

STANDARDS RESEARCH

Emerging Digital Technologies Within the Canadian Nuclear Industry

February 2023

Authors

Sean Donnelly, P. Eng., Kinectrics

Shawn MacIntosh, P. Eng, Kinectrics

Alastair McIvor, B. Eng, Kinectrics

Matthew Medri, Kinectrics

Rex Lam, P.Eng, M.A.Sc., Kinectrics

Patricia Lung, P. Eng, GSEC, Kinectrics

Project Advisory Panel

Chris Cochrane, Canadian Nuclear Safety Commission

Dominique Lachance, Bruce Power

Ernest Mileta, Ontario Power Generation Inc.

Herb Thompson, NB Power Nuclear Corporation

John de Grosbois, CANDU Owners Group

Dragica Jeremic Nikolic, CSA Group, Research Manager

Larisa Logan, CSA Group, Director

Mervah Khan, CSA Group, Strategic Initiatives Manager

Cherie Zou, CSA Group, Project Manager

Disclaimer

This work has been produced by Kinectrics and is owned by Canadian Standards Association. It is designed to provide general information in regards to the subject matter covered. The views expressed in this publication are those of the authors. Kinectrics and Canadian Standards Association are not responsible for any loss or damage which might occur as a result of your reliance or use of the content in this publication.

Table of Contents

Executive Summary 5

1 Introduction 6

1.1 Report Objectives 6

2 Methodology 7

3 Findings 8

3.1 Emerging Digital Technologies in the Nuclear Industry: Background and Example Use Cases 8

3.1.1 Advanced Analytical Methods 9

3.1.2 Plant Information Models 11

3.1.3 Augmented Reality and Virtual Reality 13

3.1.4 Advanced Condition Monitoring 15

3.1.5 Cloud Computing 15

3.2 Key Software Types 16

3.2.1 Real-Time and Process Control Systems and Software 16

3.2.2 Analytical Software 17

3.2.3 Operational Technology Systems and Software 17

3.2.4 Administrative Safety Software 17

3.2.5 Management System Software 18

3.3 Standards and Sections Relevant to Emerging Digital Technologies 18

3.3.1 Real-Time and Process Control Systems and Software 18

3.3.2 Analytical Software 18

3.3.3 Operational Technology Systems and Software 20

3.3.4 Administrative Safety Software 20

3.3.5 Management System Software 20

3.3.6 Generally Applicable Requirements 21

3.4 Concerns and Underlying Assumptions Related to Emerging Digital Technologies 21
3.4.1 Advanced Analytical Methods 21
3.4.2 Plant Information Models 25
3.4.3 Augmented Reality and Virtual Reality 28
3.4.4 Advanced Condition Monitoring 28
3.4.5 Cloud Computing 29

4 Conclusions 31
4.1 Advanced Analytical Methods 32
4.2 Plant Information Models 32
4.3 Augmented Reality and Virtual Reality 32
4.4 Advanced Condition Monitoring 32
4.5 Cloud Computing 33
4.6 Generally ApplicableFindings 33

References 34

Appendix A: Key Figures 43

Appendix B: Resources and Definitions 47
B.1 CSA Nuclear Standards 47
B.2 Emerging Technologies Literature Search Criteria and Categorization 48
B.3 Definitions, Acronyms, and Initialisms 49
B.3.1 Definitions 49
B.3.2 Acronyms and Initialisms 53
B.4 Active Standards in CSA N285, N286, and N290 Series 54

Appendix C: Detailed Software Assessment Results 56

Executive Summary

There has been rapid development and use of emerging digital technologies in the Canadian nuclear industry. In this report, emerging digital technologies refers to the use or adoption of existing or emerging digital technologies for lifecycle activities of nuclear facilities. There is a need to provide a common understanding of the different types of emerging digital technologies in the Canadian nuclear sector and how they may be used and categorized based on application context. There is also a need to identify any existing assumptions that could differ for the implementation of emerging digital technologies so the current suite of CSA nuclear standards can be assessed and updated as needed to be fit for purpose.

The research conducted for this report included a literature review to provide an overview of the current emerging digital technologies landscape in the Canadian nuclear industry. Example use cases in the nuclear industry were outlined for the following five areas of interest:

1. Advanced analytical (AA) methods;
2. Plant information models (PIMs);
3. Augmented reality (AR) and virtual reality (VR);
4. Advanced condition monitoring (ACM); and
5. Cloud computing.

A review of key software categories in relation to existing CSA nuclear standards was also conducted to map the overlap of emerging digital technologies and the software categories within existing applicable standards. This included gathering inputs from members of relevant CSA nuclear program technical committees and from subject matter experts from across the nuclear industry. Input was also gathered on the key sections of standards pertaining to each software category's interface with emerging digital technology, potential gaps in those interfaces, and methods to address those gaps. Lastly, information was gathered on risks associated with the emerging technologies, and potential changes in assumptions and underlying workflows as a result of technology adoption. This information was gathered through the use of focus groups and through surveys sent to industry experts and technical committee members.

The following key findings were identified through this research:

1. Further requirements are recommended for the handling of static and dynamic AA models within analytical and operational technology (OT) software, including real-time and process control (RTPC) software;
2. Clarification is needed on the governing standards and requirements pertaining to the use of information in a PIM for support of operational decision-making;
3. Reference to standards regarding the development and use of AR and VR applications may help to ensure that verification and human factor considerations are adequately addressed; and
4. Clarification of the categorization of AA model development software dependent on its use in either a static or dynamic model may facilitate the interpretation of requirements for the development of AA-based software.



"There has been rapid development and use of emerging digital technologies in the Canadian nuclear industry."

1 Introduction

There has been rapid development and use of emerging digital technologies in the Canadian nuclear industry. In this report, emerging digital technologies refers to the use or adoption of existing or emerging digital technologies for lifecycle activities of nuclear facilities. Specific areas of interest include:

1. Advanced analytical (AA) methods, such as artificial intelligence (AI) and its subset, machine learning (ML);
2. Plant information models (PIMs), such as building information modelling (BIM) and digital twins (DT);
3. Augmented reality (AR) and virtual reality (VR);
4. Advanced condition monitoring (ACM), such as model-based diagnostics and decision support systems, and associated predictive toolsets; and
5. Cloud-based computing and analysis systems.

There is a need to provide a common understanding of the different types of emerging digital technologies in the Canadian nuclear sector and how they are used and categorized based on application context. There is also a need to identify any existing assumptions that could differ for the implementation of emerging digital technologies so the current suite of CSA nuclear standards can be assessed and updated as needed to be fit for purpose.

1.1 Report Objectives

This report summarizes types of emerging digital technologies and provides examples of how they are currently being used or could be used in the Canadian nuclear industry. For example, digital technologies may have unique and complex failure modes resulting from hardware and software design attributes and their interaction in a specific application context. The primary focus of this report is on applications of digital technologies in nuclear facility design, operation, and maintenance because these phases typically include the most safety-related or mission critical aspects of the organization or facility lifecycle.

To support the mapping of emerging technologies and associated system and software types to applicable codes and standards, this document provides a high-level summary of the following system and software types:

1. Real-time and process control (RTPC) systems (industrial plant safety, control, monitoring, and display systems);
2. Analysis (scientific, engineering, and safety) and design software;
3. Software and systems used to support management system requirements not included in items **1** and **2** (e.g., operational technology [OT] software or administrative safety software); and
4. Other software and systems that are not expected to have any direct or indirect safety, compliance, or plant reliability impact due to failure or misuse.

Relevant existing standards used or applicable in Canada (e.g., CSA nuclear standards, international standards used by the Canadian nuclear industry) are presented for the system and software types listed above, and gaps in these current standards pertaining to the use of emerging digital technologies are identified. Other codes, standards, and industry best practices that could be used or referenced in Canada to address these gaps are also evaluated. Finally, a comparison and assessment of the differences in the underlying assumptions associated with the use of traditional technologies versus digital technologies is provided.

The key objectives of this research report are to:

1. Provide an overview of the current emerging digital technologies landscape in the Canadian nuclear industry;
2. Map technology types and related system and software types to existing codes, standards, and industry practices;
3. Identify any related gaps and topics in standards that could be impacted by the implementation of emerging digital technologies; and
4. Assess the underlying assumptions in existing standards that could differ with the implementation of emerging digital technologies compared to traditional technologies and work methods.

2 Methodology

To provide an overview of the current emerging digital technologies landscape in the Canadian nuclear industry, a literature review of the following sources was performed:

1. News articles, press releases, and operating experience (OPEX) searches on key players in the Canadian nuclear industry, including the Canadian Standards Association (CSA), International Atomic Energy Agency (IAEA), Nuclear Energy Agency (NEA), Electric Power Research Institute (EPRI), CANDU Owners Group (COG), World Association of Nuclear Operators (WANO), and Reuters Events;
2. White papers on the digitalization of power generation utilities (e.g., McKinsey, PwC, and Deloitte);
3. Journal articles on the digitalization of power generation utilities; and
4. Past conferences, such as Canadian Nuclear Society (CNS) innovation conferences and the IAEA Artificial Intelligence (AI) for Nuclear Technology and Applications Technical Meeting.

Documents from each of these sources were recovered using the source locations and search terms provided in Appendix B:, Section 1B.2 (Table 1).

The results of the literature review were compiled into a summary of the five emerging digital technology types identified in Section 1, along with a description of example applications in the Canadian nuclear industry. The examples center on applications within nuclear design, operation, and maintenance, which are the phases that typically include the most safety-related or mission critical aspects of the organization or facility lifecycle. Key examples relevant to other lifecycle phases were also summarized. Example use cases were categorized into one of the following application areas:

1. Design, including defence in depth and cyber/physical security;
2. Safety analysis, including maintenance of the safe operating envelope, management of plant risk, and reliability analysis;
3. Facility operations, including detection of abnormal operating states;
4. Plant health monitoring and inspections, including detection of process failures, fitness-for-service assessments, and long-term asset/aging management; and
5. Training and human/organizational performance.

A review of CSA standards that include software provisions was conducted to provide a high-level summary of the software types present within the existing suite of standards, or otherwise evident within industry, with a primary focus on CSA N286.7, *Quality assurance of analytical, scientific and design computer programs* [1], CSA N290.14, *Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants* [2], and the CSA N299 series, Quality assurance program requirements for the supply of items and services for

nuclear power plants [3], [4], [5], [6]. ASME NQA-1, Quality assurance requirements for nuclear facility applications [7], was also included in this review.

Industry experts and technical committee members for relevant codes and standards were consulted to provide input on which sections of the standards bear potential relevance to emerging digital technologies. Expert input was gathered through the distribution of questionnaires, requests for input by email, and through interviews and focus group sessions.

To gather additional input, experts from a variety of organizations, including Bruce Power, New Brunswick Power, Ontario Power Generation, COG, and the Canadian Nuclear Safety Commission (CNSC), were invited to complete questionnaires. The questionnaires were created to solicit input on areas of potential risk, areas of ambiguity, key issues with implementation, changes to workflows, potential gaps in the existing standards, and areas of uncertainty relating to emerging digital technologies. The questions provided example cases and included long-form answers where appropriate so participants could elaborate on potential issues, which ensured that additional key information was adequately captured. To increase the response rate, different questionnaires were distributed to members of relevant technical committees for the standards within the scope of the document, and to general industry experts.

To ensure that adequate knowledge of the technologies under review and the relevant interfacing standards was present, focus groups included members of technical committees as well as subject matter experts for relevant technologies, such as BIM, AA methods and ML, and laser scanning. The focus groups were guided using examples and questions that were aligned with the questionnaires or that were received as input from the questionnaires. Notes for each focus group were taken, and a summary of the key discussion points and conclusions was distributed for comment at the end of each focus group to ensure that the notes aligned with the participants' experience. Follow-up sessions were conducted as necessary to seek clarification on any key points and to hold additional discussions to expand on key points that could impact the workflows being reviewed.

3 Findings

3.1 Emerging Digital Technologies in the Nuclear Industry: Background and Example Use Cases

With advancements in the capability and affordability of computational systems and further development of software to take advantage of increased computational power, new software tools are emerging that show promise for application within the nuclear industry. In parallel, continuous increases in the connectivity of devices and systems has allowed for access to large amounts of processing power and digital storage on an as-needed basis, without the upfront costs of purchasing hardware, thus reducing the entry cost for application of new emerging software tools. With the wider availability of these tools and the lowered cost of entry, software techniques and use cases that have not previously been considered within existing codes and standards are now becoming feasible. These emerging technologies can be divided into the following broad categories:

1. AA methods such as AI and its subset, ML;
2. PIMs, such as BIM and DTs;
3. AR and VR;
4. ACM, such as model-based diagnostics and decision support systems, and associated predictive toolsets; and
5. Cloud-based computing/analysis systems.

Descriptions of each of these categories, as well as example use cases within the nuclear industry compared to more traditional methods, are provided in sections 3.1.1 through 3.1.5.

3.1.1 Advanced Analytical Methods

AA methods is an overarching term that refers to a variety of analytical techniques used to gather and process complex data into results that are easily interpreted and communicated in an autonomous or semi-autonomous fashion [8]. The term typically encompasses AI and its subset, ML, as well as descriptive analytics and predictive analytics. AA methods are typically applied to problems where the



"With advancements in the capability and affordability of computational systems and further development of software to take advantage of increased computational power, new software tools are emerging that show promise for application within the nuclear industry."

outputs are qualitative and difficult to define quantitatively within human programmed computer language. Example output types include determination of sentence meaning, [9], determination of road signs type based on visual input, the presence of flaws in a weld based on picture data [10], indications of flaws based on ultrasonic test data [11], or identification of misalignment in vibration data [12].

One commonly encountered example of ML is optical character recognition (OCR) through supervised ML, which allows computers to recognize written characters in image files and translate them into digitally encoded text data. At a high level, the process that allows a computer to recognize and differentiate between characters of various typefaces involves developing a system comprised of given image files, using each pixel as an input value, that is able to translate the set of pixel values from each image into a decision regarding which character value is most likely being depicted. These ML models are not programmed manually, but are instead given a large set of input data for which the correct answer to each input is known. This process is known as supervised learning. The input data and labels are training data. The model is then "trained" by changing factors within the model based on how closely the model predicts the correct answers for the entire set of data. This process is repeated until the model's performance either meets acceptable criteria or ceases to change by a meaningful amount.

Due to the large volume of labelled data required to train an AA model using ML, and the large number of iterations required to tune the weights and measures within the machine model, the process is computationally intensive, with significant hardware and power requirements to achieve results within a reasonable timeframe [13]. Progress has been made in this area through the development of hardware purpose-built for the training of ML models. These devices aim to greatly reduce the power requirements of ML model training by finding more energy efficient methods of conducting the operations common to ML models while maintaining data integrity [13], [14].

AA methods related to ML differ from traditional methods in several key areas. The tuning of these models is automated by a training algorithm that tests and modifies the model against available data. Consequently, the internal methodology used by the model to make decisions may lack definition to the developers. Further complicating this issue, the size and complexity of the mathematical models that emerge from this training process are such that it is not feasible for each of the relations to be reviewed and explained. The opacity of the mathematical models produced through AI methodology is referred to as a "black box" and remains one of the primary impediments to the application of AA methods. Additionally, in contrast to models and calculations developed from first principles, ML models are partially or entirely stochastic, similar to regression models, and thus are not always bound by agreed upon axioms or

physical laws, leading to a lack of clarity around performance limitations [15], [16]. Most ML algorithms are stochastic in nature because they make use of randomness during optimization and learning. As a result, the trained model could differ after each run, even if it is trained on the same data.

Another issue encountered across all trained ML or AI models is the introduction of bias in model decisions due to the training data provided to tune the model's performance. Here, care must be taken to ensure the training data is of sufficient quality so the model performance in the real world will match the model performance with the training data.

Unlike typical analytical methods, a subset of analytical models that are designed to continuously adjust their performance based on comparison to output data may not be static in their performance. While ML models may be trained once and remain static afterwards, they may also be continuously self-adjusting based on comparison of predicted response and measured response from the system with which the model is interacting. In this case, bounding the model performance may not be easily achievable, because the model parameters cannot be kept static. Increased automation also reduces direct involvement of staff in performing the analysis, reducing familiarity with the analysis, and increasing the likelihood of erroneous results that remain undetected by human analysts.

3.1.1.1 Design and Security Use Cases

AI has the potential to shorten the design cycle duration for both modification and new product design because neural network technologies, a form of ML, have the potential to assist designers in solving complex problems [17], which can reduce the overall cost of research and development. AI can be implemented at various stages of the design engineering process of nuclear facilities, such as nuclear power plants, and has already been applied in the digitization of documents using OCR software to make scans of paper drawings text searchable, automate replication mark-up work, and automatically place stamps across large batches of drawings [18]. Furthermore, the use of ML software for natural language processing, a subset of ML that allows software to assign and parse the meaning of spoken or written language, has potential to improve the efficiency of research, summarization, and collation of key data during the design phase.

In addition to assisting in the creation and alteration of documentation, AI has been proposed for use in design calculations, with applications ranging from optimization of material usage in components based on expected forces in design application to modelling of flow-induced corrosion rates. Several examples have been proposed in recent literature, including calculation of critical mass flow for compressible fluids [19]. In one example, an artificial neural network was used together with Marviken experimental data to produce a model that calculated critical mass flow in piping systems. While this model showed potential to be more accurate than traditional methods, the complexity of the resultant mathematic expressions made it difficult to connect the model to the underlying physical phenomena.

The use of AI-based object recognition has also shown potential for application in the security of nuclear facilities. The proposed primary use case is AI-based monitoring of surveillance videos and imagery for potential incursions, allowing for increased productivity of security personnel [20]. Beyond physical security of facilities, the use of ML has also been proposed as a method for detecting cyber security vulnerabilities and filtering emails to reduce risks posed by phishing and other malicious content [17].

3.1.1.2 Safety Analysis and Operational Use Cases

In the context of nuclear power plant operations, there are several AA use cases with potential to increase safety or reduce cost. For example, many small modular reactor (SMR) developers have plans to incorporate not only remote monitoring but also remote control of the nuclear facility, so a comparatively low number of operators are required to be physically present at the SMR. Some of these SMR developers also intend to incorporate automated functions as a part of the RTPC system, so a large portion of system control will be handled by digitized instrumentation and control (I&C) systems, which include AA methods to provide decision support to operators [21]. Furthermore, the use of AI to monitor operators for fatigue and distraction has also been proposed as a safety measure [22].

The use of natural language processing creates the potential to quickly collect, summarize, and disseminate key information from multiple OPEX sources to inform maintenance requirements, corrective action programs, and OPEX reports.

AI can also provide input on potential equipment degradation or failure, and has been proposed for use in the monitoring of equipment health data to enable early indication of system failures for operators, reducing unplanned downtime [23], [24].

3.1.1.3 Plant Health Monitoring and Inspection Use Cases

The ability to learn from example data instead of explicit model definition has made ML particularly applicable to inspection use cases, because the software can be trained to identify flaws automatically based on a variety of labelled input data. Identification of flaws, defects, or performance degradation is possible in several inspection scenarios [11], [25]. In particular, non-destructive evaluation (NDE) can leverage AI in three key areas: automated analysis of NDE inspection results, analysis of real-time NDE monitoring, and informing inspection planning through assessment of NDE history [26].

EPRI has been working to develop automated systems for the detection of cracks in steel nuclear vessels and has demonstrated significant success using convolutional neural networks to analyze data. This approach has been extended to multiple other NDE inspection techniques, including visual inspection of reactor internals, ultrasonic examination of reactor components, and eddy current data from heat exchanger tubing inspections [11].

EPRI's Nuclear Maintenance Applications Center performed a proof of concept study using ML to assist in vibration analysis. The ML model was trained on synthetic vibration data exhibiting patterns indicative of parallel misalignment of coupled rotating equipment. When applied to vibration data from existing equipment, the ML algorithm was able to identify parallel misalignment in 13 of the 16 real vibration datasets. This ML-assisted vibration analysis could be applied to existing vibration analytical software to advance fault identification capabilities [12].

In combination with the digitization of I&C systems, AA methods have been proposed to reduce the burden of inspections on personnel. AI could be used to analyze data made available by digital instrumentation, surveillance, or control systems, and to compare the online plant data with reference data to provide early indication of performance degradation or equipment failure [12].

The applications of AA methods to inspection and maintenance are not limited to analysis of NDE data. AA methods have also demonstrated capability in predicting flow-accelerated corrosion scalloping in piping. In studies conducted by the UNB Nuclear Group, various statistical models, such as linear regression, decision tree, and random forest, were tested for their fitness against known corrosion data [27].

3.1.2 Plant Information Models

PIMs, or integrated asset models, allow for detailed multifaceted modelling of a physical asset in a digital environment. These are typically computer models of a facility or process that are maintained and updated based on real-world data to allow for management of current and historical data related to asset configuration, location, input requirements, and performance [28], [21].

PIMs can take several forms, depending on the data being used and maintained within the model. They may encompass point cloud data and 3D scans of an asset, equipment locations, links to equipment documentation (e.g., catalogue ID numbers, inspection reports), links to engineering data (e.g., design temperature and pressure for equipment attached to systems), records of modification history, and links to real-time process data.

This research considered two key categories of PIMs, namely BIM and DTs. BIM is the digital representation of physical and functional characteristics of a facility [21], [28], [29]. It serves as a shared knowledge resource for information about a facility, providing a reliable basis for decisions during its lifecycle. A DT is a virtual representation that serves as the real-time digital counterpart of a physical object or process [30]. Within the literature reviewed, DTs are typically connected to the process or component that they seek to replicate, continuously collecting information from the

asset to keep the digital copy of the process aligned with the physical asset [30]. DTs may also be paired with predictive tool sets to model system response to potential changes [29], [30]. These counterparts can range from a 3D model of an object to a software model of an industrial process or assembly line. BIM systems may incorporate DTs as part of the data they contain, in addition to non-process data [31].

There are a number of considerations with respect to the implementation and use of both BIM and DT technology in the nuclear industry. The primary concern for BIM is that, given its potential application to replace current asset and configuration management systems, it will form the design basis of the facility that it serves, and will thus require adequate control and approval processes to maintain data integrity and security. Group-based access controls, data check-out processes, review workflows, approval workflows, process hand-off requirements, and version control are all available features in commercially available BIM systems. In this regard, the management of data within a BIM system does not differ greatly from the management of data in another digital record or configuration management system. However, the combination of the vast majority of a facility's design documentation, procedures, and plant configuration information into a single point of access does raise concerns regarding the potential consequences of malicious access, and the cyber security measures required as a result.

The consequences are potentially greater when considering DTs, which incorporate live data from a facility's I&C infrastructure into a building model, introducing additional concerns around their potential for use in operational decision-making, malicious injection of incorrect plant data, and actions required to verify the validity of the data provided by the DT [21], [30], [31], [32].

3.1.2.1 Design and Security Use Cases

PIMs of nuclear facilities have a number of use cases related to the design process. BIM systems have been proposed as a method for storing data for use during the design process; they could store measurement data through point cloud and computer models of plant infrastructure, as well as system documentation linked to the physical assets within the BIM system. Linking the engineering change control process to a BIM system has also been proposed, which could provide system-wide historical data on design changes within the facility, as well as access to component and equipment related information, such as catalogue identification numbers, preventative maintenance logs, and station condition reports.

In the design of new reactor systems, the use of DTs coupled with hardware-in-the-loop methodology has been proposed as a method to gain insight on thermal hydraulics within reactor designs prior to construction. In one proposed method, the heat profile of a nuclear core would be simulated, and the heat profile would be used to drive heaters in a physical model of the proposed design. Actual measurements from the physical model's heat transport loop could then be used to inform models of the system or to further develop the design [33].

3.1.2.2 Safety Analysis and Operations Use Cases

DTs have been proposed as a way to fill knowledge gaps on fault or accident conditions and provide access to a wealth of data for safety analysis and support of operational decision-making. To provide this functionality, DTs would integrate data from plant monitoring systems, scenario-based modelling and simulation, physical limits on equipment operation and setpoints, and plant operating limits and procedures, as well as information pertaining to equipment availability. This information, combined with detailed probabilistic assessment of risk scenarios, would allow for detailed accident scenario modelling [30].

An additional use for DTs that spans safety, work management, operations, and decommissioning is the overlay of radiometric data on DTs, which would then be used for dose estimation and waste management [30].

3.1.2.3 Plant Health Monitoring and Inspection Use Cases

Because of the breadth of data BIM and DTs can cover, they have been proposed as a method to increase the efficiency and coverage of plant health monitoring activities. For example, a DT can monitor the performance characteristics of multiple systems over time, which can allow facility-wide monitoring of system performance, including items such as drift from setpoints on operating equipment [34], [35].



"The primary value associated with AR is the ability to blend simulated objects into an existing environment, to allow for user interactions with elements beyond what actually exists in the real world."

3.1.2.4 Training, Planning, Human, and Organizational Performance Use Cases

DT processes have the potential to support operator training and decision-making by providing a realistic, real-time copy of the nuclear facility. A DT synched to information from across plant systems would allow for simulation of the impact of operator actions on a digital model that is consistent with current plant conditions. Training of operators could be based on real, plant-wide configurations. Moreover, the detailed models associated with BIM present the opportunity to conduct site tours, walkdown training, and public outreach functions in a more streamlined manner and with lower risk than on-site visits [31]. Furthermore, existing applications have shown promise in the management of large volumes of industrial data at scale, integrated with business applications to allow plant executives, plant managers, and workers to interact with the DT in real time [33].

BIM and DTs also present opportunities in planning support for decommissioning and waste management activities. COG has highlighted the potential to use DTs on nuclear power plants post-shutdown to allow for automation of surveillance and monitoring activities between defueling and decommissioning [36].

3.1.3 Augmented Reality and Virtual Reality

AR and VR allow for the interactive immersion of personnel within a partially or fully simulated environment. AR presents an interactive experience where real-world objects or environments are combined or enhanced by the introduction of simulated objects visible to the AR system user. In contrast, the environment presented within a VR application is wholly simulated, typically with no aspects of the real world directly visible to the user.

In both cases, the user's visual fields, location, and movements are typically tracked to allow for correct object positioning and orientation within the simulated or partially simulated environment relative to both the user and the real world. In addition to visual tracking and object positioning, certain user actions may result in environmental response. Interactions with the simulated environment can be simple visual spatial interaction, or can be extended to include audio and haptic feedback.

The primary value associated with AR is the ability to blend simulated objects into an existing environment, to allow for user interactions with elements beyond what actually exists in the real world [37]. This is particularly useful for overlaying additional data on an existing item to enhance awareness of tasks or phenomena that may not otherwise be immediately apparent. It should be noted that AR is not the simple overlay of data in a user's field of view, as would be found in a heads-up display. Instead, objects within VR being overlayed on the user's field of view must be tracked to maintain their positions within the frame of reference of the real world relative to the user.

In the case of VR, the entire environment is simulated, with the user typically not able to view the real-world environment around them without removing the hardware used to facilitate the VR experience.

With both VR and AR applications, the virtual model of plant data would require verification against plant configuration to a level commensurate with the quality assurance requirement for its use case. Additionally, the correct use of any filters in the view would have to be verified, to ensure that users are presented with the correct information for the task to be performed. This is of particular importance when the VR or AR model is being used to ensure the safe execution of work, such as when providing input on procedure execution or the location of radiation sources.

3.1.3.1 Design and Security Use Cases

The application of virtual environment technology to solve problems in design has demonstrated considerable cost savings. Virtual environments, whether viewed on screen or through AR or VR equipment, have allowed for cost savings via virtual walkdowns of laser scans, and by reducing site travel requirements and the need to return to the site for additional measurements. Furthermore, the capability to check for interferences of new equipment through the overlay of computer models of new equipment with virtual environments has reduced instances of interference issues in design and transport of equipment to installation locations [38].

3.1.3.2 Safety Analysis and Operations Use Cases

AR has potential for use in dose reduction and management of workers executing work around radioactive equipment. A proposed method for increasing working awareness of high-dose radiation areas and radiation sources is to provide those executing the work with AR headsets that superimpose radiation survey data over the area in which the work is being executed, providing a direct visual indication of areas of higher dose [39], [40]. The use of VR technology in combination with remote retrieval of point cloud data via laser imaging, detection, and ranging (LIDAR) also presents an opportunity to conduct virtual walkdowns of areas that are dose intensive or otherwise inaccessible under normal circumstances.

3.1.3.3 Plant Health Monitoring and Inspection Use Cases

The use of AR devices combined with computer-based procedures has been proposed as a method to ease place-keeping and reduce errors during execution of inspection and maintenance procedures. Using standard hardware, such as cameras and Bluetooth headsets, many of the desirable features can be integrated into a computer-based procedure that runs on an AR device [40]. With the addition of an AR headset, there is potential for overlay of instructions, equipment highlighting, travel paths, radiation survey data, dosimetry information, required equipment positions, and other relevant data on the inspector or maintainer's field of view, allowing for more efficient work execution and reduction in error rates [39], [40].

3.1.3.4 Training, Planning, Human, and Organizational Performance Use Cases

Control room and plant simulations have been a standard in the training of operations staff at nuclear stations for the majority of the nuclear energy industry's existence. VR has been proposed as a method for enhancing visualization of plant equipment. While simulations offer a view of plant processes from the control room, they lack the in-the-field elements of walkdowns and troubleshooting. A variety of simulation and VR providers have developed VR training environments that allow for simulation of various scenarios, both within a control room and throughout a simulated plant [41]. The ability to vary situations and alter the virtual training environment as needed without requiring changes to a physical mock-up offers potential increases in the breadth of available training scenarios without undue cost.

Some additional potential areas for the use of AR/VR technologies include VR walk-throughs as part of a pre-job briefing, simulation of complex tasks using VR, and the use of multiple VR sets with multiple simultaneous users to perform training exercises as a team in a detailed virtual environment.

The use of VR and AR environments for training is already beginning to take place within the industry. One example where VR was used for training was through the creation of a digital replica of two floors of the Hinkley Point B reactor facility. Risks and hazard scenarios were added for employees to navigate, allowing training on the use of plant health and safety procedures [40]. In Sellafield, a mixed-reality model of a nuclear plant crane was created using an exact

replica of the crane's operator chair, control joystick, and spatial working environment together with selected digital tools [42].

3.1.4 Advanced Condition Monitoring

Condition monitoring is the process of monitoring a parameter associated with a piece of equipment or machinery in order to identify any changes in system behaviour that may indicate a fault. It is an important component of predictive maintenance. Traditional methods of process monitoring and fault identification require a large number of assumptions and are typically time intensive to implement. Predictive analytic toolsets are software tools, many of which utilize ML models that are focused on predicting the future behaviour of a system based on prior data. In contrast to descriptive analysis, which seeks to identify patterns in past data, predictive analysis seeks to extrapolate on identified patterns or trends to provide insight on future outcomes.

Condition monitoring allows for maintenance to be scheduled on a preventative basis rather than a periodic basis. It can extend the life of equipment by identifying degradation in performance before a major fault develops. Typical methods of monitoring condition include vibration analysis, acoustic emission analysis, infrared thermography, and oil condition sensors. The use of condition monitoring is widespread with rotating equipment, valves, and motors.

ACM supplements traditional condition monitoring with digital models, advanced statistical methods, or ML to help identify possible degradation in performance more quickly, to identify potential root causes of the condition change, or to monitor performance of sections of equipment that are difficult to directly measure.

There are a number of concerns associated with the introduction of ACM technology in nuclear facilities relating to the validity, bounds of reliable operation, and overall qualification of the mathematical models that inform the ACM software's decisions. Ensuring the validity of model training data can be difficult in cases where example data is not available in large quantities. Additionally, this can impede qualification of the ACM model in general, as a dearth of available data for training is typically associated with a dearth of available data on which to test the ACM model's performance.

3.1.4.1 Plant Health Monitoring and Inspection Use Cases

Torsional vibration monitoring has been successfully demonstrated for use in monitoring steam turbine structural health. A physics-based analytical model of an example pump was constructed and analyzed under conditions representative of either nominal operation or bearing failure. Simulated responses were generated at a location on the pump shaft system deemed likely to accommodate the vibration monitoring sensor system. The simulated results indicate that it is possible to detect and identify fault signals using torsional vibration monitoring that might not be discernable with other methods [43].

The use of ACM to inform predictive maintenance was the primary suggested use case in the literature reviewed for this report. In this context, ACM would be used to increase the confidence in equipment condition and longevity by providing predictions of equipment wear and remaining operational life. The predictions made by the ACM would then be used to ascertain equipment condition. Proponents of the adoption of ACM suggest that the increased data availability could be used to supplement data gathered through inspections, potentially allowing for a reduction in required inspection frequency. One example of the push towards this use case is work conducted by Canadian Nuclear Laboratories to develop AI tools to predict common primary heat transport pump seal failures [44].

3.1.5 Cloud Computing

Cloud computing is the on-demand availability of computer system resources, particularly the storage and processing of data, using computational resources that are not managed by the end user and are typically located in an alternate location from the user. Cloud-based systems are often distributed across multiple locations that may share resources.

Cloud-based systems allow users to access computational resources owned and operated by a

third party, either software or hardware, that may be cost prohibitive or inefficient to purchase and maintain full-time. The resources service the user's request, return the processed information to the user, and are then available to an alternate user.

As digitization of control and monitoring systems becomes more common within the nuclear industry, the amount of data available and the computation capability required to process the data are growing, thus increasing the potential economic benefits of cloud computing and analysis.

The primary challenges with the use of cloud computing in the nuclear industry are centered around security, access, quality, and control of data. Because data is transmitted to and processed at a third-party location, cloud computing may be subject to nuclear export license requirements depending on the nature of the data and the location of servers. Where cloud-based computing is used for safety-related analysis, recording and analysis of system data, or for system control, there are concerns regarding the security and fidelity of the data and the software used to process it. Finally, because cloud-based computing is conducted on hardware operated by a third party, additional scrutiny regarding implementation and maintenance of the requirements for encryption, access control, and maintenance of back-ups may be required. With the possibility of remote control or processing of inspection or operating system data, the boundary of influence into a nuclear facility is no longer necessarily aligned between the physical world and the digital world.

3.1.5.1 Safety Analysis Use and Operations Use Cases

The use of cloud-based computing for analytical software has been proposed for GOTHIC, which is software used to conduct multi-phase fluid flow analysis. The main benefits of cloud computing compared to more traditional information technology (IT) infrastructure for safety analysis in the nuclear industry are protection of intellectual property, data retention, streamlining of quality assurance, and the efficient use of computational resources. For any software with burdensome computational requirements, cloud computing offers the required resources without the need to directly invest in the necessary hardware [30], [45].

However, there are a number of challenges in the cloud-based deployment of safety-related analytical software for the nuclear industry, including licensing issues because many codes are currently licenced "per user" and may also have geographic restrictions on their use. Furthermore, not all cloud computing solutions maintain a specific configuration of hardware, which can complicate code qualification when hardware or operating systems change over time.

An additional potential use case of cloud-based computing is improved data retention and distribution in the event of a natural disaster or major plant fault [46]. In these cases, cloud-based computing offers increased availability and redundancy for recorded data in a secure off-site location [46].

3.2 Key Software Types

Within existing codes, standards, and industry procedures, there are a number of terms used to describe digital systems use cases and assign requirements related to systems design, quality assurance, and allowable uses. As exact definitions of digital system types or terminology may differ between documentation, descriptions in alignment with key standards are provided below. It should be noted that the system types or groups outlined below may overlap and are not mutually exclusive.

Where available, definitions from key standards for each of the system types listed below are available in Appendix B:, Section 1B.3.1.

3.2.1 Real-Time and Process Control Systems and Software

RTPC systems are computer programs, pre-programmed digital hardware (e.g., integrated circuits), or digital software and systems used in I&C applications within a nuclear power plant or other nuclear facility [2]. RTPC software is generally intended for equipment that is part of a process required to operate equipment or a facility, and it includes the interface with the operator of that equipment or facility.

Software of this type may be pre-developed, custom, or may be considered a software engineering tool. Standards addressing RTPC software in nuclear facilities, namely CSA N290.14, also extend to pre-programmed digital hardware.

The control functions implemented by the software or digital hardware are assigned a safety category in accordance with the primary safety-related function fulfilled by the software or system it supports. These categories range from safety integrity level 4 to non-safety-related, which may also be termed commercial grade [2], [47].

RTPC software may be supported by online support tools, which are software tools that can directly influence safety-related systems during their runtime [47]. In addition, offline tools used in the development of RTPC software must also be considered. This includes software that supports a phase of the software development lifecycle but cannot directly influence the safety-related system during its runtime [47], such as a text editor, a requirements or design support tool, or a compiler. While these tools support RTPC software, they may be considered separately by standards establishing requirements.

Several existing standards that address RTPC software could also be applicable to emerging technologies. OT security requirements for RTPC software used in nuclear facilities are addressed in CSA N290.7 [48], including the relevant NIST SP-800-53 [49] requirements. Software categorization, classification, development, and qualification are addressed via IEC 61226 [50], IEC 61508/60880/61513/62138 [47], [51], [52]. [53], and CSA N290.14.

3.2.2 Analytical Software

Broadly speaking, analytical software is used to demonstrate the safety of a nuclear facility or to conduct an analysis serving that facility. The results of analysis constitute the licensing basis as embodied in plant-specific safety reports. Analytical software assesses the effectiveness of plant safety systems in the context of mandated acceptance criteria that follow from safety concerns, such as adequate fuel cooling during normal and off-normal operation. The software may serve to conduct probabilistic or deterministic safety analysis, or may be an engineering tool.

Analytical software focuses on discipline-specific areas such as system thermal hydraulics, reactor physics, and fission product release and transport. Safety analysis consists of the execution of integrated or linked analysis software. The applicability of analytical software is assessed though code applicability and is supported by validation activities.

CANDU analytical software includes software used by specific organizations as well as generic industry standard software that is used industry wide. Analytical software can be CANDU-specific, developed in Canada, or international, developed by external organizations with industry expertise and the requisite qualifications and quality assurance. Industry software is designated as the Industry Standard Toolset and is administered by COG.

3.2.3 Operational Technology Systems and Software

OT are programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment) [54]. Software and systems serving OT have considerable overlap with RTPC software, with OT being a more broadly applicable term than RTPC systems. While RTPC systems meet the definition of an OT system, not all OT systems are part of RTPC systems. See Figure 1 for a diagrammatic example of the overlap of RTPC and OT systems definitions.

Examples of OT include industrial control systems, building management systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. A physical access control system would serve, in part, to define the operational bounds of a nuclear facility.

3.2.4 Administrative Safety Software

Administrative safety software is a subset of management system software and is used to achieve a management system function directly related to safety, such as a dosimetry program database, software for tracking and accounting for nuclear material under safeguards requirements, or software in communications systems used by the security department. While the software does not have direct control of a safety function, it is key for achieving safe operation [55], [56].

3.2.5 Management System Software

The management system of a nuclear organization is a planned and integrated set of processes necessary to satisfy the requirements to achieve nuclear safety, business success, and sustainability. It includes the complete set of policies, manuals, and procedures that govern every aspect of how the organization functions. Software to support the requirements of the management system therefore includes software used across the organization that does not fall into one of the other types defined in Section 3.2 [55], [57]. Management system software can have an indirect effect on safety, such as software to monitor and plan training, while software that has a direct effect on safety is categorized as administrative safety software. Examples of management system software include software for document management and software for all corporate functions (e.g., IT, finance, legal, and human resources).

3.3 Standards and Sections Relevant to Emerging Digital Technologies

Standards and the key subsections relevant to each of the systems and software types discussed in Section 3.2 are listed in Appendix C:, Table 2. A discussion of the relevant standards, associated gaps, and potential standards or actions to address these gaps is provided in sections 3.3.1 through 3.3.6.

3.3.1 Real-Time and Process Control Systems and Software

The key CSA standard governing requirements for quality assurance of RTPC hardware and software is CSA N290.14, which defines requirements for the process of qualification of digital hardware and software for use in I&C applications for nuclear facilities [2]. IAEA's SSR-2/1 [56] also provides a number of principles applicable to this type of software, most of which have been adopted by Canada and are implemented through CNSC regulatory documents [58], [47].

To further complement these standards, the following International Electrotechnical Commission (IEC) standards provide additional guidance on I&C system requirements relevant to OT systems and RTPC systems:

- IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems* [47];
- IEC 61511, *Functional safety – Safety instrumented systems for the process industry sector* [59];
- IEC 61513, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems* [52];
- IEC TR 61838, *Nuclear power plants – Instrumentation and control important to safety - Use of probabilistic safety assessment for the classification of functions* [60];
- IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions* [51];
- IEC 62138, Nuclear power plants – *Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions* [53].

See Table 2, items 1 to 26 for additional information on standards applicable to RTPC software.

3.3.2 Analytical Software

The primary CSA standard governing analytical software is CSA N286.7, which is limited to the design basis or safety analysis basis of high energy reactors [1], not all nuclear facilities required to comply with CSA nuclear standards.

CSA N286.7 provides information on quality assurance requirements for analytical software, including qualification of software and records of qualification. Further information on the extent of qualification and level of detail required are provided in the CSA N290 series (see Appendix B, Section 1B.4 for list of active N290 series standards) where applicable, depending on the software use case. In addition, analytical software and its use are expected to comply with CNSC regulatory documents, REGDOC-2.4.1 (sections 4.4.5 and 8.4.3) and REGDOC-2.4.2 (Section 4.7) [47], [58], as applicable.



"At this time, a specific standard for analytical software that does not have the potential to impact safety or safety analysis at high-power reactor facilities has not been clearly defined."

The following COG documents provide additional guidance on activities related to compliance with CSA N286.7 and CNSC REGDOC-2.4.1 and REGDOC-2.4.2:

- ISTR-12-5044, *COG validation guidelines* [61];
- ISTO-09-5092, *Guidelines for generic methodology for estimation of computer code accuracy* [62];
- ISTR-14-5057, *Guidelines for execution and documentation of code applicability assessment* [63]; and
- COG-09-9030, *Principles and guidelines for deterministic safety analysis* [64].

Although analytical software that does not have the potential to impact safety or safety analysis at high-power nuclear reactor facilities is not subject to the scope of CSA N286.7, it must still be qualified and must comply with software requirements under CSA N286 and the CSA N299 series. At this time, a specific standard for analytical software that does not have the potential to impact safety or safety analysis at high-power reactor facilities has not been clearly defined.

Internationally, ASME NQA-1 software requirements, which are commonly credited for certain types of engineering design analysis, serve as the American counterpart to CSA N286.7. Additional software standards include the following, developed by the International Standards Organization (ISO):

- ISO/IEC 25010:2011, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models* [65];
- ISO/IEC 14598, *Software engineering – Product evaluation* [66];
- ISO/IEC 25051, *Software engineering – Software Product Quality Requirements and Evaluation (SQuaRE) – Requirements for Quality of Commercial Off-the-Shelf (COTS) software and instructions for testing* [67];
- ISO 15026, *Systems and software engineering – Systems and software assurance* [68];
- ISO/IEC/IEEE 26512, *Systems and software engineering – Requirements for acquirers and suppliers of information for users* [69];
- ISO/IEC 33001, *Information technology – Process assessment – Concepts and terminology* [70]
- ISO/IEC 33002, *Information technology – Process assessment – Requirements for performing process assessment* [71]
- ISO/IEC 33003, *Information technology – Process assessment – Requirements for process measurement frameworks* [72]
- ISO/IEC 33004, *Information technology – Process assessment – Requirements for process reference, process assessment and maturity models* [73]
- ISO/IEC 33014, *Information technology – Process assessment – Guide for process improvement* [74]
- ISO/IEC 33020, *Information technology – Process assessment – Process measurement framework for assessment of process capability* [75]

- ISO/IEC 33063, *Information technology – Process assessment – Process assessment model for software testing* [76]
- ISO/IEC/IEEE 15939, *Systems and software engineering – Measurement process* [77];
- ISO/IEC/IEEE 26514, *Systems and software engineering – Design and development of information for users* [78]; and
- ISO/IEC 14102, *Information technology – Guideline for the evaluation and selection of CASE tools* [79].

Generally, CSA N286.7 applies to software that impacts safety. Specifically, it stipulates the requirements for quality assurance programs applicable to the design, development, maintenance, modification, acquisition, and usage of analytical, scientific, and design computer programs that are used in high energy reactor applications [1].

Additionally, CSA N286.7 applies to programmed applications (e.g., scripts, macros, and spreadsheet-based analysis) written within software that is normally excluded from the standard. CSA N286.7 does not apply to programs such as those used to control plant safety systems and operational control systems, which are covered by CSA N290.14. The full list of items excluded from CSA N286.7 are:

1. Embedded software contained within items, where the software is qualified along with the item as a unit (e.g., measurement and test equipment);
2. Software used to collect or present design inputs (e.g., data acquisition systems and CAD programs);
3. Business software (e.g., work management, productivity tools, commercially available database and spreadsheet programs);
4. Software used to manage information (e.g., records management software);
5. Commercially available compilers, interpreters, and operating systems; and
6. Commercially available mathematical routine libraries [1].

See Table 2, items 27 to 38 for additional information on standards applicable to analytical software.

3.3.3 Operational Technology Systems and Software

OT systems are not distinctly defined and addressed as a separate category within the suite of Canadian nuclear standards. Where OT systems are considered to meet the criteria for another software type, such as RTPC software, the requirements are covered by the relevant standard for that software category. OT software that does not meet the criteria to be classified as another listed software type must still comply with CSA N286 and the CSA N299 series if the OT system is supporting or interfacing with a management system. Section 3.3.5 provides further discussion on the applicable standards for management system software.

3.3.4 Administrative Safety Software

Administrative safety software and systems are not explicitly defined or addressed as a distinct category within the suite of Canadian nuclear standards. Where administrative safety software supports or interfaces with an aspect of a management system and does not meet the definition of any other defined software types, it must still comply with the requirements applicable to management system software, as discussed in Section 3.3.5.

3.3.5 Management System Software

The primary standard for management system requirements is CSA N286, which applies to the integration of management system requirements for health, safety, environment, security, economics, and quality throughout the lifecycle of a nuclear facility, from conception to completion of decommissioning [55]. CSA N286 does not dictate software requirements other than the requirement for approval of the software as fit for purpose (clause 4.8.2) and subsequent configuration control of software used to conduct any work or safety analysis (clause 7.4.2) [55]. For the use of engineering design analytical software tools and safety analysis computer programs, clauses 7.3.4. and 7.4.3 of CSA N286 [55] refer to CSA N286.7. See Table 2, items 41, 42, 43, and 44 for additional information.

For software supporting management systems not already covered by standards applicable to RTPC software or analytical software, the standards dictating

the needs of the applicable QA program are the CSA N299 series, which are procurement standards for nuclear power plants in Canada that list requirements for a QA program. The N299 series includes four standards that cover Categories 1 through 4, with Category 1 being the most comprehensive and Category 4 the least comprehensive. Software requirements are listed in the N299 series for Categories 1 through 3. See Table 2, items 54, 55, 56, 57, and 58 for additional information.

The requirements discussed in this section are applicable to all software utilized within a nuclear facility or in support of its management systems, with the exception of systems considered to be RTPC or analytical software.

3.3.6 Generally Applicable Requirements

In addition to software and procurement standards, there are three additional, generally applicable standards and guidance that define software requirements for the nuclear industry, including the use of new technologies: IAEA SSR-2/1, IAEA SSG-30, and IAEA TECDOC-1787 [56], [80], [81]. These three documents are internationally defined guides of best practices, and they are applicable to this report.

The 82 requirements in SSR-2/1 are divided into general requirements for design, such as the management system for design or the requirement for defence in depth. Requirements 43 to 82 are for specific systems. Where new technology is deployed in reactor design, it would be subject to the same requirements provided in SSR-2/1 [56].

IAEA SSG-30, a safety guide published by the IAEA, provides international best practices and recommendations for structures, systems, and components in a reactor facility classification according to their significance to safety [80]. The guide is based on a subset of requirements from SSR-2/1 related to classification, and provides guidance for how those requirements can be implemented in the design process [56].

IAEA TECDOC-1787 was published after IAEA SSR-2/1 and SSG-30. It provides the most detailed guidance and suggested approach for implementing the requirements in SSR-2/1 that systems structures and components shall be classified according to their safety significance [81]. The document includes practical advice for classification implementation in practice and includes examples and a process flow diagram. Where new technologies are deployed in systems in a reactor facility, they must be classified according to their significance to safety and subject to the same performance requirements as existing technologies and components. Guidance in IAEA TECDOC-1787 is not mandatory, but represents international best practice to assist designers in achieving a high level of safety [81].

Key relevant requirements for software and technology are listed in Table 2, items 1-10, 39, 40, and 50-53.

3.4 Concerns and Underlying Assumptions Related to Emerging Digital Technologies

Emerging digital technologies present new methods to solve existing problems. As a result, the areas in which the digital technologies are applied have existing requirements, workflows, and procedures. Existing workflows are based on the methodologies that were available when the standard that provides requirements for that process was written. While these standards were typically written to be technology neutral, they may have been developed based on inherent assumptions regarding the general methodologies available to solve problems, the types of problems that software could be built to solve, and ultimately, the form that the flow of work can take.

Emerging digital technologies offer the potential for approaches that may not be well aligned with the writing of current standards. The potential high-level changes to workflows and underlying assumptions as a result of emerging technologies are discussed herein. These potential changes were noted through focus group discussions and compilation of questionnaire responses from industry and subject matter experts.

3.4.1 Advanced Analytical Methods

The application of AA models within the nuclear industry prompted a number of questions and concerns due to a lack of clarity around allowable use cases, application of requirements, and qualification methods required per standards applicable within the

nuclear industry. Key concerns, points, and actions that emerged from discussions with subject matter experts are provided in sections 3.4.1.1 through 3.4.1.3.

3.4.1.1 Associated Risks and Areas of Concern

The wide array of potential applications for AA methods also presents a number of risks and areas of ambiguity. While the potential risks introduced by AA methods are as myriad as the number of use cases, there are several major reoccurring risks and areas of ambiguity that are beneficial to consider when determining the actions required to adequately address AA methods within current standards.

The exact impact of an AA model failure would be dependent on the use case in which the model is applied, but the underlying issue would remain the same: that the model did not perform as expected. There are a number of reasons why an AA model may not meet expected performance, including lack of sufficient training data, lack of sufficient testing data, use of data outside the range for which the model was trained, and training performance being unrepresentative of production performance due to factors unknown to the creator of the AA model at the time of production.

The black box nature of the models created by AA methods, and the difficulty it introduces in the qualification of these models, is a common point of concern. The primary issue is because the model cannot be explained piece-wise, it is difficult to justify the values on which the model operates and the range of inputs for which they are applicable. This makes it infeasible to pursue qualification of a model via justification of the correct application of theory.

Further confounding this issue is the fact that the inputs to AA processes may be non-numeric in nature, making it difficult for designers and users to define the location of edge cases with undesirable behaviours. Additionally, it may be difficult to tell when one of these edge cases is encountered, because the AA model could provide confidence in an incorrect answer.

Additional concerns related to AA models pertain to their security. The majority of ML libraries are open source, which presents security and quality concerns for use in the nuclear industry. The presence of large, opaque mathematical models produced by complex libraries presents the opportunity for the introduction of malicious content to not only the library used to produce the model but also to the mathematical model itself. In this case, the primary concern is that the model could function differently in production than in a testing environment.

Areas of ambiguity surrounding AA models are not limited to mitigation of risk, but also include application of standards to these models. For example, if an AA model was to be used within the controls of a safety important system, it is unclear which standards would be applicable. Additionally, for the use of analytical software outside of a high-power reactor facility, CSA N286.7 is not strictly applicable, which leaves a potential gap in relevant standards for qualification of the AA model. The use of CSA N286.7 may be overly restrictive for non-safety-related use cases or cases not within a high-power reactor facility [1], but there is not wide agreement on which standard AA models must meet in such cases.

3.4.1.2 Discussion of Key Issues

The following key issues relating to AA methods were raised through interview, focus group, and questionnaire responses from technical committee members and subject matter experts within the nuclear industry.

Key Differences Between Static and Dynamic AA Model Workflows

Workflows surrounding the development, qualification, and use of AA models for analytical software are largely dependent on whether the AA model is static or dynamic in nature. Static models have fixed performance characteristics at the time of qualification, and their performance on representative test data is not dependant on the time at which the model is tested. In contrast, dynamic models are able to alter the function that evaluates a given input based on the function's performance in past application. Essentially, dynamic AA models are continually learning and adjusting. Because of their differing natures with respect to time, static and dynamic AA models have differing concerns regarding their qualification and use under the current CSA nuclear standards.

Process for Qualification of Static AA Models

Static AA models (e.g., static ML models) would be subject to qualification requirements similar to a regression model or other empirically derived solution. However, there are a couple of key differences in the qualification of an AA model from a typical regression model. The first is that the mathematical models created by an AA process typically have a very large number of coefficients, making determination of the exact purpose weight of any one coefficient within the model very difficult, such that the model values cannot easily be justified individually. The second key difference is that the parameters being found for the AA model do not have background theory from which to provide a justification of model behaviour (e.g., using the Arrhenius equation for a regression model). As a result, qualification of the model must be based solely on model performance against test data. In the case of a static AA model (the mathematical model itself, separate from implementation language), it could be qualified as follows:

1. Training data is reviewed for biases that could impact model results, is accurately labelled (if applicable), and covers appropriate ranges of inputs for the use case of the model, to produce a qualified training data set.
2. Test data is reviewed for biases that could impact model results, is accurately labelled (if applicable), and covers appropriate ranges of inputs for the use case of the model, to produce a qualified testing data set.
3. An AA model training software suite is reviewed for cyber security and functionality concerns, with the end goal of producing a qualified AA training software. This software is not the end-result analytical software, but instead is software to support the development of mathematical models to be used in the analytical software.
4. The mathematical model is developed by the AA model training software using the qualified training data.
5. Performance criteria are established as the minimal model testing requirements. These performance criteria are dependent on the use case of the final analytical software.
6. The mathematical model is then tested for performance against the qualified test data set, which is separate from the training data set.
7. Mathematical model performance on test data is used to provide judgement on the adequacy of the model in reference to the performance criteria.
8. The mathematical model is implemented in the software execution language.
9. The verification of the implementation of the model in the execution language under CSA N286.7 is conducted as a separate activity from assessment of the adequacy of the model after training (i.e., check that the model has been accurately transcribed and represented in the language used to execute the script).

This process is described visually in Figure 2 and Figure 3 in Appendix A.

Challenges with Qualification of Static AA Models

While the method for qualification described above is technically feasible within the framework of CSA N286.7, it may be difficult to implement to the required level of confidence for qualification given the potential lack of qualified training and test data in certain areas. In these areas, it is likely neither feasible nor advisable to use AA models, and considerable challenges are expected from the regulator with respect to the qualification of an AA model if a method is not available to demonstrate that it is consistent with state-of-the-art understanding. As a result, large and comprehensive sets of training and test data would likely be required for model qualification because, unlike personnel, mathematical models cannot be questioned regarding justification of the answers they provide.

It should be noted that there is a possibility of justifying model behaviour based on review of the model function in relation to accepted physical laws, similar to review of a regression model. However, given the complex nature of the mathematical model typical of AA methods, this is not likely to be feasible for qualification or reduction in test data requirements because the relations within the model are often not explicable. Essentially, qualification via parametric analysis is not likely to be achievable for AA models.

Potential Solutions for Qualification of Static AA Models

In addition to a methodology for the qualification of analytical software featuring AA methods, there are potential methods for increasing the confidence in model performance during execution. Two separate mathematic models can be created using separate banks of qualified training data. Test data and training methods could also be varied between models as required, provided both sets of test data are qualified for the full scope of potential analysis inputs and outputs. These two models, each created from separate training data, could then be run in parallel path and checked for agreement, triggering an error or human intervention whenever there is model disagreement. Similarly, the analytical software could be used alongside qualified personnel, comparing judgements of each. In this case, the model would not operate in isolation, but in conjunction, as a method of verification for the judgement of human personnel.

Challenges with Qualification of Dynamic AA Models

Dynamic AA models also present concerns regarding their qualification for use. The software's capability to alter the mathematical model being used to conduct the analysis without direct review adds difficulty to the qualification of the software, because the model's performance characteristics cannot be guaranteed to remain within the bounds of the acceptance criteria over time without additional measures.

Because the model is capable of altering itself, it is not only the implementation of the mathematical model in the execution language that must be verified but also the process by which the model is capable of altering its own performance characteristics, and the bounds of performance within which the model could be altered.

For inspections that are of high safety significance or that are complex in nature (which may include extensive digital processing), the CSA N285 series require adoption of formal qualification of inspection procedures (e.g., CSA N285.4:19, clauses 4.2 and 4.3) to demonstrate that the process satisfies the inspection specification requirements to detect, characterize, and size flaws. Configuration control of qualified inspection procedures will likely pose limitations on use of processes that include (active) ML.

Though the current standards are written to be neutral with respect to digital technology, the capability of a model to be continuously altered remains an area that is difficult to account for. Within the current standards framework, each time a model parameters are adjusted by the software based on outside input, such as comparison to process data versus the model's prior predictions, the change would be considered a new revision to the model, which must undergo qualification.

Additionally, unlike fixed AA models, running two different dynamic AA models in parallel and checking that the results agree is not a viable solution to increase confidence in output correctness. This is due to the fact that the models will converge after a duration, given that they are comparing themselves to the same system data to make updates.

Overall, the lack of clarity regarding the requirements and methodology needed to qualify and maintain configuration control of dynamic AA models constitutes a potential gap in the coverage of CSA N286.7.

Potential Solutions for Qualification of Dynamic AA Models

One proposed solution for the qualification of dynamic AA models is to retrain the model on a set timeframe, re-qualifying the software at each interval. However, this solution removes the continuous portion of the learning, leaving the handling of dynamic AA largely unaddressed. A proposed alternate solution is to require the inclusion of a regression test suite that allows the model to test its own performance against a fixed set of training data that fully bounds the allowable behaviour of the model. Should the model fail to meet the requirements of the benchmark test, it would be prevented from use. This method essentially automates the qualification testing of the AA model each time it is updated, and could allow for higher model alteration rates. This solution is potentially difficult to properly define and implement under the current standards.



"A large portion of the software available to construct and test the underlying mathematical models is open source. This presents a concern from the perspective of cyber security and configuration management."

General Cyber Security Concerns Associated with AA Model Development

An additional point of consideration for both dynamic and static AA models is that a large portion of the software available to construct and test the underlying mathematical models is open source. This presents a concern from the perspective of cyber security and configuration management, because the software does not originate from a qualified and security cleared supplier. To address this issue, a copy of the open source software would need to be isolated from external access and reviewed to ensure cyber security and correct implementation. This version of the software would then isolated from updates or alteration. Any pertinent error corrections or updates to the open source software would require the repetition of this process with the updated software. It should be noted that this process is not specific to a particular software use case or purpose, and could also be applied to the use of open source software for purposes other than AA model development.

3.4.1.3 Key Considerations

Key considerations with respect to aligning the CSA nuclear standards and the use of AA methods include:

- Development of nonbinding guidelines, whether via reference to an existing standard or via creation of a guidance document, on how to meet existing requirements within CSA nuclear standards for qualification of AA models via training and testing.
- Review and reference of international standards (see Table 2) for methodologies by which AA models can be implemented.
- Clarification of whether AA libraries used to train both dynamic and static models can be considered software development tools or standard mathematical libraries.
- Definition of what constitutes a standard mathematical library should be refined with consideration of AA applications.
- Exception for software development tools should be clarified to ensure that ML libraries are included in the case of static AA models.
- Clarification of which standards are applicable to software conducting analysis of data for the purposes of process control (e.g., computer vision and OCR used to sort items by serial number).
- Definition of steps required for the use of open source libraries.
- Clarification of requirements for software conducting analysis that does not fall within the scope of CSA N286.7.

3.4.2 Plant Information Models

The application of PIMs within the nuclear industry prompted a number of questions regarding allowable use cases, applicable standards, operator actions, and defence of the design basis. Key concerns, points, and

actions that emerged from discussions with technical committee members and subject matter experts are provided in sections 3.4.2.1 through 3.4.2.3.

3.4.2.1 Associated Risks and Areas of Concern

The use of PIMs within the nuclear sector presents a number of opportunities for efficiency gains, along with a number of notable concerns. The use of BIM as the central repository and single source of truth for information on the configuration of a physical asset results in the BIM and its documentation becoming the design basis of the physical asset. This raises concerns on how change management, configuration management, and maintenance of design requirements can be adequately tracked and qualified in alignment with existing nuclear standards. How the information within a BIM system will be qualified and adequately audited presents another concern.

When PIMs begin to incorporate live data from plant systems, it creates the possibility that the data will be used to make operational decisions or to otherwise inform operational judgement. The methodology for qualification of this data for use would also require that the configuration of the digital asset is aligned in real-time with the configuration of the physical asset. Should the configuration not match, or the data not be updated accurately, loss of configuration control and incorrect operational judgements could result.

An additional risk can occur in the transition to a PIM from an alternate data source. Standardized requirements for interface and exchange of data in the creation of a PIM are unclear. This presents a lack of clear requirements for the transfer of data from existing data repositories into a PIM, and also raises concerns regarding data transferability over the lifetime of the facility. PIM software is offered by a variety of vendors, and the capability to port data between alternate PIM software is not currently clearly defined. The lack of clarity regarding standardized data formats between different PIM software raises concerns about interoperability should facility owners/operators need to transfer software providers, such as in the case that the software being used becomes defunct. The inability to switch to an alternative software platform is compounded by the possibility that PIMs are offered partly or wholly through cloud services, or are in some way connected to external networks. Should the entity providing that software become unavailable, the facility using the software would be left with software with no security updates for software with online interfaces and a lack of data transferability by which to rectify the problem.

3.4.2.2 Discussion of Key Issues

The following key issues relating to PIMs were raised through interview, focus group, and questionnaire responses from technical committee members and subject matter experts within the nuclear industry.

Comparison of BIM to Standard Condition Control and Asset Management Software

Interviewees and subject matter experts noted that BIM proposed for configuration control and asset management within nuclear facilities is likely to become the design basis for the facility. The requirements of configuration control and document management within a PIM are covered under CSA N286. Because CSA N286 was written to be technology neutral, no major gaps were apparent in relation to configuration management. BIM without connection and display of live plant data can potentially be treated in a similar manner to other document repositories and configuration management software, assuming the primary change is the format in which the data is displayed. In this context, all of the required processes for verification, validation, and approval would be required to be present within the BIM, and while the display of data and interaction of databases may change, the high-level process required to meet the CSA nuclear standards for configuration management would remain similar, as shown in Figure 4.

Avenues for Configuration and Control of the Design Basis Within PIMs

BIM software typically uses a check-in and check-out system to prevent conflicting changes. There is also branch control of changes, similar to control of software revision in large codebases, and BIM software used in the nuclear industry would be required to have built-in workflows for review, verification, approval, and release of changes to the information contained within the BIM system. The capability to implement workflow

and approval processes within the BIM provides a method to meet the requirements for an authorization process surrounding the alteration, issuance, and use of data contained in the BIM, which would allow compliance with CSA N286.

Another consideration raised regarding BIM was the reduction in the number of barriers to the introduction of errors into the design basis, as a single error that makes it through the approval process would be populated across all relevant linked databases instead of having to go through the relevant expert for each database update. A potential avenue for mitigation of this concern is the use of version history within BIM and DTs. By maintaining versions of the BIM at each introduced change, back-checking can be conducted against previous configurations. Additionally, the use of BIM for management of the design basis would not eliminate the requirement to ensure alignment between the facility records and the facility in the field. To this end, walkdowns would still be a required part of the configuration management process.

An additional concern was raised regarding the process required to establish a PIM to the level of detail required to maintain the overall design basis of the facility. Interrelations between equipment and requirements are often distinctly defined within the existing information, which is where system specialists provide value in interpretation and provision of information on system interactions. Concern regarding accurate transcription of the facility information to a BIM system was a key item, but it does not directly conflict with any standard, because the processes for population of data within a BIM system are covered by the same requirements as the process of creating and maintaining other document and configuration management software.

Use of PIMs for Operational Decision-Making and Process Control

Where PIMs are used to interface with operations, there are additional considerations related to which standards are applicable. There is ambiguity surrounding the requirements set forth by the CSA nuclear standards in regard to support of operational decision-making via DTs or BIM. As with current plant information systems, one potential method is to allow the use of information from the BIM to support operational decision-making, but require verification of the status of relevant equipment via qualified means, such as annunciation panels, prior to the decision. Additionally, with the incorporation of DTs and BIM as a part of RTPC systems, the response to an accident based on indicated parameters becomes increasingly dependent on appropriate cyber security controls. Hence, the compliance of these systems to requirements that are well defined in CSA N290.7 [48] is critical.

3.4.2.3 Key Considerations

Key considerations regarding the interface of CSA nuclear standards and PIMs include:

- PIMs have the potential to become both the design basis and a source of operational data for owners/operators of nuclear facilities. The portions of each PIM responsible for configuration management, change management, document management, and collations and presentation of operational data should be clearly delineated to minimize application of standards requirements where not strictly necessary.
- Clarification of requirements regarding the use of information for operational decision-making are needed in the case of PIMs featuring operational data. A similar approach to the current use of unqualified plant information systems may provide a guide for usage of data from non-qualified BIM and DTs.
- Due to the large cost and effort associated with the creation a PIM, nonbinding guidelines on implementation and maintenance of PIMs in line with the requirements of CSA N286 could bolster confidence in a chosen path forward, aiding progress in the implementation of PIMs for configuration, asset, and document management.
- For use in configuration management, PIMs would be required to comply to the same requirements as existing configuration and change management programs, as well as the requirements for existing document management programs. Review of these requirements should be conducted with the use of PIMs in mind, and language selected such that it maintains clarity when applied within a PIM.

- The overall processes associated with configuration management, change management, and document management inside a PIM are largely similar to existing methods, with notable changes being the introduction of software specialists for maintenance of the PIM data, and the digitization of workflows. The information required to be available to ensure to alignment with the standards remains the same, as do the handling requirements at a high level.

3.4.3 Augmented Reality and Virtual Reality

The use of AR and VR technologies within the nuclear industry raised concerns about how to ensure an accurate and easily interpretable data display, especially in use cases where the display of data has a direct impact on safety. Key concerns, points, and actions that emerged from discussions with technical committee members and subject matter experts are provided in sections 3.4.3.1 through 3.4.3.3.

3.4.3.1 Associated Risks and Areas of Concern

The primary risks noted in relation to AR and VR applications were adequate display of data and appropriate human machine interface requirements. Because AR and VR have the potential to assist with conducting procedures and awareness of safety issues (e.g., radiation fields), failure of the data display could result in significant consequences, such as missing procedure steps or accruing unnecessary radiation doses.

3.4.3.2 Discussion of Key Issues

The following key issues relating to the use of AR and VR were raised through interview, focus group, and questionnaire responses from technical committee members and subject matter experts within the nuclear industry.

Application of AR and VR to Safety-Related Tasks

While AR and VR technologies provide a novel way to display data to an end user, there are concerns with the adoption of this technology related to accurate and reliable display of data. Additionally, the provision of appropriate human machine interfaces within the technology, to reduce or eliminate error-likely situations, is important. AR and VR applications are focused on displaying data for an end user, so they do not conduct analysis or provide control to facility systems. However, the technology may be used to display data to designers, operators, and maintainers, and there may be safety impacts through these interactions. It was noted that AR and VR could be used as a way to present or display information collected through managed and controlled processes. In such cases, it would be essential that valid data is provided.

There are technical documents pertaining to human factors associated with AR and VR, which include, but are not limited to:

- ISO/IEC TR 23842-1, *Information technology for learning, education, and training – Human factor guidelines for virtual reality content – Part 1: Considerations when using VR content* [82]; and
- IEEE 1589, *IEEE Standard for augmented reality learning experience model* [83].

These standards may provide additional guidance on the human factors requirements associated with AR and VR technology, as well as methodologies for reliable implementation of these technologies.

3.4.3.3 Key Considerations

Key considerations relating to AR and VR in the context of the CSA suite of nuclear standards include:

- AR and VR constitute a novel way to display data, but from the perspective of the CSA nuclear standards, they are subject to the same requirements as other human machine interfaces.
- Given their potential use as safety-related devices (e.g., visualizing radiation fields in the work area), the qualification of AR and VR software and hardware should follow a rigorous graded approach commensurate with the hazard level associated with each use case.
- Existing international guidelines for the use of AR and VR should be considered for reference in relevant CSA nuclear standards.

3.4.4 Advanced Condition Monitoring

The use of ACM within the nuclear industry prompted concerns centered on the AA models used to augment the standard condition monitoring data, which are

discussed in Section 3.4.1. Key concerns, points, and actions that emerged from discussions with technical committee members and subject matter experts are provided in sections 3.4.4.1 through 3.4.4.3.

3.4.4.1 Associated Risks and Areas of Concern

The key areas of concern associated with ACM were largely a result of, and thus aligned with, concerns related to the AA models that interpret the condition monitoring data. These risks are discussed in Section 3.4.1.1. An additional area of concern that was raised is the level of detail associated with digital models of equipment when AA models are replaced by or augmented with digital models. The method by which these models are ensured to be sufficiently accurate to provide realistic results or training data for AA methods is not clear. Furthermore, a lack of clear requirements on how to use ACM data to set or extend periodic maintenance timelines creates the potential for overly optimistic maintenance schedules justified by ACM data.

3.4.4.2 Discussion of Key Issues

The following key issues relating to ACM were raised through interview, focus group, and questionnaire responses from technical committee members and subject matter experts within the nuclear industry.

For support of any inspection and maintenance work under the CSA N285 series, the use of ACM would have to show that it satisfies the technical requirements. The use of predictive toolsets would require compliance with CSA N286.7 requirements. Changes to underlying assumptions and workflows related to the AA portion of ACM are addressed in Section 3.4.2. No major misalignments with CSA nuclear standards governing inspection were noted for the use of ACM when compared to traditional condition monitoring, with the exception of the qualification and configuration control concerns noted for AA models that support ACM.

It should also be noted that in addition to standards governing inspection, according to CSA N290.6, *Requirements for monitoring and display of nuclear power plant safety functions in the event of an accident* [84], there is nothing to preclude the use of ACM methods if they can be shown to meet requirements. CSA N290.6 encourages the use of early detection and related functions that could be improved by the use of ACM and predictive toolsets, but Clause 6.1.3 states: "The design shall account for the uncertainties and the errors associated with the instrumentation. The uncertainties related to both normal operation and accident conditions shall be considered" [84]. This could be challenging when incorporating ML, because the instrumentation would be considered part of the ML tool, where such uncertainties may be challenging to identify.

3.4.4.3 Key Considerations

Key considerations relating to ACM in the context of the CSA suite of nuclear standards include:

- The use of AA models associated with ACM is likely to encounter similar roadblocks around qualification of models that are discussed in Section 3.4.1.
- Because of the current lack of clarity in inspection standards (e.g., CSA N285.4 [85]) regarding rules or guidelines for setting or extending inspection periods, the amount of justification required to increase the inspection period (i.e., reduce inspection frequency) is not clear.

3.4.5 Cloud Computing

The use of cloud computing within the nuclear industry primarily prompted concerns pertaining to cyber security requirements. Key concerns, points, and actions that emerged from discussions within technical committee members and subject matter experts are provided in sections 3.4.5.1 through 3.4.5.3.

3.4.5.1 Associated Risks and Areas of Concern

The use of cloud computing for work relating to the Canadian nuclear industry necessitates that data is transmitted from a computer within a system that is controlled and secured in alignment with the CSA suite of nuclear standards to a data center that is secured, administered, and maintained by a party outside the direct control of the entity conducting the work. As a result, the primary concerns that were raised about cloud computing are related to cyber security and data qualification.

Some of the increased risks related to cyber security and data integrity include, but are not limited to:

- Difficulty maintaining or ensuring correct data residency;
- Reduction in the security of data transmission to and from the third-party location;
- Risk of access by unqualified parties;
- Potential for data to be altered or damaged by third parties;
- Use of the connection to the cloud site for unauthorized access to systems within the nuclear entity's own network;
- Alteration to the software or hardware on which the data is hosted or processed; and
- Loss of connection to cloud location for storage or processing.

3.4.5.2 Discussion of Key Issues

The following key issues relating to the use of cloud computing were raised through interview, focus group, and questionnaire responses from technical committee members and subject matter experts within the nuclear industry.

There were no gaps identified in the requirements of the current CSA suite of nuclear standards pertaining to the use of cloud computing. However, the cyber security requirements do limit the allowable use cases and configurations of cloud computing. The requirements that cloud computing must meet are partially dependent on the software and use case that the cloud-based computing is supporting. In all cases, compliance with CSA N290.7 is required. Some key concerns that may limit allowable use cases include capability to ensure the location and specific device on which the software is to run, given that cloud-based computing requires the computer hardware be under the control and maintenance of a party other than the licensee. Compliance with CSA N286.7 requirements for maintenance of data integrity transfer are of note when analytical software is sending data, retrieving data, or running on cloud-based systems. Similarly, compliance with the CSA N285 series (see Section 1B.4 for list of active CSA N285 series standards) is required where cloud computing is supporting inspection activities. Compliance with CSA N290.14 would be required for cloud-based computing supporting RTPC, and compliance with CSA N286 would be required for any function supporting a managed system.

The movement of data processing and storage to a third party also presents a challenge in terms of auditability and general oversight. Because the location is not within the direct control of the licensee, it may not be possible to grant auditors access to the physical location of the servers. Additionally, the physical location of the server on which the cloud data is kept may be subject to change, depending on the agreement in place for the cloud computing service.

3.4.5.3 Key Considerations

Key considerations relating to the use of cloud computing and its interface with the CSA suite of nuclear standards include:

- In cases that require physical control of the hardware executing the software and/or guarantee of hardware and software configuration, the use of cloud computing is likely limited.
- Data residency requirements, while not in conflict with the use of cloud computing, largely limit its application to services that can guarantee the use of only data centers within Canada.
- Requirements for auditor access to data and physical systems should be reviewed with the use of cloud computing services in mind.
- Guarantee of long-term retention of key data may necessitate the use of on-premises storage for any data required to be maintained under the licensee's direct control.
- As the volume of data being stored and processed increases, especially with the rise in information-centric asset management (as found in BIM and DTs), the desire for cloud computing services within the nuclear industry is likely to rise. Avenues to reconcile the difficulties associated with direct control of hardware for execution of analytical software should be examined.



"There is a need to ensure that emerging digital technologies are adequately addressed by the standards governing the Canadian nuclear industry."

4 Conclusions

With the continued development of digital technologies such as AA, PIM, and ACM, and the trend towards digitalization of industrial facilities, workflows, and document handling, there is a need to ensure that emerging digital technologies are adequately addressed by the standards governing the Canadian nuclear industry. While emerging digital technologies present opportunities, including increased design efficiency, fewer maintenance issues, automated inspections, and improved planning capabilities, they also present several risks to nuclear and conventional safety that must be accounted for and controlled within the requirements of relevant standards. The key concerns, potential gaps in coverage, and areas of uncertainty regarding these emerging digital technologies must be addressed in upcoming standards revisions to ensure that emerging technologies can be used to their full potential in the Canadian nuclear industry, in a manner that is both well bounded and not unnecessarily restrictive.

Findings related to specific emerging digital technologies are discussed in sections 4.1 through 4.5, and generally applicable findings are discussed in Section 4.6.

4.1 Advanced Analytical Methods

While AA methods and models have the potential to create both static and dynamic models capable of accurately dealing with complex inputs such as image and video information, the highly complex, opaque nature of the resultant models presents a number of challenges for their use within the nuclear industry. Whether supporting RTPC or analytical software, AA models can be difficult to qualify due to the complexity of their internal workings and the potentially impracticable nature of parametric or physical justification. In the case of fixed model development, AA tools may be described as software engineering tools, so only the static mathematical model and its performance require qualification. An additional gap was identified in the use of dynamic AA models that continue to self-adjust during operation. These models present a conflict with requirements for both qualification and configuration control of the software, and in the context of CSA N286.7, may not be well addressed. However, the use of built-in self-testing may provide an avenue to ensure that a dynamic model remains within the acceptable bounds of performance.

To facilitate the further use of AA methods in a safe and reliable manner, the following actions should be considered:

- Alignment with and reference to international standards (see Table 2) for methodologies by which AA models can be implemented;
- Development of nonbinding guidelines, whether via reference to an existing standard or via creation of a guidance document, to support meeting existing requirements within the CSA suite of nuclear standards via performance testing of AA models;

- Clarification of whether AA libraries used to train both dynamic and static models can be considered software development tools;
- Clarification of which standards are applicable to software conducting analysis of data for the purposes of process control (e.g., computer vision and OCR used to sort items by serial number); and
- Clarification of requirements for software conducting analysis that does not fall within the scope of CSA N286.7.

4.2 Plant Information Models

PIMs have the potential to handle configuration management more efficiently and to provide a wide array of useful facility information to designers and operators. For configuration management, there is potential to handle BIM in a manner similar to current configuration control software, provided the necessary security limits, sign-out, review, verification, and approval workflows to meet the requirements of CSA N286 are built into the BIM software.

The other major group of PIMs, DTs, present further challenges due to their direct link to I&C systems within the plant. The use of DT information to make operation decisions remains an area that is not clearly defined within the existing suite of standards, similar to the plant information systems in use at some nuclear facilities.

Of concern for all PIMs is compliance with CSA N290.7. With the incorporation of DTs and BIM into RTPC systems, the response to an accident based on indicated parameters becomes increasingly dependent on appropriate cyber security controls. Hence, it is critical that these systems comply to the well-defined requirements in CSA N290.7.

To facilitate the use of PIMs in a safe and reliable manner, the following items should be considered:

- Creation of guidance on how to maintain clear distinction between the portions of each PIM responsible for configuration management, change management, document management, and collation and presentation of operational data, such that requirements imposed by the standards are applicable only as needed for each section;
- Clarification of requirements regarding the use of information for operational decision-making are needed for PIMs featuring operational data. A similar approach to the current use of unqualified plant information systems may provide a guide for usage of data from non-qualified BIM and DTs; and
- Creation of nonbinding guidelines providing a roadmap for implementation and maintenance of PIMs in line with the requirements of CSA N286 would bolster confidence in a chosen path forward, aiding progress in the implementation of PIMs for configuration, asset, and document management.

4.3 Augmented Reality and Virtual Reality

AR and VR may offer significant benefits in training design and safety. No major gaps were identified in the pertinent software standards, but adoption of existing standards on AR and VR development, use, and maintenance into software and human factors related standards would provide additional clarity and value regarding the requirements for the use of these technologies.

To facilitate the use of AR and VR in a safe and reliable manner, integration and harmonization of existing international standards on the use of AR and VR for training and execution of work would be beneficial.

4.4 Advanced Condition Monitoring

ACM has the potential to provide further insight on equipment performance. However, because the models used to evaluate the monitoring data are typically developed using AA methods, qualification of these models may be an impediment to their use. Any ACM software would be required to comply with the CSA N285 series and potentially with CSA N286.7 for analysis of the signal data. The development of clear guidelines or rules on justification of reduction in inspection frequency based on ACM data would be beneficial to the full realization of ACM's benefits.

4.5 Cloud Computing

With the increase in data collection and processing required to support the further digitalization of the nuclear industry, cloud-based computing offers the potential to reduce upfront digital infrastructure

investment. No gaps were identified in the existing standards, but meeting the requirements for compliance with cyber security and relevant software standards may prove challenging given the lack of direct control the licensee has over the hardware used to facilitate the cloud-based computing.

To facilitate the use of cloud computing and its interface with the CSA suite of nuclear standards, the following key items should be considered:

- In cases that require physical control of the hardware executing the software and/or guarantee of hardware and software configuration, the use of cloud computing is likely limited;
- Data residency requirements, while not in conflict with use of cloud computing, largely limit its application to services that can guarantee the use of only data centers within Canada;
- Requirements for auditor access to data and or physical systems should be reviewed with the use of cloud computing services in mind; and
- Guarantee of long-term retention of key data may necessitate the use of on-premises storage for any data required to be maintained under the licensee's direct control.

4.6 Generally Applicable Findings

One key finding that impacts several emerging digital technologies, as well as digital technologies currently in use, was a lack of clarity on delineation between software types and how to assign requirements for software that may fit multiple categories for a given use case. For example, for analytical software that is not used in a high-power reactor facility and does not have the potential to impact safety, CSA N286.7 is not applicable and may be overly restrictive. This leaves analytical software in the category primarily covered by CSA N286, which provides minimal guidance specific to analytical software. Similar concerns were raised with respect to OT software, which does not currently have a standardized definition within the CSA nuclear framework. Finally, participants noted that the applicable standards for analytical software that provides input to a process control system are unclear.

Another notable finding that was raised as a common theme in each category of emerging digital technology is the opportunity for efficiencies presented through harmonization with international standards. In combination with the burgeoning variety of SMR designs being developed internationally, emerging digital technologies are being offered to the Canadian nuclear industry from an increasingly international market. A CSA research report on the role of standards in facilitating SMR deployment in Canada noted that the design burden resulting from differences in jurisdictional requirements can create barriers to the development and adoption of new technologies [86]. Harmonization of Canadian standards with their international counterparts presents a significant opportunity to facilitate the use of emerging digital technologies, and larger systems making use of these technologies, within Canada.

To ensure that emerging digital technologies are well addressed by the CSA suite of nuclear standards, the following key issues should be considered:

- Definition of the requirements for handling static and dynamic AA models within analytical and OT software (including RTPC software);
- Clarification of the requirements for using information in a PIM in support of operational decision-making;
- Reference to standards regarding the development and use of AR and VR technologies; and
- Clarification of the categorization of AA model development software dependent on its use in either a static or dynamic model.

References

[1] Quality Assurance of Analytical, Scientific, and Design Computer Programs, CSA N286.7-16 (R2021), Canadian Standards Association, Toronto, ON, Canada, 2016.

[2] Qualification of Digital Hardware and Software for Use in Instrumentation and Control Applications for Nuclear Power Plants, CSA N290.14:15 (R2020), Canadian Standards Association, Toronto, ON, Canada, 2015.

[3] Quality Assurance Program Requirements for the Supply of Items and Services for Nuclear Power Plants, Category 1, CSA N299.1-19, Canadian Standards Association, Toronto, ON, Canada, 2019.

[4] Quality Assurance Program Requirements for the Supply of Items and Services for Nuclear Power Plants, Category 2, CSA N299.2-19, Canadian Standards Association, Toronto, ON, Canada, 2019.

[5] Quality Assurance Program Requirements for the Supply of Items and Services for Nuclear Power Plants, Category 3, CSA N299.3-19, Canadian Standards Association, Toronto, ON, Canada, 2019.

[6] Quality Assurance Program Requirements for the Supply of Items and Services for Nuclear Power Plants, Category 4, CSA N299.4-19, Canadian Standards Association, Toronto, ON, Canada, 2019.

[7] Quality Assurance Requirements for Nuclear Facility Applications, ASME NQA-1-2022, American Society of Mechanical Engineers, New York, NY, United States, 2022.

[8] Gartner. "Gartner glossary: Advanced analytics." Gartner.com. https://www.gartner.com/en/information-technology/glossary/advanced-analytics (accessed Aug. 18, 2022).

[9] Electric Power Research Institute (EPRI), "Application of data analytics to mine nuclear plant maintenance data." EPRI, Paolo Alto, CA, United States, Mar. 26, 2021. Accessed: Aug. 16, 2022. [Online]. Available: https://www.epri.com/research/programs/0TIZ12/results/3002020120

[10] Electric Power Research Institute (EPRI), "Welding and repair technology for power plants 10th international conference program." EPRI, Paolo Alto, CA, United States, Jun. 21, 2012. Accessed: Aug. 16, 2022. [Online]. Available: https://www.epri.com/research/products/1025766

[11] H. Anderson, "Strategic R&D program 2021/22 operational plan." CANDU Owners Group (COG), Toronto, ON, Canada, COG-21-9705, 2021.

[12] Electric Power Research Institute (EPRI), "Proof of concept: Developing a machine learning algorithm trained with synthetic data that can identify parallel misalignment in real vibration data." EPRI, Paolo Alto, CA, United States, May 27, 2021. Accessed: Aug. 16, 2022. [Online]. Available: https://www.epri.com/research/programs/065755/results/3002020411

[13] K. Berggren et al., "Roadmap on emerging hardware and technology for machine learning," Nanotechnology, vol. 32, no. 1, 2021, Art. no. 012002, doi: 10.1088/1361-6528/aba70f.

[14] National Institute of Standards and Technology (NIST). "Emerging hardware for artificial intelligence." NIST.gov. https://www.nist.gov/programs-projects/emerging-hardware-artificial-intelligence (accessed Aug. 17, 2022).

[15] E. Lanus, L. J. Freeman, D. R. Kuhn, and R. N. Kacker, "Combinatorial testing metrics for machine learning," in IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Apr. 2021, pp. 81–84, doi: 10.1109/ICSTW52544.2021.00025.

[16] D. Tetzlaff, A. Smith, and C. Soulsby. (2021). Stable water isotopes in landscapes: Big data & ML opportunities to respond to current challenges on water resources under environmental change. Presented at IAEA Technical Meeting on Artificial Intelligence for Nuclear Technology and Applications. [Online]. Available: https://conferences.iaea.org/event/245/contributions/20466/attachments/10885/16464/Tetzlaff_IAEA_final.pdf

[17] A. Sozontov, M. Ivanova, and A. Gibadullin, "Implementation of artificial intelligence in the electric power industry," in E3S Web Conf. 114, 2019, doi: 10.1051/e3sconf/201911401009.

[18] D. Lanin. (2021). Actual issues of artificial intelligence implementation in design engineering process of nuclear power plants. Presented at IAEA Technical Meeting on Artificial Intelligence for Nuclear Technology and Applications. [Online]. Available: https://conferences.iaea.org/event/245/contributions/20526/

[19] D. Baraldi, O. Parera-Villacampa, and L. Ammirabile. (2021). On-going development of critical flow models in the Marviken experiments with AI methods. Presented at IAEA Technical Meeting on Artificial Intelligence for Nuclear Technology and Applications.

[20] A. Sokolov. (2021). Summary of the working group on AI for safeguards verification." Presented at IAEA Technical Meeting on Artificial Intelligence for Nuclear Technology and Applications. [Online]. Available: https://conferences.iaea.org/event/245/contributions/20453/attachments/11272/16600/%5BSG%5DWG1%20SG%20Summary.pdf

[21] P. Day. "Digital twin projects look to slash nuclear O&M costs." ReutersEvents.com. https://www.reutersevents.com/nuclear/digital-twin-projects-look-slash-nuclear-om-costs (accessed Aug. 16, 2022).

[22] G. Guzman, A. Prasanna, P. Safarik, and P. Tanwar. "Unlocking the value of digital operations in electric-power generation." McKinsey.com. https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/unlocking-the-value-of-digital-operations-in-electric-power-generation (accessed Aug. 16, 2022).

[23] H. Janin, J. Latz, K. Sato, and B. Sauer. "The digital power plant of the future." McKinsey.com. https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/the-digital-power-plant-of-the-future (accessed Aug. 16, 2022).

[24] R. Maciel and P. Safarik. "Power plant 4.0: Embracing next-generation technologies for power plant digitization." McKinsey.com. https://www.mckinsey.com/industries/electric-power-and-natural-gas/our-insights/power-plant-4-point-0-embracing-next-generation-technologies-for-power-plant-digitization (accessed August. 16, 2022).

[25] C. Warren, "Drones and AI converge for power delivery inspections," EPRI Journal, pp. 1–2, Mar./Apr. 2019. [Online]. Available: https://eprijournal.com/wp-content/uploads/2019/04/2019.03-D3_Drones-And-AI.pdf

[26] Electric Power Research Institute (EPRI), "Quick insight brief: Leveraging artificial intelligence for nondestructive evaluation," EPRI, Paolo Alto, CA, United States, 2021. Accessed: Aug. 16, 2022. [Online]. Available: https://www.epri.com/research/products/000000003002021074

[27] R. Siddarth, D. Lister, and R. Trivedi. (2020). Machine learning techniques to predict flow accelerated corrosion rate and scalloping behavior. Presented at SAIMIN-2020: 1st Symposium on Artificial Intelligence, Machine Learning and other Innovative Technologies in the Nuclear Industry.

[28] Electric Power Research Institute (EPRI), "Quick insight brief: Digital twin activities at EPRI," EPRI, Paolo Alto, CA, United States, 2020. [Online]. Available: https://www.epri.com/research/programs/065093/results/3002020014

[29] P. Day. "AI finds a place in nuclear O&M." ReutersEvents.com. https://www.reutersevents.com/nuclear/ai-finds-place-nuclear-om (accessed Aug. 16, 2022).

[30] CANDU Owners Group (COG), "Minutes of 2021 GOTHIC-IST annual user group meeting," COG, Toronto, ON, Canada, Nov. 2021. Accessed: Aug. 12, 2022. [Online]. Available: https://www.cogonline.org/Publications/Publications/RDPublications/BP-NBP-OPG-CNNO-KHNP-SNN-CE-KIN/ISTO-21-5034.pdf

[31] M. Singh, et al., "Applications of digital twin across industries: A review," Applied Sciences, vol. 12, no. 11, Jun. 2022, Art. no. 5727, doi: 10.3390/app12115727.

[32] International Atomic Energy Agency (IAEA), "Implementing digital instrumentation and control systems in the modernization of nuclear power plants," IAEA, Vienna, Austria, Tech. Rep. NP-T-1.4, 2009. [Online]. Available: https://www-pub.iaea.org/MTCD/publications/PDF/Pub1383_web.pdf

[33] Reuters Events, "Digital twin technology identified as key to increased safety and efficiency." ReutersEvents.com. https://www.reutersevents.com/nuclear/digital-twin-technology-identified-key-increased-safety-and-efficiency (accessed 21 Aug. 21, 2022).

[34] G. Banyay, B. Golchert, and C. Worrell, Pennsylvania, PA, United States. Synopsis of Westinghouse Machine Learning, Artificial Intelligence, and Digital Twin Developments for Nuclear Power Applications. (Oct. 13, 2020). [Online Video]. Available: https://youtu.be/cYDoxY9loF4

[35] G. Shao, "Use case scenarios for digital twin implementation based on ISO 23247," National Institute of Standards and Technology, Gaithersburg, MD, United States, 2021. [Online]. Available: https://doi.org/10.6028/NIST.AMS.400-2

[36] B. Bowen, "Report documenting OPEX on approaches for simulation and modelling for decommissioning," CANDU Owners Group (COG), Toronto, ON, Canada, OP-18-7065, 2020.

[37] Electric Power Research Institute (EPRI), "Advanced nuclear technology: Augmented reality technologies for new nuclear plant applications," EPRI, Paolo Alto, CA, United States, 2017. [Online]. Available: https://www.epri.com/research/products/000000003002010467

[38] CANDU Owners Group (COG), "Virtual environment software toolkit evaluation," COG, Toronto, ON, Canada, COG-96-118, 1997.

[39] I. Wright and A Mattmuller, "Augmented reality applications in nuclear power plants," Deloitte, New York, NY, United States, 2017. Accessed: Aug. 16, 2022. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-augmented-reality-applications-in-nuclear-power-plants.pdf

[40] CANDU Owners Group (COG), "Nuclear safety environment in virtual reality," COG, Toronto, ON, Canada, OPEX 56241, November 1, 2019.

[41] F. Muniz-Simas and R. Simpson. (2020). Combining simulation and virtual reality: An immersive training experience. Presented at SAIMIN-2020: 1st Symposium on Artificial Intelligence, Machine Learning and other Innovative Technologies in the Nuclear Industry.

[42] P. Day. "UK dockyard turns to VR to apply modular approach to nuclear." ReutersEvents.com https://www.reutersevents.com/nuclear/uk-dockyard-turns-vr-apply-modular-approach-nuclear.

[43] CANDU Owners Group (COG), "Torsional vibration monitoring of deep draft vertical pumps: Phase 1" COG, Toronto, ON, Canada, Final rep. OPEX 57388, May 6, 2022.

[44] T. Rector and S. El Bouzidi. (2020). Using artificial intelligence to monitor primary heat transport pump seal degradation. Presented at SAIMIN-2020: 1st Symposium on Artificial Intelligence, Machine Learning and other Innovative Technologies in the Nuclear Industry.

[45] D. Kingdon, "Minutes of 2019 COG GOTHIC-IST user group meeting," CANDU Owners Group (COG), Toronto, ON, Canada, Oct. 7, 2019. Accessed: Aug. 16, 2022. [Online]. Available: https://www.cogonline.org/Publications/Publications/RDPublications/BP-CNL-NBP-OPG-CNNO-KHNP-SNN-CE-KIN/ISTO-19-5022.pdf

[46] S. Lavanya and S. Prakasam, "Remote monitoring of nuclear power plants with the integration of IOT and cloud computing," IJARSE, vol. 4, spec. iss. no. 1, pp. 106-110, 2015.

[47] Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, IEC 61508-1, International Electrotechnical Commission, Geneva, Switzerland, 2010.

[48] Cyber Security for Nuclear Facilities, CSA N290.7:21, Canadian Standards Association, Toronto, ON, Canada, 2021.

[49] Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53, Rev. 5, National Institute of Standards and Technology, Gaithersburg, MD, United States, 2020.

[50] Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems Important to Safety – Categorization of Functions and Classification of Systems, IEC 61226:2020, International Electrotechnical Commission, Geneva, Switzerland, 2020.

[51] Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category A Functions, IEC 60880:2006, International Electrotechnical Commission, Geneva, Switzerland, 2006.

[52] Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems, IEC 61513:2011, International Electrotechnical Commission, Geneva, Switzerland, 2011.

[53] Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Software Aspects for Computer-Based Systems Performing Category B or C Functions, IEC 62138:2018, International Electrotechnical Commission, Geneva, Switzerland, 2018.

[54] Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST SP 800-37, Rev. 2, National Institute of Standards and Technology, Gaithersburg, MD, United States, 2018.

[55] Management Systems Required for Nuclear Power Facilities, CSA N286:12 (R2022), Canadian Standards Association, Toronto, ON, Canada, 2012.

[56] Safety of Nuclear Power Plants: Design, IAEA SSR-2/1 (Rev. 1), International Atomic Energy Association, Vienna, Austria, 2016.

[57] Harmonization of the Licensing Process for Digital Instrumentation and Control Systems in Nuclear Power Plants, IAEA-TECDOC-1327, International Atomic Energy Agency, Vienna, 2002.

[58] Deterministic Safety Analysis, REGDOC-2.4.1, Canadian Nuclear Safety Commission, Ottawa, ON, Canada, 2014.

[59] Functional Safety – Safety Instrumented Systems for the Process Industry Sector, IEC 61511:2022, International Electrotechnical Commission, Geneva, Switzerland, 2022.

[60] Nuclear Power Plants – Instrumentation and Control Important to Safety – Use of Probabilistic Safety Assessment for the Classification of Functions, IEC TR 61838:2009, International Electrotechnical Commission, Geneva, Switzerland, 2009.

[61] J. Pascoe, "COG validation guidelines," CANDU Owners Group (COG), Toronto, ON, Canada, ISTR-12-5044, 2019.

[62] J. Pasoe, "Guidelines for generic methodology for estimation of computer code accuracy," CANDU Owners Group (COG), Toronto, ON, Canada, ISTO-09-5092, 2019.

[63] J. Pascoe, "Guidelines for execution and documentation of code applicability assessment," CANDU Owners Group (COG), Toronto, ON, Canada, ISTR-14-5057, 2020.

[64] CANDU Owners Group (COG), "Principles & guidelines for deterministic safety analysis," COG, Toronto, ON, Canada, COG-09-9030, 2014.

[65] Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, ISO/IEC 25010, International Standards Organization, Geneva, Switzerland, 2011.

[66] Software Engineering — Product Evaluation, ISO/IEC 14598, International Standards Organization, Geneva, Switzerland, 2001.

[67] Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Ready to Use Software Product (RUSP) and instructions for testing, ISO/IEC 25051, International Standards Organization, Geneva, Switzerland, 2014.

[68] Systems and Software Engineering — Systems and Software Assurance, ISO/IEC 15026, International Standards Organization, Geneva, Switzerland, 2015.

[69] Systems and Software Engineering — Requirements for Acquirers and Suppliers of Information for Users, ISO/IEC/IEEE 26512, International Standards Organization, Geneva, Switzerland, 2018.

[70] Information technology — Process assessment — Concepts and terminology, ISO/IEC 33001, International Standards Organization, Geneva, Switzerland, 2015.

[71] Information technology — Process assessment — Requirements for performing process assessment, ISO/IEC 33002, International Standards Organization, Geneva, Switzerland, 2015.

[72] Information technology — Process assessment — Requirements for process measurement frameworks, ISO/IEC 33003, International Standards Organization, Geneva, Switzerland, 2015.

[73] Information technology — Process assessment — Requirements for process reference, process assessment and maturity models, ISO/IEC 33004, International Standards Organization, Geneva, Switzerland, 2015.

[74] Information technology — Process assessment — Guide for process improvement, ISO/IEC 33014, International Standards Organization, Geneva, Switzerland, 2013.

[75] Information technology — Process assessment — Process measurement framework for assessment of process capability, ISO/IEC 33020, International Standards Organization, Geneva, Switzerland, 2015.

[76] Information technology — Process assessment — Process assessment model for software testing, ISO/IEC 33063, International Standards Organization, Geneva, Switzerland, 2015.

[77] Systems and Software Engineering — Measurement Process, ISO/IEC/IEEE 15939, International Standards Organization, Geneva, Switzerland, 2017.

[78] Systems and Software Engineering — Design and Development of Information for Users, ISO/IEC/IEEE 26514, International Standards Organization, Geneva, Switzerland, 2022.

[79] Information Technology — Guideline for the Evaluation and Selection of CASE Tools, ISO/IEC 14102, International Standards Organization, Geneva, Switzerland, 2008.

[80] Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA SSG-30, International Atomic Energy Association, Vienna, Austria, 2014.

[81] International Atomic Energy Association (IAEA), "Application of the safety classification of systems, structures and components in nuclear power plants," IAEA, Vienna, Austria, TECDOC-1787, 2016.

[82] Information Technology for Learning, Education and Training — Human Factor Guidelines for Virtual Reality Content — Part 1: Considerations when Using VR Content, ISO/IEC TR 23842-1:2020, International Standards Organization, Geneva, Switzerland, 2020.

[83] IEEE Standard for Augmented Reality Learning Experience Model, IEEE 1589-2020, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 2020.

[84] Requirements for Monitoring and Display of Nuclear Power Plant Safety Functions in the Event of an Accident, CSA N290.6:16 (R2021), Canadian Standards Association, Toronto, ON, Canada, 2016.

[85] Periodic Inspection of CANDU Nuclear Power Plant Components, CSA N285.4:19, Canadian Standards Association, Toronto, ON, Canada, 2019.

[86] T. Ward, K. Toomsalu, S. Krishnan, H. Medina, and N. Tedford, "The role of standards in facilitating deployment of SMRs in Canada," Canadian Standards Association, Toronto, ON, Canada, 2021. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-The-Role-of-Standards-in-Facilitating-Deployment-of-SMRs-in-Canada.pdf

[87] Periodic Inspection of CANDU Nuclear Power Plant Containment Components, CSA N285.5-18, Canadian Standards Association, Toronto, ON, Canada, 2018.

[88] Periodic Inspection CANDU Nuclear Power Plant Balance of Plant Systems and Components, CSA N285.7:21, Canadian Standards Association, Toronto, ON, Canada, 2021.

[89] Commentary on N286-12, Management System Requirements for Nuclear Facilities, CSA N286.0.1:21, Canadian Standards Association, Toronto, ON, Canada, 2021.

[90] In-Service Examination and Testing Requirements for Concrete Containment Structures of Nuclear Power Plants, CSA N287.7-17 (R2022), Canadian Standards Association, Toronto, ON, Canada, 2017.

[91] General Requirements for Safety Systems of Nuclear Power Plants, CSA N290.0:17 (R2022), Canadian Standards Association, Toronto, ON, Canada, 2017.

[92] Requirements for the Shutdown Systems of Nuclear Power Plants, CSA N290.1-13 (R2018), Canadian Standards Association, Toronto, ON, Canada, 2013.

[93] Requirements for Emergency Core Cooling Systems of Nuclear Power Plants, CSA N290.2:17 (R2022), Canadian Standards Association, Toronto, ON, Canada, 2017.

[94] Requirements for the Containment System of Nuclear Power Plants, CSA N290.3:22, Canadian Standards Association, Toronto, ON, Canada, 2022.

[95] Requirements for Reactor Control Systems of Nuclear Power Plants, CSA N290.4:19, Canadian Standards Association, Toronto, ON, Canada, 2019.

[96] Requirements for Electrical Power and Instrument Air Systems of CANDU Nuclear Power Plants, CSA N290.5:16 (R2021), Canadian Standards Association, Toronto, ON, Canada, 2016.

[97] Technical Specification Requirements for Nuclear Power Plant Components, CSA N290.8-15 (R2020), Canadian Standards Association, Toronto, ON, Canada, 2015.

[98] Reliability and Maintenance Programs for Nuclear Power Plants, CSA N290.9:19, Canadian Standards Association, Toronto, ON, Canada, 2019.

[99] Human Factors in Design for Nuclear Power Plants, CSA N290.12-14 (R2019), Canadian Standards Association, Toronto, 2014.

[100] Aging Management Requirements for Nuclear Power Plants, CSA N290.20:21, Canadian Standards Association, Toronto, ON, Canada, 2021.

[101] Probabilistic Safety Analysis, REGDOC-2.4.2, Canadian Nuclear Safety Commission, Ottawa, ON, Canada, 2022.

[102] C. Grant, J. McCue, and R. Young, "The power is on: How IoT technology is driving energy innovation," Deloitte University Press, New York, NY, United States, 2015. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/energy-resources/deloitte-nl-er-the-power-is-on-iot.pdf

[103] J. Thomson, J. Wei, B. Murrell, K. Hardin, and S. Sanborn. "Digital utility asset management: Building the backbone of the energy transition." Deloitte.com. https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/digital-utility-asset-management.html.

[104] J. Wei, S. Sanborn, and A. Slaughter. "Digital innovation: Creating the utility of the future." Deloitte.com. https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/digital-transformation-utility-of-the-future.html.

[105] Nuclear Energy Agency (NEA), "Unlocking reductions in the construction costs of nuclear: A practical guide for stakeholders," OECD/NEA Publishing, Paris, France, 2020. [Online]. Available: https://www.oecd-nea.org/upload/docs/application/pdf/2020-07/7530-reducing-cost-nuclear-construction.pdf

[106] K. Thomas. "Reactor analytics drives nuclear industry towards machine learning." ReutersEvents.com. https://www.reutersevents.com/nuclear/reactor-analytics-drives-nuclear-industry-towards-machine-learning (accessed Aug.16, 2022).

[107] Nuclear Energy Agency. "Digital transformation: Opportunities and challenges for the nuclear sector." OECD-NEA.org. https://www.oecd-nea.org/jcms/pl_59345/digital-transformation-opportunities-and-challenges-for-the-nuclear-sector (accessed Aug. 16, 2022).

[108] A. Ayodeji and Y.-k. Liu, "Support vector ensemble for incipient fault diagnosis in nuclear plant components," Nuclear Engineering and Technology, vol. 50, no. 8, pp. 1306–1313, Dec. 2018, doi: 10.1016/j.net.2018.07.013.

[109] M. H. da Silva, A. C. do Espírito Santo, E. R. Marins, A. P. L. de Siqueira, D. M. Mol, and A. C. de Abreu Mol, "Using virtual reality to support the physical security of nuclear facilities," Progress in Nuclear Energy, vol. 78, pp. 19-24, Jan. 2015, doi: 10.1016/j.pnucene.2014.07.004.

[110] PwC, "Transformation in energy, utilities and resources: Strategies to confront rising demand and climate threats," PwC, 2019. Accessed: Aug. 16, 2022. [Online]. Available: https://www.pwc.com/gx/en/energy-utilities-mining/pdf/transformation-in-energy-utilities-and-resources.pdf

[111] Reuters. "Digital twin technology identified as key to increased safety and efficiency." ReutersEvents.com. https://www.reutersevents.com/nuclear/digital-twin-technology-identified-key-increased-safety-and-efficiency (accessed Aug. 16, 2022).

[112] Electric Power Research Institute (EPRI), "Quick insight brief: The value and risks of data sharing," EPRI, Paolo Alto, CA, United States, Jul. 30, 2021. Accessed: Aug. 16, 2022. [Online]. Available: https://www.epri.com/research/programs/112925/results/3002022474

[113] Electric Power Research Institute (EPRI), "Automating corrective action programs in the nuclear industry," EPRI, Paolo Alto, CA, United States, Jul. 8, 2022. Accessed: Aug. 16, 2022. [Online]. Available: https://www.epri.com/research/products/000000003002023821

[114] A. Pride, "Information and communication technology infrastructure (ICTi) in buildings," Canadian Standards Association, Toronto, ON, Canada, 2020. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-Research-Information-and-Communication-Technology-Infrastructure-ICTi-in-Buildings.pdf

[115] International Atomic Energy Agency (IAEA), "Integration of analog and digital instrumentation and control systems in hybrid control rooms," IAEA, Vienna, Austria, NP-T-3.10, 2010. [Online]. Available: https://www.iaea.org/publications/8503/integration-of-analog-and-digital-instrumentation-and-control-systems-in-hybrid-control-rooms

[116] International Atomic Energy Agency (IAEA), "Protecting against common cause failures in digital I&C systems of nuclear power plants," IAEA, Vienna, Austria, NP-T-1.5, 2009. [Online]. Available: https://www.iaea.org/publications/8151/protecting-against-common-cause-failures-in-digital-ic-systems-of-nuclear-power-plants

[117] Electric Power Research Institute (EPRI), "EPRI's nuclear laboratory facilities: The welding lab," EPRI, Paolo Alto, CA, United States, Oct. 22, 2009. Accessed: Aug. 16, 2022. [Online]. Available: https://www.epri.com/research/products/1019589

[118] CANDU Owners Group (COG), "Deficiencies in adherence to foreign material exclusion program," COG, Toronto, ON, Canada, OPEX 54592, July 6, 2017.

[119] World Association Nuclear Operator (WANO), "WANO good practice: Nuclear safety environment in virtual reality," WANO, Atlanta, GA, United States, GP 2019-26, December 11, 2019.

[120] National Institute of Standards and Technology (NIST). "Operational technology security." NIST.gov. https://www.nist.gov/programs-projects/operational-technology-security (accessed Aug. 16, 2022).

[121] International Atomic Energy Association. (2021). "Leveraging AI for the nuclear power sector." Presented at IAEA Technical Meeting on Artificial Intelligence for Nuclear Technology and Applications.

[122] World Association of Nuclear Operators (WANO), "GP ATL-11-002," WANO, Atlanta, GA, United States.

Appendix A – Key Figures

Figure 1: Software Definitions and Areas of Overlap in Current Standards

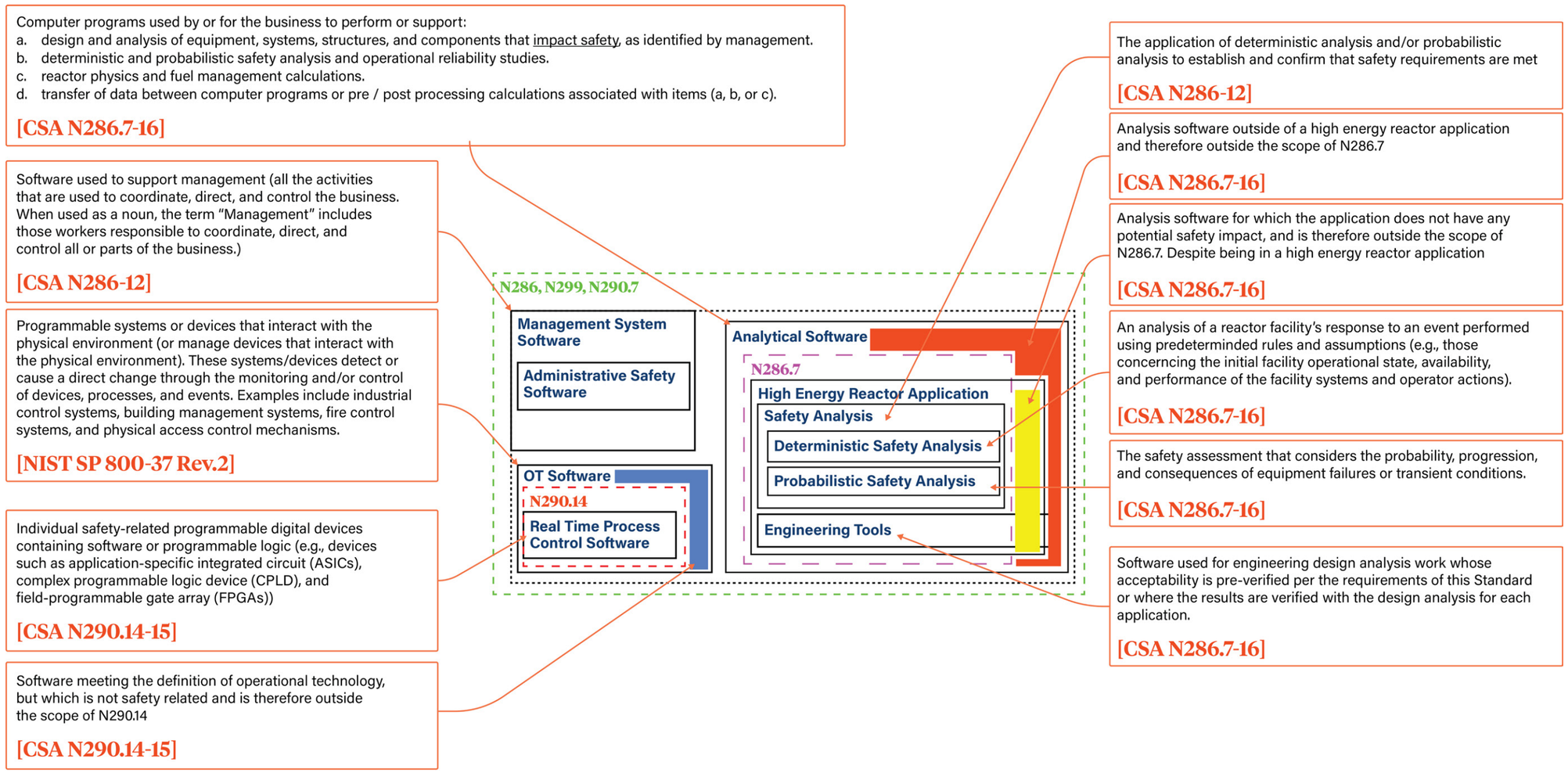


Figure 2: Qualification Methodology for Advanced Analytical (AA) Model Development Software

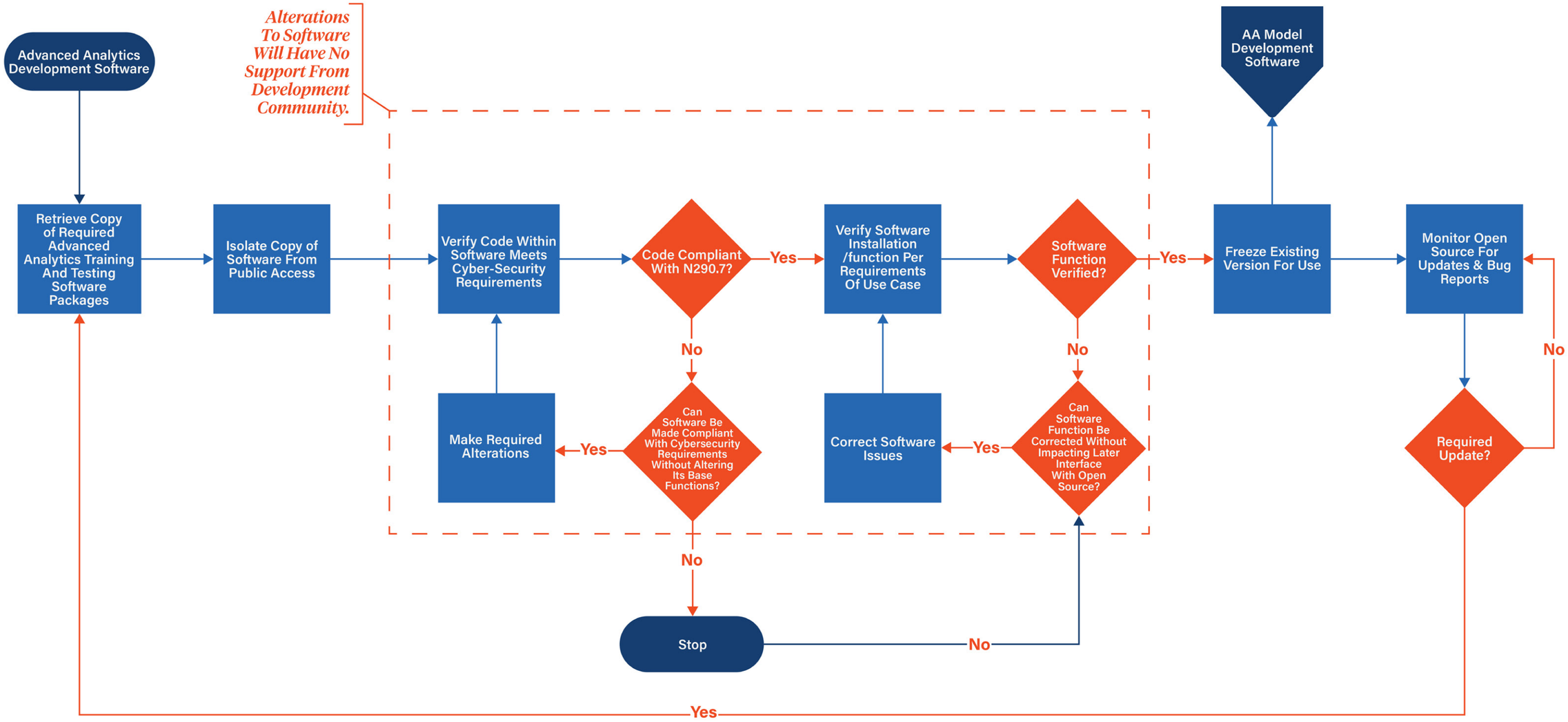


Figure 3: Flow Diagram Comparing Use of Advanced Analytical (AA) Models to Traditional Methods

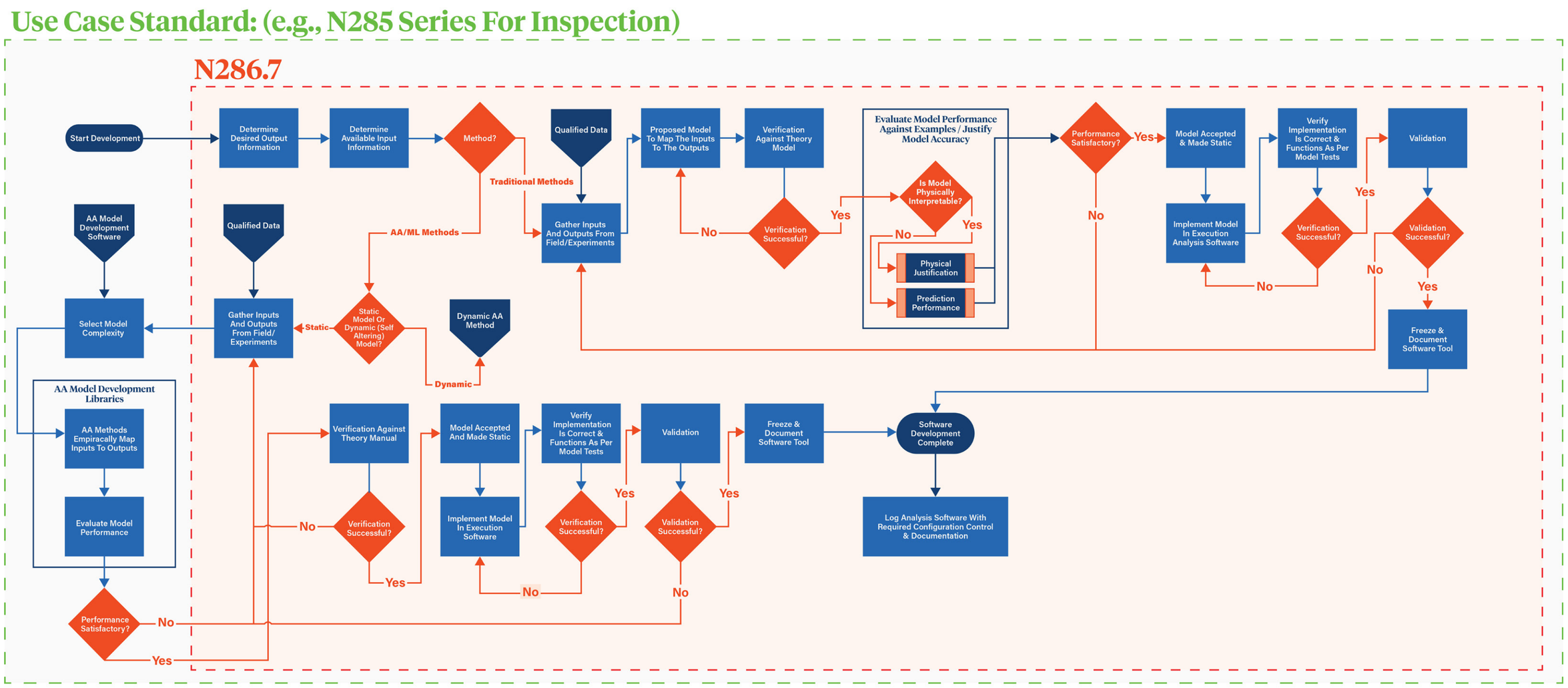
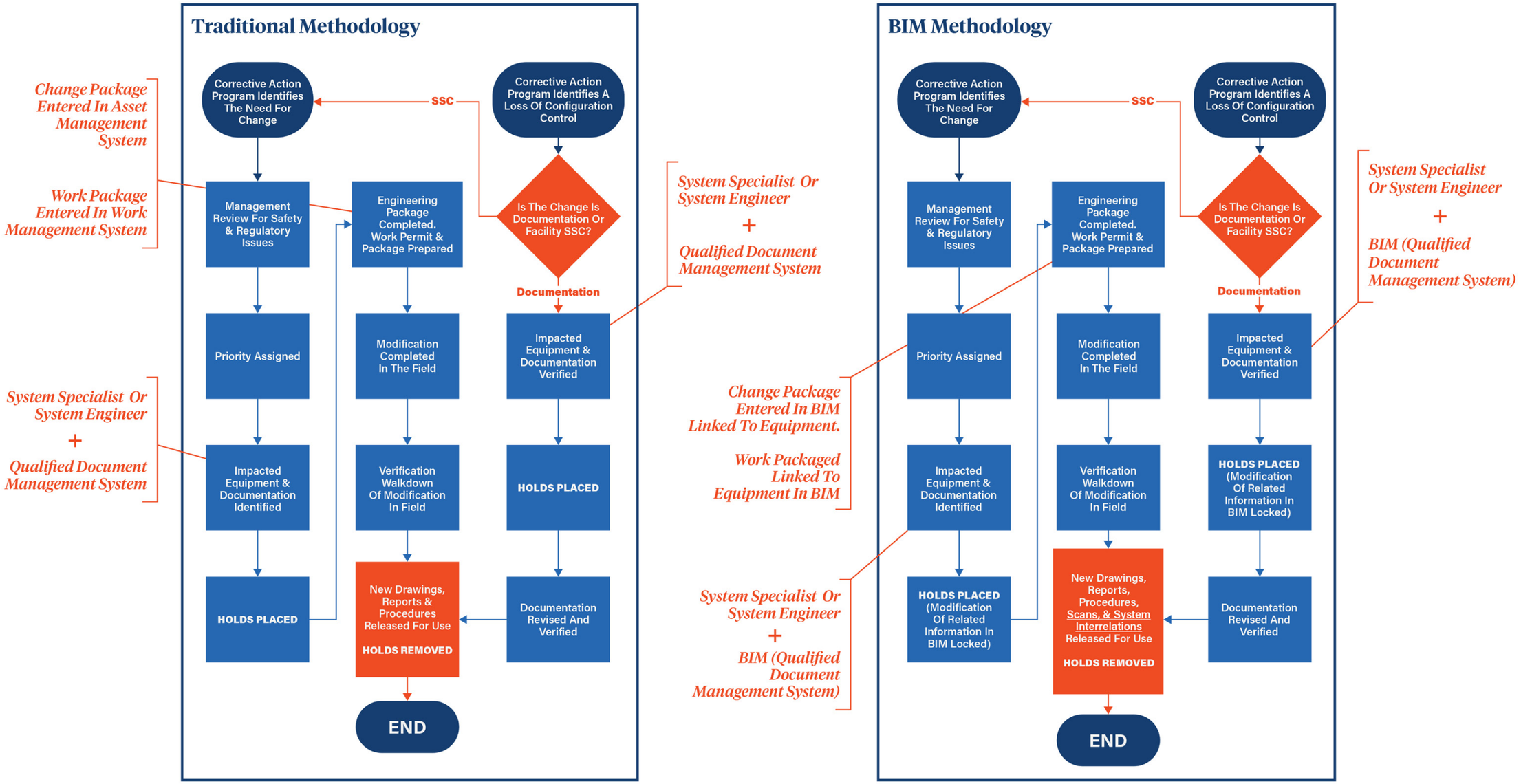


Figure 4: Configuration Management Comparing Use of BIM to Traditional Methods



Appendix B – Resources and Definitions

This appendix includes the CSA nuclear standards referenced in this report, the search terms used for the literature review, as well as relevant definitions, initialisms, and acronyms.

B.1 CSA Nuclear Standards

The following list presents the key CSA nuclear standards that were the primary focus of this report.

1. CSA N285.4, *Periodic inspection of CANDU nuclear power plant components* [85]
2. CSA N285.5, *Periodic inspection of CANDU nuclear power plant containment components* [87]
3. CSA N285.7, *Periodic inspection of CANDU nuclear power plant balance of plant systems and components* [88]
4. CSA N286, *Management system requirements for nuclear facilities* [55]
5. CSA N286.0.1, *Commentary on N286-12, Management system requirements for nuclear facilities* [89]
6. CSA N286.7, *Quality assurance of analytical, scientific, and design computer programs* [1]
7. CSA N299 series (Categories 1 through 4), *Quality assurance program requirements for the supply of items and services for nuclear power plants* [3], [4], [5], [6]
8. CSA N287.7, *In-service examination and testing requirements for concrete containment structures for nuclear power plants* [90]
9. CSA N290.0, *General requirements for safety systems of nuclear power plants* [91]
10. CSA N290.1, *Requirements for the shutdown systems of nuclear power plants* [92]
11. CSA N290.2, *Requirements for emergency core cooling systems of nuclear power plants* [93]
12. CSA N290.3, *Requirements for the containment system of nuclear power plants* [94]
13. CSA N290.4, *Requirements for reactor control systems of nuclear power plants* [95]
14. CSA N290.5, *Requirements for electrical power and instrument air systems of CANDU nuclear power plants* [96]
15. CSA N290.6, *Requirements for monitoring and display of nuclear power plant safety functions in the event of an accident* [84]
16. CSA N290.7, *Cyber security for nuclear facilities* [48]
17. CSA N290.8, *Technical specification requirements for nuclear power plant components* [97]
18. CSA N290.9, *Reliability and maintenance programs for nuclear power plants* [98]
19. CSA N290.12, *Human factors in design for nuclear power plants* [99]
20. CSA N290.14, *Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants* [2]
21. CSA N290.20, *Aging management requirements for nuclear power plants* [100]

B.2 Emerging Technologies Literature Search Criteria and Categorization

The search criteria utilized in the literature review on emerging digital technologies and associated use cases in the nuclear industry are provided in Table 1. The literature review covered a 10-year period from 1-Jun-2012 to 1-Jun-2022, with a primary focus on results that were relevant to design and operation activities.

Table 1: Emerging Digital Technologies Literature Review

Source	Query Details
CSA Group	**Area of focus** = *Nuclear Power Generation* **OR** *Information & Communication Technology*
IAEA	**Keyword** = *Digitalization* **OR** *Digital Technology* **OR** *Emerging Digital*
NEA	**Keyword** = *Digitalization* **OR** *Digital Technology* **OR** *Emerging Digital*
EPRI	**Type** = *Issues & Overviews* **AND** **Sector** = *Nuclear* **AND** **Keyword** = *Digital Twin* **OR** *Virtual Reality* **OR** *Machine Learning* **OR** *Cloud* **OR** *Data Analytics*
EPRI AI	**All material**
COG	**Keyword** = *Digital Twin* **OR** *Virtual Reality* **OR** *Machine Learning* **OR** *Cloud* **OR** *Data Analytics*
WANO	**Keyword** = *Digital Twin* **OR** *Virtual Reality* **OR** *Machine Learning* **OR** *Cloud* **OR** *Data Analytics*
NIST	**Keyword** = *Digitalization* **OR** *Digital Technology* **OR** *Emerging Digital*
Reuters Events	**Keyword** = *Digitalization* **OR** *Digital Technology* **OR** *Emerging Digital*
CNS AI Conferences	**All material**
IAEA Technical Meeting on Artificial Intelligence for Nuclear Technology and Applications	**All presentations**, including those available in the Working Groups and Plenaries
Deloitte	**Keyword** = *Power Plant Digitalization* **OR** *Digital Twin* **OR** *Virtual Reality* **OR** *Machine Learning* **OR** *Cloud* **OR** *Data Analytics*
McKinsey	**Keyword** = *Power Plant Digitalization*
PwC	**Keyword** = *Power Plant Digitalization*
Google Scholar	**Keyword** = *Power Plant Digitalization*

B.3 Definitions, Acronyms, and Initialisms

The following section provides key definitions, acronyms, and initialisms utilized within the body of the report.

B.3.1 Definitions

Analytical software	Computer programs used by or for the business to perform or support: **a)** design and analysis of equipment, systems, structures, and components that impact safety, as identified by management; **b)** deterministic and probabilistic safety analysis and operational reliability studies; **c)** reactor physics and fuel management calculations; and **d)** transfer of data between computer programs or pre-/post-processing calculations associated with items a), b), or c). ***CSA N286.7-16*** [1]
Basic process control system	System that responds to input signals from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but that does not perform any SIF. ***IEC 61511-1, Section 3.2.3*** [59]
Custom software	Software developed for a specific application from a user requirements specification. **Note:** Custom software includes such things as any software that is written specifically for the project, any software that has undergone a major revision as part of the project, and custom programmable logic controller (PLC) logic (ladder logic or function block), etc. ***CSA N290.14:15*** [2]
Deterministic safety analysis	An analysis of a reactor facility's response to an event performed using predetermined rules and assumptions (e.g., those concerning the initial facility operational state, availability, and performance of the facility systems and operator actions). ***CSA N286.7-16*** [1]
Engineering tools	Software used for engineering design analysis work whose acceptability is pre-verified per the requirements of this Standard or where the results are verified with the design analysis for each application. ***CSA N286.7-16*** [1]
Equipment under control (EUC)	Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities ***IEC 61508-4, Section 3.2.1*** [47]

Instrumented system	System composed of sensors (e.g., pressure, flow, temperature transmitters), logic solvers (e.g., programmable controllers, distributed control systems, discrete controllers), and final elements (e.g., control valves, motor control circuits) ***IEC 61511-1, Section 3.2.34.1*** [59]
Management system	The management system of a nuclear organization is a planned and integrated set of processes necessary to satisfy the requirements that must be met to achieve nuclear safety, business success and sustainability. It includes the complete set of policies, manuals and procedures that govern every aspect of how the organization functions. ***CSA N286:12, Clause 0.2*** [55]
Management system software	Software being used within a nuclear organization in capacity which supports or interfaces with the nuclear organization's management system, as defined by CSA N286-12, Clause 0.2. ***CSA N286:12, Clause 0.2*** [55]
Operational technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. ***NIST SP 800-37 Rev. 2*** [54]
Pre-developed software	Software available for use, either commercially or otherwise, prior to design processes. **Note:** Pre-developed software can include operating systems, application software, and firmware. ***CSA N290.14:15*** [2]
Probabilistic safety analysis	The safety assessment that considers the probability, progression, and consequences of equipment failures or transient conditions. ***CSA N286.7-16*** [1]

Qualification	Determination of the acceptability of a candidate product with reference to the safety-related applications for which it is intended to be used. ***CSA N290.14:15*** [2]
Qualification concern	A postulated aspect of a product that has the potential to impede the safety-related functions performed by the product or interfere with the safety-related functions performed by other systems and components. ***CSA N290.14:15*** [2]
Real-time and process control software	Individual safety-related programmable digital devices containing software or programmable logic [e.g., devices such as application-specific integrated circuit (ASICs), complex programmable logic device (CPLD), and field-programmable gate array (FPGAs)]. ***CSA N290.14:15*** [2]
Safety analysis	The application of deterministic analysis and/or probabilistic analysis to establish and confirm that safety requirements are met. ***CSA N286:12*** [55]
Safety instrumented function (SIF)	Safety function to be implemented by a safety instrumented system (SIS) ***IEC 61511-1, Section 3.2.66*** [59]
Safety instrumented system (SIS)	Instrumented system used to implement one or more SIFs ***IEC 61511-1, Section 3.2.67*** [59]
Safety integrity level (SIL)	Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest **Note 1.** The target failure measures (see 3.5.17) for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1. **Note 2.** Safety integrity levels are used for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems. **Note 3.** A safety integrity level (SIL) is not a property of a system, subsystem, element or component. The correct interpretation of the phrase "SIL n safety-related system" (where n is 1, 2, 3 or 4) is that the system is potentially capable of supporting safety functions with a safety integrity level up to n. ***IEC 61508-4, Section 3.5.8*** [47]

Safety-related	A category of applications and systems and their related components and supports that, by failing to perform in accordance with the design intent, have the potential to impact the radiological safety of the public or plant personnel. A safety-related system is a category 1, 2, or 3 system, as defined in Clause 5.2. ***CSA N290.14:15*** [2]
Software	All or part of the programs, procedures/descriptions, rules, and associated documentation of an information processing system. ***CSA N299.1-19*** [3]
Software engineering tools	Software used in development, testing, or maintenance of software. **Note:** Examples include compilers, editors, generators, drivers, and code analyzers. ***CSA N290-14-15*** [2]
Software off-line support tool	Software tool that supports a phase of the software development lifecycle and that cannot directly influence the safety-related system during its run time. Software off-line tools may be divided into the following classes: ▪ T1: generates no outputs which can directly or indirectly contribute to the executable code (including data) of the safety-related system; ▪ T2: supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software; ▪ T3: generates outputs which can directly or indirectly contribute to the executable code of the safety-related system. ***IEC 61508-4, Section 3.2.11*** [47]
Software on-line support tool	Software tool that can directly influence the safety-related system during its run time. ***IEC 61508-4, Section 3.2.10*** [47]
Software safety integrity level	Systematic capability of a software element that forms part of a subsystem of a safety-related system **Note.** SIL characterises the overall safety function, but not any of the distinct subsystems or elements that support that safety function. In common with any element, software therefore has no SIL in its own right. However, it is convenient to talk about "SIL N software" meaning "software in which confidence is justified (expressed on a scale of 1 to 4) that the (software) element safety function will not fail due to relevant systematic failure mechanisms when the (software) element is applied in accordance with the instructions specified in the compliant item safety manual for the element". ***IEC 61508-4, Section 3.5.10*** [47]

B.3.2 Acronyms and Initialisms

AA	Advanced Analytical
ACM	Advanced Condition Monitoring
AI	Artificial Intelligence
AR	Augmented Reality
BIM	Building Information Modelling
CANDU	Canadian Deuterium Uranium
CNSC	Canadian Nuclear Safety Commission
CNS	Canadian Nuclear Society
CSA	Canadian Standards Association
COG	CANDU Owners Group
DT	Digital Twin
EPRI	Electric Power Research Institute
IAEA	International Atomic Energy Agency
ISO	International Standards Organization
I&C	Instrumentation and Control
LIDAR	Laser Imaging, Detection, and Ranging
ML	Machine Learning
NDE	Non-Destructive Evaluation
NEA	Nuclear Energy Agency
NIST	National Institute of Standards and Technology
OPEX	Operating Experience
PIM	Plant Information Model
QA	Quality Assurance
SMR	Small Modular Reactor
VR	Virtual Reality
WANO	World Association of Nuclear Operators

B.4 Active Standards in CSA N285, N286, and N290 Series

N285 Active Standards

CSA N285.0-17/N285.6 SERIES-17 (R2022)	*General requirements for pressure-retaining systems and components in CANDU nuclear power plants / Material standards for reactor components for CANDU nuclear power plants*
CSA N285.0.1-18	*Commentary on CSA N285.0-17, General requirements for pressure-retaining systems and components in CANDU nuclear power plants*
CSA N285.4:19	*Periodic inspection of CANDU nuclear power plant components*
CSA N285.5-18	*Periodic inspection of CANDU nuclear power plant containment components*
CSA N285.6.0.1:22	*Commentary for CSA N285.6-17, Material standards for reactor components for CANDU nuclear power plants*
CSA N285.7:21	*Periodic inspection of CANDU nuclear power plant balance of plant systems and components*
CSA N285.8:21	*Technical requirements for in-service evaluation of zirconium alloy pressure tubes in CANDU reactors*

N286 Active Standards

CSA N286:12 (R2022)	*Management system requirements for nuclear facilities*
CSA N286.0.1:21	*Commentary on N286-12, Management system requirements for nuclear facilities*
CSA N286.7-16 (R2021)	*Quality assurance of analytical, scientific, and design computer programs*
CSA N286.10:16 (R2021)	*Configuration management for high energy reactor facilities*

N290 Active Standards

CSA N290.0:17 (R2022)	*General requirements for safety systems of nuclear power plants*
CSA N290.1-13 (R2018)	*Requirements for the shutdown systems of nuclear power plants*
CSA N290.2:17 (R2022)	*Requirements for emergency core cooling systems of nuclear powerplants*
CSA N290.3:22	*Requirements for the containment system of nuclear power plants*
CSA N290.4:19	*Requirements for reactor control systems of nuclear power plants*
CSA N290.5:16 (R2021)	*Requirements for electrical power and instrument air systems of CANDU nuclear power plants*
CSA N290.6:16 (R2021)	*Requirements for monitoring and display of nuclear power plant safety functions in the event of an accident*

CSA N290.7:21	*Cyber security for nuclear facilities*
CSA N290.8-15 (R2020)	*Technical specification requirements for nuclear power plant components*
CSA N290.9:19	*Reliability and maintenance programs for nuclear power plants*
CSA N290.11:21	*Requirements for reactor heat removal capability during outage of nuclear power plants*
CSA N290.12-14 (R2019)	*Human factors in design for nuclear power plants*
CSA N290.13:18	*Environmental qualification of equipment for nuclear power plants*
CSA N290.14:15 (R2020)	*Qualification of digital hardware and software for use in instrumentation and control applications for nuclear power plants*
CSA N290.15:19	*Requirements for the safe operating envelope of nuclear power plants*
CSA N290.16:16 (R2021)	*Requirements for beyond design basis accidents*
CSA N290.17-17 (R2022)	*Probabilistic safety assessment for nuclear power plants*
CSA N290.18-17 (R2022)	*Periodic safety review for nuclear power plants*
CSA N290.19:18	*Risk-informed decision making for nuclear power plants*
CSA N290.20:21	*Aging management requirements for nuclear power plants*

Appendix C – Detailed Software Assessment Results

Table 2: Software Type and Standards Gap Assessment Results

Item #	Software Type	Relevant Codes, Standards, and Requirements	Description of Clause, Requirement, Recommendation, or Finding	Potential Related Gaps and Issues	Recommendations to Account for Gap
1.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 4	Where new technology is used in the delivery of the fundamental safety functions (cool, control, contain), a means must be available to demonstrate the effectiveness of the technology for all plant states.	**AA, ACM, and PIMs:** The organization must confirm software is suitable for the application and confirm the software functions in the digital environment; if the system is not well understood or changes due to learning conditions, maintaining verification and validation would be a challenge. This is of particular relevance for complex software or models developed by software in such a way that the resultant model is opaque to human review (e.g., complex AA models).	No actions noted at this time.
2.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 6	Where new technology is used to provide a function important to safety, its reliability must be quantified and shown to meet safety requirements.	As stated for item 1.	No actions noted at this time.
3.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 7	Where new technology is used to implement defence in depth in the facility design, it must not reduce the independence of defence in depth levels.	As stated for item 1.	No actions noted at this time.
4.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 14	Where new technology is used in systems important to safety, it must be shown to meet defined acceptance criteria and reliability targets.	**AA:** Lack of available data to train and test AA models may pose an impediment to their use under current standards. Establishing agreed upon acceptance criteria for AA technology supporting systems important to safety or ACM of these systems may also provide an impediment to the use of this software. This is not a direct conflict with the standard, but an outcome of its requirements in relation to the opacity of AA models.	No actions noted at this time.
5.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 16	Where new technology is used in systems important to safety, its failure modes must be quantifiable so that all failure modes can be accounted for in safety analysis and demonstrated to have acceptable consequences.	**AA:** Definition of all failure modes and bounding cases for AA models remains a challenge. The opacity of the mathematical models developed by AA methods prevent direct human review, and the difference between interpolation and extrapolation is not clear for inputs such as image and video data. This is not a direct conflict with the standard, but an outcome of its requirements in relation to the opacity of AA models.	No actions noted at this time.
6.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 21	Where new technology is implemented in safety systems, it must not compromise the independence between safety systems or between redundant elements within a safety system.	**PIMs:** With the implementation of DTs linked to safety systems, if there is potential for transference of data from the DT to the SIS, the DT becomes a common link between otherwise independent SIS, potentially compromising their independence and providing an avenue for a common cause failure. While this is not a gap in the requirements of the standards, it is a limitation they impose on the technology that must be considered during its implementation.	No actions noted at this time.
7.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Reqs. 22–26	Where new technology is implemented in systems important to safety, it must be possible to assign it a safety classification based on its function, and it must meet requirements for reliability, common cause failure, the single failure criterion, and fail-safe design.	**PIMs:** For BIM and DT applications that are connected to multiple systems, if they provide direct feedback to the nuclear facility's systems, the BIM or DT would be required to take on the most stringent safety classification of the systems it provides feedback to.	No actions noted at this time.
8.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 29	Where new technology is implemented in systems important to safety, it must support testing and maintenance activities that demonstrate its reliability and performance.	**AA:** In the case of AA methods, testing is possible, but could require an amount of data that may not be practically available.	No actions noted at this time.
9.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 61	Where new technology is implemented in a reactor protection system, it must have the capability to overrule unsafe actions of the control system.	As stated for item 1.	No actions noted at this time.
10.	**Real-Time and Process Control Software**	IAEA SSR-2/1, Req. 62	Where new technology is implemented in systems important to safety, it must be designed for periodic testing to demonstrate its functionality.	As stated for item 1.	No actions noted at this time.

11.	**Real-Time and Process Control Software**	IEC 61508-7:2010-04, Annex D	A probabilistic approach to determining software safety integrity for pre-developed software. This standard is only applicable if the technology in question will be used for real-time monitoring (with credited operator action) or RTPC in a safety or safety-related system.	**AA:** May limit allowable applications if the AA model must be developed by the organization from their own process data examples and then implemented in software. Additionally, data may be lacking to provide adequate confidence on software usage, failure rates, and bounds of acceptable performance.	Potential to run AA models in parallel with traditional RTPC software and compare outputs to build a case on software performance. Can also test software using synthetic data.
12.	**Real-Time and Process Control Software**	IEC 61511-1:2017-08, Edition 2.1	This standard is only applicable if emerging technology meets the definition of "instrumented system" or "safety instrumented system" or "basic process control system."	**AA:** There are no gaps evident, but requirements may limit the use cases of AA software.	No actions noted at this time.
13.	**Real-Time and Process Control Software**	WNA, I&C Modernization: Current Status and Difficulties, Section 5.3.3: Qualification of Nuclear Safety Components (2020)	Lack of verification and validation documentation makes demonstration of compatibility of updated digital I&C systems within existing installed systems even more challenging.	**ACM, AA, PIMs, and I&C Digitalization:** This is a potential obstacle to the implementation of AA, ACM, and DTs within existing nuclear facilities.	No actions noted at this time.
14.	**Real-Time and Process Control Software**	IAEA, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, Section 4.1.4: I&C implementation using a qualified platform (2009)	This standard applies to digital I&C systems and will be applicable to any system that will be used in nuclear facilities.	**ACM, AA, PIMs, Cloud Computing, and I&C Digitalization:** No gaps noted.	No actions noted at this time.
15.	**Real-Time and Process Control Software**	IAEA, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, Section 4.1.28: Major phases in the licensing process (2009)	Verification steps are aimed at building confidence; however, they should not be regarded as partial approvals that would commit the regulator to an approval of the final product. In the licensing process, the following typical regulatory aspects must be considered: ▪ Scope, categorization, and system definition; ▪ Quality assurance/quality control; ▪ Engineering process; ▪ Strategies and plans; ▪ Assumptions, preconditions, design basis, and requirements; ▪ Regulations, codes, standards, and guidelines; ▪ System architecture and functional, system, and detailed design; ▪ HFE, main control room, HSI; ▪ Verification and validation of plant I&C; ▪ Product platform qualification; ▪ Installation and integration in plant; ▪ Plant documentation; ▪ Organization and competence assurance; and ▪ Operation, maintenance and modifications.	**ACM, AA, PIMs, Cloud Computing, and I&C Digitalization:** Potential lack of detail provided by the licensee and potential lack of knowledge from all parties to understand when gap is present in new technology.	No actions noted at this time.
16.	**Real-Time and Process Control Software**	IAEA, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, Section 4.1.29: Criteria for acceptability (2009)	In regard to digital I&C system implementation, an acceptance of methods and tools to be used in the design phase may require an early audit at the production site of the selected vendor.	**I&C Digitalization:** Important milestones such as factory acceptance tests should be communicated to the regulator to enable their participation if considered necessary.	No actions noted at this time.
17.	**Real-Time and Process Control Software**	IAEA, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, Section 4.1.29: Criteria for acceptability (2009)	Another dimension in the licensing process is to separate between requirements placed on the I&C platform and the requirements placed on the application of the platform.	**I&C Digitalization:** Practical experience has revealed a need to consider both I&C and the corresponding process equipment at the same time to assess additional needs for redundancy and diversity.	No actions noted at this time.

18.	**Real-Time and Process Control Software**	IAEA, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, Section 5.2: Recommendations (2009)	**a.** It is important that all parties establish a mutual understanding of the implementation and licensing process. Simultaneously, addressing the regulatory concerns and those of the utility in the modernization process will expedite the implementation process. **b.** Since the plant lifetime is typically two to three times longer than I&C system lifetime, every utility should have a detailed I&C modernization strategy. Under this strategy, a utility has to develop a comprehensive plan based on the conditions of the existing systems, outage schedules, and remaining life of the plant. **c.** Preference should be given to vendors with an understanding of the relevant licensing/engineering processes. Although the utility is responsible for satisfying regulatory requirements, this can be very difficult to achieve without adequate vendor support. **d.** The requirements/expectations should be defined upfront in order to identify proprietary issues initially and understand the limitations this may present. **e.** Knowledge retention is another major issue in I&C modernization projects. Adequate training and knowledge management strategies should be in place to ensure long-term successful operation of the plant.	**I&C Digitalization:** No gaps noted.	No actions noted at this time.
19.	**Real-Time and Process Control Software**	IAEA, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, Section 4.1.7: Training (2009)	Training of operating personnel should be in phases starting with basic training for handling the HSI, leading up to comprehensive training of the new HSI and functions in the plant simulator. This training should, if feasible, be performed before the factory acceptance test (FAT) and be used as an additional verification and validation activity to validate the new system. After any final rework, the FAT should be performed, and a second round of training should be executed with the reworked function before the upcoming outage in which implementation is scheduled to occur.	**I&C Digitalization:** No gaps noted.	No actions noted at this time.
20.	**Real-Time and Process Control Software**	IAEA, NP-T-1.4, Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants, Section 4.1.10. Design base (2009)	It may be necessary to regenerate the design base upon digitalization of I&C systems.	**AA, ACM, & General Digitization:** The assessment of the design base and its potential reconstitution may require considerable resources with adequate tacit knowledge. In addition, it is necessary to comply with the requirements and boundaries of the safety analysis report and the plant's technical specification.	No actions noted at this time.
21.	**Real-Time and Process Control Software**	CSA N290.14, Sections 1.1 and 1.3	Scope covers digital devices, both software and hardware, used in the I&C of operation of nuclear power plants (NPPs), but does not apply to business systems, analysis software, or passive devices not part of a safety-related system. "1.1. This Standard defines requirements for the process of qualification of digital hardware and software for use in instrumentation and control applications for NPPs." "1.3. This Standard does not apply to business systems (e.g., business applications, desktop computers, email, business networks), analysis software (e.g., scientific, engineering, and safety analysis software), or passive devices (e.g., wires), unless they are part of a safety-related computing system."	**AA:** Embedded digital devices are not clearly identified as applicable. Furthermore, smart devices and self-calibrating devices are not clearly identified as applicable within the standard, and uncertainty may be present on their qualification.	NUREG/CR-7273 looks at emerging technologies in embedded digital devices.
22.	**Real-Time and Process Control Software**	CSA N290.14	All categories are covered, from Category 1 to Category 4, and address how qualification can be achieved.	**I&C Digitalization:** No gaps noted.	No actions noted at this time.
23.	**Real-Time and Process Control Software**	CSA N290.14, Section 5.2.1	The assignment of a safety category for functions fulfilled by emerging technology is covered under 5.2.1. This section refers to IEC 61508-5, IEC 61513, IEC 61226, IEC 61513, and COG-95-264-I for alignment and assignment of safety category. "5.2.1 Functions that are intended to be implemented by the candidate product shall be identified and assigned a safety category in accordance with a standard selected from the reference standards given in Table 1. The safety category of the proposed application shall be determined using the most safety significant function."	**I&C Digitalization:** No gaps noted.	No actions noted at this time.

24.	**Real-Time and Process Control Software**	CSA N290.14, Section 6.2 and Annex A	Per Section 6.2, the candidate product is to be assessed against concerns given in Annex A. Any emerging technology applied to RTPC software will require assessment against Annex A.	**I&C Digitalization:** No gaps noted.	Additional industry effort is required to obtain consensus on a method to address this gap.
25.	**Real-Time and Process Control Software**	CSA N290.14, Section 6.3	Section 6.3 dictates failure analysis requirements for software serving process control purposes. "6.3.1. For Category 1 applications, failure modes shall be identified and analyzed for the candidate product, using a rigorous technique (e.g., FMEA, fault tree analysis (FTA), Hazard and operability analysis (HAZOP), Systems theoretic process analysis (STPA), etc.). Note: For guidance on failure analysis techniques recognized standards such as the following may be used: **a.** IEC 62502 for event tree analysis; **b.** IEC 60812 for failure mode and effects analysis; **c.** IEC 61882 for hazard and operability studies; **d.** IEC 61025 for fault tree analysis; and **e.** EPRI 3002000509 for hazard analysis. 6.3.2. For candidate products that are determined to perform Category 1 functions, or where candidate product complexity warrants, more than one complementary technique should be used. 6.3.3. For Category 2 and 3 applications, failure modes should be identified and analyzed for the candidate product, using a rigorous technique (e.g., FMEA, FTA, HAZOP, STPA, etc.)."	**AA, PIMs, ACM, and I&C Digitalization:** Exhaustive identification of failure modes for complex systems, such as models developed by ML processes or DTs, may not be practical. This issue is of particular note in relation to ML models, because the number of inputs and terms within the mathematical model, as well as the reason behind each one, make reasoning contained within the mathematical model opaque. Furthermore, the potentially qualitative nature of inputs to AA systems (e.g., picture or video inputs), make definition of performance boundaries challenging.	Additional industry effort is required to obtain consensus on a method to address this gap.
26.	**Real-Time and Process Control Software**	CSA N290.14, Section 6.4	Section 6.4 dictates qualification activities for digital items, allowable methods based on safety classification, and applicable development standards by safety class.	**AA:** Emerging technologies may not have the service years or number sold to qualify using the mature product method.	Additional industry effort is required to obtain consensus on a method to address this gap.
27.	**Analytical Software**	IAEA SSR-2/1, Req. 10	Where new technology is used in safety analysis, its output must be verified by independent evaluation.	**AA:** Potential conflict with self-altering AA programs, because changes to the weights and measures within the model would require re verification of the model and its subsequent implementation in the software. This is not feasible for software that alters the model on a relatively continuous basis.	If analytical software is built with a regression suite or set of tests that ensure any updates the software makes to the mathematical model remain within acceptable performance bounds on a qualified static set of test data, it may provide an avenue to verify the analytical software and any model it is capable of producing as a single entity.
28.	**Analytical Software**	CSA N286.7, Clause 1.2 d)	Software used to develop and contain a PIM that is used for analysis is covered by Clause 1.2 d) of N286.7: "programmed applications (e.g., scripts, macros, and spreadsheet-based analysis) written within software normally excluded from this Standard." It should be noted that use of the PIM for configuration management would be covered under CSA N286.10.	**PIMs:** If the analysis portion of the software is not easily separable from the PIM as a whole, the PIM may need to meet the requirements of N286.7, which could present a major impediment to the use of such a system.	Should the software supporting a PIM be used for analysis or operational decision-making, the portions of the software being used to conduct analysis should be clearly and easily separable from the portions of the software providing the analysis inputs. This will allow verification of the analysis portion of the software without requiring verification of the PIM as a whole, beyond its qualification for document and configuration management.

29.	**Analytical Software**	CSA N286.7, Clause 11.2	Use of data from PIMs is covered by Clause 11.2 of N286.7: "11.2. Specific requirements The following requirements shall be met and documented in a form that facilitates independent verification: **a.** Computer programs shall be validated for the intended use in accordance with Clause 10; **b.** Computer programs shall be verified for use on the target platform(s) in accordance with Clause 9.3; **c.** The computer program shall only be used within its documented range of applicability; **d.** The validation basis shall be assessed to ensure that it adequately supports the intended application (see Clause 10.3 f)); **e.** The input data shall be verified to ensure that it adequately represents the physical system or process analyzed; **f.** The derivations and sources of input data shall be documented in a form that facilitates independent verification; **g.** The configuration of the computer program and the input data shall be identified clearly such that results can be reproduced; **h.** The results produced by the computer program shall be reviewed to confirm that they are acceptable; **i.** User qualifications are specified, and the necessary training shall be provided; and **j.** Use of experience shall be in accordance with Clause 4.3."	**PIMs:** No gap evident. Provided the analytical software has a defined boundary from the PIM, the requirements listed here apply for information retrieved from or supplied by the PIM in support of analysis.	No actions noted at this time.
30.	**Analytical Software**	CSA N286.7, Clause 1.3	Development and maintenance of ACM and predictive toolset software is exempt from N286.7, per Clause 1.3: "1.3. This Standard does not apply to computer programs such as: **a.** those used to control plant safety systems and operational control systems; **b.** Note: See CSA N290.14 for example of safety and operational control systems. **c.** embedded software contained within items, where the software is qualified along with the item as a unit (e.g., measurement and test equipment); **d.** software used to collect or present design inputs (e.g., data acquisition systems and CAD programs); **e.** business software (e.g., work management, productivity tools, commercially available databases, and spreadsheet programs); **f.** software used to manage information (e.g., records management software); **g.** commercially available compilers, interpreters, and operating systems; and **h.** commercially available mathematic routine libraries." However, use of data gathered by ACM and predictive toolsets could be used as analysis inputs (initial conditions) or to validate analytical software. In these cases, N286.7 requirements for use of data and validation would apply.	**AA:** No gap evident regarding applicable scope with respect to AA methods by use case. However, there is ambiguity about the extent and applicability of exceptions where AA software packages are concerned. Whether AA software libraries are considered standard mathematical libraries is not confirmed within the standard. Additionally, clarification on the applicability of this exception in static versus dynamic AA models is also required, because in static models, AA libraries cannot impact the model after completion of training, testing, and validation. It was noted that there may be a lack of clear requirements for the handling of analytical software when it is being used to support, or is a part of, RTPC software. This presents a challenge with respect to the use of AA methods within I&C.	Clarification of requirements for an AA library to be considered a "routine mathematical library" is recommended. Validation and verification of these libraries would require a level of effort that may highly constrain or otherwise limit the use of AA methods within the industry. Language within N286, N286.7, and N290.14, on requirements for the use of mathematical models created by AA methods within RTPC software, should be reviewed to ensure that the use of static and dynamic AA models is well handled by the standards and the requirements based on use case are clearly defined.

31.	**Analytical Software**	CSA N286.7, Clauses 6–9	The following clauses govern the development and maintenance of cloud-based software: "6. Software configuration management; 7. Change control; 8. Design, development, and maintenance; and 9. Acquisition." If analytical software is maintained on a cloud-based platform but transferred to a local platform for execution, Clause 9.3 would apply: "9.3. Software transfers When software is physically or electronically transferred from one location to another, the receiving business or organization shall verify: that the specified version was received; and b) the software execution through application of the installation verification test suite"	**Cloud Computing:** No gaps noted.	No actions noted at this time.
32.	**Analytical Software**	CSA N286.7, Clauses 10.1.1 and 10.1.2	Validation of software for its intended use case is required per N286.7: "10.1.1. Computer programs and their models shall be validated for their intended use. 10.1.2. Validation shall **a.** assess adequacy and applicability of the models employed in the computer program; **b.** demonstrate computer program capabilities and limits; and **c.** determine computer program accuracy."	**AA:** Whether the AA model must undergo validation depends on whether it is calculating a physical parameter. If it is not, the AA model is not required to undergo validation under N286.7, only verification. Validation of the model may be difficult to achieve under N286.7, because the large-scale and opaque nature of the models developed through methods such as ML make justification of individual model parameters and overall calculation methodology in comparison to accepted physical laws infeasible. This makes validation via comparison to relevant closed-form mathematical solutions and relevant solutions to standard problems difficult. Additionally, the creation of AA models is typically stochastic in nature, meaning that the same set of training data and same learning algorithm could produce two different models. These models would be similar in performance capabilities, but their exact values would not be identical. This problem is more pertinent for dynamic AA models, which cannot simply be tested for performance against test data, because the models themselves change during operation.	Separating validation of the model from verification of the analytical software is a potential avenue for qualification of analytical software, which uses mathematical models developed by AA methods. The mathematical model performance is verified to meet the accuracy requirements of the intended use case under the standard governing that work. The verification of the software is then consist of checking the correct implementation of the mathematical model in the execution software, and the alignment of the performance of the execution software with that of the qualified model. It should also be noted that this method encounters problems for continually self-adjusting AA models, because there is difficulty ensuring the model performance remains within allowable bounds.
33.	**Analytical Software**	CSA N286.7, Clause 10.1.3	For AA methods that are not used to calculate physical parameters, or outcomes through calculation of the parameters, validation under N286.7, Clause 10 is not applicable. "10.1.3. Computer programs that do not calculate values of physical parameters shall be exempt from the requirements of Clause 10. Note: Validation as defined in this Standard cannot be performed on computer programs that do not calculate a physical parameter. Such computer programs include those used for probabilistic safety assessments (e.g., event tree and fault tree analysis)."	**AA:** As noted in item 32.	As noted in item 32.

34.	**Analytical Software**	CSA N290.9, Clause 4.4	The sources of data, methods, assumptions and judgments, justifications, limitations, models, activities, results, assessments, performance measures, and corrective actions that constitute the reliability and maintenance programs shall be documented such that they can be **a.** independently reviewed; **b.** independently reproduced; and **c.** applied in activities at the NPP.	**AA:** As AA models are typically developed through stochastic means, supplying the same learning algorithm and same training data to an independent reviewer does not guarantee that the model produced is identical. The mathematical model may be similar in performance and coefficients, but it is unlikely to be identical. This presents challenge to the requirement that the model can be independently reproduced if that reproduction must be identical.	This gap could be bridged through justification that reproduction of model performance from qualified training data and a qualified AA algorithm constitutes independent reproduction of the model, even if the model factors are not identical.
35.	**Analytical Software**	CSA N290.9, Clause 6.4	Clause 6.4 applies to reliability modelling. Any software-based models used for reliability modelling would require compliance with this section.	**ACM:** Probabilistic risk assessments and reliability models calculate component failure rates based on the number of failures that occur during routine surveillances (e.g., safety-related system tests and calibration). The models assume that these tests are performed at routine and short intervals. Using performance-based maintenance, utilities have been able to significantly reduce the frequency of routine surveillances. It is not clear that an industry consensus has been achieved on how to incorporate real-time monitoring and the use of performance-based maintenance into probabilistic safety assessments and reliability models that rely on surveillances performed at routine and short intervals.	Additional industry effort is required to obtain consensus on a method to address this gap.
36.	**Analytical Software**	CSA N299.1-19, Clause 4.5.1 c)	Software employed in work methods or tools shall be verified or validated, as appropriate.	**AA:** The organization must confirm software is suitable for the application and confirm the software functions in the digital environment; if the system is not well understood or changes due to learning conditions, maintaining the verification and validation would be a challenge.	Additional industry effort is required to obtain consensus on a method to address this gap.
37.	**Analytical Software**	CSA N299.1-19, Clause 7.10 b)	For all measuring and testing equipment (M&TE) used for item and service acceptance, the supplier shall verify and document the ability of the software to satisfy the intended application for cases where software is used in the actual calibration of the M&TE prior to initial use, and re-verify when changes to the software are implemented.	**AA:** The organization must confirm software is suitable for the application and confirm the software functions in the digital environment; if the system is not well understood or changes due to learning conditions, maintaining the verification and validation would be a challenge.	Additional industry effort is required to obtain consensus on a method to address this gap.
38.	**Analytical Software**	ASME NQA-1-22, Part II, Subpart 2.7-202	Software verification shall include, as appropriate, verification activities of the completeness and testability of the software requirements, verification of the technical adequacy of the design, verification that the software design and test cases are traceable to the software requirements, and verification of the maintainability and correctness of the software.	**AA:** The organization must confirm software is suitable for the application and confirm the software functions in the digital environment; if the system is not well understood or changes due to learning conditions, maintaining the verification and validation would be a challenge.	Additional industry effort is required to obtain consensus on a method to address this gap.
39.	**Management System**	IAEA SSR-2/1, Req. 2	Where new technology is used in the implementation of the designer's management system, it must not prevent the ability of the designer to demonstrate that all safety requirements have been implemented in the final design.	No gaps noted.	No actions noted at this time.
40.	**Management System**	IAEA SSR-2/1, Req. 8	Safety, security and safeguards measures must be implemented in such a way that one does not compromise another. This requirement applies to new technology used in safety, security or safeguards elements of the facility design.	No gaps noted.	No actions noted at this time.

41.	**Management System**	CSA N286, Clause 4.8.2	"Conduct of work shall be authorized and carried out using controlled (b) software, including engineering tools and analytical software."	**AA:** Control of software that is self-adjusting, such as AA models, is difficult to define, because determining the performance of the software, given its ability to self-adjust, requires bounding software performance not only for the mathematical model that the software starts with but also for any mathematical model it could produce during self-alteration. **Cloud Computing:** Control of software is complicated by the use of third-party hardware.	AA software that can adjust the mathematical model used for analysis remains a poorly defined area in terms of qualification requirements. One possible method for qualification includes bounding the allowable changes to the model against a "regression suite" that tests whether the changes made to the model still meet the required performance criteria prior to use of the altered model. Where cloud computing is used, requirements for cyber security, configuration control, and supply of supporting software are present in the CSA nuclear standards.
42.	**Management System**	CSA N286, Clause 7.4.2	"Safety analysis activities shall be controlled and include **a.** identification of the following… **iii.** the mathematical models used to simulate the physical processes and their limitations; **iv.** the acceptance criteria applicable to safety analysis results; and **v.** the tools, analytical software, and test apparatus used in the safety analysis. The selected tools shall be validated to confirm that they are suitable for performing the safety analysis"	**AA:** Validation of AA models may present challenges as noted in item 32.	As noted in item 32.
43.	**Management System**	CSA N286, Clause 7.3.4	Design tools shall be appropriate for the application and controlled. Scientific and analytical computer programs shall be controlled in accordance with CSA N286.7.	**AA:** Control of design tools using AA methods present challenges as noted in item 41.	As noted in item 32.
44.	**Management System**	CSA N286, Clause 7.4.3	Safety analysis tools shall be appropriate for the application and controlled. Scientific and analytical computer programs shall be controlled in accordance with CSA N286.7.	**AA:** No gaps noted.	No actions noted at this time.
45.	**Management System**	CSA N299.1-19, Section 7.16.4.1	"Records shall: **a.** be retrievable, maintained, and routinely inspected to ensure that they are in good condition; **b.** be stored in suitably maintained environmental conditions during the established retention period for the preservation, legibility, and prevention of degradation, damage, and loss of all records, including electronic record media. Activities detrimental to the records shall be prohibited in the records storage areas; **c.** for electronic record media, remain retrievable and readable, notwithstanding changes in hardware, software, and technology; **d.** be controlled and restricted to authorized personnel when processing, storing, and retrieving records."	**Cloud Computing:** The organization (i.e., record generator/owner) does not have control of records, per the standard, for full retrievability. There are also export controls to consider because servers may not be within Canadian borders.	Additional industry effort is required to obtain consensus on a method to address this gap.
46.	**Management System**	ASME NQA-1-22, Part I, Section 17-200 c)	Records to be generated, supplied, or maintained shall be specified in applicable documents, such as design specifications, procurement documents, test procedures, and operational procedures.	**Cloud Computing:** The organization (i.e., record generator/owner) does not have control of records, per the standard, for full retrievability. There are also export controls to consider because servers could be in any country.	See Revision 1 of EPRI NP-5652 and TR-102260, Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications.
47.	**Management System**	CSA N299.1-19, Section 4.5.1 b)	Software employed in work methods or tools shall be placed under configuration control	**Cloud Computing:** Software used may not be able to be placed under configuration control if the organization does not have control of the software.	Additional industry effort is required to obtain consensus on a method to address this gap.

48.	**Management System**	ASME NQA-1, Part II, Subpart 2.7-203	Software configuration management shall include, but is not limited to, configuration identification, change control, and configuration status control. Configuration items shall be maintained under configuration management until the software is retired.	**Cloud Computing:** Software used may not be able to be placed under configuration control if the organization does not have direct control of the software or hardware.	Additional industry effort is required to obtain consensus on a method to address this gap.
49.	**Management System**	CSA N299.1-19, Sections 7.6.5, 7.7.3, and 7.21.2 ASME NQA-1-22, Part I, Section 18-100	Assessments, audits, and inspections are required to be performed physically on-site. While not explicitly stipulated in the standards, they do require such assessments to be performance-based and in-person.	**AR and VR:** Audits and assessments are performance-based and, notwithstanding some minor instances, must be performed physically on-site. However, with sufficient simulated or AR, being physically on-site may not be necessary.	See EPRI 3002020796, Remote Assessment Techniques.
50.	**All Software Types**	IAEA SSR-2/1, Reqs. 9 and 18	Requirement for items that are important to safety to follow proven engineering practices. "Items important to safety for a nuclear power plant shall preferably be of a design that has previously been proven in equivalent applications, and if not, shall be items of high quality and of a technology that has been qualified and tested."	**All Software Types:** This requirement may be difficult to meet for emerging new technologies. The specific wording in REGDOCs (developed from SSR-2/1 and legally in effect in Canada) should be consulted to identify an approach for compliance. SSR-2/1 allows for safety to be demonstrated through R&D and testing.	No actions noted at this time.
51.	**All Software Types**	IAEA SSR-2/1, Req. 39	When new technology is implemented in a nuclear facility, it must not provide a pathway for unauthorized access to systems within the facility.	**All Software Types:** Cloud computing, remote control of inspection equipment, and I&C equipment connected to a PIM that is not completely separated from networks external to the facility all provide the potential for unauthorized access to facility systems. The use of open source AI software for the creation of AA models also provides a potential avenue for access to plant systems, because the software cannot be developed entirely under the control of a nuclear qualified supplier.	Existing cyber security requirements under N290.7 address the allowable use cases and security needs for items such as remote control of inspection equipment and encryption and access control requirements for plant information within a PIM. Similarly, for analytical software, software supporting RTPC, and management support software, the CSA nuclear standards speak to requirements for cyber security, configuration control, and maintenance of data integrity in both storage and transfer. The use of open source software is not prevented by the standards, provided the instance of the software to be used is removed from public access and verified to be compliant with the requirements of the relevant standards (see Figure 2).
52.	**All Software Types**	IAEA SSR-2/1, Req. 41	New technology used in systems that are important to safety must not cause a loss of safety function as a result of fluctuations in electrical power supply.	**All Software Types:** The more interconnected software providing direct support to SIS becomes, the more vulnerable it is to fluctuations in power supply. This is particularly key in the use of cloud computing to support software interacting with SIS, because off-site infrastructure will not be supported by the facility's back-up power supplies. If data from PIMs becomes integral to the operation of a SIS, the PIM must remain reliable regardless of power fluctuations, unless the safety function of the device connected with the PIM is capable of functioning independently of that connection.	No actions noted at this time.
53.	**All Software Types**	IAEA SSR-2/1, Req. 63	New technology implemented in systems that are important to safety at a nuclear facility shall be developed under a quality management system.	**All Software Types**: Existing software quality assurance standards may have gaps regarding the lifecycle management of new technologies.	Additional industry effort is required to obtain consensus on a method to address this gap.

54.	**All Software Types**	CSA N299, Clauses 1.3.1 and 1.3.2	Per clauses 1.3.1 and 1.3.2, N299.1–4 is applicable across software types, except for analytical software. "1.3.1. The requirements of this Standard apply to the control of the use of software employed in the operation of process, production, inspection, and test equipment." "1.3.2. This Standard does not apply to the design, use, development, or coding of analytical software. Note: When a QA program is needed for these aspects, then a standard written specifically for them should be used."	**All Software Types:** No gaps noted.	Additional industry effort is required to obtain consensus on a method to address this gap.
55.	**All Software Types**	CSA N299, Clauses 4.4.1 and 4.4.2	N299.1–4 places documentation, configuration control, and verification and validation requirements on software, and requires performance testing for software, including when embedded into items or services. "4.4.1. Software employed in work methods or tools shall be **a.** documented and approved; **b.** placed under configuration control; and **c.** verified or validated as appropriate." "4.4.2. Software that forms part of or is incorporated into items or services shall be subject to performance testing and final acceptance in accordance with this Standard. When known, the customer shall be promptly notified that an item to be supplied includes embedded software."	**All Software Types:** No gaps noted.	No actions noted at this time.
56.	**All Software Types**	CSA N299, Clause 5.5.2.7	"5.5.2.7. When software is used for design analysis of the item or service, the supplier shall **a.** control the software and verify that the software is adequate for its intended use; **b.** identify the computer, the computer program name and revision/version, and the method(s) used for verification supporting the application of the computer program to the specific physical problem; and **c.** control and maintain the records in accordance with Clause 5.5.14."	**All Software Types:** No gaps noted. However, verification of analytical software may present challenges as a result of the complexity of the models developed. Additionally, the requirement for identification of the computer on which the software is to run presents challenges for cloud-based computing with analytical software.	Requirements for guarantee of device location and/or specific device usage may be put in place for cloud computing implementation to ensure alignment with cyber security requirements.
57.	**All Software Types**	CSA N299, Clause 5.5.4 b)	Covers requirements for software used in measurement and testing equipment. "5.5.4. For all measuring and testing equipment used for item and service acceptance, the supplier shall: b) verifies and document the ability of the software to satisfy the intended application for cases where software is used in the actual calibration of the measuring and testing equipment prior to initial use, and re-verify as necessary."	**All Software Types:** No gaps noted.	No actions noted at this time.
58.	**All Software Types**	CSA N299, Clause 5.5.6 k)	Covers requirements for software used in inspections and tests: "5.5.6. The supplier shall identify the following in the inspection and test planning document(s): k) where software is used for verifying item or service quality, that verification of the ability of software to satisfy the intended application has been performed and documented prior to initial use."	**All Software Types:** No gaps noted.	No actions noted at this time.

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™

© 2023 Canadian Standards Association. All Rights Reserved.