RPT-24-78848
Revision 0

Framework for a Digital Documented Safety Analysis

June 2024

M2RC-24IN020404—Develop a roadmap/architecture for leveraging digital tools in performing systems engineering approaches in support of a digital (DOE) authorization

Matthew Lund, Kevin O'Rear, Jacob Rymer, Kevin Terrill, and Peter Suyderhoud
Idaho National Laboratory

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

NRIC National Reactor Innovation Center

DISCLAIMER

REVISION LOG

Revision No.	Date	Affected Pages	Description
0	06/20/2024	All	Initial Revision.

SUMMARY

This framework presents a system and structure with a phased approach to develop a digital documented safety analysis (DSA) for future reactor development, using digital engineering tools instead of a traditional documented safety analysis. The engineering design and licensing process for nuclear reactors is currently burdened by a document-based approach that leads to duplications and errors due to a lack of traceability among numerous static documents. Changes to design information require labor-intensive manual tracing through these documents, creating a high potential for human error. The adoption of a digital ecosystem, utilizing a digital thread to link various aspects of project design and analysis, promises dynamic documentation generation, automatic updates, and error reduction. Model based definition (MBD) and product lifecycle management (PLM) tools are central to this digital transformation. They enable a single source of truth for design information, reduce the need for manual data entry, and allow for automated updates across different software platforms, thus expediting the delivery of safety documentation and reducing rework costs.

A digital DSA would use a data-driven approach, including the use of advanced software for requirements engineering, model-based systems engineering (MBSE), workflows, pipelines, and dynamic analytical models. In a phased approach, leveraging artificial intelligence (AI) and automation can further enhance document processing and generation, leading to more efficient and accurate development of safety documentation. The framework also describes how workflows, pipelines, and automation improve the systematic analysis of hazards and hazard control selection, and the evaluation of normal, abnormal, and accident conditions, to reduce project cost and timelines. In later phases, the information generated through these tools would then dynamically generate a digital DSA that is dynamically accessible through a graphical user interface (GUI). The framework concludes with changes to Department of Energy (DOE) requirements to accept digital documentation, improve cybersecurity standards, and provide proper training and understanding of the digital ecosystem to fully capitalize on the benefits of digital engineering tools to reduce timelines, regulatory burden, and cost.

ACKNOWLEDGMENTS

This document was sponsored by the National Reactor Innovation Center (NRIC). NRIC is a national program funded by U.S. Department of Energy's Office of Nuclear Energy and is dedicated to the demonstration and deployment of advanced nuclear energy.

CONTENTS

FIGURES

ACRONYMS

AEC	Atomic Energy Commission
AI	Artificial Intelligence
API	Application Programming Interface
BIM	Building Information Model
CAD	Computer-Aided Design
CFR	Code of Federal Regulations
CMP	Configuration Management Plan
CSDR	Conceptual Safety Design Report
CSP	Cloud Service Providers
DBA	Design Basis Accidents
DID	Defense in Depth
DOE	U.S. Department of Energy
DOORS	Dynamic Object-Oriented Requirements System
DSA	Documented Safety Analysis
EG	Evaluation Guideline
EPC	engineering, procurement, and construction
FedRAMP	Federal Risk Authorization Management Program
FEA	Finite Element Analysis
FMEA	Failure Modes and Effects Analysis
GUI	Graphical User Interface
INL	Idaho National Laboratory
MBD	Model Based Definition
MBSE	Model Based Systems Engineering
MEL	Master Equipment List
ML	Machine Learning
NEI	Nuclear Energy Institute
NLP	Natural Language Processing
NQA	American Society of Mechanical Engineers Nuclear Quality Assurance
NRC	Nuclear Regulatory Commission
NRIC	National Reactor Innovation Center
PDC	Principal Design Criteria
PDSA	Preliminary Documented Safety Analysis

PLM	Product Lifecycle Management
PRA	Probabilistic Risk Assessment
PSDR	Preliminary Safety Design Report
QA	Quality Assurance
RG	Regulatory Guide
RMP	Requirements Management Plan
RSF	Required Safety Functions
SAR	Safety Analysis Report
SDS	Safety Design Strategy
SEMP	Systems Engineering Management Plan
SOT	Single-Source of Truth
SSC	Structures, Systems, and Components
USQ	Unreviewed Safety Question
V&V	Verification and Validation

Framework for a Digital Documented Safety Analysis

1. INTRODUCTION

The traditional processes for reactor safety analyses to develop a Documented Safety Analysis (DSA) for the United States Department of Energy (DOE) authorization or safety analysis report (SAR) for the Nuclear Regulatory Commission (NRC) licensure occur through iterative design cycles. Design criteria or information are generated by separate groups often working in discipline specific silos. Each group generates analyses and documentation that are then distributed from group to group. The safety analyst documenting the DSA spends significant time each cycle documenting each set of changes and verifying that requirements, assumptions, and conclusions are cohesive and coherent between the design, analyses, and documentation to demonstrate the plant's safety. This workflow results in a serial path with multiple sources of information that require validation across groups. This slows down the design process, causing the safety analysis to be the last design work completed due to waiting for the delivery of design deliverables. Waiting for the design finalization and DSA development often results in project delays that significantly impact timeline and cost.

After submitting a DSA, or any of the preceding development analyses or submittals, regulatory review incurs significant cost and time delays for new reactors, representing a substantial portion of the total cost and time for new nuclear projects. INL/RPT-23-72206, “Recommendation to Improve the Nuclear Regulatory Commission Reactor Licensing and Approval Process,”[1] describes reforms that could decrease review time, and also denotes the staggering volume of information reviewed by regulators for a license. For example, the NRC’s review of NuScale, which completed the first NRC review of an advanced reactor application, took 41 months after the application was docketed. The NRC spent over a quarter-million hours, reviewing and auditing roughly two million pages of documentation and about 100 gigabytes of test data. These figures illustrate the extensive resource and time commitment required to review a safety analysis for a reactor, contributing to the high cost of developing new nuclear reactors.

This document outlines a new framework and phased approach for automating the development of nuclear safety basis documents. Digital engineering and artificial intelligence tools would improve the design process through parallel work, integrating safety into design, and providing faster access to information. These living digital safety bases would replace the traditional documents historically generated by creating real-time snapshots of the design at the current time sourced from the digital single-sources of truth (SOT). This document also introduces a methodology where digital SOTs could eventually replace legacy document formats, increasing developer and regulator reliance on native and rich data sets.

This new process would dramatically reduce development costs by reducing DSA authoring and regulatory review time through automation and increased review efficiency. The adoption of digital engineering and digital twin technologies have shown the ability to reduce the probability of project schedule delays by ~20% [Ritter, 2023]. General Electric has achieved $1.05B in customer, production, and mechanical losses avoided through the use of digital engineering technologies [GE]. Huntington Ingalls Industries, America's largest military shipbuilding company, has claimed to save about $150 million through the use of digital engineering in the construction of the USS Gerald R. Ford aircraft carrier. These reports highlight the immense potential digital engineering has in reducing costs associated with legacy project activities.

1.1 Background

The DSA documents the extent to which a nuclear reactor may be operated safely with respect to workers, the public, and the environment. It includes a description of the conditions, boundaries, and hazard controls that ensure safety.[2] In DOE regulations, the DSA itself is documentation of the process through which safety is integrated into the design that serves as the safety basis for DOE facilities. The NRC uses the term SAR for the documented safety basis for licensing commercial nuclear facilities, so DOE laboratories often use the terms DSAs and SARs interchangeably.

The origins of the SAR can be traced back to the Atomic Energy Commission (AEC), the federal agency responsible for the development and regulation of nuclear energy in the United States from 1946 to 1983. In the early days of nuclear power, the AEC recognized the importance of safety in nuclear power plant design and operations. The AEC issued its first regulations for reactor safety in 1954, which required applicants to submit detailed safety analyses as part of the licensing process. These safety analyses were used by the AEC to evaluate the design and safety features of proposed nuclear power plants.

The early safety analyses were relatively simple and focused primarily on the reactor core design and coolant system. However, as the complexity of nuclear power plant designs increased, the need for more detailed and comprehensive safety analyses grew. In the 1960s, the AEC issued the "Standard Review Plan for Nuclear Power Plants," which outlined detailed safety analysis requirements. This plan required applicants to identify and evaluate potential accidents and their consequences and to demonstrate that safety systems and procedures were adequate to mitigate those consequences.

In 1983, the AEC was split into the DOE and the NRC, which assumed regulatory responsibility for nuclear safety. Both regulators still use very similar guidance and requirements for DSAs and SARs, but with slightly different terminology in issuing more stringent regulations ensuring the safety of nuclear applications. Due to the complexity of the regulatory requirements and design, the safety analysis process often becomes a significant impediment to licensing, making it a major cost driver for new nuclear reactor deployment.

The safety analysis process, as documented in the DSA, is a collaborative effort involving several groups, including the engineering design team, nuclear safety analysts, and operational staff. In DOE, this licensing process is called DOE authorization, and it is governed by 10 Code of Federal Regulations (CFR) 830. The NRC uses different terminology, with a licensee undergoing their process to receive a construction and operating license will do so under 10 CFR 50, 10 CFR 52, or 10 CFR 53 guidance. DOE and NRC use the DSA and SAR to evaluate the safety of the proposed nuclear facility design and to ensure that the plant will meet the regulatory requirements. During the process, regulators may request additional information or modifications to the DSA to address any safety concerns.

For DOE, 10 CFR 830.204 clearly describes the required content of the DSA stating the DSA shall: **Error! Bookmark not defined.**

(1) Describe the facility (including the design of safety structures, systems and components) and the work to be performed;

(2) Provide a systematic identification of both natural and man-made hazards associated with the facility;

(3) Evaluate normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents which may be beyond the design basis of the facility;

(4) Derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment, demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards, and define the process for maintaining the hazard controls current at all times and controlling their use;

(5) Define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including (where applicable) quality assurance, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection;

The NRC's SAR content follows standard guidance evolved from the AEC as described in NRC Regulatory Guide (RG) 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants."[3] For non-power reactors, a simplified format was released by the NRC in NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,"[4] due to the relative simplicity of non-power reactors. Both formats and their content are deterministic, with prescriptive content and requirements for traditional light water reactors. The deterministic approach often poorly matches the designs of advanced nuclear reactors.

DOE nuclear reactors historically have used either RG 1.70 or NUREG-1537 for content and format; however, newer DOE reactors have successfully applied a systematic approach that is technology-neutral, as described in DOE-STD-3009, "Preparation of Nonreactor Nuclear Facility Documented Safety Analysis."[5] This adaptive approach has allowed some flexibility for advanced reactor designs.

Recent efforts by the industry, DOE, and NRC have resulted in a new approach to licensing that follows a risk-informed, performance-based methodology described in the Nuclear Energy Institute (NEI) 18-04, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development,"[6] and NEI 21-07, "Technology Inclusive Guidance for Non-Light Water Reactors."[7] Figure 1 shows the process for developing the DSA following NEI 18-04 guidance. In this process, the analyst uses a Probabilistic Risk Assessment (PRA) to analyze the design for safety.

The risk-informed process starts with a qualitative hazard identification and evaluation combined with design development to inform a PRA and select Design Basis Accidents (DBAs). From preliminary PRA results, an analyst chooses required safety functions and Principal Design Criteria (PDCs) that inform the selection of safety structures, systems, and components (SSCs). These SSCs are evaluated against the DBAs through accident analysis to determine doses to the public, workers, and the environment. The analyst then compares the dose consequences from each accident against Evaluation Guidelines (EGs), which are the dose

regulatory limits. An analyst then evaluates Defense in Depth (DID), updating the selection of safety SSCs and special treatments until reaching a solution that meets regulatory requirements.

DID is a strategy used to meet regulatory requirements. It uses multiple layers of redundant and diverse safety systems and administrative controls to protect against potential accidents to mitigate the failure consequences, and to ensure that no single layer's failure leads to a hazardous situation.

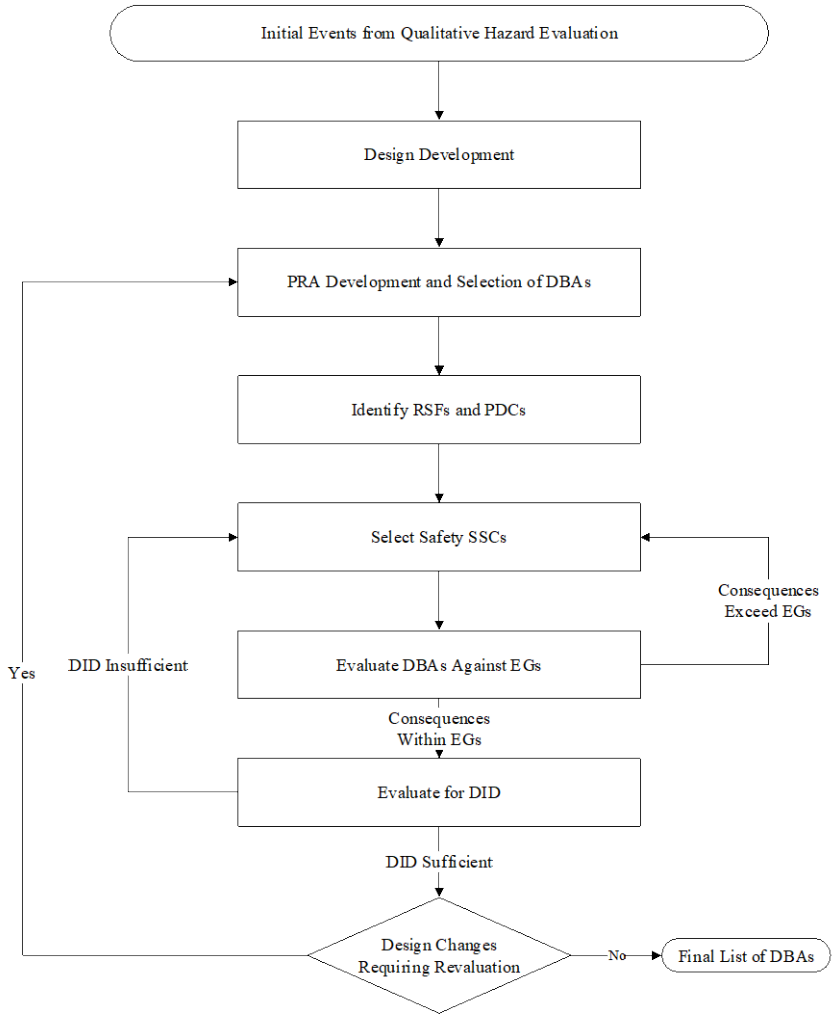

Figure 1. NEI-18-04 process for safety analysis

The DSA is a living document that is updated throughout the life of a reactor. Changes in plant design or operational practices require analyses against the existing DSA before approval through an unreviewed safety question process for DOE or a 10 CFR 50.59 process for NRC. Nuclear operators regularly spend significant time updating the DSA/SAR for facilities from the engineering process throughout the plant's lifetime.

1.2 Current State of DOE Design and Nuclear Licensing

DOE-funded projects must meet the requirements described in DOE O 413.3B, “Program and Project Management for the Acquisition of Capital Assets,”[8] which governs the project management and acquisition processes of major capital projects. Although this order is not applicable to all nuclear projects, it provides a rigorous outline of deliverables, project phases, and required documentation. It also invokes other DOE directives, such as DOE-STD-1189, “Integration of Safety into the Design Process,”[9] and DOE O 420.1C, “Facility Safety.”[10] DOE O 413.3B breaks the design of a new facility or nuclear reactor into clearly defined design stages, as shown in Figure 2, associated with milestones called Critical Decisions. Nuclear safety deliverables are included for each phase and Critical Decision milestone for project evaluation. This approach is similar to industry best practices with discrete design phases generally used by projects licensed under NRC.

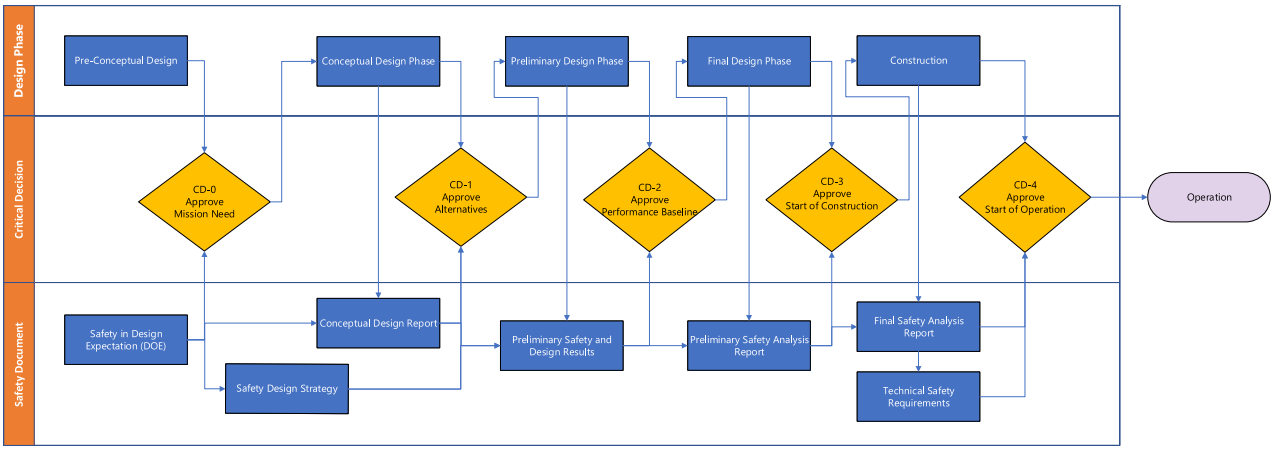

Figure 2. DOE O 413.3B design phases.

The typical DOE design process begins with a pre-conceptual design phase where project objectives and constraints are defined, design alternatives are identified, and preliminary site selection and layout are performed. A conceptual design basis is developed with preliminary safety requirements documented in a Safety Design Strategy (SDS). The SDS outlines design commitments so that safety is integrated into the design, and it describes how the safety analysis will be completed.

The next phase is the conceptual design phase. It involves defining the design basis and specifications, selecting the design concept and layout, creating design basis documents, and performing a conceptual safety analysis documented in a Conceptual Safety Design Report (CSDR). The CSDR provides early regulatory acceptance and records the conceptual design decisions and safety considerations for a nuclear facility or system. It includes the design basis, safety systems, and potential hazards, providing a foundation for the subsequent design phases.

The preliminary design phase follows with detailed design basis documents and design layouts. After detailed analysis, preliminary design drawings are created. Design reviews ensure that the design meets all requirements. During this phase, a Preliminary Safety Design Report (PSDR), typically written in the same format as a PDSA, may be submitted for regulatory acceptance.

The final design phase is where the final design basis documents and layouts are developed. Again, detailed design analysis and reviews are performed, and final design documents, drawings, and specifications are created. This phase includes obtaining necessary approvals and permits and performing final design reviews. Upon completion of the final design, the PDSA is submitted for regulatory approval.

Construction, procurement, and validation completion activities make up the execution phase. Tasks may include demolition, radiological decontamination, fabrication, excavation, installation of structures and equipment, quality compliance/conformance inspections or tests, and initial SSC troubleshooting/commissioning tests.

Finally, the post-construction phase involves performing post-construction testing and inspections, obtaining necessary regulatory approvals through the submission of the Final Documented Safety Analysis (FDSA), and beginning operations and maintenance activities.

As part of the design process, DOE requires that safety is integrated into the design from the pre-conceptual to final design phases, as outlined in DOE-STD-1189. Integrating safety reduces the need for design iterations because important safety decisions are made as part of the design process, reducing the potential for rework. This commitment to integrating safety into the design is captured through the SDS documentation.

Figure 3 shows a detailed diagram of a typical workflow for the development of any reactor at DOE, using a systems engineering approach that integrates aspects of the NEI 18-04 methodology. The top line of the diagram illustrates the role of engineering, while the bottom row depicts the typical nuclear safety analysis process. Although the workflow specifically shows the DOE authorization process with required submittals of the SDS, CSDR, PSDR, and PDSA, the process is similar to NRC licensing, which involves varying levels of regulatory engagement with a single submittal of the PDSA. Actions are shown in gray boxes, design documents in green boxes, design review documents in aqua, and safety deliverables in red.

The iterative engineering design workflow, as shown in Figure 3, consists of designing components, analyzing their performance, completing failure modes and effects analysis (FMEA) along with reliability analysis, verifying design requirements, documenting design, and conducting design reviews. This design cycle typically occurs in discrete phases as described above, lasting from 3 months to several years, depending on the project. The hazard and accident analysis described in the bottom loop occurs in a similar manner to the design process; however, depending on the organization, this is sometimes done serially after a design cycle is complete instead of in parallel, due to the wait for design finalization to be added into the safety analysis. This serial workflow can add anywhere from 3 to 6 months of additional time between design cycles, resulting in a very inefficient design process, especially for organizations that compartmentalize information. Each iteration of this loop adds more detail and completeness to the design, progressing from conceptual to preliminary to finalized design.

Figure 3 also shows the interconnection between design documents that are inputs into the safety analysis process. Typically, information is shared through traditional documents, denoted in green boxes, with both engineering and nuclear safety working somewhat independently. A safety analyst reviews design information to identify hazards and evaluate their effects. SSCs are chosen from those available for the plant to meet safety functions. The analyst then completes accident analysis by crediting the selected SSCs and determining the dose consequences from those accidents as mitigated or prevented by the SSCs selected. The analyst then determines appropriate special treatments for the SSCs, such as applying industry codes and standards, and determining design, reliability, environmental, quality assurance, special programs, and surveillance requirements. These analyses are then documented for regulatory approval in phases, as shown in red boxes in Figure 3, and also send back additional safety requirements to the engineering team to make the necessary engineering changes.

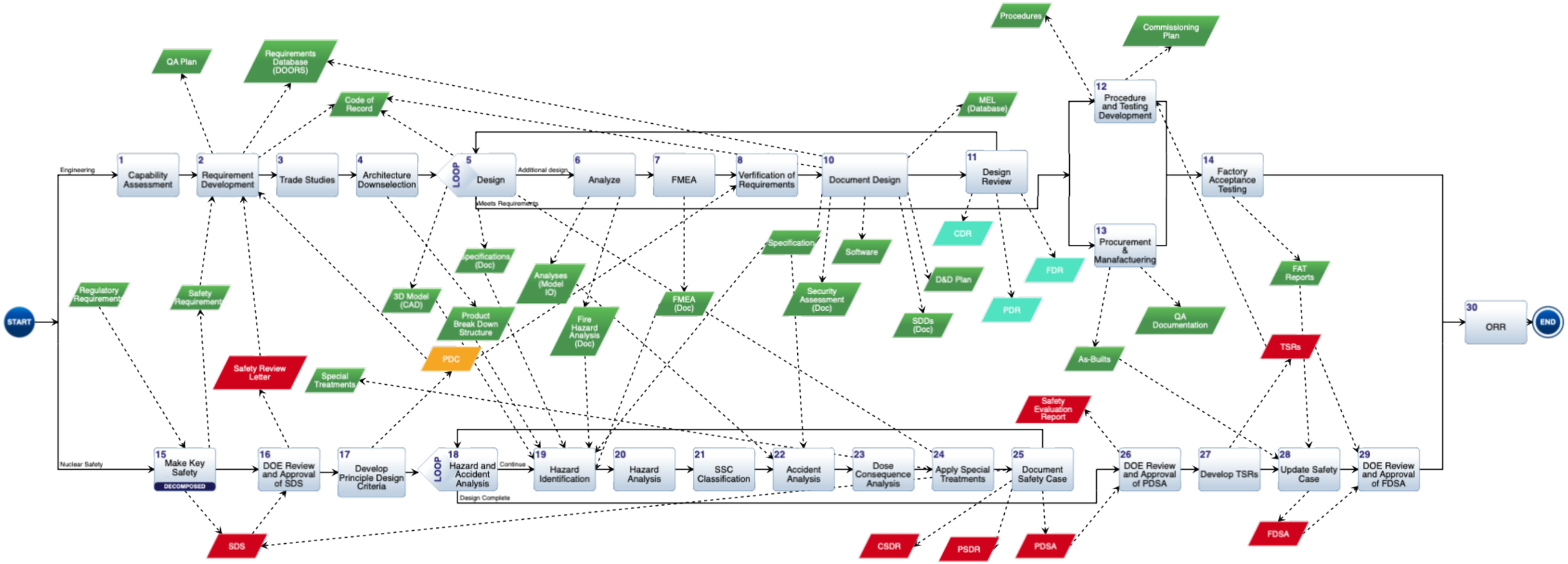

Figure 3. Detailed breakdown of design analysis cycle for a reactor project

1.3 Desired State of DSA Reviews with Digital Tools

The ideal future state of the digital DSA leverages digital tools to enhance development and provide full transparency of the design to reviewers and regulators. Achieving this result requires an agile implementation strategy, incorporating additional capabilities in a phased process to facilitate adoption effectively. Critical considerations include understanding what regulators need to review and how to create tools that accelerate these reviews. This necessitates a collaborative effort with the DOE's reviewers to develop a tool that best suits their needs.

Section 2 discusses the digital tools and their implementation into the development for design and reviews, while Section 3 outlines the implementation strategy planned for the project.

2. DIGITAL DSA FRAMEWORK

As described in the preceding section, several static artifacts are generated over the course of a reactor project. Static data, as opposed to native data, refer to documents and drawings in PDF format that are snapshots exported from native authoring tools for record retention and configuration management purposes. For example, reports are often written using Microsoft Word or similar word processors. The file is stored on local or shared computing infrastructure and can be modified at will using the authoring application. When a PDF is generated and saved in its archival format, it may contain the same information as the native file, but the native file can be subsequently changed. However, the nuclear energy industry, driven by regulation, has historically relied on PDFs as the SOT for the design at any given project lifecycle stage. The paradox is that this static output is, by nature, out of date and out of sync with the native information upon its creation, since it no longer is a one-to-one representation of what is contained within the file it is sourced from.

This section proposes a paradigm shift in generating the required safety basis documentation for a nuclear reactor project. Instead of being forced into a reactionary position to receive, review, and use static information from engineering disciplines, safety analysts are integrated into continuously updating, modern software solutions. These software solutions automate the safety basis documentation process, and in its future state, safety documentation may take a new format as a digital product.

Living, automated safety basis documentation would enable regulators, design engineers, safety analysts, and operations personnel to dynamically navigate through contents, including facility descriptions, systematic hazard identification, evaluation of normal, abnormal, and accident conditions, derivation of hazard controls, and definitions of safety management program characteristics. This digital product requires the integration of digital engineering databases through workflows under configuration management, accessible via dynamic web interfaces. The data from these software platforms is coalesced into a common data language, or ontology, that can translate the proprietary formats of various tools into a single format. This ontology also captures the relationship between objects from different engineering domains, forming a knowledge graph that can be searched for and, most importantly, reported from. This "digital thread" enhances understanding and clarity of the design, improves safety, and reduces regulatory burden through design and future operations.

The following sections describe the necessary process changes needed to facilitate this paradigm shift as they relate to the necessary content of a DSA per 10 CFR 830.

2.1 Describing the Facility Through Digital Engineering Tools

The current document-based approach to engineering design, and consequently the licensing process, imposes a burden on reactor development projects. Information developed during the design phase of a reactor project is duplicated in several static artifacts with little to no traceability between them. When changes are required to design information, tracing the impact through thousands of artifacts becomes manually intensive, leading to a potential human performance error trap. Additionally, documents are typically written in narrative format, relying on the English language to communicate complex design intent that is not always best explained in this format. As an example, piping and instrumentation diagrams (P&ID) are far more useful to an engineer or reviewer than paragraphs attempting to describe a design.

Utilization of new digital engineering concepts, as explored in the following subsections, to develop the facility description for a reactor safety basis can expedite the delivery of safety documentation and reduce rework expenditures.

2.1.1 Model Based Definition, Product Lifecycle Management, and Building Information Modeling

To understand the full scope of equipment to be procured and installed as part of a new reactor project, engineering, procurement, and construction (EPC) firms typically create equipment schedules and bills of materials (BOM) that collectively serve as the sources of truth for equipment identification tags, quantities, and important parameters associated with each piece of equipment. However, these lists are almost always developed manually, referencing other drawings and populating these tables with data from various sources or offline spreadsheets. Often, engineers will comb diagrams such as P&IDs, single line diagrams, and wire connection diagrams to obtain equipment and quantities for populating schedules.

Model-based definition (MBD) is an approach to creating two and three-dimensional (3D) computer-aided design (CAD) models such that they effectively contain all the data needed to define SSCs. These data, which supplement the geometry of CAD, are stored within the native file format of the model instead of a separate list or spreadsheet. With MBD, the model becomes the source authority for quantities and important parameters that drive downstream engineering activities. This approach to capturing and recording SSCs properties of interest replaces legacy schedules.

Complementing MBD is product lifecycle management (PLM), a combination of processes and software used to manage the entire lifecycle of a product, such as a nuclear power plant, from conception to disposal. PLM tools are designed to natively import dynamic MBD CAD from various authoring software. PLM also serves as the storage location for project files, including documents and reports. When models, documents, and drawings are uploaded, parameters are extracted from the file and pushed to the central database of the application, enabling the user interface to display this information in a web browser. The version and history of each object stored in the system is recorded and timestamped, ensuring complete traceability from the creation of a design file. Most PLM tools include workflow capabilities to track reviews of stored files and documents, allowing the design review process to remain entirely within a single software solution, avoiding the use of floating emails and disparate share drives.

Building Information Modeling (BIM) is a digital representation process for the design, construction, and management of buildings and infrastructure. It goes beyond traditional blueprints or 2D plans by creating 3D, facility-scale models that also incorporate data about time

(4D), cost (5D), environmental impact (6D), and facility management (7D). BIM enables architects, engineers, contractors, and owners to work together more effectively by sharing and managing design and construction information in a single digital format. BIM allows for the simulation of construction processes and building performance, facilitating better outcomes in terms of sustainability, operational costs, and lifecycle management. BIM is not just for the design and construction phase but also for the entire building lifecycle, supporting facilities management and renovation or demolition planning. This level of modeling is typically performed at a lower level of definition than CAD, due to the expansive nature of projects employing BIM. Various levels of detail are used, spanning from level of detail (LOD) 100, where model objects are represented with a symbol or other generic representation, to LOD 500, where model elements are modeled as they were exactly constructed. BIM can be integrated with PLM tools to manage the state and version of model files, as well as to decompose these large facility models into their discrete elements, and to tie these elements to other objects in the project lifecycle.

Typical DSA development is an iterative process wherein design details are provided to the safety analysts who then respond with any comments they may have. A central repository for files allows the safety analyst to have access to the current up-to-date information associated with the design. This not only removes iterative communication but can reduce the lag time between interfaces by allowing safety analysts to retrieve the information without waiting for a transmittal from the design organization. An example of this interconnection between model, assets, and documents stored in PLM is shown in Figure 4.

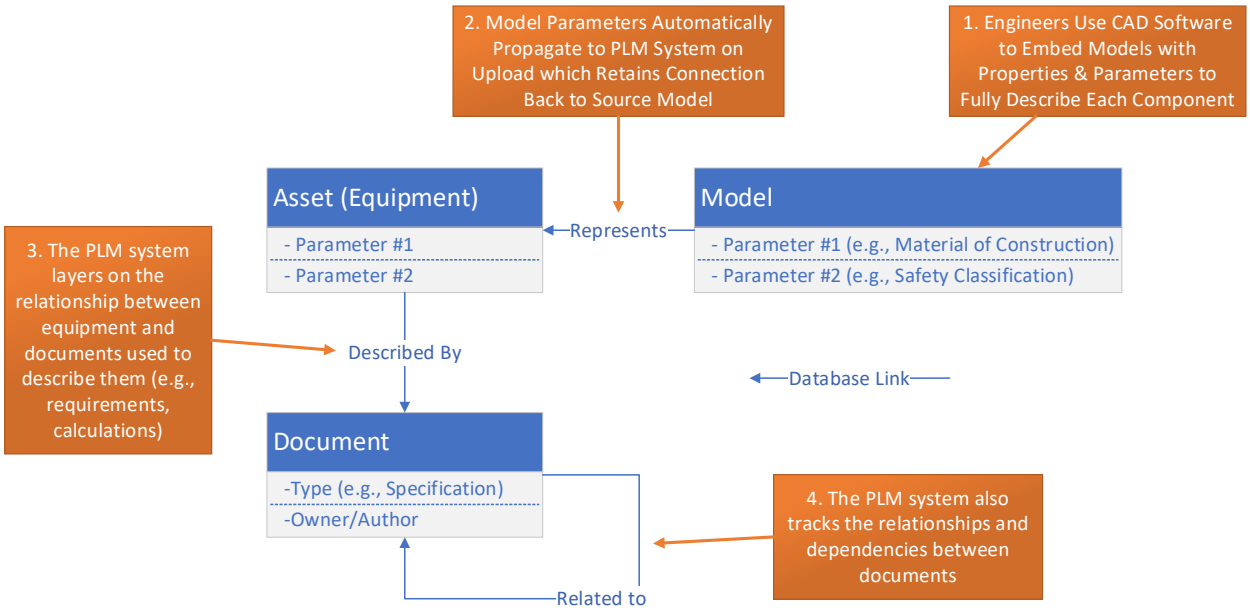

Figure 4. Data objects and their relationships in PLM

2.1.2 Data-Driven Requirements Engineering

Project requirements in the nuclear energy industry are typically documented and managed in a series of documents. In a digital engineering approach, all project requirements, including program, regulatory, safety, functional, performance, and quality, are stored in a single requirements management tool. Each requirement also includes supplemental attributes such as the rationale, an explanation of why the requirement exists and why it has particular value, or

the project discipline responsible for incorporating the requirement in the design. Requirement objects within the requirements management tool are linked together by relationships which explain the association between them. For instance, a stakeholder requirement may be linked using a “derives” relationship to a lower-level system requirement that further refines or decomposes the concept introduced by the stakeholder. This decomposition provides essential traceability from the highest levels of the requirements tree to verification activities that objectively prove the requirements are met by the design configuration. Using requirements development and management software for documentation provides unique identification, assignment to project SSCs, and the ability to generate and manage requirements throughout the project lifecycle.

Requirements management software reduces the effort needed to track the systems engineering process. The reasoning and rationale for each requirement can be clearly traced back to the deriving requirements. These linkages also assist in the design verification process and significantly reduce the effort of performing labor-intensive verification efforts. Some requirement management tools also allow for the generation of documents. Most importantly, this class of tools can be used to show the relationship between regulatory requirements, imported from regulatory databases such as the online Code of Federal Regulations (CFR), and their implementing, project-specific requirements in a single software platform. This traceability instills confidence that the project has 1) identified and documented all regulatory inputs and 2) linked them into their implementation within the design. This process is often attempted using descriptive documents, where traceability matrices exported from requirements management tools offer a vastly superior method of consuming the same information. The relationships established within a requirements management tool are shown below in Figure 5.

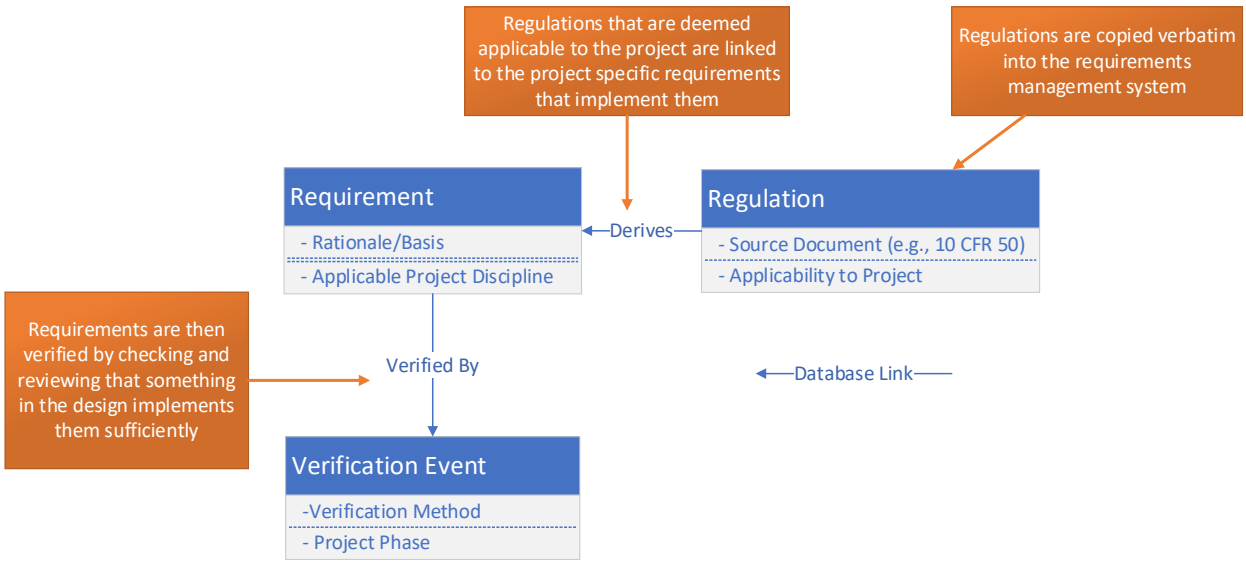

Figure 5. Data objects and their relationships in requirements management

2.1.3 Integration of MBSE Software in Systems-Based Design

Model-Based Systems Engineering (MBSE) is a methodology that focuses on creating and exploiting domain models as the primary means of information exchange between engineers, rather than relying on traditional document-based approaches. MBSE is used to support the requirements, design, analysis, verification, and validation activities beginning in the conceptual design phase and continuing throughout development and later lifecycle phases. MBSE

software can be used to create links between requirements, plant or system functions, and components and systems (collectively referred to as assets) within the design. These applications promote the use of standardized modeling languages like the lifecycle modeling language and system modeling language, which helps in maintaining consistency across diverse teams, projects, and software packages. Requirements, functions, and assets can include attributes or properties that further describe them. These can include nuclear safety information such as safety classification and seismic category.

MBSE software may also facilitate the failure modes and effects analysis (FMEA) process. FMEA identifies the potential failure modes of SSCs, their causes, and the effects of those failures on system performance and nuclear facility safety. The process involves analyzing various components, subsystems, and system functions to identify potential failures and their cascading impacts. Figure 6 illustrates how each requirement links to a function and failure item. As each component is designed, adding the appropriate metadata into the MBSE database allows for automating the generation of FMEA that import into safety analysis. As SSCs are updated, the FMEA is constantly updated with the changes in the system with a SOT.

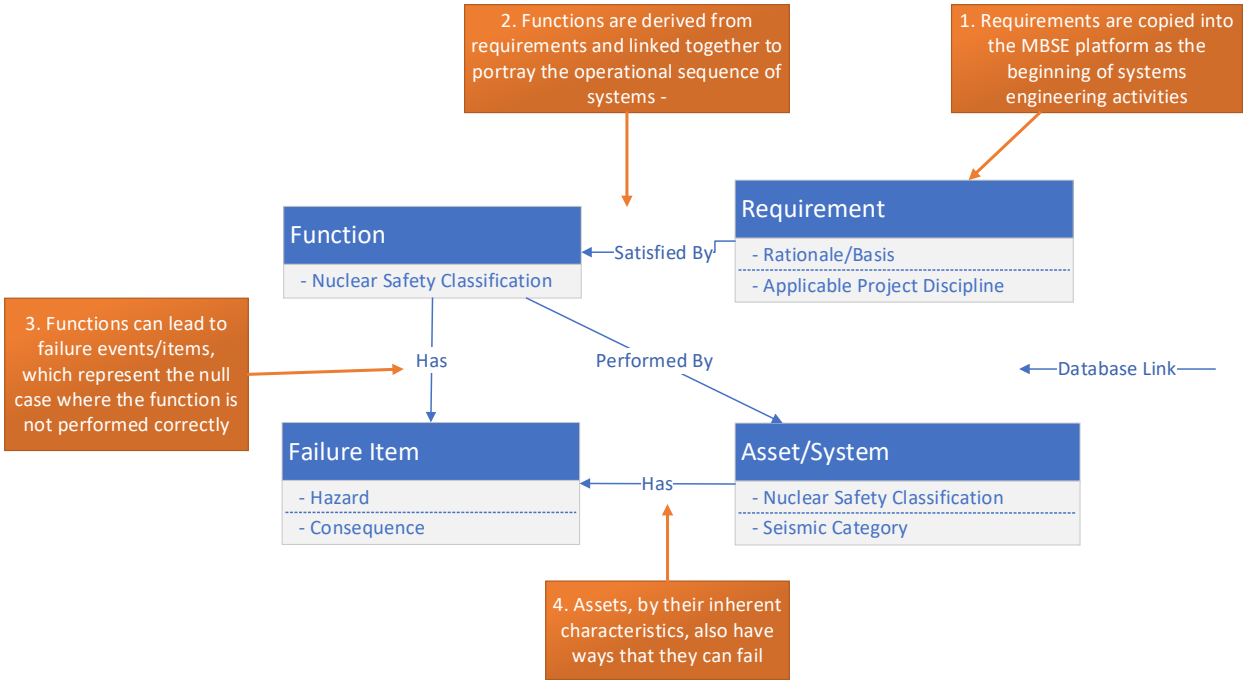

Figure 6. Data objects and their relationships in MBSE with FMEA

MBSE also enables the evolution of system functional modeling in creating digital twins. Digital twins are virtual models of physical systems that operate, function, and simulate system interactions with real-time data collected from a physical system. These models form a virtual version indistinguishable from the physical counterpart. Digital twins allow for the collection of operational data and the application of analytic methods to analyze and predict system behavior. Digital twins of nuclear facilities have many identified potential benefits for design, licensing, construction, operation, and decommissioning. Additionally, the development of digital twins provides simulation of the physical system's performance and operation prior to construction. This could potentially be used to integrate function and failure analysis and streamline the design and safety iterations for the facility. During active operations, digital twins can be utilized to train operators or update safety documents and models derived from changes, ensuring that the virtual representation remains aligned with the physical system.

2.1.4 Digital Thread Aggregation

A digital thread refers to the framework that enables a connected data flow and integrated view of a project's data throughout its lifecycle, from initial design to field service and operation. It is a communication framework that connects traditionally siloed elements and provides an integrated view of a project.

Objects used in the digital ecosystem follow a defined ontology, as detailed in Section 2, and illustrated in Figure 4 through Figure 6. These objects from requirements management, PLM, and MBSE are extracted from their sources of truth, mapped to classes and associated relationships within a common ontology, and loaded into a central data warehouse for storage. The links between data objects maintained within the source databases are also preserved upon import to the single data warehouse. Additional relationships are created across software domains to enhance the knowledge graph created in the data warehouse. For instance, if a single relationship is created between a function and its performing asset in a MBSE tool, and a separate relationship is created between an asset and its descriptive documentation in the PLM system, then a chain of relationships is carried into the data warehouse where the function is linked to the asset which is linked its descriptive document. This capability enables the association of data that is not possible in standard off-the-shelf offerings.

Different software generates or uses types of objects based on their roles in the project's ontology. These software tools can generate dynamic documentation using these objects, constructed via database objects in natural language. Dynamic documents not only reference the objects but also link to them, including their properties and relationships. This dynamic use of objects allows for the automatic updating and sharing of project objects and parameters. For instance, constructing a DSA can reference components and result values from part files or analyses stored within the PLM tool, which will update as their SOT updates. Figure 7 illustrates this relationship, showing how dynamic data links regulations to requirements to assets.

Using objects across multiple tools requires linkage to an SOT owned by a specific database, with changes allowed only through an approval process. For example, a value given in requirements might be tracked down to an analysis. If the analysis determines a new value should be used, it will push the updated value to the requirements database for review and approval by the cognizant engineer. Once approved, the change will propagate to any other linked location or analysis, ensuring consistency and accuracy throughout the project documentation.

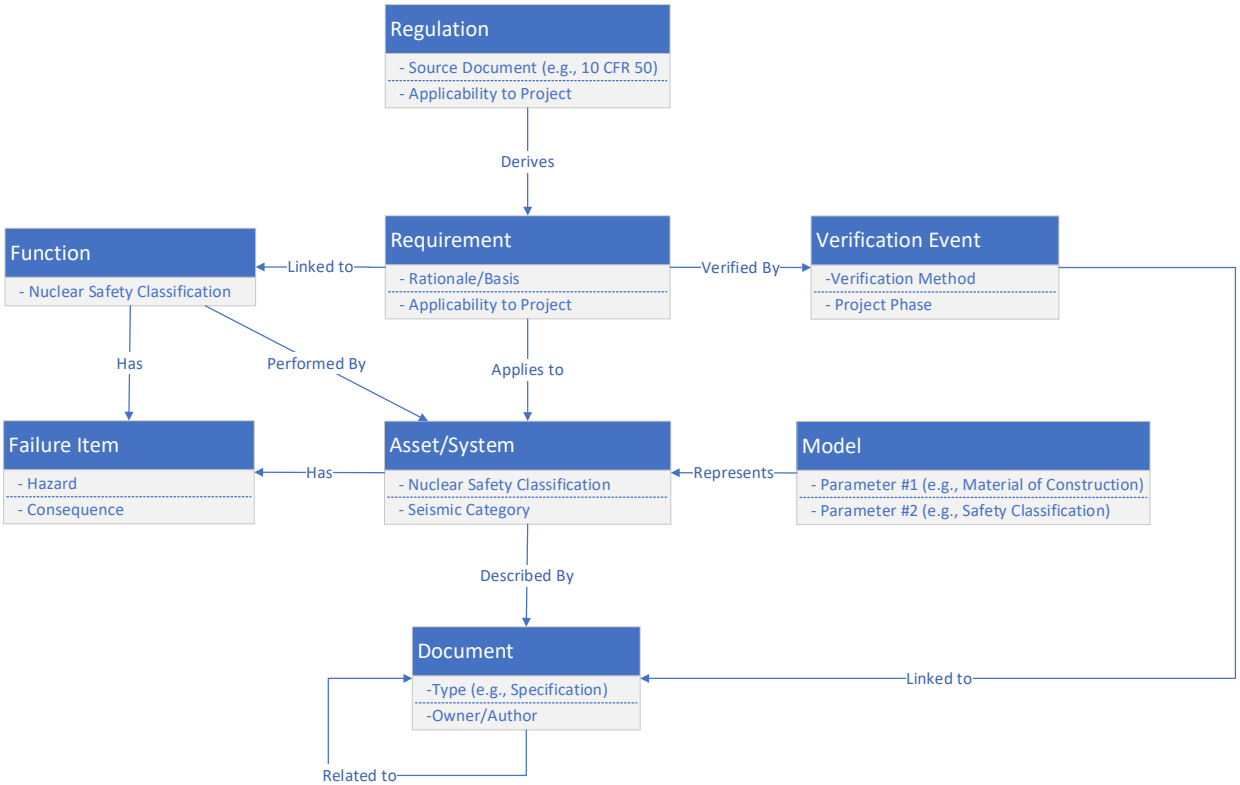

Figure 7. Compiled Data Objects in a Digital Thread

2.1.5 Digital Change Management Processes

DOE O 414.1D and the ASME NQA-1 require strict adherence to configuration management as defined by the project quality assurance program. These quality assurance requirements for configuration management ensure that nuclear facilities are designed to high standards of safety and reliability. Configuration management ensures that the design reflects the as-built facility and that any changes are properly assessed and documented.

In a traditional design environment, configuration management is completed by design review boards that manually determine any changes during the design or lifespan and affected documentation, which is manually updated to match the changes. Digital tools transform this process through dynamic impact analysis that automatically determines any impacted documentation and propagates the changes to any linked SSCs and analyses.

In a digital thread environment, information can be automatically and dynamically updated, reducing human effort and eliminates errors associated with manually replicating data in downstream systems, which provides stricter configuration management control.

Digital tools also allow for design control that ensures that design requirements are correctly translated into design outputs, verified and validated, and that design changes are controlled by showing the correlation and connection of requirements to actual analyses results within the digital ecosystem. Configuration management also requires that design interfaces are identified and controlled. In a digital ecosystem, design interfaces may be controlled by restricting access to changes through the digital approval process. For example, existing PLM and requirements tools already provide a record of who and when changes are made and allow for locking of requirements to change workflows that must be authorized by approved users. The approval workflow within these tools may be easily updated to match the requirements of project QAPs.

Currently developed PLMs can generate tasks for cognizant engineers, system oversight, or other impacted personnel to review the change and approve, disapprove, or provide comment. In a future state of development, the digital ecosystem may even be able update the engineering analyses impacted by the change to inform the change originator of the true impacts resulting in more informed decisions at initiation.

QA also requires as part of configuration management that design information must be uniquely identified, controlled, and maintained. Existing tools already assign unique identification numbers and allow for ease of navigating information via those unique identifiers, as well as automatically tracking any changes to the design information.

2.1.6 Leveraging Automation and Artificial Intelligence

Artificial intelligence (AI) and machine learning (ML) models can revolutionize documentation processing and generation. Research indicates that applying various AI and ML models to text yields more valuable results than traditional optical character recognition processing. This has led to numerous commercial offerings for AI-driven data processing and analytics. AI-powered document processing is already in use across various industries, including banking, government applications, healthcare, and telecom, where natural language text is processed for database environments.

In the context of project information, such as vendor data sheets for equipment or requirements/code documents, AI document processing and ML models could significantly reduce the human effort involved in data ingestion tasks. Natural Language Processing (NLP) and named entity recognition can be employed to identify objects—such as component identification, parts, parameters, and requirements—within documentation, thereby developing objects and relationships. For example, applying NLP to equipment reliability report data such as in [Mandelli, 2023], shows promising results for identifying objects and parameters in natural text and relationships between objects. By populating the database, these technologies create the digital thread, which can be used to generate other project documents, such as the DSA, using the opposite process. Instead of parsing narrative text into data objects, connected data objects can be transformed into narrative text.

Several services, including Amazon AWS Intelligent Document Processing, Adobe Acrobat AI Assistant, and Google Document AI, offer the application of NLP and Large Language Models (LLMs) to documents and text to extract data and values. While these services are commercially available, it is important to note that not all are approved by FedRAMP.

In addition to ingesting information using AI to create objects, AI can also use database objects to generate narrative sentences, paragraphs, and their assembled documentation. Using AI to automatically generate DSA documentation from database objects—such as 3D parts, requirements, and parameters—can streamline the document creation process. Although

human approval of AI-generated documents remains crucial to ensure accuracy, this approach can significantly reduce the overall effort required for document generation. Companies like Microsoft are actively developing commercial solutions for automated documentation generation.

2.1.7 Dynamic Facility Description Generation for DSA

With the digital thread in place, documentation can be dynamically and automatically generated, replacing traditional manual documentation methods, eventually leading to a full digital deployment of a digital DSA or SAR. Generating project documents using database objects results in smart documents that contain links to back to their underlying data in the digital thread. Embedding these objects into document text creates dynamic links, ensuring there are no conflicts in information across different documents. This approach ensures that each document serves as the SOT for the respective objects it references. Utilizing object-based documentation minimizes the risk of rework associated with outdated information and aids in impact analysis. By identifying where an object is used, project personnel can assess the number of potential changes associated with any document update in the SOT. Dynamic documentation significantly reduces rework and errors by maintaining and leveraging an SOT.

As previously discussed, AI can generate natural language text for traditional or digital DSAs. Applying AI and ML techniques to project data can automate the creation of dynamic documentation. This approach ensures that generated documents are linked to database objects and their original sources via the digital thread. The process involves ingesting data into the data storage solution and subsequently generating object-based dynamic documentation, whether the data are extracted from a document or taken directly from a database.

Below, Figure 8 illustrates the flow of information from source text to dynamic documentation. An example of processing natural text for object recognition is shown in Figure 9. By using this approach, a dynamic digital DSA can be developed, leveraging the interconnected and up-to-date nature of the digital thread.

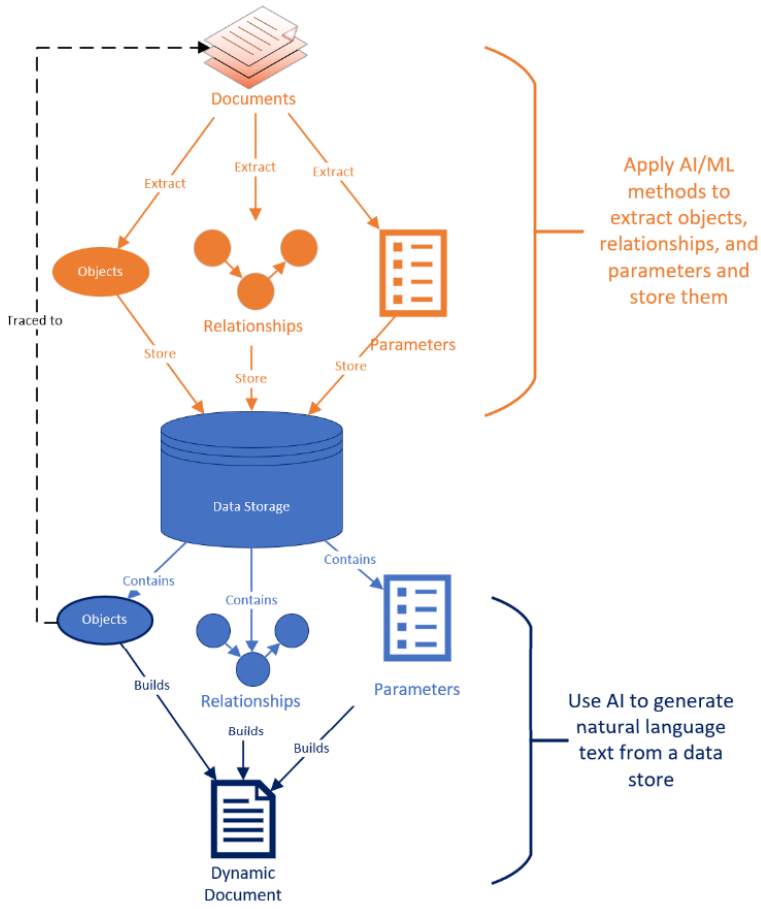

Figure 8. Using AI to generate objects from documents and documents from objects

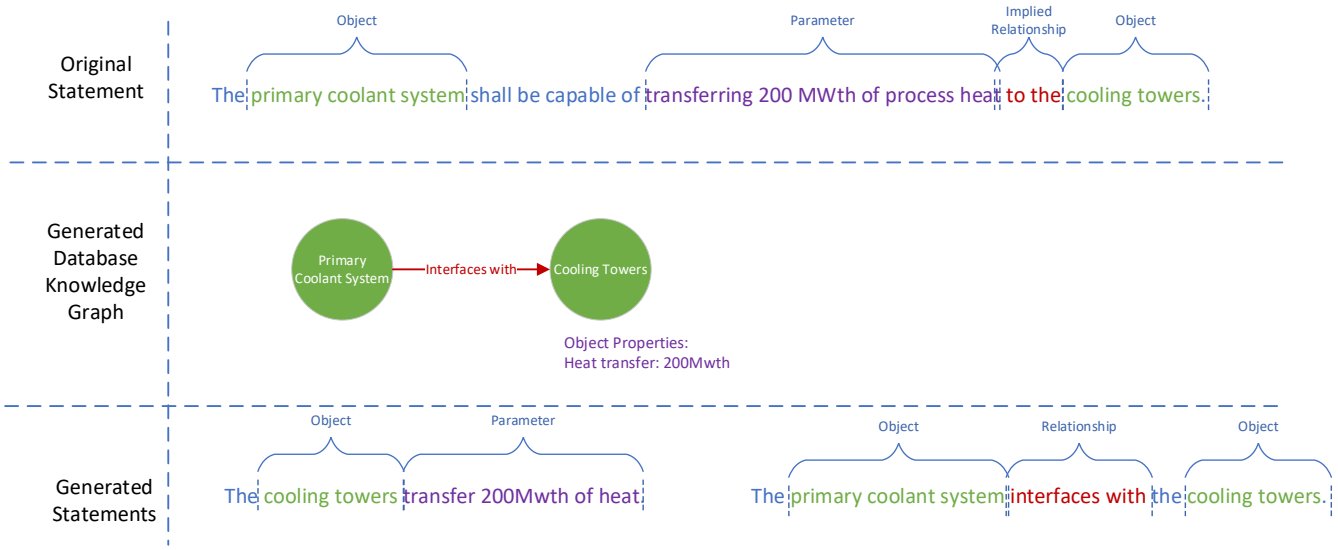

Figure 9. Example text parsing and generation

In a fully digital DSA environment, data would be seamlessly interconnected across databases through dynamic links managed by a central repository. The repository clarifies which analysis, database, or requirement holds the ultimate SOT. Figure 10 illustrates an example of interconnected digital information sources (ontology) within MBSE tools linked to a digital DSA.

Adopting a comprehensive systems-based approach in digital engineering begins with the derivation of requirements. Here, a nuclear safety analyst initiates the process by integrating regulatory and safety requirements at the outset of the design phase, embedding these into a centralized requirements database, often managed using tools like DOORS. This database captures a broad spectrum of requirements, encompassing engineering specifications, safety classifications, regulatory codes and standards, special treatments, and matrixes for verification and validation (V&V).

Throughout the design process, the engineering team develops a 3D model that dynamically links back to these requirements. This linkage ensures that any changes in information are automatically updated across related documents. The 3D model contains detailed component designs, including dimensions, tolerances, system breakdowns, descriptions of systems, SSCs, and other metadata crucial for design integrity.

Subsequently, the 3D model serves as the basis for generating a Master Equipment List (MEL) and Bill of Materials (BOM), which track each individual component within the design. During operational phases, this MEL evolves into a database used for maintenance, surveillance, spare parts management, and other operational functions throughout the lifecycle of the facility.

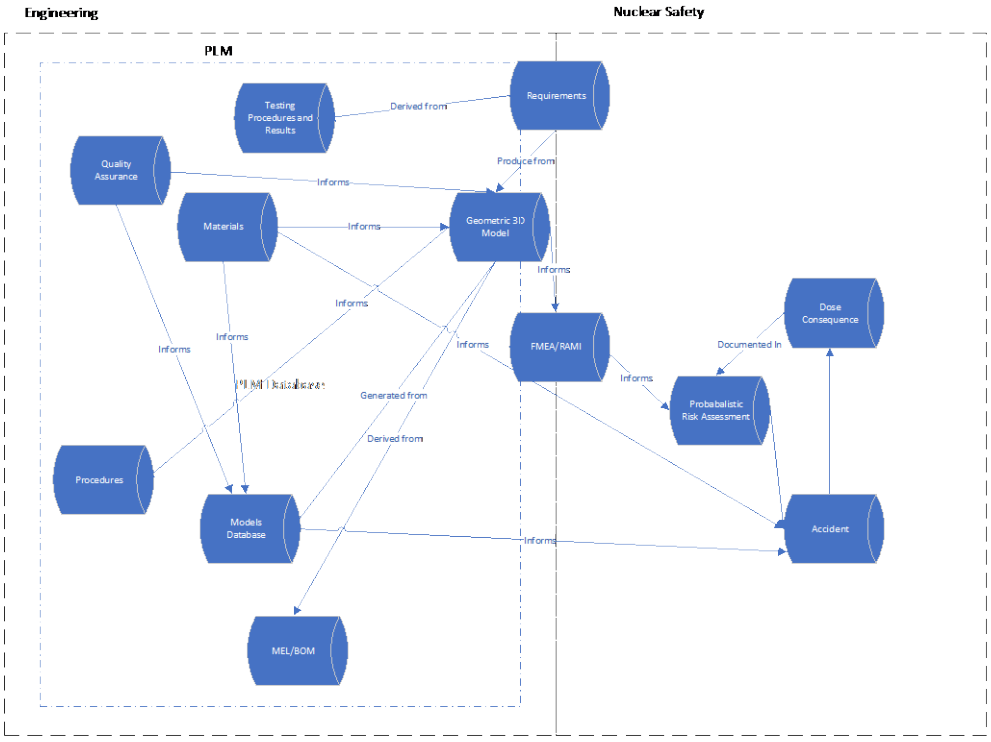

Figure 10. Interconnection of data in digital DSA

A materials database provides essential data such as chemical composition, heat transfer coefficients, thermal-mechanical properties, and more, crucial for specifications, detailed analysis models, and accident analyses. This integration facilitates automatic updates of properties throughout the design as linked materials in the model are modified.

In traditional design processes, documents are individually approved and stored in a dedicated document repository. Each design cycle concludes with a snapshot of these documents in their current states, often including a design report and DOE regulatory report, such as a CSDR, PSDR, PDSA, or FDSA. In a digital environment, similar configuration management steps adhere to appropriate regulations and American Society of Mechanical Engineers Nuclear Quality Assurance (NQA) Level 1 requirements. In a digital DSA process, configuration management involves creating a locked snapshot of digital information of a project at a discrete phase (e.g. CSDR, PSDR, PDSA, or FDSA), with approvals following the required engineering and regulatory requirements, integrating the do, check, approve methodology.

In this model, system engineers and analysts develop the initial SSCs and analyses that embed the appropriate deep links to information. As the design progresses, their role transitions to verifying and approving changes as part of configuration management, rather than manually updating information.

Under this framework, traditional documents such as system design descriptions (SDD) are no longer manually generated through the design process. Instead, they are automatically generated from data and metadata within the digital thread. For instance, a reactor's primary cooling SDD dynamically retrieves requirements from the database, system and component descriptions from 3D model metadata, reliability data from FMEA or reliability, availability, maintainability, and inspect ability (RAMI) databases, and surveillance and calibration requirements from the MEL database. The DSA then compiles this metadata from the SDDs to automatically populate relevant content in the DSA.

2.2 Systematic Identification of Hazards by Workflows

Traditionally, nuclear safety analysts employ systematic approaches such as “Hazard and Accident Analysis Handbook,” (DOE-HDBK-1224) along with checklists, what-ifs, FMEA, hazard and operability study (HAZOP), or PRA to identify hazards through a manual documentation process. This method involves analyzing design documentation and recording results in a methodical, iterative manner, which can be slow and time-consuming as the design evolves.

In contrast, workflows within a digital ecosystem and MBSE software significantly reduce the time required to systematically identify hazards and dynamically update analyses with design changes. Workflow wizards are interactive programs that guide users through creating, maintaining, and reviewing workflow tasks. Leveraging existing workflow wizards and processes in various software suites can enable project personnel to make full use of the dynamic ecosystem. Within individual software packages, workflow wizards for tasks such as document creation and review (e.g., in DOORS or Windchill) assist personnel in effectively using the tools and streamlining the design process.

Additional project guidance and workflows for the digital ecosystem will be provided in the systems engineering management plan for the project. This includes instructions for linking to dynamic objects, importing information (if applicable), and identifying the SOT for different types of information, presented in a graphical format for quick reference. Commercial software, such as ServiceNow, can create workflows for various tasks and provide workflow wizard assistance to users.

Templates or forms for common analyses and documents streamline the creation of manually produced documentation. Some software packages include templates for various document types, ensuring uniformity and ease of generation and review. Project-specific document templates further enhance these capabilities by guiding project personnel on additional analyses or safety reports. Examples of safety documents that benefit from standardized templates include Fire Hazard Analysis, Hazard Identification, Hazard Analysis, Quality Assurance (QA) Reports, FMEA, and SDDs.

The use of workflow and template guidance reduces the labor involved in generating and reviewing documentation. Digital tools significantly accelerate the safety analysis process by automating many routine tasks required during safety analysis updates throughout the design process. For example, transitioning updates from FMEA data to PRA models is traditionally done in discrete cycles. By dynamically connecting FMEA and PRA databases, the PRA can automatically update as the design progresses, reflecting details such as failure probabilities for individual components. This integration speeds up model updates, ensuring all information is derived from an SOT shared by the engineering and safety analysis teams. For instance, if a core dimension is increased based on optimization studies by an engineering design group, that change will automatically update neutronics, thermal-hydraulics, thermal-mechanical, transient, and accident analyses to match the new size. This information then automatically updates all related documentation, including the digital DSA.

Workflows can automate many processes traditionally completed manually by nuclear safety analysts, such as collecting hazardous or chemical substance inventories, determining total fuel mass, updating source terms from burnup calculations, or extracting system design descriptions directly from 3D model metadata. This information can be automatically updated throughout the design cycle, streamlining each step of hazard identification and analysis.

The safety analysis process combines workflows and databases to generate the required safety analysis for a DSA, as shown in Figure 10 and Figure 11. In the Figure 11 workflow, similar to NEI 18-04, a safety analyst identifies the appropriate regulations, codes, and standards as inputs to the requirements database. The analyst then identifies RSF and PDCs for the design, which are recorded in the requirements database. The analyst extracts information from engineering databases to generate hazard identification and evaluation. The workflow then guides a PRA analyst to perform a PRA, connecting the hazard analysis and FMEA database into event and fault trees. These trees, combined with design information, link to input conditions and assumptions in the accident analysis, then provide conditions for radionuclide boundaries into the dose analysis. The dose analysis results are then integrated back into the PRA model. Finally, the workflow guides analysts to compare the PRA results with EGs and complete the DID evaluation of the design.

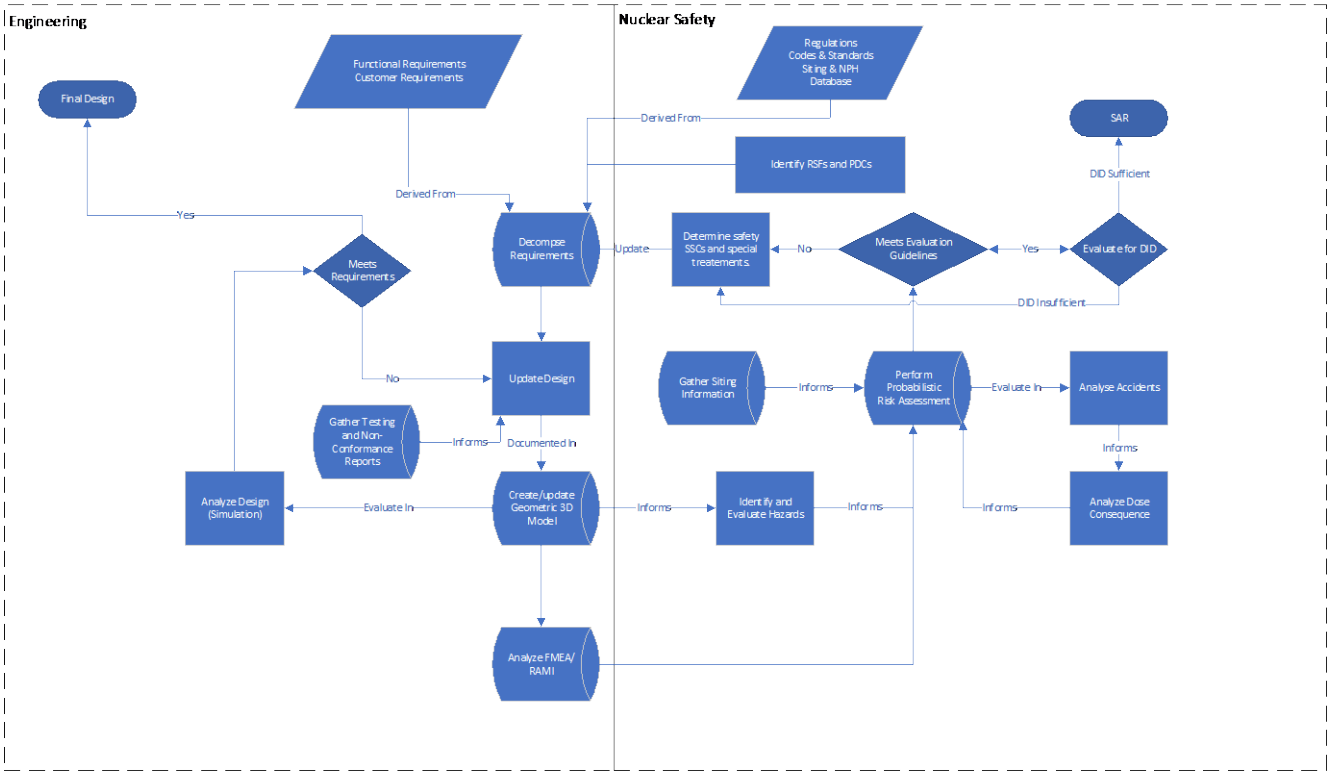

Figure 11. Workflow for the development of a digital DSA

2.3 Evaluation of Normal, Abnormal, and Accident Conditions Through Pipelines

Traditionally, reactor analyses are conducted independently by separate groups, each simplifying the system for their specific model. These analyses are then manually transferred between groups. In a digital workspace, data pipelines enable engineers to link their analyses from the 3D model to neutronics, thermal-hydraulics, thermal-mechanical, transient, and accident analyses.

By creating an object-oriented database for project models, parameters, requirements, results, and other relevant data, the digital ecosystem leverages these objects across project software and tools to form information pipelines. Integration of this object database with various tools facilitates the automatic or semi-automatic generation of analyses, documentation, and 3D models. Embedding these objects directly into the digital DSA establishes a link to the SOT, eliminating duplication errors.

Relationship links from descriptions and requirements to 3D objects and CAD assemblies create a digital thread connecting textual descriptions to design objects. Parameters associated with the 3D objects and analyses can be automatically imported when the object is referenced within an analysis.

Using these named entities for subsequent analyses, system descriptions, safety documentation, and other purposes creates digital threads from requirements and parameters to the components themselves and any downstream analyses or assemblies that utilize those

components. Database objects used in text are related according to the project's ontology. This allows for the creation of sentences that describe objects, their parameters, and their relationships in a way that software can understand. The use of ontology-based text-to-object links in documents enables software to ingest and generate text based on project objects, resulting in dynamic documents written in natural language that are easily understood by both project personnel and software. Applying the project's ontological relationships and classes allows digital tools to ingest or generate documents based on project objects.

Existing software that allows for external objects and parameters implements text-to-object linkages to some extent. However, additional effort is needed to create full linkages between multiple software tools and the objects stored within a PLM tool. This can be achieved by utilizing APIs from the software to access and link information between tools and the central project database. All tools used for nuclear analysis should develop APIs to integrate analyses with full linkages. For example, the further development of APIs to convert CAD models to input meshes for thermal-hydraulic codes or native geometries for neutronics codes are necessary.

An object-oriented database that dynamically connects engineering models and safety documentation will save time in the design process. This database and pipeline automation will update CAD models, performance models, and safety documentation for the DSA as design updates occur. The ideal process will involve changes in the design process automatically updating the CAD model, analysis model inputs, running steady state and accident analysis models, and updating results in the DSA. This process will track and flag changes and impacted documents for review.

2.3.1.1 DYNAMIC ANALYTICAL MODELS

The use of requirements, parameters, and part objects from the SOT that can be directly updated in analyses, system models, and calculations creates dynamic analytic models. The digital ecosystem supports the creation of these dynamic models through objects stored within project databases and the digital thread. These objects can be utilized in various software or analysis tools, referring to an SOT rather than duplicating information. Objects used for analyses may be outputs from other project documents or parameters from common documentation.

Figure 12 illustrates how parts and parameters in the project PLM could be used in analysis tools. By utilizing these API importers, the integration of data from the PLM system into analysis software is streamlined, ensuring that the most up-to-date and accurate information is used in simulations and evaluations. This connectivity allows for dynamic updates and consistency across various project stages, reducing manual data entry errors and enhancing the overall efficiency of the project lifecycle.

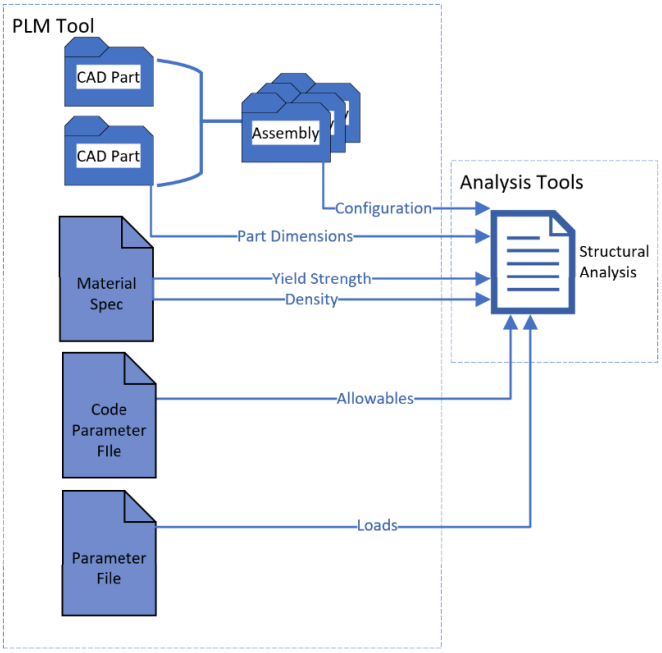

Figure 12. Part and Parameter Usage

Software-generated reports and analyses are then published back to the project database or PLM tool. Analysis outputs are stored as object-based text documents with specific outputs as objects for continued referencing in downstream project documentation. Linking outputs and inputs through various analyses and project documents enables higher fidelity impact analysis and verification/validation efforts.

Configuration management for shared data objects within the project protects analyses from inadvertent updates. Implementing an impact analysis/alert tool or notification system for input/output object updates provides alerts when external objects used within an analysis have changed. Potentially, direct source objects could be linked to analyses, with dynamic changes shown as an "update available" notification, streamlining the use of external objects. These capabilities will need to be developed on top of the existing features of a PLM or analysis tool as part of the digital ecosystem development.

For example, software such as PTC Mathcad and MathWorks MATLAB/Simulink allows for the creation, import, and use of parameters in analyses and models. These tools can utilize external objects stored within the project PLM database to create dynamic analytic models. Similarly, they can create and store their own objects in the PLM tool, allowing the use of outputs in other documents or analyses. These software tools comply with FedRAMP standards to varying degrees.

Cost reductions for impact analysis and parameter propagation are key benefits of using stored objects as inputs/outputs in dynamic analytic models. Linking objects stored in the PLM database reduces the risk of project errors related to using outdated design information or analysis results in dependent analyses. System functional modeling ensures that all requirements are met from a functional standpoint in an easily understood graphical format. Like analyses, system modeling can be combined with existing objects stored for the project, such as parameters, models, or requirements.

2.3.1.2 3D OBJECT LINKAGE

Hosting 3D mesh objects in a database as part files allows for the linking of requirements down to the individual part level. From these 3D part files stored within the database, comprehensive 3D models and CAD assemblies can be built. This also facilitates the relationships between individual parts, models, analyses, requirements, documents, and other elements. The creation of assemblies and individual part files further enables the automatic generation of master equipment lists and material quantifications, enhancing cost estimation accuracy.

Various BIM or CAD tools, such as Autodesk Revit, Autodesk Construction Cloud, and Aveva E3D Design, provide integration of part files within larger assemblies or facilities. These tools allow for the estimation of material quantities (e.g., concrete volume, pipe linear feet) and the generation of master equipment lists. Some of these software packages are FedRAMP compliant. Additionally, the integration of systems within a facility model, as enabled by BIM or CAD tools, allows for the identification of clashes between components/systems. This clash detection capability helps eliminate interferences or design deficiencies prior to procurement or construction.

The ability to identify design issues from part, system, and facility integration in models reduces rework. Moreover, defects caught during the design phase using these integrated tools are less costly to correct than those discovered during construction. Generating more accurate estimates of material quantities or exact part usage also increases the fidelity of cost estimates for procurement and project budgeting.

With 3D objects, engineers can extract information from the 3D model into the analysis space. The single SOT database provides the assumptions, model descriptions, input files, output files, software QA, results, and conclusions digitally. These can be easily connected to each component in the 3D model for viewing or integrated into the DSA. For instance, an analyst might script a neutronics input file in the database to pull core dimensions from the 3D model. The output can then be linked to thermal-hydraulics or thermal-mechanical analyses by using parameters stored in the database to connect all these models together.

Furthermore, workflows could be utilized to create an engineering calculations workflow, where an analyst documents open items, assumptions, inputs, outputs, and ties the conclusion back to the output values, even including appropriate figures for the DSA. Using dynamic analytical models and 3D objects, automation will dynamically pull all this generated information to populate vast sections of required information for the DSA, aiding in the evaluation of normal, off normal, and accident conditions.

2.4 Derivation of Hazard Controls and Demonstrating Adequacy through Workflows and Requirements

As described in Section 2.2, workflows will automate the systematic analysis of the design. These workflows can be enhanced to include the derivation of hazard controls by updating the safety requirements in a requirements database that will store the hazard controls for a reactor. Typical hazard controls include the designation of safety-related SSCs with appropriate special treatments or administrative controls. Throughout the design process, a safety analyst must clearly derive the safety function, functional requirements, performance criteria, and performance evaluation as part of the derivation of hazard controls. These requirements for each SSC can be easily stored and categorized within the requirements database, with appropriate flags for propagation into the design.

For instance, a safety function is the specific task or capability that a safety-related SSC is designed to perform to protect against potential hazards and ensure the reactor's safe operation. This safety function is stored in the requirements database, enabling the identification of SSCs by safety function. The functional requirement is a detailed specification outlining the conditions under which the SSC must operate and the standards it must meet to fulfill its safety function and special treatments. These requirements, derived from a comprehensive analysis of potential risks and operational demands, are recorded into the requirements database for export to the digital DSA.

Special treatments for SSCs ensure that they perform their intended safety function when needed, especially under accident conditions. These treatments include rigorous design and QA processes, thorough testing and maintenance procedures, and strict regulatory oversight. In the design process, system engineers and nuclear safety analysts incorporate conservative safety margins and environmental qualifications, including seismic, flooding, and natural phenomena hazard conditions, into these design requirements. QA requires meeting NQA-1 standards, which involve meticulous documentation, traceability of materials and components, and adherence to stringent codes and standards. Regular testing verifies operational readiness, while preventive maintenance helps avoid degradation that could impede performance.

Performance criteria are the quantifiable standards set to ensure that the SSC performs its safety function reliably and effectively. These criteria include parameters such as response times, capacity, accuracy, and environmental tolerances that the SSC must meet or exceed during normal and accident conditions. In this digital environment, each criterion would link with appropriate special treatments to verify these criteria recorded within the database. Performance evaluations verify that the SSC meets the established performance criteria through a combination of testing, inspection, monitoring, and analysis to confirm the SSC's capability to perform its designated safety function when required.

In a digital DSA, workflows and automation can be used to select and classify appropriate safety SSCs by comparing the results of PRA and dose consequence analysis with EGs. When an EG is exceeded, the system, in an iterative loop, selects different or additional SSCs flagged for safety. The workflow automation then updates the event trees affected by the designation of new safety SSCs and completes accident and dose consequence analysis to verify if the dose is below EGs. If the dose is not sufficiently below EGs, the system continues to iterate until selecting the minimal solution needed to achieve the required safety. Subsequently, the system may perform an additional DID evaluation for the design.

This functionality can also be extended to alter special treatments for those same safety SSCs. For example, the system designated as safety related or significant would update to apply the appropriate functional requirements and performance criteria, such as environmental qualification to meet natural phenomena hazard conditions, configuration management requirements, and adherence to industry codes and standards. This automation could also extend to iterative loops to determine acceptable failure probabilities for QA by completing iterative loops of analysis to reach a failure probability acceptable within an appropriate likelihood category for an accident in the PRA. Once these special treatments are denoted in the requirements database, they propagate throughout the design and supporting analyses. For example, the designation of a component as safety related or significant would trigger the appropriate performance evaluation of the component for each performance criterion, such as seismic analysis. As the engineer completes the performance evaluation analyses, they will be linked back to the performance requirement for validation.

As areas requiring administrative controls or other special considerations are identified in the design, such as emergency planning, those requirements would be added to the database and tracked through the design into the DSA. The digital DSA would then pull all the safety requirements for SSCs, special treatments, and administrative controls into the correct location, along with their corresponding supporting analyses and bases to show the derivation of hazard controls.

Each requirement in the database is marked with an appropriate V&V method, such as inspections, analysis, demonstration, or testing. As the design progresses and each SSC with special treatment is verified, an engineer would link the requirement back to a specific analysis or test result to validate the requirement, linking performance criteria and performance evaluations. This allows the requirements database to export a V&V matrix, demonstrating compliance with safety requirements that can be easily viewed by designers and regulators to verify the adequacy of the hazard controls. This matrix then automatically populates the appropriate sections of the DSA, showing the performance criteria with corresponding V&V results for performance evaluation.

2.5 Defining Special Management Program Characteristics

Special Management Programs (SMPs) are comprehensive frameworks designed to maintain the safety and reliable operation of a plant. These programs encompass QA, conduct of operations, fire protection, radiation protection, criticality, environmental management, emergency management, industrial safety, maintenance, waste management, safeguards, and security. Advanced reactors will have unique characteristics that must be incorporated into these programs. Digital engineering, particularly the integration of these programs into a database, provides a logical place to store these requirements for input into the DSA.

For example, in the conduct of operations, additional information such as testing procedures and results, surveillance requirements, and operator training and qualification can be dynamically linked to the requirements database for validation and verification. These can also be linked to the 3D model for descriptions and specifications. Components in the MEL within the PLM software can be linked to appropriate maintenance requirements, which can then be tracked for compliance and completion within the required time frames. Digital procedures would automatically pull information from requirements and geometric 3D models to update procedures as the design changes, thereby reducing human performance errors in tool development.

Another example involves QA. Information captured in testing or non-compliance reports can be input directly into the geometric 3D model, updating aspects such as material properties, dimensions, and tolerances, which then feed back into the model's database. This provides automatic updates for the QA program along with tracking those QA requirements. Any unique characteristics for QA would be stored within the specification in the PLM and requirements database for propagation through documents and into the DSA.

Typical characteristics within the DSA include lists such as combustible loading, which limits the maximum number of combustible materials in a facility. The digital ecosystem would export a complete list of materials from the design for incorporation into the fire protection system. Furthermore, digital workflows could automate the process of fire hazard analysis, similar to the safety analysis described in Section 2.2. The workflow would automatically pull the correct number of combustibles from the design into the fire hazard analysis, linking the physical location and components of a fire protection system in the 3D CAD model to show compliance. Similarly, security workflows and 3D models could be used to derive security assessments, with the requirements database storing any requirements imposed on the security programs.

During the safety analysis process, workflows would guide analysts to record specific information and requirements from accidents for integration into emergency management, criticality safety, and environmental management programs. Analyses required for radiation protection and criticality safety would automatically pull input parameters from the 3D model and PLM database, as described in Section 2.3, reducing time and cost for updating SMPs as the design changes over time.

2.6 Submittal and Review

Reviewing documentation for the approval of a reactor safety basis requires a comprehensive understanding of the DSA ontology and the digital ecosystem. Key project documentation such as the systems engineering management plan, requirements management plan, and configuration management plan provide essential information on the interactions of tools and objects within the digital ecosystem. A design review plan for projects employing a full digital ecosystem should detail how and where each type of review will be conducted, including regulatory reviews or approvals, and engagement points with regulators, such as at the PDSA and FDSA stages.

Documentation releases for regulatory reviews and transmittals can be managed using various methods enabled by the project software. Multiple PLM and requirements management tools allow for the bundling of various objects and documents into a single review release, which can be used either within the tool or exported for off-line users. Tools like Windchill and DOORS include features for compiling objects into a single review package that can be performed within the tool or exported for off-line users. By leveraging the packaging features of a PLM tool, project personnel can compile analyses, design documents, safety documentation, etc., into a review package for regulatory review. Supporting information for the review of a DSA would be included in the review package from the PLM tool, or links would be provided to the SOT for that information, such as the requirements management tool for requirements.

The advantage of using these review packages within the tool, rather than off-line, is that all information, both within and external to the review package, is available to the reviewer through the linked system. Any additional tools or links to external software, such as requirements management from PLM, can be provided to the reviewers to ensure all necessary information is accessible. Utilizing the review features within the digital ecosystem also allows reviewers to fully leverage the digital thread to trace derived information back to its source.

This digital thread also records review comments, open items, and closure of those items by combining these tools with action item tracking software. This creates a succinct engineering practice that clearly shows the regulator the design and review process, including the level of design completion. This integration also allows project management to track design status to control cost and completion.

After each cycle, the design would be locked in configuration control for regulatory approval, similar to a traditional cycle, but with an important caveat: the regulator could easily review only the changes made during the cycle, much like a redline. This approach significantly reduces the manpower needed to review a regulatory submittal, cuts down review time, and lowers review costs through a differential review versus a full analysis. V&V matrixes, as discussed in Section 2.4, would also greatly reduce regulatory review time, as automation could be used to check compliance with regulatory requirements and the completion of V&V matrixes.

3. IMPLEMENTING FRAMEWORK

The integration of these tools into a digital DSA can be implemented in phases, as illustrated in Figure 13. Phases 1-3 can be easily incorporated into the engineering process today using existing tools with minimal development. In fact, the first phase has already begun, with developers and Idaho National Lab (INL) implementing digital engineering tools into the design process, such as a requirements database, 3D models, and a PLM database. This initial stage of implementation should now focus on ensuring that all safety requirements are fully integrated into the database, including complete requirements decomposition, the addition of descriptions and metadata into 3D models to capture design details, and the storage of analyses and 3D model details in the PLM tools.

Once additional information has been integrated into existing databases, the next phase should involve developing workflows and automation for the safety analysis process. This phased approach allows for a gradual, manageable integration of digital tools, ensuring that each step builds upon the previous one and leverages existing capabilities while gradually introducing more advanced functionality.

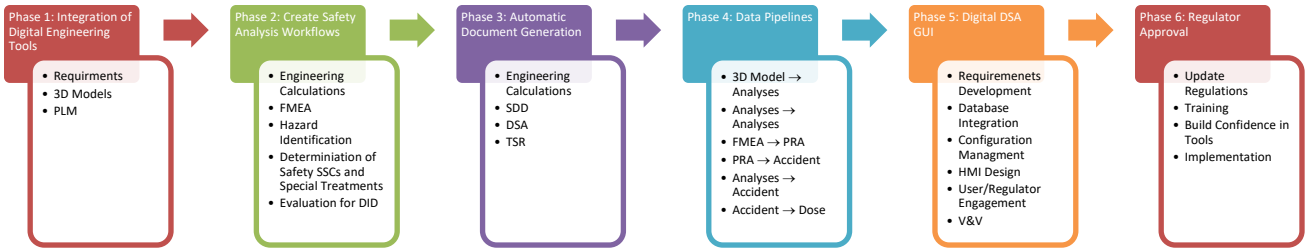

Figure 13: Implementation process for digital DSA.

The creation of safety analysis workflows should focus on automating tasks and storing information in useful databases. For example, traditional engineering calculations and FMEAs, typically completed in documents, can be transitioned to workflows with forms that ask engineers for critical aspects and store the results in a database, including attaching input and output files. Traditional “What If” analyses, DOE-HDBK-1224 hazard checklists, etc., would be automated in a workflow to identify hazards systematically. Analysts would complete checklists linked to specific components in the 3D model, navigating system by system through the design and storing results in a database. INL’s DeepLynx system can link data between these workflows and existing databases.

The focus of Phase 3 will be identifying existing software tools and AI engines that already allow automatic generation of documents from databases. This phase involves developing appropriate document templates and interconnecting data fields. For example, INL has used the DOORS requirements database to export a Code of Record and SDDs for the DOME project.

Phases 4 through 6 will require additional resources and development time. Current tools allow for some data interconnection between tools but transferring complex information such as geometries from a 3D CAD model to analytical tools (neutronics, thermal-hydraulics, or thermal-mechanical analyses) is challenging and requires many manual steps due to the unique requirements of each tool. Developing tools and scripts to integrate with 3D CAD software will be necessary, simplifying the geometry and converting it into appropriate combinatorial geometry or simplified meshes for analytical tools. Additionally, tools to transfer data from FMEA to PRA need to be developed.

Phase 5 will require software development for a DSA graphical user interface (GUI). Stakeholders, including safety analysts, engineers, operators, and regulators, should outline the desired functionalities, performance criteria, security needs, and regulatory considerations. Database integration is crucial to ensuring the GUI has access to necessary data, with attention to data integrity, privacy, and efficiency. Collaboration with regulators is essential to establish configuration management processes, including data retention and approval requirements. The human-machine interface (HMI) design should focus on creating a user-friendly and intuitive interface, considering ergonomic factors and user experience. Continuous user and regulator engagement is vital for gathering feedback and ensuring compliance with relevant regulations. To make it ready for deployment, the system should undergo rigorous V&V in accordance with NQA-1 requirements to ensure reliability under all anticipated conditions. This comprehensive approach ensures a robust, compliant, and user-centric software development lifecycle for a DSA GUI, which should be piloted with a future reactor demonstration at INL.

Updating regulations may require time, so identifying affected regulations and starting discussions with regulators to outline acceptable solutions is crucial during the initial phases. After completing an initial pilot digital DSA and proposing necessary updates to regulations, the focus should shift to training regulators and users on the new tools and developing updated procedures. Once this training and development are complete, confidence in the new digital ecosystem must be established. In the transition, comparison between the digital DSA and a traditional documented DSA may be required to instill confidence and show the significant improvements. Once confidence in the digital ecosystem and the updates to the required regulations are approved the digital DSA process can be fully implemented for use.

This phased approach ensures a gradual, manageable integration of digital tools, ensuring each step builds upon the previous one and leverages existing capabilities while incrementally introducing more advanced functionalities.

4. CHANGES TO DOE REQUIREMENTS

Transitioning to a digital ecosystem for documentation, design, and licensing represents a paradigm shift. To fully realize the benefits of this transition, commitments will be required from the DOE in their regulatory role. These commitments include process acceptance, training and ecosystem understanding, and assistance in meeting cybersecurity obligations.

4.1.1 Acceptance of Digital Documentation

The current PDF transmittal-based approach to licensing and safety reviews may need alteration to enable the use of digital design tools. These dynamic tools can create traditional PDF document transmittals more efficiently than traditional methods due to the efficiencies gained through the digital ecosystem. While simply moving to a dynamic tool environment will benefit document preparation, regulatory review within the digital ecosystem presents the highest degree of efficiency gains. To fully leverage the digital ecosystem, including in-ecosystem reviews and approvals, the regulator must accept the process, and move away from traditional PDF reviews.

The path to the ideal end state of a fully digital ecosystem may require a staged approach to automation and dynamic object usage. The extent to which automatic updates and dynamic object propagation are acceptable will need to be agreed upon by DOE. Successive levels of automation may be implemented in a pilot program, allowing DOE to gain experience with automatic documentation and to identify, understand, and mitigate any implied risks by removing certain human actions from the ecosystem. The degree of automation and the necessary human interactions within the loop must be identified and agreed upon before implementing the digital ecosystem.

Moving further away from traditional documents will require a concerted effort between system designers and the DOE to understand DOE needs and requirements for the digital DSA and its GUI interface. Early engagement with the DOE to understand their preferred way of navigating through content and reviewing information will help create a more user-friendly tool that has a higher likelihood of being acceptable to regulators.

By fostering collaboration and clear communication between system designers and the DOE, the digital ecosystem can be tailored to meet regulatory needs while enhancing efficiency and reducing errors. This approach ensures that the transition to a digital environment is smooth, effective, and widely accepted.

4.1.2 Design/Documentation Process Understanding

Using enhanced documentation capabilities in a digital ecosystem will require additional education and training for developers, regulators, and reviewers. As part of the project, comprehensive SEMP, RMP, and CMP must be developed for use with the project's Project Management and Project Execution Plans. This suite of design documentation will help inform project personnel and regulatory reviewers about the tools used, and their purposes and interactions in design and licensing. These plans help form the foundation of design data interactions and their controls, which can be effectively communicated to reviewers.

By ensuring that all stakeholders understand the digital tools and their applications, the project can maintain clarity and consistency in the design and review processes, facilitating a smoother transition to the digital ecosystem.

4.1.3 Training

Full commitment to addressing issues of streamlining the licensing process will require additional training commitments by the DOE for reviewers. The level of additional reviewer training will depend on the tools used within a digital ecosystem since each one tool would require some level of familiarity to use or review information. Provision of reviewer aids and training will be required to enable licensing reviewers to easily navigate the digital ecosystem. For initial projects, this may come in the form of a training plan from the project design or project

Management groups. It is unlikely that all project budgets will include allowances for training of regulatory personnel. DOE will need to ensure regulators and reviewers are trained on common software and services used within digital ecosystems. Although this requires additional upfront cost for training of DOE personnel, the reduced review time from these tools will reduce the overall cost.

4.1.4 Cybersecurity Acceptance

DOE is concerned with the cybersecurity and vulnerability of services and software for nuclear information and facilities. The DOE Cybersecurity Strategy identifies the adoption and improvement of digital documentation and software as a departmental goal. While DOE recognizes cybersecurity for integrated data and cloud systems as a concern, it is also a priority and an identified area for improvement. The requirements for cloud software to be compliant with FedRAMP presents a significant burden on the development, procurement, and usage of cloud software systems.

Advancement of federal and industry cooperation for FedRAMP approval and DOE buy-in is crucial for the digital transformation of the safety process. The current FedRAMP approval process is lengthy and costly for businesses since it takes several months to years to achieve and hundreds of thousands of dollars or more for cloud service providers. Streamlining this process will enable industry partners and service providers to approve and utilize additional cloud services in a timely and cost-effective manner. Software availability increases the opportunities for companies and the DOE to collaborate in digital ecosystems and enhances interconnectivity between design and regulation.

5. CONCLUSION AND FUTURE DEVELOPMENT

5.1 Future Development

In future project phases, accessed through a GUI interconnected with a digital twin and engineering tools, the digital DSA would create a dynamic environment where users can explore hazard and accident analyses, navigate the plant in 3D, and select SSCs to view detailed descriptions, analyses, and interfaces. The GUI would feature a dashboard-like home page for quick access to modules such as 3D model visualization, hazard and accident analysis, safety requirements, validation matrices, and analyses. Each module would be represented by clear, descriptive icons or tiles, allowing users to recognize and access desired functionalities with minimal clicks. The 3D model navigation module would offer a responsive and detailed viewer, equipped with tools for zooming, panning, rotating, and isolating specific components or layers of the model. Users could click on individual elements within the 3D models to access linked metadata, source documents, and related analyses, with an interactive timeline or version history feature to view the evolution of design changes over time.

The DSA GUI would emphasize a user-centric design catering to varying levels of technical expertise, incorporating an onboarding tutorial, tooltips, and contextual help to facilitate quick learning and ease of use. A search bar with predictive text and NLP capabilities would allow users to input queries in everyday language and locate information swiftly from within the DSA. To ensure a seamless HMI, the system would adapt to different user roles and permissions, providing customized views that highlight relevant data and tools tailored to the user's job function. For instance, regulators can use a V&V matrix to see the interconnections between key regulatory requirements and supporting design and analyses. They can click a link to access all related requirements, view the SSCs in the 3D model, see component specifications and P&IDs, navigate to supporting analyses, and review quality reports to understand the system's compliance with regulations.

For a nuclear safety analyst, the GUI would streamline navigation through hazard and accident analysis, allowing quick access to information, especially when reviewing design changes and following the USQ process for the DOE or the 10 CFR 50.59 process for the NRC. This review process for changes can be conducted through a workflow that guides analysts through the appropriate USQ/50.59 steps, dynamically pulling engineering information to expedite determinations. Fully leveraging digital tools in the development of DSAs for future nuclear facilities and advanced nuclear technologies is crucial. The INL digital engineering team is focused on establishing APIs to ensure consistency across the digital thread, facilitating integration between PLM systems like Windchill, requirements databases like DOORS, and 3D modeling tools like CREO. These API connections should be streamlined to maximize efficiency and minimize technical debt, reducing system maintenance and error rates.

The greatest benefit of digital engineering tools is the creation of an SOT and an informed change management process throughout engineering design activities by linking artifacts within various databases. For example, an impact notification system within the PLM can identify downstream impacts from changes, supporting real-time collaboration across all engineering disciplines. This approach prevents the formation of discipline-specific silos, ensuring analyses are informed by shared information. Real-time collaboration and artifact management automation significantly enhance the efficiency and accuracy of the engineering process. Committing to the use of digital tools is essential to ensure universal consistency and access throughout the development and review process. Adopting a consistent ontology for relationship building between databases, developing input and output forms, or conversion software, and enhancing user interfaces for both review and development processes are critical steps. AI-based language models like ChatGPT, LaMDA, or Gemini, or developing GUIs similar to websites or encyclopedias, are potential solutions. Evaluating and obtaining necessary approvals for software and cloud services via the FedRAMP process will also be required.

Applications of AI or ML models could significantly benefit the generation and management of project documentation. An ML model could ingest text into the project database, enabling rapid identification of objects, parameters, and relationships. Conversely, these models can generate information from project objects, parameters, and relationships for the project ontology. Currently, ML models are primarily applied to generating ontologies from text. Further efforts are needed to generate text from objects stored in an ontological database to achieve full functionality. Additionally, developing the use of named entities for subsequent analyses, system descriptions, and safety documentation can create digital threads. Objects from the database would be inserted into text and related according to the project’s ontology, allowing software to understand and generate sentences that describe objects, their parameters, and their relationships. This ontology-based text-to-object linking in documents enables the creation of dynamic documents written in natural language, easily understood by project personnel and software alike. Further development is needed to refine tools for geometry simplification, mesh

extrapolation, and surface/shape extraction for downstream analysis tools. Digital twins of nuclear facilities are an emerging technology with many benefits for design, licensing, construction, operation, and decommissioning, but further research is needed to achieve commercial adoption of digital twins in nuclear reactor operation.

5.2 Conclusion

The application of digital tools to the engineering design and development of DSAs offers significant opportunities for cost and risk reduction compared to the status quo. Digital tools enable more efficient design and development through the automation and integration of data and through real time collaboration. These are the key reasons digital tools are advantageous for this application:

1. **Enhanced collaboration and communication:** Digital tools facilitate real time collaboration among engineering disciplines, breaking down siloed analyses and ensuring all team members have access to the latest information. Relying on information stored within the tools instead of printed to static documents reduces miscommunications and errors that arise from outdated or incomplete data. This allows agency reviewers the opportunity to review information or data from the latest release.

2. **Single source of truth:** By integrating various databases through a digital thread and creating a single SOT, digital tools ensure consistency and accuracy across the project and the review stages. Identifying and using an SOT maintains consistency and accuracy between information used throughout the project. This reduces the risk of discrepancies and the need for rework, which can be costly and time-consuming for both the design team and the reviewing agency.

3. **Improved change management:** Various digital tools provide an automated change management process, providing impact analysis and notifications for linked artifacts. Additionally, interfaces for tools that do not have inherent change management can be achieved via APIs. This aids the project team in making informed decisions quickly and reduces the risk of unintended consequences.

4. **Automation of routine tasks:** Many existing repetitive or routine tasks can be automated using digital tools, freeing up the design team to focus on more complex and value-added activities. This reduces the labor demand for typical project activities such as document generation for reviews and eliminates the potential for transcription errors.

5. **Enhanced data analysis and decision making:** Advanced digital tools provide powerful data analysis capabilities, allowing for better decision-making based on comprehensive and accurate data. Documentation of project decisions and requirements that are accessible in analyses allows identifying where changes can be made and why.

6. **Reduced development time:** Digital tools streamline the design and development processes. This will impact the development time necessary for the DSA, with real impacts of reducing the time required to bring a project from concept to completion. This not only cuts costs but also accelerates the development of the advanced reactor technologies with the DSA.

7. **Risk mitigation:** Digital risk management tools may be directly applied throughout the design process creating artifacts linked directly to requirements, schedule milestones, or impacts to construction, operations, and maintenance activities. The early identification of these risks and the mitigation plans applied to them further enhance the collaboration within the design team and inform the reviewers of the methodologies employed throughout each design phase.

8. **Consistency and standardization:** Digital tools enforce consistent methodologies and standards across projects, which reduces variability and ensures that all SSCs meet the required specifications. This applies to both the design of the project and the review activities undertaken. The reviewing agency would become experienced in the review procedures and processes required for the application of a digital DSA resulting in quicker, more effective design reviews.

In contrast, traditional tools used for both the engineering design and review processes require manual generation and configuration, which are prone to human error, inefficiencies, and inconsistencies. They also lack the integration and real-time capabilities of digital tools, leading to slower response and review times and higher risks of project overruns, missed deadlines, and failures. Overall, the adoption of digital tools in the development of engineering projects requiring DOE authorization reviews leads to more efficient, accurate, and cost-effective outcomes.

6. REFERENCES

General Electric. (2024). Industrial Digital Twins: Real Products Driving $1B in Loss Avoidance. https://www.ge.com/digital/blog/industrial-digital-twins-real-products-driving-1b-loss-avoidance. [Accessed May 25, 2024.]

Ritter, C., Rhodes, M., 2023, September. Incorporating Digital Twins In Early Research and Development of Megaprojects To Reduce Cost and Schedule Risk. INCOSE Insight., vol. 26, issue 3.

Stewart, R., Shields, A., Pope, C., Darrington, J., Wilsdon, K., Bays, S., Heaps, K., Scott, J., Reyes, G., Schanfein, M. and Trevino, E., 2023, May. A digital twin of the AGN-201 reactor to simulate nuclear proliferation. In Proceedings of the INMM/ESARDA 2023 Joint Annual Meeting.

Baviskar, D., Ahirrao, S., Potdar,V., Kotecha, K., 2021, Efficient Automated Processing of the Unstructured Documents Using Artificial Intelligence: A Systematic Literature Review and Future Directions. In IEEE Access, vol. 9, pp. 72894-72936.

Mandelli, D., Wang, C., Cogliati, J., Agarwal, V., 2023, Data Fusion of Numerical and Textual Equipment Reliability Data: A Knowledge-Graph-based Approach. In Proceedings of the Probabilistic Safety Assessment and Management (PSAM) 2023 Topical Conference.

Yadav, V., Wells, A., Pope, C., Andrus, J., Chwasz, C, Trask, T., Eskins, D., Carlson, J., Ulmer, C., Chandran, N., and Iyengar, R., 2022, Regulatory Considerations for Nuclear Energy Applications of Digital Twin Technologies. Idaho National Laboratory Technical Report INL/RPT-22-68124.

[1] INL/RPT-23-72206, “Recommendation to Improve the Nuclear Regulatory Commission Reactor Licensing and Approval Process.” April 2023. Idaho National Laboratory.

[2] 10 CFR 830.3, “Nuclear Safety Management.”

[3] RG 1.70 “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants.” Nuclear Regulatory Commission.

[4] NUREG-1537 “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors.” Nuclear Regulatory Commission.

[5] DOE-STD-3009, “Preparation of Nonreactor Nuclear Facility Documented Safety Analysis.” Department of Energy.

[6] NEI 18-04, “Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development.” Nuclear Energy Institute. 2018.

[7] NEI 21-07, “Technology Inclusive Guidance for Non-Light Water Reactors.” Nuclear Energy Institute. 2021.

[8] DOE O 413.3B, “Program and Project Management for the Acquisition of Capital Assets.” Department of Energy.

[9] DOE-STD-1189, “Integration of Safety into the Design Process.” Department of Energy.

[10] DOE O 420.1C, “Facility Safety.” Department of Energy.