technical specifications
- Technical specifications include items in the following categories: safety limits, limiting safety system settings, and limiting control settings.

10 CFR 50.46 – Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors
- Although an AR may not be an LWR, the cooling performance must be calculated in accordance with an acceptable evaluation model, it must include sufficient supporting justification to show that the analytical technique realistically describes the behavior, and uncertainty must be accounted for to show that there is a high level of probability that the criteria would not be exceeded.

10 CFR 50.55a(h)(3) — IEEE 603-1001
- Independence must be maintained between safety systems and other systems.

10 CFR 50.59 — Changes, tests and experiments
- Licensees could backfit a DT into the control system.

10 CFR 50.90 — Application for amendment of license
- If the application of a DT cannot be installed under 50.59, then a licensee would be required to submit a license amendment request (LAR).

10 CFR 50, Appendix A, GDC 1 — Quality standards and records
- The DT must be of sufficient quality to minimize the potential for challenges to safety systems.

10 CFR 50, Appendix A, GDC 24 — Separation of protection and control systems
- Failure of the DT cannot cause the failure of the protection system.

10 CFR 50, Appendix K – Emergency core cooling system (ECCS) evaluation models
- Appendix K, Part II, "Required Documentation," sets forth the documentation requirements for each evaluation model. Note, if an AR has an ECCS it may be passive rather than active.

10 CFR 55.46 — Simulation facilities
- Plant-referenced simulators can be characterized as "limited simulation and modeling" DTs.
- A DT would have increased scope and fidelity compared to a simulator used for operator training.

10 CFR 110—Export and Import of Nuclear Equipment and Material
- Nuclear-related commodities are under the export licensing authority of the Department of Commerce

10 CFR 810, "Assistance to Foreign Atomic Energy Activities," (DOE)
- Restricts the transfer of technology for the development, production, or use of equipment or material especially designed or prepared for any of the activities listed in 10 CFR 810.2(b). This part does not apply to exports authorized by the NRC, Department of State, or Department of Commerce.

15 CFR 730-774, (Department of Commerce [DOC])
- US Department of Commerce (15 CFR 730-774) has a family of export control classification numbers related to Simulators for NPPs (2A291/2D290/2E001).

- The “Software” “specially designed” or modified for the “development,” “production,” or “use” of items controlled by 2A290 or 2A291 are export controlled.

The specific requirements for a DT will be dependent on its functionality.

3.2.1 Classification

In the nuclear power industry, I&C systems have been historically classified according to their safety significance. This classification approach is based on a deterministic assessment of the system functions' ability to ensure safety.

Safety classification is one of the fundamental safety concepts used to ensure that NPPs pose minimal risk to public safety. Classification of SSCs identifies their importance to safety and the consequence of its failure. SSC classification is closely related to plant states and postulated initiating events.

The term *plant states* can refer to the events to be considered for plant operation—normal operating states and anticipated operational occurrences (AOOs), or the term can be used to identify the status of the plant to be reached after an event has occurred, such as physical conditions such as pressure, temperature, or radiation.

10 CFR 50 establishes a classification approach for SSCs in a nuclear facility. 10 CFR 50.2 [11] defines safety-related SSCs in terms of their ability to remain functional during and after design basis events to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain a safe shutdown condition, and (3) the capability to prevent or mitigate the consequence of accidents that could result in unacceptable offsite exposures.

In addition to the traditional deterministic classification approach, a risk-informed approach to safety classification has been established in 10 CFR 50.69 [12]. Specifically, SSCs are divided into risk-informed safety classes based on deterministic safety classification and probabilistic significance to plant safety. In this classification approach, insight from a PRA on the safety significance of the function performed by a system is captured based on its ability to reduce the risk of release of radioactive material to the environment. 10 CFR 50.69 defines a *safety-significant function* as “a function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk.”

The United States has the most coarsely graduated classification scheme—safety/nonsafety—and a more finely graduated scheme based on 10 CFR 50.69—risk-informed safety class (RISC) values. GDC 1, quality standards and records, and GDC 21, protection system reliability and testability, provide some flexibility in that the systems important to safety, including the protection system, shall be designed fabricated, erected, and tested to quality standards *commensurate* with the importance of the safety functions to be performed.

The classification of the DT will depend not only on whether it will be used in a safety aspect, but it will also depend on its functionality. The higher the functionality and autonomy, the greater the need to ensure safety.

If the DT will be used for a safety function, then it must meet the requirements of a safety-related I&C system. More specifically, the DT must meet 10 CFR 50, Appendix B; IEEE 1012 (endorsed by RG 1.168); IEEE 603, (see Section 3.1 on general I&C requirements).

If two-way communication capabilities are added to the DT, then the DT now behaves like an I&C system, and common cause failures (CCFs) are a potential contributor, so the safety classification category would be higher.

3.2.1.1 Software

Current NRC guidance and review standards provide a system-based perspective on developing software for safety systems. If the DT is classified as safety-related or important to safety, then it must follow the guidance for safety-related software. For example, IEEE 603 addresses quality, SRP Branch Technical Position (BTP) 7-14, and RG 1.173 address the development of a software lifecycle process, and RG 1.152 addresses a secure development environment for safety-related software.

To minimize the potential for control system failures that could challenge safety systems, control system software should be developed using a structured process similar to that applied to safety system software [13]. Elements of the review process may be tailored to account for the lower safety significance of control system software.

Although the waterfall lifecycle model is presented as an example in RG 1.152, several system development lifecycle methodologies are available.[3] No specific lifecycle model is required or endorsed by the NRC, but whichever lifecycle model is used, the basic processes remain similar. The system development lifecycle is a conceptual model describing the stages involved in a system development project—beginning with an initial feasibility study and progressing through maintenance of the completed application. In addition, documentation is crucial, regardless of the type of model chosen or devised for any application. Documentation it is typically developed and maintained in parallel with the development process.

The waterfall lifecycle phases provide a framework for a digital safety system development process. RG 1.152 identifies the following phases:

- Concepts
- Requirements
- Design
- Implementation
- Test
- Installation, checkout, and acceptance testing
- Operation
- Maintenance
- Retirement

Both sets of software characteristics—functional and process—are important in safety system software [14, 15]. Because these characteristics are both part of the software development process, the design outputs from the software development process exhibit both functional and process characteristics [15, 16].

3.2.1.2 Control of access

Control of physical and electronic access to digital computer-based control system software and data prevents changes by unauthorized personnel. Historically, the isolated nature of an industrial control system (ICS) has limited its vulnerabilities. Historically, critical infrastructures and manufacturing processes have been monitored and controlled using supervisory control and data acquisition (SCADA)

[3] Various system development lifecycle methodologies include the waterfall model, rapid application development (RAD) joint application development (JAD), the fountain model, the spiral model, build and fix, and synchronize and stabilize. Several models may be combined into a hybrid methodology such as the rational unified process (RUP).

systems that have operated in isolated environments. These control systems rarely shared information with outside systems and were typically built using propriety hardware and software components designed specifically for control operations.

Because of the generally isolated nature of infrastructure and processing systems, the security of ICSs was considered a trivial consideration that could be managed through the use of either traditional information technology (IT) security efforts or internal safety processes.

In an effort to have access to real-time information from any location, to improve performance, and to reduce costs, ICSs have been transitioning from proprietary technologies to the less expensive technologies prevalent in the IT world, such as ethernet, transmission control protocol/internet protocol (TCP/IP), and Microsoft Windows. Unfortunately, many of these popular applications, protocols, and operating systems (OS) have a significant number of widely known vulnerabilities. Increased access from any location means that these previously standalone control systems are now being connected to systems not directly related to process control. Even though they are rarely directly connected to the internet, 80–90% of all control networks are now connected to the corporate network, which in turn is interconnected to the internet [17]. The increase in communication capabilities increases vulnerabilities.

3.2.2 Functionality

DTs are software that combine

- Plant data
- Numerical models (e.g., computational fluid dynamics [CFD] or finite element analysis [FEA])
- Statistical analysis (predictions)

DTs, using displays and monitors, can provide a virtual simulation of what is being modeled:

- Components
- Systems
- Processes

Function relates to purpose and could serve as a primary basis for establishing safety classification. Much of the guidance on functionality acknowledges the difference between control and noncontrol functionality. However, a low functionality DT may still provide a control function. In addition, the functionality of the DT may differ from the functionality of the components in the model. For example, a DT that only performs diagnostics could be present for monitoring the health of a pump without having a control function, or that of a sensor without having a monitoring function.

SRP BTP 7-17 [18] states, the following:

> *The safety classification of the hardware and software used to perform automatic self-testing should be equivalent to that of the tested system unless physical, electrical, and communications independence are maintained such that no failure of the test function can inhibit the performance of the safety function.*

A device with diagnostic or display functionality must maintain physical, electrical, and communications independence from the control functionality; otherwise, it must be considered part of the control functionality or must be designated as an “other auxiliary feature.”

A risk-informed / graded approach based on the functionality of the DT would evaluate the complexity of the DT with its function to set the level of review sufficient to reach a safety conclusion. At the lowest end of a graded approach, simple monitoring, the lowest complexity level, minimal consequences of failure, and other similar factors would not require guidance on software tools or type of digital device. At the other end of the graded approach, existing guidance will apply to control DTs that perform a control function with more scrutiny added if the component performs a safety function. Therefore, an understanding of the DT's functionality can be applied to facilitate a graded approach to qualification, testing, and inspections.

Even a device with noncontrol functionality must demonstrate that its failure would not compromise a safety function, either by demonstrating non-interference or by constructing a safety demonstration that considers the nonsafety functions as if they are safety functions.

Software CCF is always a concern for digital systems. The functionality of the DT will greatly influence the concern of a software CCF. If the functionality is to monitor, provide information (human–machine interface [HMI]), or perform diagnostics or a user interface, then its failure would be more of a nuisance than a safety concern. A risk-informed approach may recognize the minimal risk if the DT is used in this way. However, control failures could pose a safety concern if its failure challenges a safety system.

If the DT was designed to accomplish only one clearly defined function or only a very narrow range of functions, then the complexity is low, and V&V efforts on a quality-designed component should minimize the likelihood of a latent fault. Furthermore, if the DT is designed so that it is reprogrammable after manufacturing, or if its functions can be altered in a general way so that it performs a conceptually different function, then it would not be considered a simple device. To maintain a low functionality only predefined parameters should be able to be configured by users.

A DT used for diagnostics or display must maintain physical, electrical, and communications independence from the control functions; otherwise, it must be considered part of the control system, or it must be designated as an "other auxiliary feature."

This project categorized the functionality of DTs into *noncontrol* (monitoring, diagnostics, display), *control*, and *communications* categories. The functionality/function(s) of the DTs discussed in NRC workshops, IAEA workshops, and public meetings could be binned into one of these categories.

Noncontrol functionality (Advisory)

Monitor the components inputs (process variables)

- Monitoring can be used to provide component health information or process variables, or it can be performed by licensees to reduce the need for surveillance activities and extend calibration intervals of I&C equipment.
- There could be an interface between the DT and the sensors, or the sensor could be part of the DT and thus independent from the RPS / reactor coolant system (RCS) sensors; this would indicate that the values may not be the same as the actual plant values.
- Monitoring component inputs could include condition-based monitoring.

Diagnostics

- Self-diagnostics of plant components are one means that can be used to assist in detecting partial failures that can degrade the capabilities of the plant system but may not be immediately detectable by the system.

- Diagnostics are typically coupled with a monitor or a display device. The diagnostics can be separate from the control device and could even be developed and certified to different safety integrity levels (SILs).
- A software-to-system interface provides the data necessary for diagnostic coverage and alarm for outside acceptable variables.
- Diagnostics are typically coupled with a monitor or a display device.
- The diagnostics can be separate from the control device.
- A software-to-system interface provides the data necessary for diagnostic coverage and alarms.

Display (i.e., provide an HMI)

- HMIs used in the industrial context are mostly screens or touchscreens that connect users to machines, systems, or devices. HMIs can be simple screen displays mounted on components, advanced touchscreens, multi-touch–enabled control panels, push buttons, computers with keyboards, mobile devices or tablets.
- In industrial facilities, factory operators use HMIs to control and automate machinery, as well as their production lines. An HMI with a control function that has 2-way communication should follow guidance for systems rather than guidance tailored for devices.
- The basic HMI display of the process variables monitored can display alerts if a variable is outside of expected parameters, and it can display diagnostic results.
- The HMI screen can be integrated with a control function to allow operators to turn on/off components or to allow for adjustment of parameter displays, DT operating parameters and other functions.
- There will be an interface between the DT and the display monitor (i.e., HMI).

Control functionality (shared)

- An example of a DT control function would be to compare a reference signal in the process to the setpoint and then to change the output to the control device accordingly to minimize the error.
- A device with limited functionality (i.e., a device that has been designed to accomplish only one clearly defined function or only a very narrow range of functions) could have a control function.

Communications functionality (generally Advisory)

- Communications capability would greatly increase the functionality of the DT. If a DT is connected and communicating with the control system (with possible voting logic), then its functionality would affect system-level concerns such as independence between redundant trains or safety/non-safety interactions, and this would require review. Current regulations and guidance adequately cover this issue, but it complicates the design criteria and licensing of a DT.
- For this assessment, digital communications are not considered to be a functionality of a DT because the communication function would be in support of a control function rather than to inform the operator and staff. If the primary purpose of a digital device is communications, then this would be a part of the RCS as opposed to an independent DT.
- Communication capabilities with other auxiliary software may be present to allow for the capability to perform diagnostics, maintenance, or software updates. These types of capabilities may not require networking and would be one-way communications.

The monitoring and display functionality of a DT would likely be limited to information or data extraction and would not support the capability for control execution, manipulation of input/output (I/O), or for sending parameters or data to a central processor for control. The functionality of monitoring is the display of component health, information, and parameters of interest such as current, voltage, frequency,

power factors, diagnostic results, and so on. Monitoring functionality may also be coupled with control functionality.

The functionality of diagnostics allows the health of a component to be monitored continuously and remotely through one-way communications. Components with two-way communication capabilities being used in industry can be configured remotely, and some devices allow firmware updates to be installed remotely. The process industry uses diagnostics to identify degradations, thus allowing corrective action to be taken and avoiding an upset condition.

3.2.2.1 Monitor

Some NPP licensees are in the process of demonstrating new approaches (e.g., Nuclear Energy Institute [NEI] 18-10, 2018) for meeting regulatory requirements in 10 CFR 50.65 [19]. The new approach in NEI 18-10 is a departure from the current preventative maintenance assessment paradigm (e.g., establishing SSC performance criteria) and is intended to allow for a more dynamic assessment of maintenance effectiveness based on the use of data and risk trending analytics. As a result, however, the licensees have also opted to discontinue use of the NRC-endorsed approach in NUMARC 93-01 (NEI 2011) for meeting requirements in 10 CFR 50.65. As such, NRC resident inspectors are tasked with understanding the underlying technologies employed in these new approaches (e.g., AI, ML, and data analytical tools) to ensure the adequate inspection of the licensee's ability to meet the requirements in 10 CFR 50.65 [20].

Characterization of critical components (e.g., heat exchangers) combined with automation of maintenance task execution through ML and early detection of faults is expected to reduce staffing requirements and O&M cost.

Current commercial analysis software provides more detail faster (close to real time) than ever before– this is key to the implementation and use of DTs. Westinghouse [21] uses DT to create a condition-based monitoring DT with ML that can evaluate primary equipment to enable movement away from the time-based paradigm. The following examples of some of the services offered by Westinghouse that are essentially DTs that integrate monitoring and diagnostics:

WESTEMS is a Windows-based integrated diagnostics and monitoring system. It is modular in design, using project-based models and a family of plug-in programmable components. Projects developed in WESTEMS use integrated models that contain plant thermal-hydraulic models, mechanical interaction models, local stress models and Green's functions, and supporting utilities. The physical system requires a dedicated data acquisition computer/server (machine may be physical or virtual).

The Modular Accident Analysis Program (**MAAP**) simulates LWR system response to a severe core accident. MAAP5 can predict the progression of accident scenarios to a safe, stable, coolable state within the core. It also can predict the occurrence of vessel failure and can model the containment performance with successful debris cooling or pressurization of containment to a predefined failure condition. MAAP5 contains engineered system and operator action models that allow detailed simulation of emergency operating procedures and severe accident management guidelines. It also contains enhanced graphics models (MAAP5-GRAPH), as well as code enhancements to MAAP4 for best-estimate and design basis analysis (DBA)-type modeling for the reactor core, reactor coolant system, containment, and used fuel pool [22].

BEACON (Best Estimate Analysis of Core Operations - Nuclear), a core monitoring and operational support package developed by Westinghouse, has been installed at many operating PWRs worldwide [23]. The BEACON system is a real-time monitoring system that can be used in plants with both fixed and movable incore detector systems, and it uses an online nodal model combined with core instrumentation data to provide continuous core power distribution monitoring. In addition, accurate

core-predictive capabilities utilizing a full core nodal model updated according to plant operating history can be made to provide operational support. Core history information is kept and displayed to help operators anticipate core behavior and take pro-active control actions. The BEACON system has been licensed by the NRC for direct continuous monitoring of departure from nucleate boiling ratio (DNBR) and peak linear heat rate. This allows BEACON to be integrated into the plant technical specifications to permit significant relaxation of operating limitations defined by conventional technical specifications.

3.2.2.2 Diagnostics

Diagnostics and prognostics provide the technical means for enhancing affordability and safe operation of ARs over their lifetime by enabling lifetime management of significant passive components and reactor internals [24]. Here, *diagnostics* refers to the ability to determine the presence and cause of any specific condition or quantity of interest, whereas *prognostics* refers to the prediction of the expected level of change in this condition over time [25]. All systems for diagnostics and prognostics (often referred to as *prognostic health management* [PHM] systems) have several technical elements, including [24] "(1) sensors for performing measurements of both process parameters, as well as indicators of degradation; (2) diagnostic algorithms that use the sensor measurements to estimate the condition of the component; (3) prognostics algorithms to calculate the RUL [remaining useful life] of the component with degradation; and (4) interfaces to decision and control systems that are used to make O&M decisions." While the use of DTs for diagnostics and prognostics are a relatively recent phenomenon, these systems have always required robust models that enable diagnostic and prognostic algorithms to perform their function. Fundamentally, these models (traditional regression-based models, physics models, or DTs) and the associated algorithms are required to accomplish the following:

- Provide early warning of potential degradation, especially in difficult-to-access components leading to failure in AR environments.
- Provide enhanced situational awareness of plant equipment and component conditions and margins to failure, particularly for conditions in which knowledge of physics-of-failure in the AR environment is limited.
- Enable lifetime management of significant components operating in harsh environments (high-temperature, fast flux, and corrosive coolant chemistry).
- Relieve the cost and labor burden of currently required periodic inspections.
- Support a science-based justification for extended plant lifetime by ensuring reliable component operation.

Typically, these technologies have been proposed for non-safety–significant components, and as such, they have required limited regulatory review. To date, the methods and models used have been largely data driven and statistical in nature, although some physics-based models (probabilistic fracture mechanics) have been applied for passive component diagnostics and prognostics. The technology development focus has largely been on validating and assessing the risk to plant safety associated with deploying these techniques—specifically, the risk due to a missed detection or misdiagnosis of a fault condition.

Safety evaluations by the regulator on similar technologies (for instance, online monitoring for drift/fault detection) have also tended to focus on these issues, with the need to demonstrate proper performance, the need to quantify associated uncertainty bounds, and the need to incorporate alternative monitoring technologies to address concerns of missed detection.

3.2.2.3 Displays and HSIs

The displays and interfaces with the DT may become important depending on how the DT is used. The NRC reviews the human factors engineering (HFE) aspects of NPPs to ensure that their design uses state-of-the-art HFE principles. These reviews help protect public health and safety by ensuring that the operator's performance and reliability are supported appropriately. The main guidance supporting these safety reviews is included in the following publications:

- NUREG- 0800, Chapter 18, "Human Factors Engineering" [26]
- NUREG-0700, Rev. 3, *Human-System Interface Design Review Guidelines* [27]
- NUREG-0711, Rev. 3, *Human Factors Engineering Program Review Model* [28]

The NRC's current review guidance was developed for large light-water reactors (LLWRs). A strong regulatory basis was developed for LLWR reviews consisting of regulatory requirements in the CFR and detailed safety review guidance in NUREG-0800 and supporting regulatory documents.

NUREG-0800, Chapter 18, "Human Factors Engineering," requires that licensees submit a control room design that reflects state-of-the-art HFE principles before committing to the fabrication or revision of fabricated control room panels and layouts. Chapter 18 identifies those regulations that address general requirements that influence the HFE design and the specific requirements related to the main control room that influence the HFE design. This is the most encompassing HFE related regulation. Chapter 18 identifies NUREG-0700 and NUREG-0711 as sources that can be used to meet the acceptance criteria for HFE design attributes required by the CFR.

NUREG-0700 describes acceptance criteria for the physical and functional characteristics of HSIs.

The regulatory guidance provided in NUREG-0711 addresses all the human factors elements of the requirements identified in NUREG-0800, Chapter 18. NUREG-0711 identifies 12 elements needed for successful integration of human characteristics and capabilities into the design.

To ensure that review guidance is current, the NRC conducts research to identify potential human performance issues associated with new and advanced NPP designs, prioritizes the issues, and develops the technical bases needed to address issues of particular importance. Two of the top-priority issues are related to automation: "levels of automation" and "interfaces to automation" [29]. BNL divided the levels of automation into the following topics:

- Automation's reliability, operator trust, and the use of automation
- High levels of automation and operator performance
- Intermediate and low levels of automation and operator performance
- Varying levels of automation, adaptive automation, and operator performance

Trust is a key factor governing how operators use automation. If operators do not develop a level of trust that an automated system will function appropriately (in this case, the DT), then they are unlikely to use the system. The automation's reliability is an important consideration in the development of trust; operators tend to trust a reliable system.

A DT may be incorporated into the control console and display panels in the control room, or it may be a local control station that provides data and analytics. Local control stations are not specifically addressed in the regulations. However, NRC staff often review changes to important human actions (risk-important human actions and certain deterministic human actions identified by the accident analyses) that are

conducted using local control stations. In these cases, the staff uses a graded approach to evaluate those important human actions that are conducted from local control stations.

SRP Chapter 18, Subsection III, "Acceptance Criteria," contains a list of HFE-related requirements (see Table 1) that may be applicable to the interface with a DT.

Table 1. HFE CFR general requirements related to the main control room

• 10 CFR 50.34(f)(2)(ii) – continuing improvement of HFE and procedures
• 10 CFR 50.34(f)(2)(iv) – safety parameter display system
• 10 CFR 50.34(f)(3)(i) – use of operating experience
• 10 CFR 50.54 (i) to (m) – staffing
• 10 CFR 52.47 – level of detail required in DCs
• 10 CFR 52.47(a)(8) – inclusion of 10 CFR 50.34(f) for Part 52 applications
• 10 CFR 52.79 – content of COL applications
Specific requirements related to the main control room
• 10 CFR 50.34(f)(2)(v) – automatic indication of the bypassed and operable status of safety systems
• 10 CFR 50.34(f)(2)(xi) – relief and safety valve indication
• 10 CFR 50.34(f)(2)(xii) – auxiliary feedwater system flow indication
• 10 CFR 50.34(f)(2)(xvii) – containment related indications
• 10 CFR 50.34(f)(2)(xviii) – core cooling indications
• 10 CFR 50.34(f)(2)(xix) – instrumentation for monitoring post-accident conditions that includes core damage
• 10 CFR 50.34(f)(2)(xxi) – auxiliary heat removal (boiling water reactor [BWR])
• 10 CFR 50.34(f)(2)(xxiv) – reactor vessel level monitoring (boiling water reactor)

10 CFR 50.34(f)(2)(iii) and 10 CFR 52.47(a)(8) [requires inclusion of 10 CFR 50.34(f)] are crucial for HFE, requiring an applicant to provide a control room design for NRC review that reflects state-of-the-art human factor principles. This must be done prior to committing to fabrication or revision of fabricated control room panels and layouts. This requirement is important in that it provides the regulatory basis for the NRC's general approach to HFE review as described in Chapter 18 of the *Standard Review Plan* (SRP) [NUREG-0800].

3.2.2.4 Control

Based on GDC 1 [30], GDC 13 [31], and 10 CFR 50.55a(a)(1) [32], NPP control systems should be "appropriately designed and of sufficient quality to minimize the potential for challenges to safety systems" and "capable of maintaining system variables within prescribed operating ranges" [13]. The plant control systems in general and the reactor control system in particular are designed to maintain the plant in its normal operating conditions.

The purpose of the control system is to maintain system variables such as reactor power, coolant flow rate, power-to-flow ratio, reactor outlet temperature, coolant level, and turbine status, within prescribed operating ranges. Exceeding a control system setpoint results in a plant transient and a challenge to plant mitigating systems, including a potential challenge to plant safety systems.

An example of a DT control function would be to compare a reference signal in the process to the setpoint and then change the output to the control device accordingly to minimize the error. As noted, the degree of control will dictate the requirements. If the DT performs a safety function, then its requirements and review will be the same as those for a safety system, and the software must be developed and operated in a secure environment. Cybersecurity will also be a concern.

If the DT performs control functions, then the software must still be developed using a procedure such as the waterfall process. Cybersecurity could be an issue if the failure of the DT could affect operation of a protection system. The degree of autonomy could also increase the requirements (see Section 4, "Autonomous control").

3.2.3 Programmability and Configurability

Programmability is the capability of the hardware and software to change: that is, to accept a new set of instructions that alter its behavior. *Programmability* generally refers to program logic. Configurable logic and flip-flops can be linked together with programmable interconnects. Memory cells control and define (1) the function that the logic performs, and (2) how the logic functions are interconnected. Programmable logic devices (PLDs) come in a range of types and sizes, ranging from simple programmable logic devices (SPLDs) to field programmable gate arrays (FPGAs). A DT could use one of these types of devices, or it could be installed on a microprocessor.

Configurability is the extent to which the system/component facilitates selection, set-up, and arrangement of its modules to perform I&C tasks. Configuration can be accomplished through (1) hardware, such as through the use of wiring, setting jumpers or switches, inserting modules, or (2) software configuration methods such as selecting and setting parameters, programming, inserting software modules, and downloading programs [33]. As configurability increases, so does the likelihood for errors in requirements, design, implementation, operations, and maintenance.

Examples of configurability and programmability are shown below:

- **Nonconfigurable, nonmodifiable firmware:** oven controller, diesel generator, pump
- **Configurable, nonmodifiable firmware:** fire alarm control panel, flowmeter, spectrometer
- **Modifiable firmware:** programmable logic controller (PLC), programmable array logic (PAL), programmable logic array (PLA), complex programmable logic device (CPLD), FPGA

The configurability, programmability, and complexity can vary greatly between the different types of DTs. A DT may be configurable but not programmable (i.e., the software cannot be modified), in which case it cannot be reprogrammed, nor can its functions be altered in a general way so that it performs a conceptually different function. In these types of DTs, only predefined parameters can be reconfigured by users.

The more complex the DT is, the more likely that it will be configurable. The design should account for I&C parameters that must be configurable or verified and validated during operation, and it must provide the means to execute these requirements (e.g., RPS trip settings, calibration constants, and software configuration settings). HMI can significantly increase the capabilities and ease of changing DT configurability. It is important to note that the ancillary functions that provide configurability must also be evaluated.

3.2.4 Consequences

As with classification, consequences must be defined. NRC generally invokes three categories of consequences: two are in regulations 10 CFR 20 and 10 CFR 50.34, and one is in the safety goal policy that provides a quantitative health objective (QHO). The DOE consequence threshold is set for the public, the co-located worker (CLW), and the facility worker (FW) based on the total effective dose equivalent (TEDE) for the public, TEDE for a CLW, and the prompt death of an FW.

Safety-related systems are designed to reduce the frequency or probability of the hazardous event and/or the consequences of the hazardous event. An increase in the severity of the consequence must be determined based on the function not operating as compared to when the function operates as intended. This can be done by considering the consequences if the DT fails to operate and then considering what difference will be made if the mitigation function operates correctly. When considering the consequences that would occur if the system, or in this case the DT, failed to operate, several outcomes, all with different probabilities, should be considered. The principal consequence that physical barriers are designed to preclude is the uncontrolled release of radioactivity. Therefore, for the purposes of this review, the term *consequence* means *dose*.

The three physical barriers that provide defense-in-depth are

1. Fuel and clad boundary
2. RCS boundary
3. Containment boundary

Safety systems must be in place to mitigate the consequences of accident events. Maintaining the integrity of these three barriers can prevent or mitigate the consequences of an accident event.

In this review, the focus is on the DT and its effect on the plant. The objective is to assess the consequences resulting in the action or inaction of a DT on plant systems and then to assess the consequences of the failure on those systems. This is different than evaluating the use of the DT to mitigate the consequences of an accident event.

If a licensee wanted to install a DT in an existing operating plant, 10 CFR 50.59 (iv) requires a LAR if a malfunction of an SSC important to safety results in more than a minimal increase in the consequences of a previously evaluated event specified in the final safety analysis report (FSAR). There are three ways to assess whether the failure has an increased consequence of a previously evaluated event:

a. Its failure is modeled in the PRA or failure modes and effects analysis (FMEA), and its consequences can be calculated.

b. The safety class of the SSC is known.

c. Appropriately evaluated supporting issues may allow for a risk-informed approach for the review and use of DTs. The quality process (10 CFR 50, Appendix B), very high usage, operating experience outside the nuclear industry, completeness of diagnostic coverage, and other factors, may inform a graded approach on the review and use of DTs.

A consequence-based approach for evaluating DTs could be similar to NASA-GB-8719.13 [34] grading based on consequences of the failure's impact on the system. (NASA-GB-8719.13 supersedes NASA-GB-1740.13 [35]) A consequence-based approach could result in the use of a graded approach in the requirements of a DT by relaxing the IEEE SIL 4 requirements for safety SSCs. Based on the guidance in

Annex B of IEEE Standard (Std.) 1012-2004, a risk-based approach would categorize a DT with announced failures or with diagnostics as IEEE SIL 1–2. DTs with unannounced failures would range anywhere from IEEE SIL 1–4. If other devices monitor the same parameter of interest to the DT, then the failure of an individual DT becomes less important with a corresponding lower SIL requirement.

Control devices can be categorized as either active or on-demand. A DT could be placed in either category. The primary difference between active or on-demand categories is that the failure of an active control device will be evident either through faulty output or diagnostics. The failure of an on-demand device is not known until the device is demanded for service or if the built-in testing/self-diagnostic features indicate that there is a failure present in the device prior to demanding its service.

The software and review could be classified based on how an error affects the software and system containing the software (see Section 3.2.1, "Classification").

3.2.5 CCFs

Hardware and software are both susceptible to CCF. The potential for CCFs exists because of common components, identical hardware, identical software, the same requirements, and the same operating environment. If such commonalities are identified, justification should be provided to demonstrate that the potential for CCF is low. Hardware and software CCFs may cause identical components to fail at the same time. However, a CCF could also cause an operator to take an inappropriate action based on information provided by the DT or diagnostics even if the DT is not connected to a safety or important-to-safety system.

A software design defect in a DT can occur in the OS or application system software. The defect can cause one or more controllers to simultaneously generate erroneous outputs, or it can cause the outputs to freeze in their current state.

- The OS alone does not perform any application-specific logic that would be designed for influencing or controlling any SSC.

- An OS can be a commercially available, multi-tasking, real-time package available from a third party, or it can be a single task, once-through firmware program designed by the equipment vendor and embedded in their digital product.

- OS and application software often have different characteristics that are under the control of different entities.

For a software CCF to occur simultaneously in multiple DTs, two conditions must be present:

- An identical, latent defect must exist in the software (firmware) of multiple DTs.

- A triggering condition must occur, almost simultaneously in multiple DTs, that exposes the latent defect.

BTP 7-19, Revision 7 [36], provides guidance to the NRC staff on evaluating the defense-in-depth and diversity of a digital instrumentation and controls (DI&C) ***system***. However, as in a system, the DT's testability could be used to eliminate consideration of CCF.

Regulatory Issue Summary (RIS) 2016-05 [37] identifies NRC regulatory requirements to address potential vulnerabilities to CCFs for safety-related equipment. Supplement 1 to RIS 2002-22 offers

potential relief through qualitative assessment of the likelihood of failure. The RIS addresses two potential outcomes of the qualitative assessment:

1. Failure likelihood is sufficiently low
2. Failure likelihood is not sufficiently low

In embedded systems, uninitialized variables can often be the source of latent software bugs [38]. Failure of the software and hardware specifications to correctly model the physical environment and functioning of the process can result in a CCF. Software failures can also result from design defects (i.e., faults or bugs) in the code and can be caused by incorrect requirements, misunderstanding of requirements, and coding mistakes.

Simultaneous failure of multiple redundant digital components is possible if all components are executing the same program with essentially the same inputs and outputs and are more or less synchronous, as in software CCF. For a software CCF to occur in a DT, there must be a latent defect in the OS or application software. However, if the DT is used as a control device, then a CCF could transmit erroneous signals to multiple components.

Following the established methods for software development and qualification provides reasonable assurance that the likelihood of failure resulting from software defects is sufficiently low. Software development for DTs, which should follow the same requirements and guidance as that for I&C systems, should also provide reasonable assurance on the likelihood of defects in the software. Quality is one of the key defenses against hardware and software CCFs resulting from a design defect.

NRC provides guidance in protecting against software CCFs. For example, despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors may mean that a defect-free DT cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and to support reaching a reasonable assurance of safety. This may occur if the development process is not of the same quality as that required by the NRC regulations and guidance, if it is different from NRC guidance (but equivalent), or if its pedigree is unknown.

A defensive measure to minimize the likelihood of a hardware or software CCF is through the application of testing and operating experience. This is the US Department of Defense (DoD) approach—to have continuous or frequent operation continuously, with failures announced and observed.

Although a control system is not classified as a safety system, it still plays an important role in defense-in-depth. NUREG/CR-6303 [39] and NUREG/CR-7007 [40] provide guidance on diversity and defense-in-depth assessments. Although failures in the control system may challenge the protection system, the control system can mitigate most disturbances without the need for action by the protection system. Furthermore, during an incident in which one of the protection system echelons (reactor trip or engineered safety features actuation system [ESFAS]) fails to perform its safety function because of a CCF, the control system may be able to mitigate the associated disturbance.

The DT's functionality will determine whether defense-in-depth is required, and if so, to what level of diversity (Table 2). For example, if the functionality is a noncontrol function, then a CCF would not cause an overall system failure, but it could create unreliable values that could cause an inappropriate action/inaction (Table 2). If the DT has a control function, then in addition to independence, diverse sensor values may be required to meet reliability demands. Any DT with communications functionality will require more thorough reviews because of the increased communication capabilities that digital systems employ and the susceptibility to propagating failures and misinformation.

Table 2. Functionality determines diversity

	Malfunction cannot prevent/block SCRAM	Diverse means of seeing the current values
Non control functionality	Expected to be fully independent of protection system	Possible solution for diverse means of seeing current values; reliability/confidence of DT predictions may be necessary
Control functionality	Requires review to ensure independence; reliability/confidence of DT predictions may be necessary	Possible need for diverse source of information
Communications functionality	Complicates review (if vital to essential operation)	Complicates review (if vital to essential operation)

3.2.6 Plant Integration

Several requirements and guidance documents have been developed to ensure that the DT will operate properly when integrated into the plant. Because of the lack of history in using a DT to provide real-time monitoring and operational decisions, the requirements for ensuring that it will perform properly are of importance and should be addressed.

System integration is one aspect of the software lifecycle. In integration testing, software components and/or hardware components are combined and tested to evaluate their interaction. The objectives of integration V&V are to ensure that (1) the system architectural design is implemented correctly through integration, (2) the integrated system meets the system requirements, (3) the system integration strategy is consistent with the system architecture, (4) the integration test plan and procedures are traceable to the system architectural design, (5) the unavoidable constraints of integration that influence requirements are addressed correctly, (6) the integration of human performance into systems and their operation is correct, and (7) the nonconformances resulting from integration actions are recorded and addressed [41].

GDC 1 in 10 CFR 50, Appendix A requires that quality standards be established and implemented to provide adequate assurance that SSCs important to safety will satisfactorily perform their safety functions. The criteria in Appendix B apply to all activities—such as design, purchase, installation, testing, operation, maintenance, or modification—that affect the safety-related functions of such SSCs.

10 CFR 50.55a(a)(1) requires, in part, that systems and components be designed, fabricated, erected, tested, and inspected to quality standards commensurate with the safety function to be performed. The regulations in 10 CFR 50.55a(h) require that reactor protection and safety systems satisfy the criteria in IEEE Std. 603-1991 (including a correction sheet dated January 30, 1995), or IEEE Std. 279.

RG 1.168 [42] provides guidance on verification, validation, reviews, and audits for digital computer software used in safety systems of NPPs and applies to all aspects of the software lifecycle within the system lifecycle context. RG 1.168 endorses IEEE Std. 1012-2004 [43] and IEEE Std. 1028-2008 [44] for meeting these requirements. The component and integration test plans in IEEE 1012-2004 describe methods for measuring software reliability that should serve as criteria for determining if software elements correctly implement software requirements.

10 CFR 52 enables the licensee to construct a plant and to operate it once construction is complete if certain standards identified in the combined license are satisfied. These standards are termed *inspections, tests, analyses, and acceptance criteria*, or ITAAC. The requirements regarding ITAAC for DC, manufacturing license, and COL applications are set forth in 10 CFR 52.47, 52.80, and 52.158.

4. AUTONOMOUS CONTROL

Automated control describes a self-acting reactor response based on fixed setpoints, whereas *autonomous control* describes the capability of a reactor to take independent action based on consideration of multiple inputs and trends [45]. Automated control based on fixed setpoints is a basic form of autonomous control, with follow-up operator actions expected. However, more complex autonomous reactor control systems can operate at very high levels of performance and reliability with little or no human assistance required to adjust power level, move control elements, start or stop pumps, open or close valves, and so on, in response to plant operations, transients, or casualties.

To be autonomous, a control system should provide adequate control actions in the presence of significant uncertainties. The key attributes of highly autonomous control systems are as follows [46]:

1. Effective performance under all process operating conditions and performance demands
2. The ability to compensate for system failure without external intervention.

Vagia et al. [47] present a literature review of the evolution of the levels of autonomy from the end of the 1950s up until 2015. The primary motivation of this study was to gather and compare existing literature on taxonomies on levels of automation. Technical developments within computer hardware and software have made it possible to introduce autonomy into virtually all aspects of human–machine systems. The current study focuses on how different authors approach different levels of automation.

In older systems, allocation of responsibilities for function performance was straightforward—functions were either automated (i.e., performed essentially without human involvement) or manual (i.e., performed by plant personnel without automation). However, as computers became more involved in process control, the nature of automation changed. Recent approaches to automation involve the cooperation and sharing of responsibilities between automatic systems and plant personnel.

Increasingly, designers use intermediate levels of automation, resulting in a gradation from manual to automatic. Therefore, the relative responsibilities of humans and automation for performing tasks vary. This concept often is referred to as *levels of automation*. This concept has been around for some time.

In 1992, Sheridan defined three global levels of automation: manual control (all control is accomplished by humans), supervisory control (some or all of the control loop is closed by the computer, but the human supervisor can assert control), and fully automatic control (all control is automatic, and the human cannot vary the process except perhaps to terminate it). As technology has evolved, Sheridan [48] offered more fine-grained distinctions between these levels of automation (see Table 3).

As shown in Figure 3, the level of automation for a DT can be at the advisory level (2) or as high as *8–full autonomy* [49]. The distinctions among levels range from the logic for selecting a control action being fully automated and communicated to a human operator who can choose to implement a different action (condition 6), to a logic in which the decision process and its implementation are performed with no human intervention (condition 8).

Table 3. Sheridan's levels of automation [48]

Level	Description
1	The computer offers no assistance; the human must do it all
2	The computer suggests alternative ways to do the task
3	The computer selects one way to do the task and (see Level 4)
4	The computer executes that suggestion if the human approves, or (see Level 5)
5	The computer allows humans a restricted time to veto before automatic execution, or (see Level 6)
6	The computer executes automatically and then necessarily informs the human, or (see Level 7)
7	The computer executes automatically and then informs the human only if asked
8	The computer selects the method, executes the task, and ignores the human

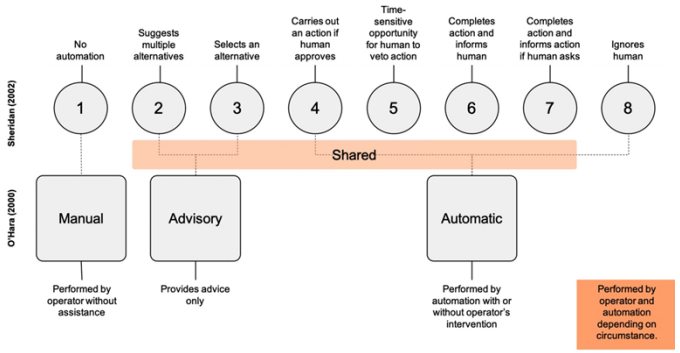


Figure 3. Levels of automation in a control system [50].

NUREG-0700 [27] and NUREG-0711 [28] have identified five levels of automation (Table 4). BNL found examples of automation at every level in NPPs; none were identified that did not fit into the modified scheme [29]. However, these systems often are complex, so a system (or portions of it) may sometimes be characterized at one level and at other times at another.

Table 4. Levels of automation for NPP applications

Level	Automation functions	Human functions	NPP example
1. Manual operation	No automation	Operators manually perform all functions and tasks	Demineralized water system
2. Shared operation	Automatic performance of some functions/tasks	Operators perform some functions/tasks manually	Suppression pool cooling mode of residual heat removal service water system
3. Operation by consent	Automatic performance when directed by operators to do so under close monitoring and supervision	Operators monitor closely, approve actions, and may intervene with supervisory commands that automation follows	Advanced BWR startup process
4. Operation by exception	Essentially autonomous operation unless specific situations or circumstances are encountered	Operators must approve of critical decisions and may intervene	Automatic depressurization system / safety relief valve system BWR automatic depressurization system AP1000 passive containment cooling
5. Autonomous operation	Fully autonomous operation. System or function not normally able to be disabled, but may be manually started	Operators monitor performance and perform backup if necessary, feasible, and permitted	RPS

For the existing fleet of operating LWRs, the response time for safety actions to some types of events is short. For example, for the design basis loss-of-coolant accident (LOCA), emergency core cooling systems must operate immediately to prevent core damage, so most RPS actions are automated. In fact, typically no regulatory credit can be taken for a manual action that would be required within 30 minutes of the start of the event [51]. Nevertheless, for the current generation of reactors, the operating staff are a key element to ensure that plants are operated safely. Although safety actions are typically automated, they are always performed under the eye of the operating crew. With no human intervention, the supervisory control system (SCS) must be able to detect and predict changing conditions and disturbances, to identify the best response(s) for actual or predicted plant conditions, and to continuously reevaluate operational status. The key question regarding control is, *what is the appropriate level of automation?*

An SCS uses a graded autonomy to execute any decision. An SCS also uses the alarm system to inform the operator of a decision (alert), or it requests confirmation of a decision (alarm). In the nominal range, the SCS is fully autonomous, and decisions are probabilistically informed. As the system progresses closer to a trip setpoint, autonomy decreases by informing the operator of the action taken or requesting concurrence from the operator before an action is taken.

The key question regarding control is, *what is the appropriate level of automation for a DT?* The HMI functions can provide the operator with proper interfaces to guide and direct the control system through the use of a properly organized and managed alarm system.

Alarms are classified according to their severity and their time response requirements to differentiate between long-term maintenance items and critical items demanding immediate attention. Figure 4 shows that as the system moves away from the nominal state space, the status indication increases from *alerts* to *alarms*.[4]

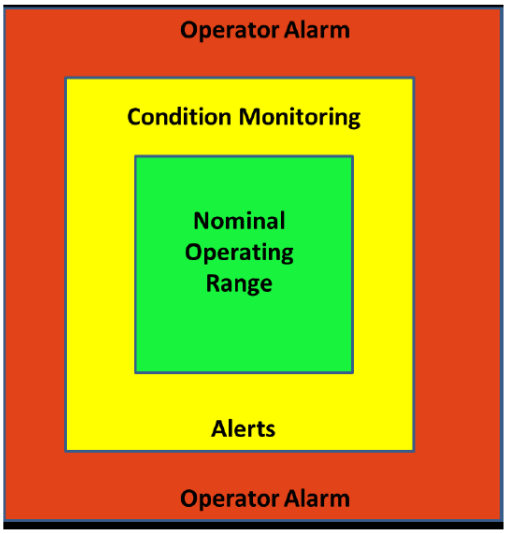


Figure 4. Relationship of alarm categories.

If the system parameters progress into the degraded region of control (i.e., moving from alerts to alarms), then operator awareness and involvement with the DT increases. The three levels of operator involvement, based on the scale of degrees of automation, are [49] as follows

1. **Nominal operating range:** the computer decides everything and acts autonomously, with no need to inform the operator of actions taken. No operator's response or intervention is needed. Sufficient monitoring information is available to the operator to confirm that the system is operating within the nominal operating range.

2. **Alerts:** the computer determines a complete set of action alternatives, selects one, executes automatically, and then necessarily informs the operator.

3. **Operator alarm:** the computer determines a complete set of action alternatives, selects one, and then executes the selected alternative if the operator approves.

If the functionality of the DT is to provide control, then a graded autonomy could be used to execute any decision. The alarm system informs the operator of a decision (alert) or requests confirmation of a decision (alarm). In the nominal range, the DT is fully autonomous. As the system progresses closer to a

[4] An *alert* is a notification for the operator to be watchful and is lower priority than an alarm. An *alarm* indicates if and when the value or the rate of change value of a measured or initiating variable is out of limits, has changed from a safe to an unsafe condition, and/or has changed from a normal to an abnormal operating state or condition.

trip setpoint, autonomy decreases by informing the operator of the action that was taken or requesting concurrence from the operator before an action is taken.

Reactors regulated by the NRC have numerous licensing challenges for any level of autonomous control. The requirements specified in 10 CFR 50.54 [52] provide a basis for licensing issues for any reactor design that intends to implement a high degree of autonomous control. These issues include the following [53]:

- Staffing
- Number of licensed operators
- Manipulation of controls
- Technical specifications (TSs)
- Cybersecurity
- Notifications

4.1 IMPACT ON STAFFING [10 CFR 50.47, 10 CFR 50.54]

Current regulations, as written, do not provide for reducing the number of licensed operating staff for cases with or without DTs, without exception. However, apart from this, staffing reduction may be possible in other areas, such as maintenance.

10 CFR 50.47 establishes requirements for NPP emergency response plans. 10 CFR 50.47(b)(2) requires that adequate staffing be provided, with no regulatory requirement specified as to the number of licensed operators required to provide for on-shift accident response. NUREG-0654 [54] provides evaluation criteria for determining what constitutes adequate staffing and provides guidance on staffing levels that the NRC has determined to be acceptable. Staffing at a microreactor with a colocated facility may allow for smaller staffing levels and fewer security forces, but complete elimination will be more problematic. The use of a DT should not affect the staffing levels required for emergency response plans.

Current regulations regarding licensed operator staffing levels are based on existing large LWRs that rely primarily on active safety systems and operator actions to address plant transients and design basis accidents. 10 CFR 50.54(k) and (m) are very specific regarding control room staffing. 10 CFR 50.54(m)(2)(i) specifies the minimum requirements for onsite staffing by licensed operators and senior operators. The requirements of 10 CFR 50.54(m) tend to prohibit reducing the operating staff by taking credit for a reactor design with a highly autonomous DT (i.e., the DT does not replace an operator).

An exemption from the requirements of 10 CFR 50.54(m) can be requested and granted. NuScale, a multimodular NPP, has requested an exemption on the number of control room operators based on the number of operators present at the plant compared to a per-unit basis. The NRC staff advised NuScale that if the control room staffing does not meet the requirements in 10 CFR 50.54(m) and the guidance in NUREG-0711, Section 6.4, “Review Criteria,” Criterion 2 [28], then the staff will follow the guidance in NUREG-1791 [55] to determine whether the staffing proposal provides adequate assurance that public health and safety will be maintained at a level comparable to compliance with 10 CFR 50.54(m) [56].

One might expect a future arrangement in which a DT could support reducing operator numbers and other O&M staffing levels. NuScale demonstrated that exemptions can be granted. A significant difference from fully autonomous control using a DT compared to NuScale is that NuScale is a multimodule NPP that will have fewer operators per unit but will still have operators present. Thus, staffing levels, especially those for emergency response, may need to be revisited in the context of using a DT. Because current regulations tend to prohibit reducing the number of licensed operating staff in a control room by

taking credit for DT, further review and update of regulations will be required as DTs become more widespread.

4.2 NUMBER OF LICENSED OPERATORS [10 CFR 55]

From the time a reactor commences operation until the plant is decommissioned, regulations require that licensed operators be continuously present at the controls. Additionally, the licensed operator at the reactor controls should be under constant supervision as specified in 10 CFR 50.54(k) and (l):

(k) An operator or senior operator licensed pursuant to [10 CFR 55] of this chapter shall be present at the controls at all times during the operation of the facility.

(l) The licensee shall designate individuals to be responsible for directing the licensed activities of licensed operators. These individuals shall be licensed as senior operators pursuant to [10 CFR 55] of this chapter.

Licensed operators continuously turn plant responsibility over, including official designation of who is responsible for the controls at any moment. These transitions extend to bathroom and food breaks. Each licensed operator is granted a license by the NRC as noted in 10 CFR 55.3, License Requirements:

> *A person must be authorized by a license issued by the NRC to perform the function of an operator or a senior operator as defined in this part.*

An *operator* is defined in 10 CFR 55.4 as "any individual licensed under this part to manipulate a control of a facility." Likewise, a *senior operator* is defined as "any individual licensed under this part to manipulate the controls of a facility and to direct the licensed activities of licensed operators." Exemptions are provided in 10 CFR 55 for individuals in training to manipulate the controls under the direction of a licensed operator or senior operator. The NRC will grant a license (10 CFR 55 Subpart F) to an individual who meets medical requirements (10 CFR 55 Subpart C) and who passes written and operating tests (10 CFR 55 Subpart E). Licenses are conditional, as specified in 10 CFR 55.53, including:

(b) The license is limited to the facility for which it is issued.

(c) The license is limited to those controls of the facility specified in the license.

Each license expires after 6 years and must be renewed by continuing to meet medical requirements and pass written and operating tests.

It is conceivable that the reactor control room may not be colocated with the NPP because of the implementation of highly autonomous controls in the design and remote siting. However, licensed operators dedicated to that facility are required under current regulations. Thus, a DT with autonomous control that is implemented either on- or off-site given the current regulations will not affect the number of licensed operators required. The current requirement is based on current regulations and regulatory guidance, which appear to lag the state-of-the-art use of DTs. These regulations will likely be revisited if a DT can be shown to be trustworthy for use in autonomous control.

4.3 MANIPULATION OF CONTROLS [10 CFR 50.54(M) AND 10 CFR 55]

The RPS may automatically shut down the reactor if an unsafe condition or direction is sensed. However, licensed operators must be fully aware of any other manipulation of reactor controls, including any apparatus and mechanism other than controls that may affect the reactor's reactivity or power level, as

discussed in 10 CFR 50.54. This requirement will impact any consideration of highly autonomous reactor operation. Regulations are very specific regarding manipulation of the controls that affect the reactivity or power level of the reactor. 10 CFR 50.54(i) and (j) specify that:

> *(i) Except as provided in [10 CFR 55.13], the licensee may not permit the manipulation of the controls of any facility by anyone who is not a licensed operator or senior operator as provided in [10 CFR 55].*
>
> *(j) Apparatus and mechanisms other than controls, the operation of which may affect the reactivity or power level of a reactor shall be manipulated only with the knowledge and consent of an operator or senior operator licensed pursuant to [10 CFR 55] present at the controls.*

Licensed operators must be fully aware of any manipulation of reactor controls, including apparatus and mechanisms other than controls that may affect the reactivity or power level of the reactor as discussed in 10 CFR 50.54(i) and (j). Operator knowledge and consent are key components of this regulation. Highly autonomous reactor designs must prove significant safety margins regarding reactivity insertions and power level changes.

Highly autonomous reactor designs must prove significant safety margins regarding reactivity insertions and power level changes. The requirement for prior licensed operator knowledge and consent of reactivity and power level changes must be explored in detail regarding a highly autonomous reactor design. This approach magnifies the importance of the operators having trust in the DT.

4.4 TECHNICAL SPECIFICATIONS [10 CFR 50.36, 50.54, 50.46, AND APPENDIX K]

Highly autonomous reactor designs must consider TSs as discussed in 10 CFR 50.36, *Technical Specifications*. As noted in the regulation, the "TS will be derived from the analyses and evaluation included in the safety analysis report," and highly autonomous reactor designs must consider design safety limits, limiting safety settings, and limiting control settings based on these analyses. The limits and associated settings are defined in 10 CFR 50.36(c):

> *Safety limits for nuclear reactors are limits upon important process variables that are found to be necessary to reasonably protect the integrity of certain of the physical barriers that guard against the uncontrolled release of radioactivity. If any safety limit is exceeded, the reactor must be shut down.*
>
> *Limiting safety system settings for nuclear reactors are settings for automatic protective devices related to those variables having significant safety functions. Where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting must be so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded.*
>
> *Limiting conditions for operation [LCO] are the lowest functional capability or performance levels of equipment required for safe operation of the facility. When a limiting condition for operation of a nuclear reactor is not met, the licensee shall shut down the reactor or follow any remedial action permitted by the technical specifications until the condition can be met.*

10 CFR 50.36 requires that a TS LCO be established if any of the following criteria are met:

1. *Installed instrumentation that is used to detect, and indicate in the control room, a significant abnormal degradation of the reactor coolant pressure boundary.*

2. *A process variable, design feature, or operating restriction that is an initial condition of a design basis accident or transient analysis that either assumes the failure of or presents a challenge to the integrity of a fission product barrier.*

3. *A structure, system, or component that is part of the primary success path and which functions or actuates to mitigate a design basis accident or transient that either assumes the failure of or presents a challenge to the integrity of a fission product barrier.*

4. *A structure, system, or component which operating experience or probabilistic risk assessment has shown to be significant to public health and safety.*

Surveillance requirements relate to "testing, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met." Likewise, administrative controls provide the necessary "provisions relating to organization and management, procedures, recordkeeping, review and audit, and reporting necessary to assure operation of the facility in a safe manner." Therefore, a highly autonomous reactor design must operate the reactor within TS guidelines, provide for appropriate equipment surveillance, and provide acceptable recordkeeping and other administrative controls. Onsite licensed and unlicensed operators currently provide for equipment surveillance and the associated recordkeeping.

Various requirements in 10 CFR 50.54 reference operating in accordance with TSs. 10 CFR 50.54(n) requires that a licensee shall not, except as authorized pursuant to a construction permit, make any alteration in the facility constituting a change from the TSs previously incorporated in a license or construction permit pursuant to § 50.36 of this part.

If the DT is used to support analysis used in a safety analysis/calculation, then it is governed by 10 CFR 50.46 [57], 10 CFR 50, Appendix K [58], and some form of software V&V, most likely ASME NQA-1. 10 CFR 50.46 requires that a BWR or PWR have an ECCS. 10 CFR 50.46(b) requires that the cooling performance be calculated in accordance with an acceptable evaluation model and that it must be calculated for a number of postulated LOCAs of different sizes, locations, and other properties sufficient to provide assurance that the most severe postulated LOCAs are calculated. The evaluation model must include sufficient supporting justification to show that the analytical technique realistically describes the behavior of the reactor system during a LOCA. Comparisons to applicable experimental data must be made, and uncertainties in the analysis method and inputs must be identified and assessed so that the uncertainty in the calculated results can be estimated. This uncertainty must be accounted for to show that there is a high level of probability that the criteria would not be exceeded. Appendix K, Part II, "Required Documentation," sets forth the documentation requirements for each evaluation model. Thus, a DT that relies on thermal hydraulics analyses would require an acceptable evaluation model, with comparisons to experimental data and uncertainties calculated.

If the DT is to be used for determining TSs, surveillance intervals, and so on, then 10 CFR 50.46; 10 CFR 50, Appendix K; ASME NQA-1; and some additional V&V will serve as the governing requirements.

Various requirements in 10 CFR 50.54 reference operation in accordance with TSs. Therefore, highly autonomous reactor designs must consider TSs regarding design safety limits, limiting safety settings, and limiting control settings as discussed in 10 CFR 50.36. A highly autonomous reactor design must operate the reactor with TS guidelines, provide for appropriate equipment surveillance, and provide acceptable recordkeeping and other administrative controls. Onsite licensed and unlicensed operators currently provide for equipment surveillance and the associated recordkeeping.

One potential use of DTs is to provide insights into the completion times (CTs) and surveillance frequencies (SFs) in the licensing basis through changes in the plant's technical specifications. RG 1.177 [59] describes methods acceptable to the NRC staff for assessing the nature and impact of proposed TS changes by considering engineering issues and applying risk insights. This RG provides the staff's recommendations for utilizing risk information to evaluate changes to TS CTs and SFs in order to assess the impact of such proposed changes on the risk associated with plant operation. RG 1.177 provides guidance concerning an approach that the NRC has determined to be acceptable for analyzing issues associated with proposed changes to a plant's TS and for assessing the impact of such proposed changes on the risk associated with plant design and operation. Additional or revised guidance might be provided for new reactors (e.g., advanced LWRs [ALWRs]) licensed under 10 CFR Part 52, *Licenses, Certifications, and Approvals for Nuclear Power Plants*.

Licensees are expected to provide strong technical bases for any TS change. The technical bases should be rooted in traditional engineering and system analyses. TS change requests based on PRA results alone should not be submitted for review. TS change requests should give proper attention to the integration of considerations, such as conformance to the standard technical specifications (STSs), generic applicability of the requested change if it is different from the STS, operational constraints, manufacturer recommendations, and practical considerations for test and maintenance. Standard practices used in establishing CTs and SFs should be followed (e.g., CTs are typically 8 hours, 12 hours, 24 hours, 72 hours, 7 days, 14 days, and so on, and SFs are typically once per 12 hours, 7 days, 1 month, 3 months, and so on.) Using such standards greatly simplifies implementation, scheduling, monitoring, and auditing. Logical consistency among the requirements should be maintained, (e.g., CT requirements for multiple trains out of service should not be longer than that for one of the constituent trains).

4.5 CYBERSECURITY [10 CFR 50.34, 10 CFR 52.79, AND 10 CFR 73]

Security, including cybersecurity, is a required condition of any license as directed in 10 CFR 50.54(p)(1):

> *(p)(1) The licensee shall prepare and maintain safeguards contingency plan procedures in accordance with appendix C of [10 CFR 73] for affecting the actions and decisions contained in the Responsibility Matrix of the safeguards contingency plan. The licensee may not make a change which would decrease the effectiveness of a physical security plan, or guard training and qualification plan, or cybersecurity plan prepared under 10 CFR 50.34(c) or 10 CFR 52.79(a), or 10 CFR 73 of this chapter. . . .*

CFR 50.34(c) and 10 CFR 52.79(a) specify the content of license applications under varying licensing paths. Both specify that a cybersecurity plan is required as set forth in 10 CFR 73.54, *Protection of Digital Computer and Communication Systems and Networks*:

> *(a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks. . .*

Within 10 CFR 73.54, the licensee is directed to protect digital computer and communication systems and networks associated with the following:

- Safety-related and important-to-safety functions
- Security functions
- Emergency preparedness functions, including offsite communications
- Support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions

Specifically, the cybersecurity program must be designed to:

- Implement security controls to protect the assets identified above from cyber attacks
- Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks
- Mitigate the adverse effects of cyber attacks
- Ensure that the functions of protected assets are not adversely impacted due to cyber attacks

Highly autonomous reactor designs will interface directly with safety-related and important-to-safety systems and functions. Therefore, cybersecurity will be an important consideration for any highly autonomous reactor design to demonstrate adequate protection of the health and safety of the public and the environment. Providing appropriate cybersecurity will be complicated if the design implements an offsite control room to support a remotely sited reactor.

Security, including cybersecurity, is a required condition of any license as directed in 10 CFR 50.54(p)(1) and as expanded upon in 10 CFR 73.54. Each licensee must provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks. Highly autonomous reactor designs will interface directly with safety-related and important-to-safety systems and functions. Therefore, cybersecurity will be an important consideration for any highly autonomous reactor design to demonstrate adequate protection of the health and safety of the public and the environment. Providing appropriate cybersecurity will be complicated if the design implements an offsite control room to support a remotely sited reactor.

4.6 EVENT NOTIFICATIONS [10 CFR 50.54 AND 10 CFR 72]

The condition of any license under 10 CFR 50.54(z) requires that

> *Each licensee with a utilization facility licensed pursuant to sections 103 or 104b. of the [AEA] shall immediately notify the NRC Operations Center of the occurrence of any event specified in [10 CFR 50.72].*

As noted, the staff notification requirements for operating reactors are provided in 10 CFR 72, Immediate Notification Requirements for Operating Nuclear Power Reactors. 10 CFR 72(a)(3) specifically requires the following:

> *The licensee shall notify the NRC immediately after notification of the appropriate State or local agencies and not later than one hour after the time the licensee declares one of the Emergency Classes [as specified in the licensee's approved Emergency Plan].*

In addition to notification of the declaration of an emergency class, notification of many other events must be made in a timely manner. This includes:

- The initiation of any nuclear plant shutdown required by the plant's TS
- Any event that results or should have resulted in emergency core cooling system discharge into the RCS
- Any event or condition that results in actuation of the reactor protection system when the reactor is critical
- Any event or situation related to the health and safety of the public or onsite personnel or protection of the environment for which a news release is planned or notification to other government agencies has been or will be made
- The condition of the NPP, including its principal safety barriers, being seriously degraded

- The NPP being in an unanalyzed condition that significantly degrades plant safety
- Any event or condition that at the time of discovery could have prevented the fulfillment of the safety function of structures or systems that are needed to:
    - Shut down the reactor and maintain it in a safe shutdown condition,
    - Remove residual heat,
    - Control the release of radioactive material, or
    - Mitigate the consequences of an accident.

Therefore, a highly autonomous reactor must be designed so that operating staff are apprised of any notifications that must be made in a timely manner.

The condition of any license under 10 CFR 50.54(z) requires that a licensee immediately notify the NRC Operations Center of the occurrence of any event specified in 10 CFR 50.72. This would include declaration of an emergency class as specified in the licensee's approved emergency plan. Required notifications also include the following:

- Any event or situation related to the health and safety of the public or onsite personnel or protection of the environment for which a news release is planned or notification to other government agencies has been or will be made
- The condition of the NPP, including its principal safety barriers, being seriously degraded
- The NPP being in an unanalyzed condition that significantly degrades plant safety
- Any event or condition that, at the time of discovery, could have prevented fulfillment of the safety function of structures or systems that are needed to accomplish the following:
    - Shut down the reactor and maintain it in a safe shutdown condition,
    - Remove residual heat,
    - Control the release of radioactive material, or
    - Mitigate the consequences of an accident.

Therefore, a highly autonomous reactor must be designed so that (1) notifications are made automatically as required, or (2) operating staff are apprised of notifications that must be made in a timely manner.

Highly autonomous reactors will likely be required to demonstrate a high degree of passive safety and a small source term. Such attributes will allow a minimal emergency plan, which could lead to reduced onsite staffing and will potentially allow a remotely located control room.

5. SIMULATORS [10 CFR 50.34, 10 CFR 55]

A full-scope simulator provides the capability to train plant operators in a replica control room that represents the control consoles, control panels, and displays in the plant control rooms. The plant's dynamic behavior and process control are simulated via a plant dynamic model executing in a multiprocessor plant model computer. In many cases, the operating system is a Windows-based operating system. The control room human–system interface (HSI) is stimulated, thereby maintaining high-fidelity operator interaction, whereas the control systems are translated to support plant dynamics on a single computer platform.

In the 1980s, full scope simulators became common and were capable of evaluating processes and plant responses in real-time simulation. The main circuits used fast running transient codes coupled with 3D emulation of the reactor core. All process pipelines, automation, instruments, and electrical systems were simulated with the level of accuracy needed for the creating signals and measurements for the operator interface. A family of program tools was developed for building the simulator software. In the 2000s,

nuclear plants had to face a new reality when manufacturers stopped producing analogue components. Simulators were now required to validate new I&C components rather than just being able to reliably predict process behavior. The new simulators could also factor in human errors that could inform tests and training.

Simulator upgrade required changing the simulated control room from analogue components to programmed components and wall panel and panel board concepts. In the new development, the full scope simulator may be a replica of the cathode-ray tube (CRT)-based control room, and the program modules of the automation may be used directly in the simulator software.

The simulators in use today may be divided roughly into four groups: (1) full-scope simulators, (2) basic principle simulators, (3) partial scope simulators, and (4) nuclear plant analyzers [60]. Full scope simulators include the user interface as a control room mock-up. The process behavior in the stationary, transient, and accident conditions is simulated in real time. A full scope simulator is not a tool for individual training, but for the whole operator team. The basic principle simulator may describe the main function of the plant, or only a subsystem (turbine, generator, feedwater system, core control). There are several variations of the partial scope simulators. The physical models may be the same as in the full scope simulators, except the user interface is compressed into one or more CRT, whereas the partial scope simulator is an individual training version of a full scope simulator. In the nuclear plant analyzer, accurate analysis (neutronics, thermohydraulics, automation, and electronics) is controlled with an advanced user interface. In the plant simulation, this means there are numerous process diagrams on different pages, different operator functions may be actuated, and process status is diagnosed by clicking a component mimic on the interface panel.

If DTs are used for training purposes or to conduct operating tests, then they would be acting as a simulator.

10 CFR 55 defines the term *simulation facility* in 10 CFR 55.4, “Definitions,” as meaning one or more of the following components, alone or in combination, used for either the partial conduct of operating tests for operators, senior operators, and license applicants, or to establish on-the-job training and experience prerequisites for operator license eligibility as (1) a plant-referenced simulator, (2) a Commission-approved simulator under 10 CFR 55.46(b), or (3) another simulation device, including part-task and limited scope simulation devices approved under 10 CFR 55.46(b). In particular, 10 CFR 55.46, “Simulation Facilities,” addresses the use of a simulation facility to administer the operating test and the use of plant-referenced simulators to meet experience requirements for applicants for operator and senior operator licenses. 10 CFR 55.59, “Requalification,” addresses, in part, the use of a simulation facility to perform required control manipulations and plant evolutions not performed at the plant for on-the-job training of licensed operator and senior operators. This appears to be the role of many of the proposed DTs.

RG 1.149 [61] helps ensure that simulation facilities used to meet the requirements of 10 CFR Part 55 are sufficient in both scope and fidelity for the regulatory purposes for which they are being used with respect to (1) operating tests, as described in 10 CFR 55.45(a), (2) licensed operator requalification training requirements, as described in 10 CFR 55.59, and (3) performance of control manipulations that affect reactivity to establish eligibility for an operator’s license, as described in 10 CFR 55.31(a)(5).

As noted in RG 1.190 for determining neutron fluence on pressure vessels [62], the simulator benchmarks provide accurate measurements *but typically do not provide an accurate representation of the actual plant configuration*. The operating reactor measurements, on the other hand, represent the actual as-built plant configuration, but they typically include substantial measurement uncertainties. The simulator

benchmarks, together with the operating reactor measurements, generally provide an acceptable measurement database. This is applicable to DTs that use virtual data rather than actual plant data.

Regulations and guidance that address the capability of a plant simulator are provided in the following:

- 10 CFR 50.34(f)(2)(i), which requires applicants to provide simulator capability that correctly models the control room and includes the capability to simulate small-break LOCAs
- 10 CFR 55.31, How to Apply [Applications]
- 10 CFR 55.45, Operating Tests
- 10 CFR 55.46, Simulation Facilities
  - The simulator is approved for use in accordance with 10 CFR 55.46(b) or 10 CFR 55.46(c)
  - A licensee commits to maintain the simulator to assure continued simulator fidelity in accordance with 10 CFR 55.46(d)
- RG 1.149, Nuclear Power Plant Simulation Facilities for Use In Operator Training, License Examinations, and Applicant Experience Requirements
  - RG 1.149 endorses ANSI/ANS-3.5-1998, "Nuclear Power Plant Simulators for Use in Operator Training and Examination"

In addition, NRC expects an applicant to describe how it ensures that the proposed simulator correctly models its control room [63].

The requalification program for plant operators must contain a commitment that each operator will perform or participate in a combination of reactivity-control manipulations based on the availability of plant equipment and systems. Those control manipulations and plant evolutions that are not performed on the actual plant may be performed on the plant-referenced simulator. This may be applicable to DTs; however, the results and fidelity of the DT must meet that of the simulator. The use of the TSs should be maximized during the simulator control manipulations [64]. Senior operator licensees are credited with these activities if they directly control manipulations as they are performed. This credit may not apply if the system is autonomous.

DTs can be used to perform operator reliability experiments such as those performed using simulators [65].

The use of a plant-referenced simulator for operator training and testing is addressed in 10 CFR 55.46. The simulator features a physical replica of a plant control room and interfaces via an I/O system with a plant simulation. The simulation executes models that replicate plant systems, functions, and the underlying physical phenomena that drive plant performance. Such models include electrical systems, analog and digital control systems, hydraulic systems, radiation detection systems, alarms, emergency response systems, thermo-hydraulic response, core physics, and various other models as required to present plant operators with an integrated operational environment identical to that of the physical plant modeled. The simulator must demonstrate expected plant response to operator input and to normal, transient, and accident conditions with a level of fidelity specified by federal regulations. Recently, NPPs have begun supplementing their plant-referenced simulators with entirely digital glass panel simulators (GPSs). A GPS uses the same simulation and models as the plant-referenced simulator but replaces the physical panels and I/O system with an entirely digital graphical interface. Although a GPS is currently not authorized for plant operator qualification training, it provides additional capability for general staff training and in some cases, evaluation of plant changes. Companies such as CORYS, GSE Systems, Inc., L3 MAPPS, and Western Services Corporation provide plant-referenced and GPSs to the nuclear industry.

6. ML AND AI [10 CFR 50.55a(h)(3), 10 CFR 50.46, 10 CFR 50 APPENDIX B, AND 10 CFR 50 APPENDIX K]

Artificial intelligence (AI) is an umbrella term referring to any computer algorithm that makes decisions intended to mimic or replace those made by a human. *Machine learning* (ML) is a subset of AI and is a collection of computer algorithms that learn to make decisions based on the observation of training data. However, *deep learning* (DL) relies less on human feature engineering to preprocess the data of interest. Therefore, ML and DL are classes of AI. ML and AI are often used interchangeably, because ML is the leading class of AI algorithms used today in many industries to perform or assist decision-making by relying on digital data that are difficult or inefficient for a human to process. Assisting decision making has been the focus within the nuclear industry, because risk-informed decision making is used throughout many operational and design challenges. Because AI algorithms should always be used in tandem with a human domain expert for the performance of safety critical tasks, the term *augmented intelligence* is more appropriate when describing AI and ML usage in nuclear applications. However, this term has not yet reached sufficient awareness to be commonplace. Nevertheless, it is critical for the industry and regulator to understand the human role in any AI and ML nuclear application.

AI and ML can have a varying degree of influence over the decision-making process. With higher order influence comes higher cost and complexity of the algorithms. For example, this relative value and complexity of using AI and ML to determine and assist in the design of additively manufactured components is shown in Figure 5. At low end is computer vision (CV), that can be used for anomaly detection. At the top, AI can be used to predict part properties (e.g., fracture toughness) based in-situ data, process parameter information, and part geometry. Finally, a prescriptive AI would autonomously modify a part design to improve the predicted performance.

Under the Transformational Challenge Reactor (TCR) program at ORNL [66], AI and ML are being used extensively to detect material defects, visualize them, and ultimately determine the material properties based on in-situ data alone.

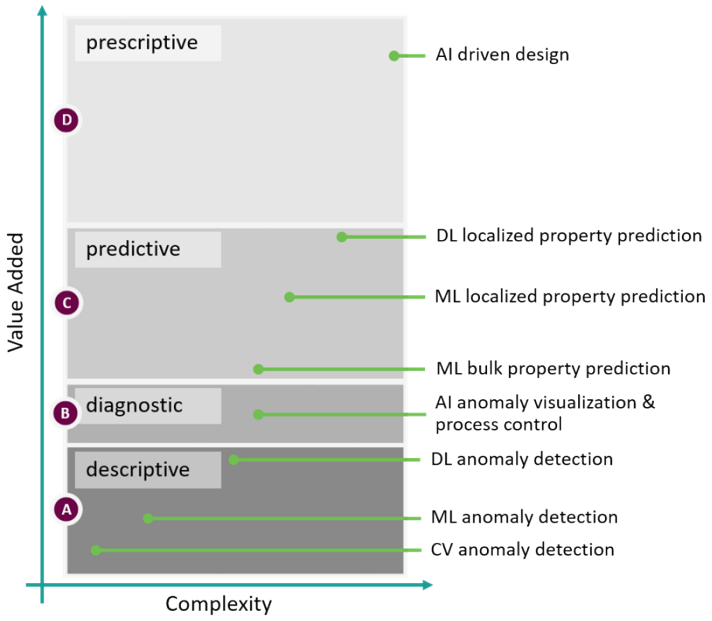


Figure 5. Relative value and complexity of different types of AI algorithms [66].

Many other examples of AI and ML are used within the nuclear industry for applications beyond DT. For example, ML is being used to predict DNBR, which is critical for LWR thermal hydraulic design [67]. ML is also being used to support nuclear data [68]. For more examples, see the comprehensive report INL prepared for the NRC, which consists of an industry survey and overview of AI and ML for nuclear applications [20].

AI and ML are often associated with DTs because the operational data are often used to detect and diagnose potential issues in the physical system through simulation and comparing against the digital system. Additionally, significant research is being performed to predict future physical system issues, also referred to as *predictive maintenance,* with AI and ML tools [69, 70, 71].

For any nuclear component, part, or system, QA and traceability are paramount. This has led to the concept of a *digital thread* [72]. Ideally, the digital thread contains all the information and operational data relevant for manufacturing, QA, safety analysis, potential design modification, maintenance planning, and other applications for all lifecycle stages (i.e., from design inception to decommissioning). This thread is then carried with the part/component/system between manufacturing stages, applications, and organizations. This opens a wealth of potential AI applications, because it can be assured that the DT is identical to the physical twin in all relevant areas.

A key aspect of digital threads is the common data models that act as a standard across a domain so that central datastores are consistent with the design and analysis models. Ultimately, digital thread success is based on both the success of the product lifecycle management and the model-based systems engineering implementations. In this sense, the digital thread serves as the instructions for creating the DT. Figure 6 illustrates the digital thread and the connected threads associated with analysis, data collection, inspection and maintenance, and decisions.

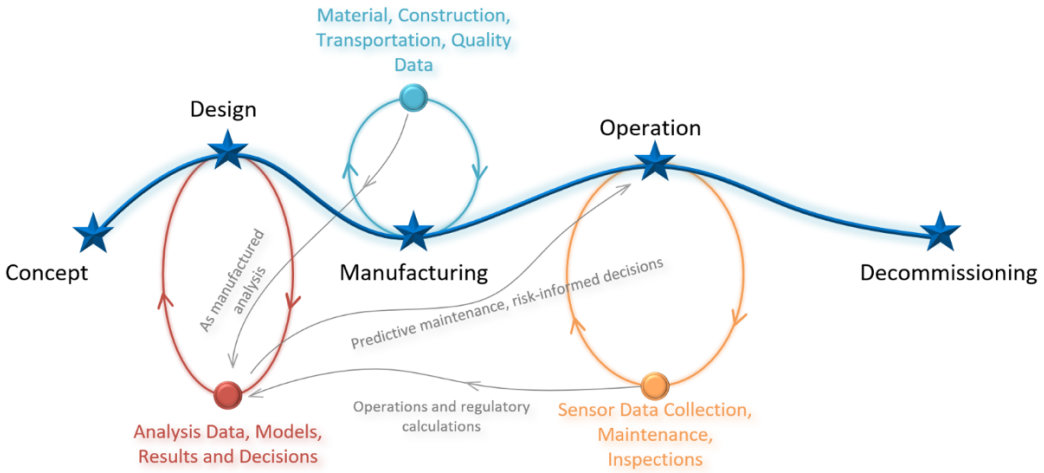


Figure 6. Digital thread life-cycle concept.

In terms of regulating AI and ML applications, the NRC is still mostly in an information collection phase, seeking input from stakeholders and holding workshops to better understand the technology and its potential nuclear applications [73, 74]. However, a report developed by INL and ORNL through an NRC contract [75] outlines the technical challenges and gaps in DT-enabling technologies for nuclear reactor applications. When considering AI/ML as applied to DT, the report summarizes three specific challenges related to licensing and regulatory activities:

1. Quality/optimum input data
2. Identification and selection of appropriate AI/ML algorithms

3. Explainability of the I/O relationships contained within the AI algorithms

Regarding the input data, one gap can occur when data in digital form are insufficient to employ ML and AI algorithms. The quality of the data is also paramount for nuclear safety applications. Poor data may lead to false output relationships or large uncertainties.

A wide array of different AI/ML algorithms are available to select. The specific application will reduce this array to a short list of suitable algorithms. At this point, the selection of the appropriate algorithm will depend on many factors, such as the desired performance, size, and complexity of the training data, scalability of the algorithm, and deployment and business case criteria (software implementation, legacy solutions, cost, etc.). Eliminating bias—or proving that this approach is systematic and fits the specific application—is a significant challenge.

Finally, explainability will be critical for regulatory and public acceptance. At every step, the process will require textual and graphical explanations. "Black-box" types of arguments may not adequately explain the underlying processes. The algorithm must generate an explanation in human natural language of (a) what it did, and (b) the rationale for what it did. Explaining the performance of the algorithm is equally important. From the output, the analyst or regulator should be able to clearly recognize if the model succeeds better than chance or if a human could achieve a better result.

Similar needs were identified in other ML research activities related to nuclear energy regulatory questions [76]. Sun et al. [76] examined the state of art in ML for nondestructive examination (NDE) applications in nuclear energy in-service inspection. Key needs identified in this review included data, algorithm selection, and validation. In this context, the term *data needs* refers to the need for relevant and representative reference data sets that may be used in developing and validating ML performance. The needs are not only for sufficient data, but also for quality data. The wide range of algorithms available requires a mechanism for identifying the appropriate technique and demonstrating that the selected algorithm is appropriate for the application. Validation of the data used, algorithm selection, and algorithm performance are essential to building the necessary level of confidence for regulatory and public acceptance. Similar studies [77] have led to the development of a methodology for qualifying AI/ML for nuclear energy use that provides guidance on best practices for addressing these various needs.

The list of potential AI and ML tools/frameworks is extensive and too long to list here. However, many popular tools and framework packages are being used by nuclear industry, some of which include:

1. TensorFlow [78]
2. PyTorch [79]
3. Google cloud AutoML [80]
4. MATLAB [81]
5. OpenNN [82]
6. Microsoft CNTK [83]

If the DT uses AI/ML in an instrument/control system that is a safety system, then 10 CFR 50, Appendix B; IEEE 1012 (endorsed by RG 1.168); 10 CFR 50.55a(h)(3) (i.e., IEEE 603-1991),and others, would apply.

If the DT has AI and ML that are to be used as a support analysis in a safety analysis/calculation, then the DT will be governed by 10 CFR 50.46 [57]; 10 CFR 50, Appendix K [58]; and some form of software V&V, most likely ASME NQA-1.

If the DT has AL and MI that are to be used as a support analysis in a safety analysis/calculation or for TSs, surveillance intervals, and so on, then the DT will be governed by 10 CFR 50.46; 10 CFR 50, Appendix K; and ASME NQA-1, and possibly some additional V&V.

7. CONCLUSIONS

The regulatory requirements for a DT will be directly dependent upon how it is to be used (i.e., its functionality).

- If the DT is to be used for a safety application, then it must meet the requirements of a safety-related I&C system. More specifically, the DT must meet 10 CFR 50, Appendix B; IEEE 1012 (endorsed by RG 1.168); IEEE 603, and so on.

- If the DT is to be used to support analysis of a safety analysis/calculation, then it would be governed by 10 CFR 50.46; 10 CFR 50, Appendix K; and some form of software V&V, most likely 10 CFR 50, Appendix B.

- If the DT is to be used for determining TSs, surveillance intervals, and so on, then 10 CFR 50.46; 10 CFR 50, Appendix K; and 10 CFR 50, Appendix B, and possibly some additional V&V will be the governing requirements.

- The development of a DT may be export-controlled information, and its development and operation should be performed within these constraints.

Regulations are based upon providing reasonable assurance of adequate protection and do not presume a particular technology. As described above, the current regulatory environment regarding the use of I&C and information technologies is based on a heritage of predominately isolated, independent, hardwired systems based on analog technology that provide protection, control and monitoring functions. Over the past four decades, the application of digital technologies and the integration of data and functionality has proceeded slowly for the nuclear power industry. For existing plants, implementation of digital technology has progressed through piecemeal upgrades of standalone systems. In response, NRC developed additional guidelines and endorsed acceptable practices to address the unique behavior characteristics of software-based digital systems. Meanwhile, the nuclear power industry has developed and begun construction of ALWRs incorporating more comprehensive use of digital technologies to provide highly reliable integrated command and (data) communications capabilities. Additionally, advanced reactors, SMRs, and microreactors have been and continue to be designed based on greater degrees of automation and optimal asset management (e.g., PMx) to optimize human resource usage and minimize O&M cost profiles. The use of DTs and potential application of AI/ML techniques follow from this trend.

As noted, the current regulatory framework for nuclear energy in the United States is focused on the use of defense-in-depth measures to provide a reasonable assurance of safety. Generally, such measures include architectures based on redundant and/or diverse systems, quality assurance programs and documented evidence (qualification reports, V&V findings), and periodic inspection and testing of safety significant components, with preventive maintenance performed on a time-based schedule to ensure component operability.

With the slow transition to digital I&C technologies for existing plants, the NRC has adapted its review processes and supplemented its regulations and guidelines to account for the evolution of plant I&C systems, operational techniques, and maintenance approaches. The deployment of DT technology may

require additional considerations and requirements such as specific documentary evidence of performance, particular forms of technical data, and so on, prior to acceptance in modes that are part of or could impact safety-significant systems and components. The information on regulations and review processes captured with this report establish the regulatory framework within which DTs will be evaluated for approval.

Of the various prospective ***uses for DTs*** identified in this report, the primary focus of the current research involves support ***for design, operations, and maintenance***. Regarding design support, there is current experience using engineering simulators as the basis for design and testing of control systems and full-scope simulators to validate operational procedures and constraints. If the DT use fits one of these categories, then the level of review would be similar to that covered in regulatory treatment of control system or review of operational procedures. Key evidence would involve documentation of the quality and fidelity of the tool (DT) used for the designated purpose (control algorithm development, operational procedure determination, or validation of similar outcomes). The use of DTs to support design iterations for a plant or system could involve regulatory review of the design products if used in a safety-related application except for failures of a nonsafety-related DT affecting the operation of a safety system. It is also noted that if the DT is used during design to provide insights into TS limits, it could be subject to review to show compliance with 10 CFR 50.36, *Technical Specifications*.

Regarding the ***use of DTs for operations support***, the safety classification of the functions provided or supported by the DT and the nature of its role in operations would be key factors in determining the regulations that apply, as well as the scope and rigor of a regulatory review. Safety (e.g., RTS, ESFAS) and safety-related (control systems, communications systems) designations would lead to assessment against the applicable regulations to the degree associated with the safety significance of the functions performed. As noted, regulatory reviews are not as onerous for control systems as for protection systems. It is anticipated that DTs will not be implemented as an integral part of any independent line of defense within a plant's I&C architecture (i.e., no protection functions will rely upon or be incorporated into a DT). Thus, it is likely that classification of DTs employed for operations support may range safety to safety significant, non-safety related, to nonsafety. Nevertheless, even a system that does not involve a safety or safety-related function must be evaluated to show that its failure would not compromise a safety function.

The regulatory treatment of DTs will depend not only on whether they are to be used to support safety systems, but it will also depend on the embedded functionality. In this report, the functional roles for DTs are grouped into categories that are generally consistent with NRC characterizations of levels of automation. The main categories are identified as (1) non-control functionality (advisory), (2) control functionality (shared), and (3) communications functionality (generally advisory).

- Regarding the noncontrol functionality category, the role of the DT would be to provide information or advice to the operator but not to directly affect the plant or its operation. The main issues involve quality, correctness, and fidelity of the information provided to the operator (i.e., related to the trustworthiness of the information), and the potential risk to plant safety arising from deployment and reliance on these techniques. Thus, review might address whether proper performance, determination of uncertainty, and transparency of the basis for the information have been demonstrated. Consequently, the depth of the review would depend on the impact of erroneous or uncertain performance on safety and human reliability.

- Regarding the control functionality, the consideration is the degree to which responsibility for actions is shared between the operator and DT. This could range from the boundaries of manual control with the DT advising of expected responses to potential control actions to autonomous control utilizing an embedded DT for predictive control and/or automatic adaptation. The extreme

end of autonomy is not anticipated as a near-term application of DTs or AI/ML. The range of control functionality introduced into a DT would lead to more rigorous regulatory review and a greater level of evidence on the safety impact of the system. Plants with high degrees of passive safety would seem to be good candidates for implementing AI.

- Regarding the communications functionality, the level of regulatory review would depend on the safety significance of the data being transmitted. If vital communication of safety-related data is involved, then the communications functionality provided by the DT would necessarily be subject to safety or safety-related review. This would include independence, isolation, reliability, fault-tolerance/accommodation, and so forth. If the communications functionality is solely advisory or non-vital, then the review would be similar to that of other non-control functionality.

Another characteristic to consider in anticipating the regulatory considerations for use of a DT involves complexity, which directly relates to the capability to predict its behavior under normal and faulted conditions and to its vulnerability to change by accident or incursion. The significance of these characteristics is tied to the functionality implemented in the DT and its potential impact on safety.

As noted in the report, a risk-informed / graded approach based on the functionality of the DT would evaluate the complexity of the DT with its function to set the level of review sufficient to reach a safety conclusion. Simple monitoring, the lowest complexity level, minimal consequences of failure, and other such aspects would not require guidance on software tools or type of digital device. At the other end of the graded approach, existing guidance will apply to control those DTs that perform a control function, while more scrutiny would result for components that perform safety functions. Thus, an understanding of the DT's functionality can be applied to facilitate a graded approach to qualification, testing, and inspections.

To summarize, the current regulatory framework does not explicitly address DTs, autonomous control, or AI/ML. Assessment of regulations and current practices leads to the conclusion that regulatory requirements for a DT will be very dependent upon how it is used (i.e., its functionality). In many anticipated cases, the DT may receive limited regulatory attention. However, as the safety classification, operational functionality, or importance of the DT's information or performance increase in significance, the regulatory burden associated with a safety justification will grow. The capability to classify the DT by safety significance, functionality, complexity and other characteristics can provide the basis for a graded approach to implementing or licensing such technologies.

Gaps in uses and regulatory requirements will be addressed in the next phase of this task under Milestone 5.2

8. REFERENCES

1. J. Carlson et al., *Proceedings of the Workshop Enabling Technologies for Digital Twin Applications for Advanced Reactors and Plant Modernization*, Virtual Workshop, September 14–16, 2021, RIL 2021-16 (ADAMS Accession No ML21348A020).
2. V. Yadav et al., "The State of Technology of Application of Digital Twins," TLR/RES-DE-REB-2021-01, June 2021.
3. V. Yadav et al., *Proceedings of the Workshop on Digital Twin Applications for Advanced Nuclear Technologies*, Virtual Workshop, December 1–4, 2020, RIL 2021-02, March 2021 (ADAMS Accession no. ML21083A132).
4. VanDerHorn, Eric, and Sankaran Mahadevan. "Digital Twin: Generalization, characterization and implementation." Decision Support Systems (2021): 113524.

5. Paolo Pileggi, Armir Bujari, Oliver Barrowclough, Jochen Haenisch, and Robert Woitsch, "Overcoming 9 Digital Twin barriers for manufacturing SMEs," Change2Twin, April 2021. https://www.change2twin.eu/wp-content/uploads/2021/04/Change2Twin_Position-Paper_Overcoming-9-Digital-Twin-Barriers-for-manufacturing-SMEs-.pdf [accessed Aug. 5, 2022]
6. Dave Kropaczek, "Advanced Modeling and Simulation and its Future Role in Nuclear Systems," *Proceedings of the Workshop on Digital Twin Applications for Advanced Nuclear Technologies*, Virtual Workshop, December 1–4, 2020, RIL 2021-02, March 2021 (ADAMS Accession no. ML21083A132).
7. T. Braudt and S. Vaughn, X-energy, "Xe-100 Licensing Perspectives: Steps Toward Realization of Digital Twins," *Proceedings of the Workshop Enabling Technologies for Digital Twin Applications for Advanced Reactors and Plant Modernization*, Virtual Workshop, September 14–16, 2021, RIL 2021-16 (ADAMS Accession No ML21348A020).
8. A. Chillers, "Digital Twin Development for Advanced Reactors: Accelerating Time to Market, Increasing Safety Margins, Maximizing Value," Kairos Power, RIL 2021-02, *Proceedings of the Workshop on Digital Twin Applications for Advanced Nuclear Technologies, Virtual Workshop*, December 1, 2020 (ADAMS Accession No. ML21083A132).
9. P. Keutelian, Radiant, "Using Digital Twins to Support Regulations," *Proceedings of the Workshop Enabling Technologies for Digital Twin Applications for Advanced Reactors and Plant Modernization*, Virtual Workshop September 14–16, 2021, RIL 2021-16 (ADAMS Accession No ML21348A020).
10. M. Rowland and S. Guerra, Working Group # 3 Report to the Technical Meeting Participants, "Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors," February 25, 2022.
11. 10 CFR 50.2, "Definitions."
12. 10 CFR 50.69, "Risk-Informed Categorization and Treatment of structures, Systems and Components for Nuclear Power Reactors."
13. NUREG-0800, Rev. 6, *Standard Review Plan*, Chapter 7.7, "Control Systems" (August 2016) (ADAMS Accession no. ML16020A095).
14. SRP App. 7.1-D, Rev. 1, *Guidance for Evaluation of the Application of IEEE Std 7-4.3.2*, Clause 5.3.1, "Software Development (IEEE Std 7-4.3.2, Sub-Clause 5.3.1)," August 2016 (ADAMS Accession no. ML16019A114).
15. SRP App. 7.0-A, Rev. 6, *Review Process for Digital Instrumentation and Control Systems*, Fig. 7.0-A-3, "Overview of the process for reviewing digital instrumentation and control," August 2016 (ADAMS Accession no. ML16019A085).
16. SRP App. 7.0-A, Rev. 6, *Review Process for Digital Instrumentation and Control Systems*, C.2, "Review Process for Software in Digital Instrumentation and Control System," August 2016 (ADAMS Accession no. ML16019A085).
17. "Employees May Be a Company's Biggest Cybersecurity Risk: The Threat of Social Engineering," November 16, 2014. *http://blog.trendmicro.com/employees-may-companys-biggest-cybersecurity-risk-threat-social-engineering/* [Accessed: Nov. 12, 2019]
18. SRP BTP 7-17, Rev. 6, *Guidance on Self-Test and Surveillance Test Provisions*, August 2016 (ADAMS Accession no. ML16019A316).
19. 10 CFR 50.65, *Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants*.
20. Z. Ma, H. Bao, S. Zhang, M. Xian, and A. Mack, "Exploring Advanced Computational Tools and Techniques with Artificial Intelligence and Machine Learning in Operating Nuclear Plants," NUREG/CR-7294, February 2022 (ADAMS Accession No. ML22042A662).
21. B. M. Golchert and G. A. Banyay, "Synopsis of Westinghouse Machine Learning, Artificial Intelligence, and Digital Twin Developments for Nuclear Power Applications," for the Workshop on Digital Twin Applications for Advanced Nuclear Technologies, December 2020 (ADAMS Accession No. ML20314A108).

22. Westinghouse Nuclear Services / Engineering Services, "Modular Accident Analysis Program," NS-ES-0216, September 2011, https://www.westinghousenuclear.com/Portals/0/operating%20plant%20services/engineering/safety%20analysis/NS-ES-0216%20MAAP5_PWR_BWR.pdf [Accessed: Jun. 10, 2020].
23. R. J. Buechel, W. A. Boyd, and A. L. Casadei, "The Westinghouse BEACON On-Line Core Monitoring System." *Proceedings of the 10 Meeting on Reactor Physics and Thermal Hydraulics*, p. 563. Brazil, 1995.
24. P. Ramuhalli et al., PNNL-24377R0, "Component-Level Prognostics Health Management Framework for Passive Components Advanced Reactor Technology Milestone," M2AT-15PN2301043, June 2015.
25. P. Ramuhalli, C. Walker, V. Agarwal, N. Lybeck, *Development of Prognostic Models Using Plant Asset Data*, ORNL, ORNL/TM-2020/1697, 2020.
26. NUREG-0800, Chapter 18.0, Rev. 3, "Human Factors Engineering," December 2016 (ADAMS Accession No. ML16125A114).
27. J. M. O'Hara and S. Fleger, *Human-System Interface Design Review Guidelines*, NUREG-0700, Rev. 3, July 2020 (ADAMS Accession no. ML20162A214).
28. J. M. O'Hara, J. C. Higgins, S. A. Fleger, and P. A. Pieringer, *Human Factors Engineering Program Review Model*, NUREG-0711, Rev. 3, November 2012 (ADAMS Accession No. ML12324A013).
29. J. M. O'Hara and J. C. Higgins, *Human-System Interfaces to Automatic Systems: Review Guidance and Technical Basis*," BNL-91017-2010, January 31, 2010.
30. 10 CFR Part 50, *Domestic Licensing of Production and Utilization Facilities*, Appendix A, "General Design Criteria for Nuclear Power Plants," Criterion 1, "Quality Standards and Records" (Jan. 1, 2021 edition).
31. 10 CFR Part 50, *Domestic Licensing of Production and Utilization Facilities*, Appendix A, "General Design Criteria for Nuclear Power Plants," Criterion 13, "Instrumentation and Control" (Jan. 1, 2021 edition).
32. 10 CFR Part 50.55a(a)(1) (Jan. 1, 2021 edition).
33. EPRI TR-1001503, *Identification and Description of Instrumentation, Control, Safety, and Information Systems and Components Implemented in NPPs*, Electric Power Research Institute, Palo Alto, CA, June 2001.
34. NASA-GB-8719.13, "NASA Software Safety Guidebook," National Aeronautics and Space Administration, March 31, 2004.
35. NASA-GB-1740.13, "NASA Software Safety Guidebook."
36. Branch Technical Position 7-19, Rev. 7, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems Review Responsibilities," August 2016.
37. RIS 2016-05, *Embedded Digital Devices In Safety-Related Systems*, April 29, 2016 (ADAMS Accession No. ML15118A015).
38. H. Hecht et al., *Review Guidelines on Software Languages for Use in NPP Safety Systems*, NUREG/CR-6463, June 1996 (ADAMS Accession No. ML063470583).
39. NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, December 1994.
40. NUREG/CR-7007, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, February 2010.
41. IEEE, Std. 1012-2012, *IEEE Standard for Software Verification and Validation*, Piscataway, NJ, 25 May 2012.
42. RG 1.168, Rev. 2, *Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*," July 2013 (ADAMS Accession no. ML13073A210).
43. IEEE, Std. 1012-2004, *IEEE Standard for Software Verification and Validation*, Piscataway, NJ, 2004.
44. IEEE, Std. 1028-2008, *IEEE Standard for Software Reviews and Audits*, Piscataway, NJ, 2008.

45. R. T. Wood et al., "An Autonomous Framework for Advanced Reactors," *Nucl. Eng. Technol.*, Volume 49, July 2017, pp. 896–904.
46. H. Basher and J. S. Neal, *Autonomous Control of Nuclear Power Plants*, ORNL/TM-2003/252, ORNL, October 2003.
47. M. Vagia, A. A. Transeth, and S. A. Fjerdingen, "A Literature Review on the Levels of Automation during the Years. What Are the Different Taxonomies That Have Been Proposed?" *Appl. Ergon.* 53 (2016) 190e202.
48. T. Sheridan, *Humans and Automation: System Design and Research Issues*, New York: Wiley & Sons, 2002.
49. T. Sheridan, *Telerobotics, Automation, and Human Supervisory Control*, The MIT Press, Cambridge, Massachusetts (1992).
50. C. Kovesdi et al., *Development of an Advanced Integrated Operations Concept for Hybrid Control Rooms*, INL/EXT-20-57862, Revision 0, March 2020.
51. NUREG-0800, Appendix 18-A, Rev. 0, *Crediting Manual Operator Actions In Diversity And Defense-In-Depth Analyses*, April 2014 (ADAMS Accession No. ML13115A156).
52. 10 CFR 50.54, *Conditions of Licenses.*
53. R. J. Belles and M. D. Muhlheim, *Licensing Challenges Associated with Autonomous Control,* ORNL/SPR-2018/1071, December 2018.
54. NUREG-0654/FEMA-REP-1, Rev. 2, *Criteria for in Support of Nuclear Power Plants Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness, Final Report*, December 2019.
55. NUREG-1791, *Guidance for Assessing Exemption Requests from the Nuclear Power Plant Licensed Operator Staffing Requirements Specified in 10 CFR 50.54(m)*, July 2005 (ADAMS Accession No. ML052080125).
56. F. Akstulewicz, *NuScale Control Room Configuration and Staffing Levels, NRC letter to NuScale Power*, January 14, 2016 (ADAMS Accession No. ML15302A516).
57. 10 CFR 50.46, *50.46 Acceptance Criteria for Emergency Core Cooling Systems for Light-Water Nuclear Power Reactors*, March 24, 2021.
58. 10 CFR 50, Appendix K, "ECCS Evaluation Models," March 24, 2021.
59. RG 1.177, Rev. 2, *An Approach for Plant-Specific, Risk-Informed Decisionmaking [sic]: Technical Specifications*, January 2021 (ADAMS Accession No. ML20164A034).
60. J. Miettinen, "Nuclear Power Plant Simulators: Goals and Evolution," THICKET 2008 – Session III – Paper 07. https://www.osti.gov/etdeweb/servlets/purl/21510319 [Accessed: Jun. 10, 2020].
61. RG 1.149, Rev. 4, *Nuclear Power Plant Simulation Facilities for Use in Operator Training, License Examinations, and Applicant Experience Requirements*, April 2011 (ADAMS Accession no. ML110420119).
62. RG 1.190, *Calculational and Dosimetry Methods for Determining Pressure Vessel Neutron Fluence*," March 2021 (ADAMS Accession no. ML010890301).
63. RG 1.206, Rev. 0, *Part I: Standard Format and Content of Combined License Applications*, C.1.13.2.1.1.1 Licensed Plant Staff Training Program, June 2007 (ADAMS Accession No. ML070630017).
64. NUREG-0800, 13.2.1, Rev. 4, *Reactor Operator Requalification Program; Reactor Operator Training*, August 2015 (ADAMS Accession No. ML15006A035).
65. EPRI. *Operator Reliability Experiments Using Power Plant Simulators*. EPRI NP-6937 Volumes 1-3. EPRI: Palo Alto, CA. July 1990 (proprietary document - contact EPRI for availability).
66. A. Huning et al., *Digital Platform-Informed Certification of Components Derived from Advanced Manufacturing Technologies*," ORNL, ORNL/TM-2021/2210 (September 2021).
67. U. Rohatgi, *Machine Learning-based Prediction of Departure from Nuclear Boiling Power for the PSBT Benchmark*, Brookhaven National Laboratory, BNL-222878-2022-COPA (June 2022).
68. P. A. Grechanuk, M. E. Rising, and T. S. Palmer, "Application of Machine Learning Algorithms to Identify Problematic Nuclear Data," *Nucl. Sci. Eng.*, 195, pp. 1265–1278 (2021).

69. A. K. Sleiti, J. S. Kapat, and L. Vesely, "Digital Twin in Energy Industry: Proposed Robust Digital Twin for Power Plant and Other Complex Capital-Intensive Large Engineering Systems," *Energy Rep.* 8, pp. 3704–3726 (2022). https://doi.org/10.1016/j.egyr.2022.02.305 [Accessed: Jun. 10, 2020].
70. Y. You, C. Chen, F. Hu, Y. Liu, and Z. Ji, "Advances of Digital Twins for Predictive Maintenance," *Procedia Comput. Sci.* 200, pp. 1471–1480 (2022). https://doi.org/10.1016/j.procs.2022.01.348 [Accessed: Jun. 10, 2020].
71. J. Browning, A. Slaughter, R. Kunz, J. Hansel, B. Rolston, K. Wilsdon, A. Pluth, and D. McCardell, "Foundations for a Fission Battery Digital Twin," *Nucl. Technol.* (2022). https://doi.org/10.1080/00295450.2021.2011574 [Accessed: Jun. 10, 2020].
72. L. Scime, A. Singh, and V. Paquit, "A Scalable Digital Platform for the Use of Digital Twins in Additive Manufacturing," *MFGLET* 31, pp. 28–32 (2022). https://doi.org/10.1016/j.mfglet.2021.05.007 [Accessed: Jun. 10, 2020].
73. NRC, "Virtual Workshop on Digital Twin Applications for Advanced Nuclear Technologies," Virtual Workshop, December 1–4, 2020, Adams Accession No. ML20314A108, (December 2020).
74. NRC, "Enabling Technologies for Digital Twin Applications for Advanced Reactors and Plant Modernization," Virtual Workshop, September 14–16, 2021, Adams Accession No. ML21228A082 (September 2021).
75. V. Yadav et al., *Technical Challenges and Gaps in Digital-Twin-Enabling Technologies for Nuclear Reactor Applications,* INL, ORNL, and NRC, TLR/RES-DE-REB-2021-17 (December 2021).
76. H. Sun, P. Ramuhalli and R. Jacob, "Machine Learning for NDE Literature Review," Submitted to *Ultrasonics*, 2022.
77. ENIQ Recommended Practice 13, *Qualification of Non-destructive Testing Systems that Make Use of Machine Learning*, Issue 1, ENIQ Report 65, European Network for Inspection Qualification (ENIQ), June 2021. Available at https://snetp.eu/wp-content/uploads/2021/06/ENIQ_RP13_Issue1.pdf . [Accessed: Jun. 10, 2020].
78. TensorFlow, "An End-to-End Open Source Machine Learning Platform," https://www.tensorflow.org/ [Accessed: Jun. 10, 2020].
79. PyTorch, "From Research to Production," https://pytorch.org/ [Accessed: Jun. 10, 2020].
80. AutoML, https://cloud.google.com/automl [Accessed: Jun. 10, 2020].
81. MathWorks, MATLAB, https://www.mathworks.com/ [Accessed: Jun. 10, 2020].
82. OpenNN neural networks, https://www.opennn.net/ [Accessed: Jun. 10, 2020].
83. Microsoft, "The Microsoft Cognitive Toolkit," https://docs.microsoft.com/en-us/cognitive-toolkit/ [Accessed: Jun. 10, 2020].