INL/RPT-23-74867
Revision 1

Digital Engineering and Cybersecurity Decision Analysis in Early Phases of SMR-Driven IES Projects

September 2023

DOE-NE Cybersecurity Milestone Report

Shannon Eggers, Robert Youngblood, Matthew Overlin, Ruixuan Li, Joseph Mahanes, Katya Le Blanc
Idaho National Laboratory

Idaho National Laboratory

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

INL/RPT-23-74867
Revision 1

Digital Engineering and Cybersecurity Decision Analysis in Early Phases of SMR-Driven IES Projects

DOE-NE Cybersecurity Milestone Report

Shannon Eggers, Robert Youngblood, Matthew Overlin, Ruixuan Li, Joseph Mahanes, Katya Le Blanc
Idaho National Laboratory

September 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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

Page intentionally left blank

ABSTRACT

Considerable efforts are underway to ensure cybersecurity is integrated into the systems engineering lifecycle. Cyber-informed engineering and security-by-design frameworks are intended to identify and engineer out cybersecurity risks throughout the lifecycle. While these approaches are valuable for promoting the need to include cybersecurity considerations in early design phases to create more secure systems, they may not consider the entirety of digital risks. Digital risks in a digital instrumentation and control system include adversarial and unintentional risks from internal and external factors, such as human performance errors, design flaws, environmental conditions, and equipment degradation or failure. This report provides a detailed discussion on digital risk prior to describing the background and concept of operations for a small modular reactor-driven integrated energy system connected to industrial applications. The challenges of competing objectives and competing stakeholder requirements are discussed and the impacts on digital engineering, security considerations, and interdependencies are evaluated for mission-level, facility-level, and system-level decisions.

Page intentionally left blank

TABLE OF CONTENTS

FIGURES

TABLES

Page intentionally left blank

ACRONYMS

ACE	area control error
AGC	automatic generation control
CIE	cyber-informed engineering
BES	bulk electric system
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CONOPS	concept of operations
DOE	Department of Energy
EPRI	Electric Power Research Institute
GDC	general design criteria
H_2	hydrogen
HTSE	high temperature steam electrolysis
I&C	instrumentation and control
ICCP	inter-control center communications protocol
IEC	International Electrotechnical Commission
IES	integrated energy systems
INPO	Institute for Nuclear Power Operations
LFC	load-frequency control
MBSE	model-based systems engineering
MED	multi-effect distillation
MWe	megawatt electric
MWth	megawatt thermal
NASA	National Aeronautics and Space Administration
NPP	nuclear power plant
NSSS	nuclear steam supply systems
OT	operational technology
PFC	primary frequency control
PRA	probabilistic safety analysis
RIMES	Risk-Informed Management of Enterprise Security
RTO	regional transmission operator
SBOM	software bill of materials
SMR	small modular reactor
SNM	special nuclear material
SSC	structures, systems, and components
STPA	system-theoretic process analysis

Page intentionally left blank

Digital Engineering and Cybersecurity Decision Analysis in Early Phases of SMR-Driven IES Projects

1. INTRODUCTION

The cyber-informed engineering (CIE) framework is an approach to integrate cybersecurity into the systems engineering lifecycle of physical systems or devices that have digital connectivity, monitoring, or control [1]. CIE includes fundamental design and operational principles, as well as organizational principles, to identify and engineer out cybersecurity risks early and often throughout the lifecycle to reduce the impact from intelligent and adaptive adversaries [1]. While a CIE strategy is imperative to change fundamental behaviors and processes associated with ensuring nuclear digital instrumentation and control (I&C) systems are built with cybersecurity in mind, there is still an unmet need to develop a decision analysis framework that includes all forms of digital risk, including non-adversarial risk.

An ultimate objective of CIE is to ensure cybersecurity is simply part of the baseline systems engineering development processes alongside all the other design inputs and considerations, such as functionality, performance, and safety. A systems engineering process for digital I&C systems should include all forms of risk, especially intentional and unintentional risk from internal and external factors, such as adversarial actions, human performance errors, equipment condition, and environmental hazards. A goal of this report is to demonstrate how cybersecurity can be integrated as another discipline within the early phases of the design process in nuclear digital engineering projects. Additionally, since functionality, safety, and security are often competing objectives in nuclear applications and separate development teams on large projects may have competing priorities, this report also provides guidance on how to evaluate, document, and maintain the underlying decisions affecting security.

2. BACKGROUND

2.1 Systems Engineering Lifecycle

INCOSE defines systems engineering as a “transdisciplinary approach and means to enable the realization of successful systems” that satisfy the needs of the customers, users, and other stakeholders [2]. The set of systems may include typical digital I&C components, such as hardware, software, and firmware, as well as people, information, techniques, facilities, services, and other support elements [2]. While some authorities define digital engineering as the use of digital technology to enable the systems engineering process, in this report digital systems engineering is the set of systems engineering lifecycle activities used specifically for operational technology (OT) or digital I&C systems.

A systems engineering lifecycle includes all phases throughout the life of a system, from conceptual design to low level, detailed design, manufacturing, operation, and disposal or decommissioning. Systems engineering requires analysis, specification, and design, as well as verification and validation to ensure requirements (e.g., function, operation, safety, performance, security, quality, cost) are balanced to meet the needs of the stakeholders. This report is focused on the early systems engineering lifecycle for nuclear engineering projects. Figure 1 illustrates the systems engineering v-model denoting the early design phases of concept exploration, concept of operation, and system definition and design. Stages in these early design phases include business planning, feasibility studies, identification of stakeholder and functional requirements and the start of high-level design. Nuclear engineering projects must satisfy numerous stakeholders in design, operational, regulatory, and business continuity areas. Further, nuclear engineering projects often have stringent safety requirements that often constrain the degree to which other stakeholder objectives can be satisfied.

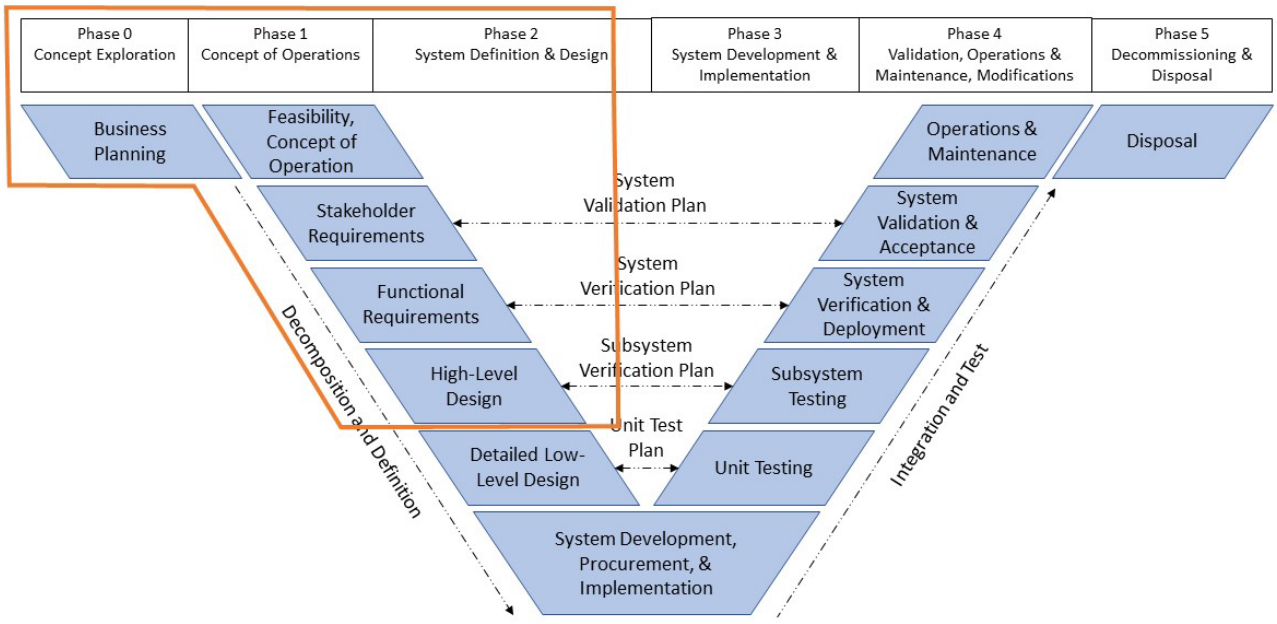

Figure 1. The systems engineering v-model indicating the early design stages.

2.2 Digital Systems Engineering in the Nuclear Industry

In the nuclear power industry, there are many U.S. [3-8] and international [9-15] standards and guidance documents for the design of digital safety systems that may be used to comply with State nuclear regulations. From a safety perspective, general design criteria (GDC) for nuclear safety systems typically include independence, safety, function redundancy, separation and other single-failure criterion in I&C systems, such as electrical isolation, defense in depth, and technology diversity [4, 6]. The objective is to ensure no single failure or component will interfere with the safety function and proper operation of the safety system [6]. There are also many standards and guidance documents for design of non-safety digital systems [16-18].

Additionally, the Electric Power Research Institute (EPRI) issued multiple documents under their integrated digital systems engineering framework, including the "Digital Engineering Guide (DEG): Decision Making Using Systems Engineering" [19]. The Institute of Nuclear Power Operations (INPO) also issued NISP-EN-04 revision 2, "Standard Digital Engineering Process," [20] which is intended for use in conjunction with IP-ENG-001, "Standard Design Process," [21] and the EPRI DEG. NISP-EN-04 identifies digital engineering activities to execute for engineering changes, while the EPRI DEG provides guidance on how to execute the activities.

From a security perspective, nuclear digital engineering projects in the U.S. must satisfy the requirements of 10 C.F.R.§73, *Physical Protection of Plants and Materials* [22], which includes 10 C.F.R.§73.54 [23], *Protection of Digital Computer and Communication Systems and Networks,* colloquially known as "the cyber rule." EPRI also issued a "Cyber security technical assessment methodology" [24] to address cybersecurity as part of their DEG process. Internationally, there is also a body of international standards and guidance documents for computer security of industrial control systems [25-38]. Further, for nuclear engineering projects that interface with the bulk electric system (BES), there are a series of standards for operation, reliability, and security [39-42].

2.3 Digital Risk

2.3.1 Digital risk

Although severe accidents are often considered when "risk" is mentioned in connection with nuclear power plants (NPPs), risk can be viewed more broadly as the potential for performance shortfalls relative to management intent based on stakeholder requirements. For this report, it is appropriate to focus on the categories of unacceptable consequences that could occur when critical functions in an NPP are adversely impacted via digital means. As shown in Figure 2, these consequences may include undesired impacts to public health and safety, worker safety, nuclear material and accounting, environmental health, capacity factor, financial health, and organizational/industry reputation.

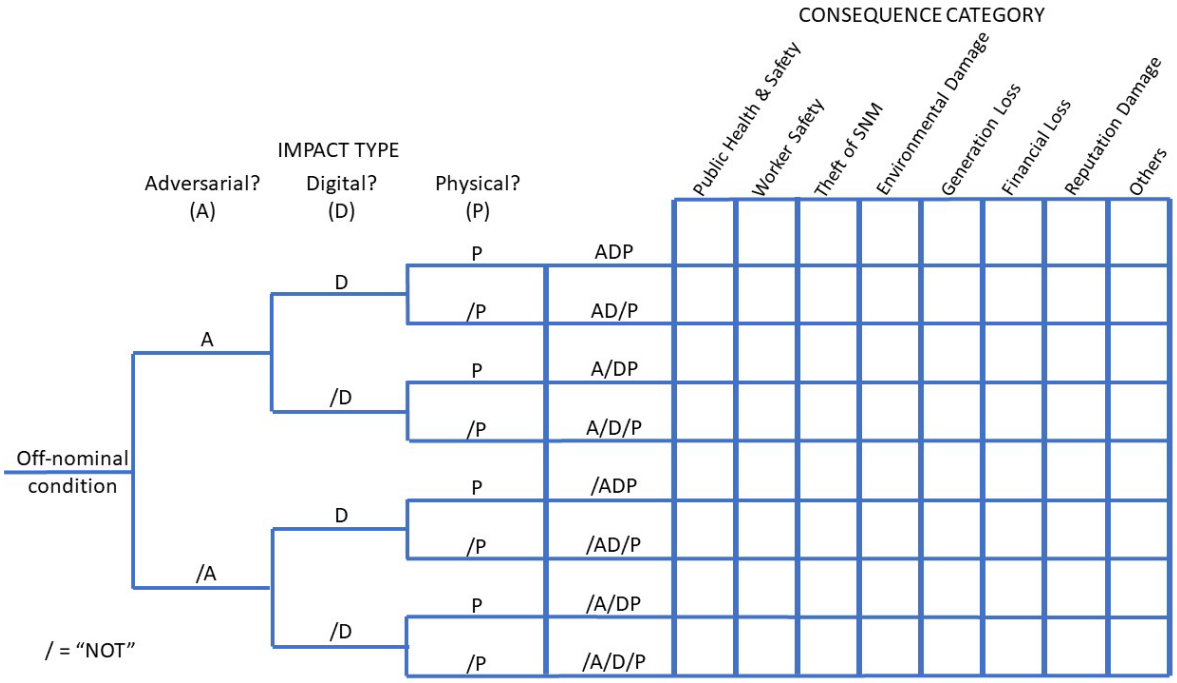

Figure 2. Event tree with impact types and consequence categories.

Figure 2 illustrates an example of a high-level event tree leading to undesired impacts. The figure represents a systematic way of thinking about stakeholder requirements, recognizing different types of adverse consequences that need to be prevented and different modes in which those consequences might be caused. Moving from left to right through the tree structure corresponds to a class of scenarios, characterized by the symbols in Table 1.

Note that the figure and tables are potential tools for evaluating stakeholder requirements. There are likely different scenarios or sequences that can be identified for a given project or system. For instance, while Table 1 and Table 2 indicate that D and P are digital and physical "impacts," another analysis could also evaluate D and P as "incident occurrence pathways" (e.g., digital-enabled attack, physical-enabled attack). Regardless, it is important to analyze both digital and physical impacts as well as digital and physical pathways.

The high-level consequence categories shown in Figure 2 do not represent an exhaustive list, especially for industrial facilities other than NPPs. Systems engineers and stakeholders must identify and prioritize the high-consequence events that should be addressed during engineering design. Of course, NPPs are constrained by the need to satisfy regulatory requirements aimed at preventing radiological

release or theft of special nuclear material (SNM). Sections 3.1 and 3.2 discuss these competing objectives and competing stakeholder requirements in further detail.

Table 1. Description of each symbol indicated in Figure 2.

Symbol	Definition	Description
A	Adversarial action	Caused, at least partly, by a bad actor.
/A	Non-adversarial action	Not caused by adversarial means. For instance, caused by unintentional human actions, failure or degradation of components, or environmental conditions.
D	Impact to digital SSCs	Involves denial, degradation, disruption, or destruction of information flow, including failure of digital structures, systems, or components (SSCs) or corruption of data flow.
/D	No impact to digital SSCs	Information flow and digital SSCs are not impacted.
P	Impact to physical SSCs	Involves denial, degradation, disruption, or destruction of physical SSCs.
/P	No impact to physical SSCs	Physical SSCs are not impacted.

Table 2. Scenario classes derived from Figure 2.

Sequence	Description	Examples
ADP	Adversarial attack with impact to both digital and physical SSCs	Adversary creates a denial-of-service attack to disrupt function of a feedwater controller, which results in automatic shutdown of a feedwater pump and plant trip.
AD/P	Adversarial attack with impact to digital SSC	Adversary gains access into an NPP digital I&C network to insert malware, which corrupts heat balance calculations used by operators.
A/DP	Adversarial attack with impact to physical SSC	An adversary sabotages a facility by drilling a hole in reactor coolant piping to cause a loss of coolant accident.
A/D/P	Adversarial attack with no impact to digital or physical SSC	An adversary gains access into a facility but is captured prior to adverse impact. An adversary gains entry into a networked system but security information and event monitoring software alerts personnel who mitigate the situation before damage occurs.
/ADP	Non-adversarial incident with impact to both digital and physical SSCs	Digital I&C software is programmed incorrectly on a crane, which causes a load to fall. Severe weather causes rain to leak into a building on top of a fire control panel, which results in short-circuit of the control panel and failure of the fire system to actuate.

Sequence	Description	Examples
/AD/P	Non-adversarial incident with impact to digital SSC	Unintentional human performance event in which the configuration of a network switch is improperly performed, allowing unauthorized access into network components.
/A/DP	Non-adversarial incident with impact to physical SSCs	An environmental event (e.g., earthquake, fire) occurs, which damages equipment. Project personnel de-tension the reactor building in preparation to cut a hole for a steam generator replacement project, which results in delamination of the containment building.
/A/D/P	Non-adversarial incident with no impact to digital or physical SSCs	Normal plant operation.

2.3.2 Characterization of risk

Risk is often defined in terms of "expected [adverse] consequences," but much of the time, that definition is refined to better serve the discussion in specific contexts. The National Aeronautical Space Administration (NASA) defines risk as "the potential for shortfalls with respect to achieving explicitly established and stated objectives" [43]. NASA translates these objectives for programs and projects into performance requirements, which may be related to mission execution domains (e.g., mission success, safety, physical security, cybersecurity, cost, and schedule) or institutional support for mission execution[a] [43]:

Following formal risk analysis approaches, NASA operationally characterizes risk as a set of triplets where: [43]

1. The scenario(s) leading to degraded performance with respect to one or more performance measures (e.g., scenarios leading to injury, fatality, destruction or compromise of key assets; scenarios leading to exceedance of mass limits; scenarios leading to cost overruns; scenarios leading to schedule slippage).
2. The likelihood(s) (qualitative or quantitative; unconditional or conditional) of those scenarios.
3. The consequence(s) (qualitative or quantitative severity of the performance degradation) that would result if those scenarios were to occur.

Uncertainties are included in the evaluation of likelihoods and identification of scenarios.

Additionally, NASA writes a risk statement in straightforward language that avoids excessive use of technical terms or jargon. It is generally written in a format of "given that [CONDITION], there is a possibility of [DEPARTURE] adversely impacting [ASSET], thereby leading to [CONSEQUENCE]" [44].

[a] A risk is an uncertain future event, or combination of events, that could threaten the achievement of performance objectives or requirements. A "problem," on the other hand, describes an issue that is certain or near certain to exist now, or an event that has been determined with certainty or near certainty to have occurred and is threatening the achievement of an objective or requirement. It is generally at the discretion of the decision authority to define at what level of certainty (i.e., likelihood) an event may be classified and addressed as a "problem" rather than as a "risk." A risk may actually be conditional upon a problem, i.e., an existing issue may or may not develop into performance-objective consequences, or the extent to which it is at the present time uncertain.

Formalizing the risk statement enables articulation of clear risk management process requirements. The statement does not necessarily refer to aggregate risk, such as the annual risk of core damage at an NPP; it refers to specific issues (or vulnerabilities) in enough detail to initiate sensible discussion of how to prevent the occurrence of adverse consequences stemming from the specific departure mentioned in the risk statement. This type of risk statement could correspond to an accident sequence, a family of accident sequences, or even a specific risk model cut set.

The NASA risk management approach is noteworthy for not over-relying on quantification of scenario likelihoods. It is scenario-based to support discussion of what specific scenario elements can best be prevented. It also accommodates consequence-driven approaches. With this approach it is possible to make sensible risk management decisions based on rather broad characterization of scenario likelihood.

2.3.3 Risk analysis in early design phases

Early risk analysis applications [45, 46] were aimed at existing NPPs, for which operating experience was available to provide at least limited support to quantification of scenario likelihoods and to provide a sanity check on the identification of scenarios having adverse consequences. Noteworthy distinctions, among others, of these early applications when compared to current applications include the following:

- The stakeholder requirements governing those analyses were related mainly to the prevention of severe accidents potentially affecting public health and safety. Analysis of other consequence types, such as generation risk, was not a focus at that time.
- Because the analyses were completed for existing facilities, rather than at early design stages, the subject designs were specified at a high level of detail.
- Correspondingly, the analyses were carried out at a high level of detail in the specification of component failure modes. A given scenario type could be caused by any one of hundreds of thousands of distinct cut sets (e.g., combinations of component failures, human errors, system outages, etc.). This scope supported evaluation of issues relating to the reliability and availability of NPP safety systems.
- The role of a given NPP in an integrated energy systems (IES) and/or an electrical grid was not a focus of the analyses. The stakeholder perspective was that of a resident living near an NPP and the radiological safety concerns resulting from a severe accident. Plant economic performance and grid stability were not considered.

The style of the early NPP risk analyses is ill-suited to consideration of some issues. For example, generation risk can, in principle, be modeled similarly to early probabilistic risk analyses (PRAs) for severe-accident risk, but in general, choice of analysis method needs to be informed by the scale of potential consequences and the value of the extra effort needed to execute a given method. The premise of nuclear safety design and safety risk analysis is that initiating events randomly occur and it is unlikely that that multiple random events occur simultaneously. This assumption is invalid with digital risk, especially when considering adversarial and intentional actions.

Barring the introduction of new severe-accident risks by including an NPP in an IES, a higher-level, less detailed, more qualitative approach is warranted if the goal is to understand the behavior of IESs. A partial example can be found in [47]. That study performed a hazard analysis, rather than a PRA, to understand potential risks. In PRA, the attempt is to characterize scenarios, frequencies (likelihoods), and consequences, and to determine whether facility modifications are needed. In design-stage hazard analysis, the decisions are driven by scenarios and consequences, not judgment-based assessments of likelihood, because the very point of the analysis is to decide on measures that are needed to engineer a sufficiently low likelihood for severe-consequence scenarios.

Moreover, quantification of the likelihood of security-related scenarios has long been recognized as a fundamental challenge. The original Nuclear Regulatory Commission (NRC) safety goal policy [48] explicitly excluded comparison of physical security risks with safety goals (note that in 1986, cybersecurity was not yet a widely-recognized issue). It was noted that there was no basis on which to provide a measure of risk related to the possible effects of sabotage or theft of SNM. In fact, PRAs are not intended to model intelligent adversaries who intentionally perform an action and who can change their strategy at will.

2.3.4 A different approach to managing adversarial risk

Much of the conventional wisdom regarding risk management views the decision problem (what actions, if any, to manage risks) as being adequately handled with classical (utility-based) decision analysis. Within that paradigm, uncertainties are handled with probability distributions in which expected utility (or a convenient proxy) is calculated for each possible course of action, and the risk management actions taken are the actions that maximize expected utility. For example, we do not know whether a large earthquake will occur in the future—in fact, we have very significant uncertainty about the earthquake hazard—but we believe that we know (or can find out) enough about earthquake likelihood to make rational risk management decisions.

However, the problem is more complicated if the risks are due to adversarial or intentional actions. For instance, while earthquake likelihood is independent of political policies or criminal intentions, likelihood of adversarial action may be dependent on these political and socio-economic factors. In fact, security risk is often characterized by the knowledge, capability, intention, and motivation of the adversary and their ability to exploit facility vulnerabilities. It is very difficult to know what to believe about attack likelihood, and there is no reason to believe that attack likelihood is constant in time. Under these conditions, risk decisions based on likelihood are difficult if not impossible.

A classicist might argue that despite the difficulties, one should do the best possible job of uncertainty analysis, compute expected utilities, and act on the result. Others might argue that the results of such a process will be assumption-driven rather than representative, and that instead, one should apply “robust” decision-making, or decision-making under “deep uncertainty.” Since we do not know the future, these ideas, and related ideas, seek to promote decisions that will perform better under a wider range of possible futures. Those decision alternatives might not be considered optimal, but within some of these alternative paradigms, they will be selected because their potential downsides are less unsatisfactory than the potential downsides of some alternatives.

For physical security, some researchers have advocated a Risk-Informed Management of Enterprise Security (RIMES) approach. RIMES is motivated, in part, by the fundamental challenges associated with using attack likelihood within a classical (utility-based) risk management paradigm. The history of such approaches, and arguments against them, are summarized in a recent review article by Wyss and Williams [49]. A useful overview of RIMES is provided by Figure 3, excerpted from a briefing given by Wyss [50].

The black portion of Figure 3 shows a plot of consequence (of a given scenario) versus scenario difficulty. Every triangle symbol on the figure corresponds to a particular scenario, with the coordinates set to scenario difficulty and consequence. In the lower right of the figure, there is a high density of scenarios, which are difficult for an adversary to achieve, and which do not have particularly high consequences. Above and/or to the left of that region are scenarios that are less difficult and/or have higher consequences. The argument of RIMES is that in risk management, if a facility is modified to reduce easy to achieve scenarios that have high consequences, then overall security risk is reduced. The authors of RIMES argue that one does not, and cannot, know enough about “likelihood” to reason in the classical way.

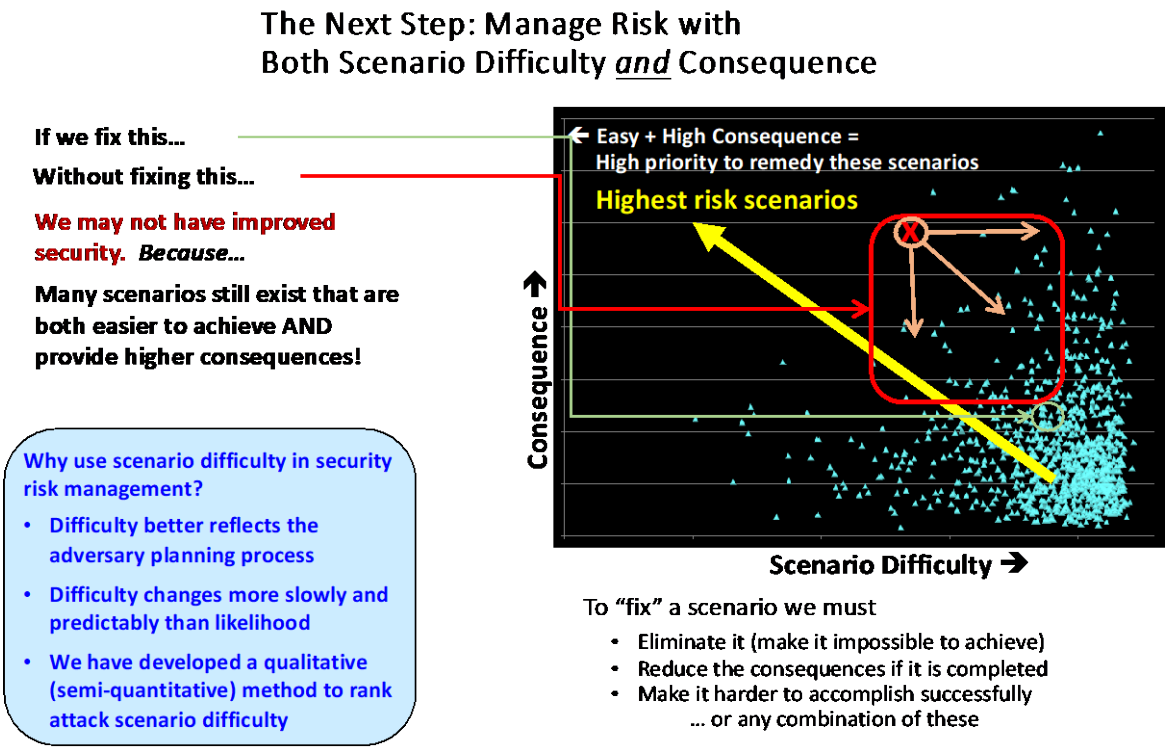

Figure 3. Overview of the RIMES approach [50].

RIMES has been promoted as an approach for physical security, not cybersecurity, but the authors of this report believe the approach could be adapted to cybersecurity. The approach illustrated in Figure 3 has certain items in common with other decision-analytic ideas. One of those ideas is robust decision-making (RDM), an approach that informs decisions under deep uncertainty (e.g., conditions that are unknown or not agreed upon with regard to likelihood of future scenarios). The objective of RDM is to provide a technique for "systematic, shareable reasoning and decision making under conditions of deep uncertainty.[b]" Instead of seeking predictive analysis, RDM supports "the systematic construction, testing, and selection of short-term actions that will be consistent with long-term goals over many alternative futures.[b]"

The concept of deep uncertainty is similar to the likelihood of attack issues raised by the RIMES researchers. Assessing likelihood of attack is not the same thing as predicting the future, but it has key elements in common. The problem that RDM is trying to solve is that specific predictions about the future (e.g., which attacks are most likely?) will drive the analysis to recommendations that will not work well if the wrong futures (attacks) have been allowed for in the recommendation. Security risk management that is predicated on assumptions about attack likelihood may not allow for the right possibilities. Since future adversarial actions are unknown, allowing a wide range of possibilities is beneficial. RIMES focuses on determining (and mitigating) scenarios with high consequences that are easier for adversaries to achieve. Depending on how adversaries think about their problem, the RIMES approach might tacitly reflect likelihood considerations. But more fundamentally, assuming completeness of scenario identification and soundness of the assessment of scenario consequences, the RIMES approach attempts to limit the worst-case consequences an attacker could achieve at a given level of attack difficulty. RIMES is similar to

[b] https://www.rand.org/pardee/methods-and-tools/robust-decision-making.html

applying the "minimax" concept[c] to each interval on the "difficulty" axis in order to reduce the consequences of the worst-case scenario(s) at that level of difficulty.

RIMES uses the large body of work in modeling the difficulty of physical attacks. Using the RIMES approach literally for cybersecurity would require us to develop an analog of "difficulty" for cyber-attacks. If it were practical to do that, a potential refinement or adaptation of RIMES, not yet mentioned in public discussions of RIMES, might be achievable by considering what elements the envelope of scenarios have in common and identifying whether those elements offer a more efficient way to reduce consequences in each difficulty interval.

2.4 Small Modular Reactors

In order to provide flexible power generation for a wide range of users and applications, small modular reactors (SMRs) and microreactors are under development. SMRs are generally identified as those generating less than 300 MWe, are deployable in single or multi-module configurations, and include inherent and passive safety features. Their smaller size generally makes them more cost effective for use in IES and co-located with industrial applications and/or located in remote locations. SMRs may use existing light water reactor technology, or they may incorporate advanced reactor technology, such as gas-cooled, molten salt-cooled, or molten metal-cooled designs. While there are at least 50 SMR designs and concepts internationally, only one commercial SMR is in operation with a few claiming to be near-term deployable.[d] There is one operational Russian floating NPP that incorporates two 35 MWe reactors.[e] Additionally, the 100 MWe Linglong-1 light water reactor is currently under construction in China.[f]

2.5 Integrated Energy Systems

2.5.1 IES Overview

Due to ongoing concerns with energy diversity, reliability, and sustainability there is a transformational shift underway to develop integrated systems to connect power plants and other renewable energy sources to non-traditional heat and electricity demands for industrial, commercial, and residential applications, such as district heating, electric vehicle charging, water purification, and hydrogen (H_2) production. Additionally, there is strong motivation to use the thermal and electrical energy from NPPs to broaden the customer base to improve the economic viability of both existing and new reactors. In general, an IES can maximize the output of networked energy sources to provide flexible, reliable, and efficient use of energy for multiple purposes.

Three broad categories are used to define the physical and digital connections between integrated systems and subsystems based upon the specified project goals [51]:

- Tightly coupled IES. As shown in Figure 4, multiple generating sources, energy storage, and industrial processes are co-controlled and are thermally and electrically integrated via one connection operated by one financial organization to optimize the economic performance of all components together.

[c] https://en.wikipedia.org/wiki/Minimax

[d] https://www.iaea.org/topics/small-modular-reactors

[e] https://pris.iaea.org/pris/CountryStatistics/ReactorDetails.aspx?current=895

[f] https://pris.iaea.org/PRIS/CountryStatistics/ReactorDetails.aspx?current=1111

- Thermally coupled IES. As shown in Figure 5, thermally and electrically connected subsystems are tightly coupled to the heat power supply. These subsystems are operated by one financial organization, may not be co-located, and may have multiple grid connection points.
- Loosely coupled IES. As shown in Figure 6, there is no direct thermal coupling between subsystems, and the generators are only electrically connected to industrial energy users. Thermal energy for industrial applications could be created by converting electrical energy to thermal energy. This solution may have fewer regulatory obstacles for existing generating facilities.

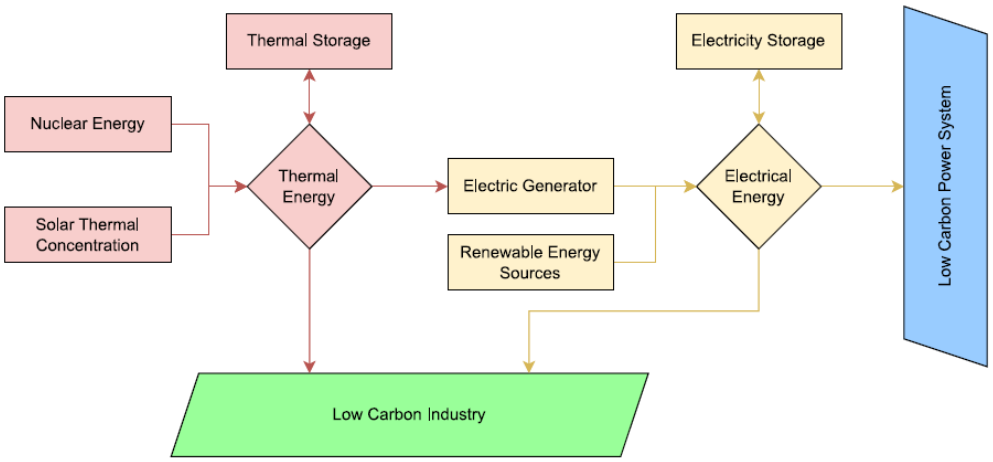

Figure 4. Tightly coupled IES [51].

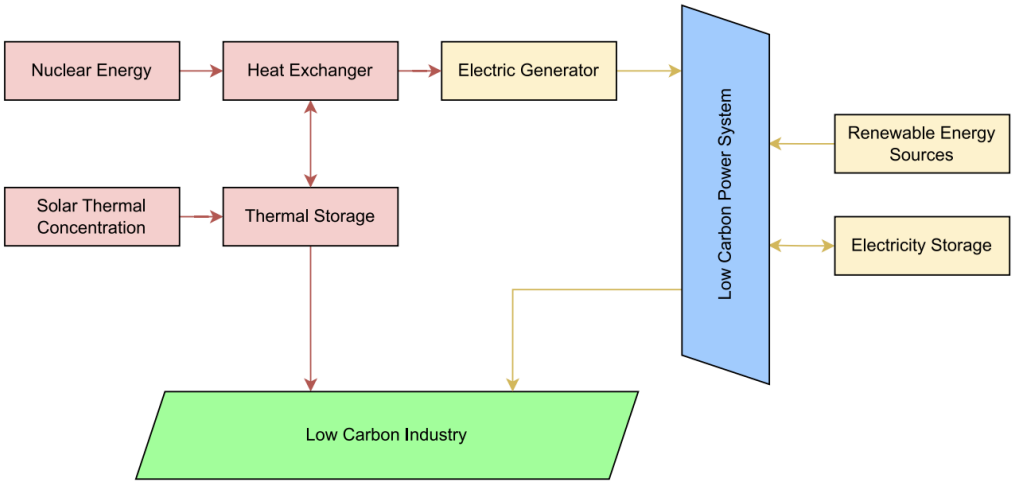

Figure 5. Thermally coupled IES [51].

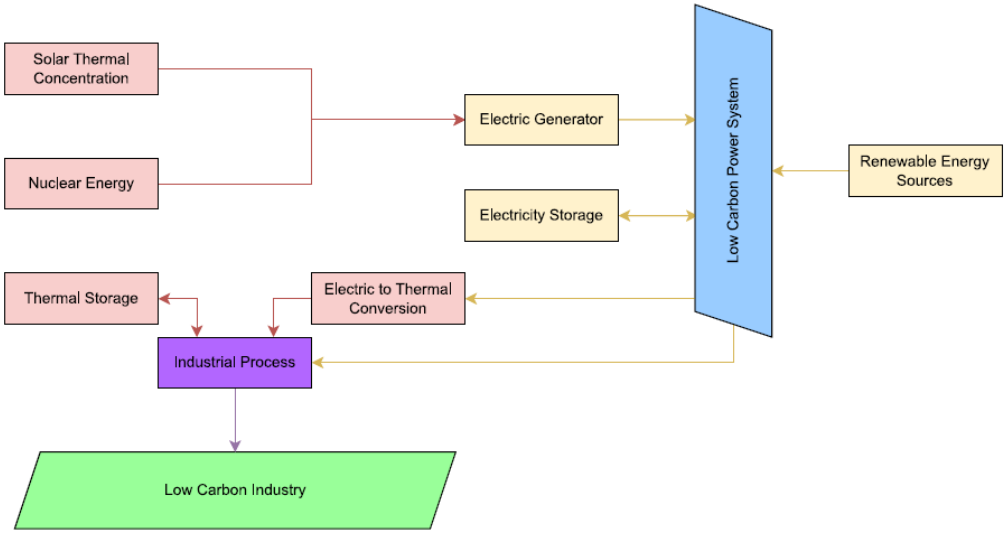

Figure 6. Loosely coupled IES [51].

2.5.2 Relevant standards for energy market communications

The inter-control center communications protocol (ICCP or IEC 60870/TASE 2.0) is a commonly used standard for communication among different grid-integrated assets in the electric power sector.[g] The standard provides general information and guidelines for operating conditions, electrical interfaces, communication protocols, and other performance requirements. With the standardization of communication protocols, many different grid-integrated assets can coordinate across a large geographical area. Aside from the IEC 60870 standard and its parts, there are many other IEC standards. For example, the IEC 62325 standard and its parts are particularly relevant for establishing guidelines for energy market communications.

While some of the IEC 62325 parts are more relevant for European markets, the following parts of it are relevant for North American operations:

- IEC 62325-301:2018, Framework for Energy Market Communications – Part 301: Common information model (CIM) extensions for markets [39].
- IEC 62325-452:2021, Framework for Energy Market Communications – Part 452: North American style market profiles [40].
- IEC 62325-550-2:2021, Framework for Energy Market Communications – Part 452: Common Dynamic Data Structures for North American style market profiles [41].

2.5.3 BES load balancing options

Load from a generating source can be balanced on the BES using several methodologies. Some of these methodologies do not require external communications, while others may need to receive changes in power generation setpoints in response to grid events.

- Manual control is the traditional method of grid control for an NPP. Despite the growing interconnectedness of the BES through smart technologies, manual generation control remains

[g] https://www.oracle.com/utilities/ot-integration/what-is-iccp/#:~:text=ICCP%20allows%20the%20exchange%20of,accounting%20data%2C%20and%20operator%20messages.

prevalent in the nuclear industry. When it becomes necessary to adjust generation on an hour-ahead or real-time basis, a balancing authority or energy control center (ECC) operators will speak directly with SMR control room operators via telephone or similar means.

- Primary frequency control (PFC) is a type of automatic generation control that responds to local frequency changes. When there is excess load in a BES, generation assets may operate at a lower frequency. That is, the frequency will decrease ("droop") [52]. When the frequency drops below a certain setpoint, PFC triggers an increase in generation to restore the frequency. External communication is not typically required in this case because generator turbine control only needs to follow preset setpoints, local frequency measurements, and control logic (see Figure 7).

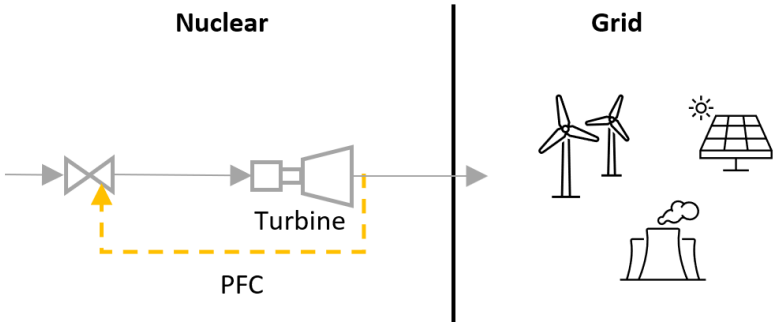

Figure 7. A simplified diagram describing PFC.

- Automatic generation control (AGC) is a load-following method that involves adjusting generation setpoints based on commands from the BES supervisory control and data acquisition (SCADA) system via ICCP. It serves as the secondary control for restoring the nominal frequency. AGC manages multiple generation units using frequency measurements and area control error (ACE), which calculates the deviation of combined tie-line flows from their scheduled values. The North American Electric Reliability Corporation (NERC) requires that the balancing authority operates with performance indicators in compliance with requirements related to cumulative and average ACE [53, 54]. The primary objective of AGC is to ensure that the electric grid system maintains the nominal frequency and adheres to the scheduled tie-line interchange levels by dispatching generation accordingly. Some AGC systems also incorporate economic dispatch aspects. Thus, AGC is commonly used when coal or natural gas are prevalent fuel sources.
- Load frequency control (LFC) is another type of load following methodology that requires external communication capabilities for generator control units. Compared to AGC, LFC needs a higher level of direct observability of the BES operation area's internal state through information and communication technology. It monitors power system imbalances and captures frequency and tie-line power transfers to estimate the dispatch amount. Instead of matching scheduled tie-line interchange, LFC focuses on matching the power generation with the actual power demand [55].

2.5.4 IES concept of operations

The concept of operations (CONOPS) for integrated systems will vary depending on the regulations, IES coupling choice, and overall IES objectives, including objectives for the generating facility and connected facilities, systems, and subsystems. For example, a thermally coupled IES in which steam is provided from an existing NPP to an industrial application may have different safety and regulatory requirements when compared to a new microreactor connected electrically to a microgrid.

Additionally, the CONOPS should address a wide variety of failure scenarios in the IES, which may or may not be adversarial as illustrated in Figure 2. For instance, an IES or its subsystems could fail due to equipment degradation or component failure. Further, damage or compromise may remain digital in nature and may not impact physical SSCs. Since nuclear-driven IESs will contain digital I&C systems (e.g., sensors, computer systems, data acquisition hardware, actuation components, etc.) to monitor and control the thermal and electrical distribution from the NPP to industrial applications and the BES, robust operation of these systems is critical to ensure safe, secure, reliable, and resilient operation.

The CONOPS should also define responsible entities for interfacing with the ECC, as it is possible to have more than one IES stakeholder capable of responding to generation change requests. Determining which entity should interface with the ECC will affect necessary interconnectivity and interdependency of the SMR, BES, and process heat applications. This decision further impacts the design of the digital I&C systems used to monitor and control the multiple applications and electrical generation. For instance, there is a different digital risk to a facility if the design is tightly coupled between one or more entity (i.e., one control system that monitors and controls equipment at different entities at the system or device level) or loosely coupled (i.e., separate control systems at each facility that then communicate to each other at the facility level).

As an example, consider the following possible SMR and high temperature steam electrolysis (HTSE) integration concepts:

- Changing reactor power to accommodate fluctuations in BES and thermal energy extraction demands. In this concept, the SMR may be required to make centralized command and control decisions to match the HTSE's thermal energy and electricity demands by raising or lowering control rods. The interconnections are shown in Figure 8 where the orange color shows the information flow.

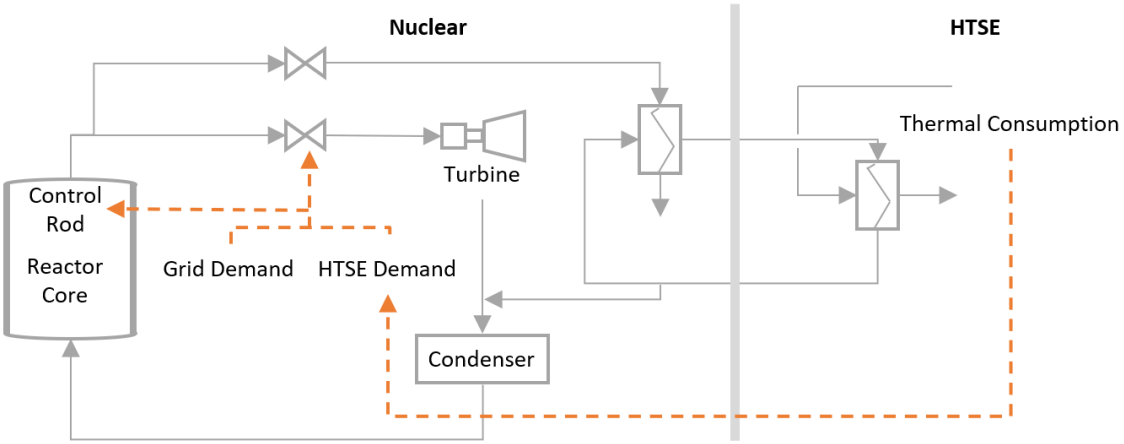

Figure 8. Reactor power adjusted to meet BES and thermal energy demand.

- Using thermal energy extraction demand to determine the electricity generation while maintaining the constant reactor power. HTSE initiates the response to the BES demand first. Even though the HTSE and SMR are separate entities, commands for generation changes (e.g., AGC, PFC) can be directed to the HTSE instead of the SMR. Agreements (e.g., demand response, spinning reserves) can be established among HTSE, SMR, and the BES entities to align their goals and priorities. As shown in Figure 9, in this concept the SMR does not necessarily require direct digital connectivity to the grid since changes in thermal demand can be indicated by the water flow back from HTSE, affecting the electrical generation adjustments. The orange color indicates the information flow.

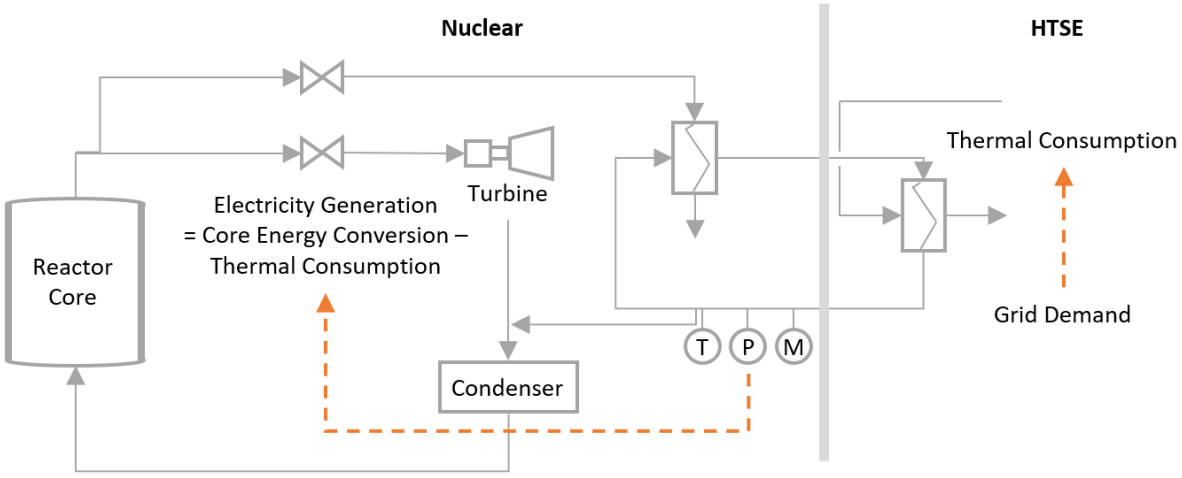

Figure 9. Thermal energy extraction determines electrical generation.

- Using electrical generation to determine the thermal energy extraction while keeping the reactor power constant. In this concept, the SMR receives commands for generation adjustments and sends thermal extraction requests to the HTSE plant as shown in Figure 10, where the orange color shows the information flow. Due to limited benefits and high interconnectivity requirements, this concept may not be the preferred choice.

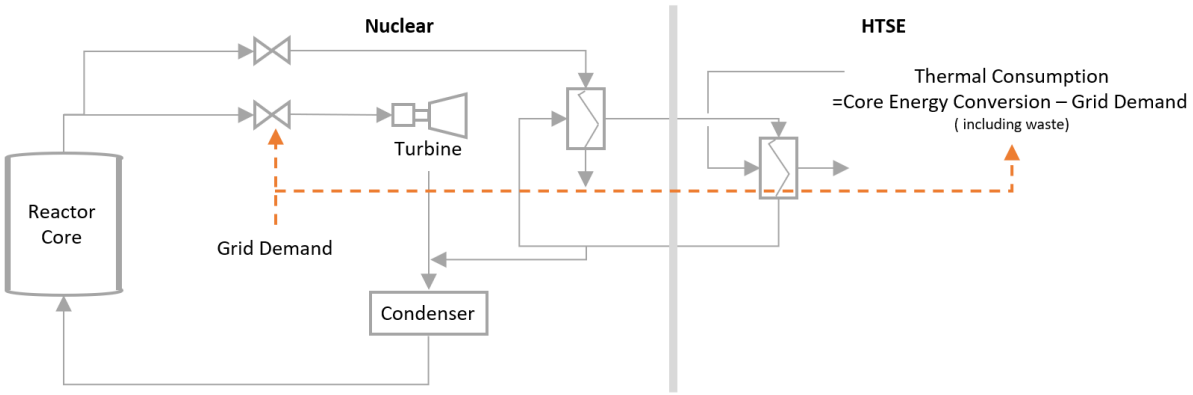

Figure 10. Electricity generation determines the thermal energy extraction.

3. DIGITAL SYSTEMS ENGINEERING CHALLENGES

3.1 Competing Objectives

Appendix A provides a mapping for each of the activities through the first few phases of the systems engineering lifecycle for nuclear digital engineering projects, including concept exploration, concept of operations, and system definition and design. These maps also include constraints, enablers, inputs, and outputs.

In the early design stages of digital systems engineering projects there are often competing objectives. Overall mission goals must be balanced with project goals, project goals must be balanced with system goals, and system goals must be balanced with SSC capabilities. Additionally, nuclear engineering projects have external and internal constraints that impact these objectives. For instance, in the U.S. there are laws and regulations that impact the nuclear design of safety-related I&C modifications [4, 6], the physical and cybersecurity of assets in an NPP [22, 23, 56, 57], and the security of assets in the BES [42]. There are also internal constraints, such as organizational commitments and policies.

In digital engineering projects there is often a need to balance functional operation with safety, security, and reliability. Often system-level objectives are inversely related. Consider the following:

- Adding a security or safety feature may adversely impact operations.
- Adding diversity and redundancy for safety and reliability may increase complexity of operations.
- Adding functionality (e.g., wireless capability, remote access) may increase the attack surface and create additional vulnerabilities.

Considering the operation of an NPP-driven IES, a fine balance is needed between redundancy and simplicity. And, in digital engineering, redundancy without diversity does not necessarily reduce adversarial risk. With respect to networked digital I&C systems, the system architecture should allow for benevolent actors to manipulate controls and monitor important parameters, but lateral movements and interaction capability should be limited in the event an adversary gains unauthorized access. On the other hand, some redundancy is desired in systems that are critical to the operation of the IES. This may seem contradictory, but redundancy can be achieved in some parts of the IES while minimalism is achieved in other parts of the IES.

At a higher level, there may be competition between mission and organizational objectives. For example, if the organizational mission is to maintain the economic viability of an NPP for shareholders, it is possible that initial costs from connecting an existing NPP's steam system to an H_2 facility may cause a decrease in shareholder price. Of course, the integration of these connecting systems between an NPP and H_2 facility also likely increases risk, both from a safety and security perspective.

Thus, a primary activity in early design phases is to analyze, evaluate, and document all mission, project, and systems objectives, including the analysis of competing objectives and the reasons for choosing the specific option. The project team should clearly identify the potential risks of their decision(s), begin to evaluate risk treatments, and understand the remaining residual risks. These decisions should be reviewed and updated as necessary as the project team moves through each phase of the systems engineering lifecycle.

3.2 Competing Stakeholder Requirements and Expectations

Similar to competing mission and project objectives, there are often also competing requirements and expectations from external and internal stakeholders in nuclear digital engineering projects. Thinking comprehensively about stakeholder requirements during early design phases results in better design

decisions. On the other hand, overly narrow consideration of stakeholder requirements may result in increased digital risk due to inherent vulnerabilities from less secure design decisions.

3.2.1 External Stakeholders

External stakeholders are generally broader groups of people who have interests in the successful and safe outcome of the project. External stakeholders include shareholders, government and regulatory entities, BES operators, members of the public who live near the NPP, and the broader public served by the NPP. In an NPP-driven IES, external stakeholders may also include those entities involved in an interconnected system including other electrical generators, H_2 production facilities, thermal storage facilities, and other industrial applications.

External stakeholders are strongly influenced by safety and/or economic factors. Each category of external stakeholders will have its own characteristic interests. For instance, the regulator and nearby residents are primarily interested in safe operations while the broader public is interested in low rates and reliable electricity with low (or zero) power outages. Additionally, shareholders, business partners, and interconnected system entities are primarily interested in economic gain, which requires stable and reliable thermal and electrical generation and distribution from the NPP. This also includes safe, efficient, and reliable control of integrated systems to maximize profit while minimizing downtime and unused generation capacity.

The requirements for each external stakeholder must be determined and evaluated to understand their priorities. The project team must also evaluate how these external stakeholder requirements are balanced with the mission and project objectives. The goal in nuclear digital engineering projects is to document the requirements and evaluate their impact to function, safety, security, and reliability. If a strict requirement introduces new vulnerabilities, the team should use secure-by-design principles to evaluate appropriate risk treatments during these early design phases.

As an example, consider an application in which an existing NPP is connected to an H_2 production facility where one stakeholder requires the addition of new control logic for automatic load following. A requirement for many other external stakeholders, of course, is that the grid remains operational with no blackouts or power outages. These are competing requirements since automatic load following creates new digital vulnerabilities that could cause loss of generation. The project team should evaluate the effects of a software error in the load following application—could it cause the NPP to shut down, resulting in cascading failures in the regional BES like what happened during the Northeast blackout in 2003[h] which was caused by a software error in an alarm application? Could a cyber-attack or human performance error cause a similar fault?

Although NPPs can, in principle, load follow up to a point, existing NPP technology lends itself better to running at a constant thermal power. Accordingly, within a hypothetical IES concept of operations, when electricity is valuable enough (i.e., the grid is willing to pay enough) to justify NPP operation, the NPP should supply electricity to the grid. And, when the grid cannot beneficially use the NPP's electricity at a price that would justify NPP operation, the NPP can divert its energy production to generate hydrogen or deposit heat into thermal storage, or, of course, downpower.

As mentioned, even brief local electricity outages are undesirable, rolling brownouts are worse, and widespread outages can be catastrophic. For the BES to be stable, there must be a particular balance between supply and demand, and this cannot be achieved without energy suppliers. Sometimes a power plant may trip offline, upsetting the current equilibrium between supply and demand. Depending on the supply margin at the time of plant trip, the ECC may need to dispatch electricity from other energy suppliers (i.e., the missing step in the Northeast blackout). Planned plant outages occur as well; these also

[h] https://en.wikipedia.org/wiki/Northeast_blackout_of_2003

must be coordinated by the balancing authority in the ECC. Thus, communication is highly important between all the involved external stakeholders.

Figure 11 illustrates potential, notional top-level objectives for the ECC and energy suppliers, respectively. Both figures have a left/right asymmetry where the objectives on the left are mission objectives (i.e., the reason the entity exists) and the objectives on the right are the fundamental safety and reliability objectives. Regulatory requirements relating to safety, security, and environmental protection belong to the right. As most energy suppliers are "for profit" companies, the profit motive is a primary objective of the energy supplier, as shown in Figure 11. This is not just a matter of rewarding investors; rather, in this example, it is (among other things) part of the mechanism by which generation assignments are established.

In summary, many external stakeholders are involved in supplying energy to the entities in an IES and significant coordination is necessary for proper information and communication between all parties. Most importantly, load and supply must be balanced in the BES by understanding the current load and how it is likely to evolve in time, coordinating with its numerous suppliers, and rapidly responding to upsets.

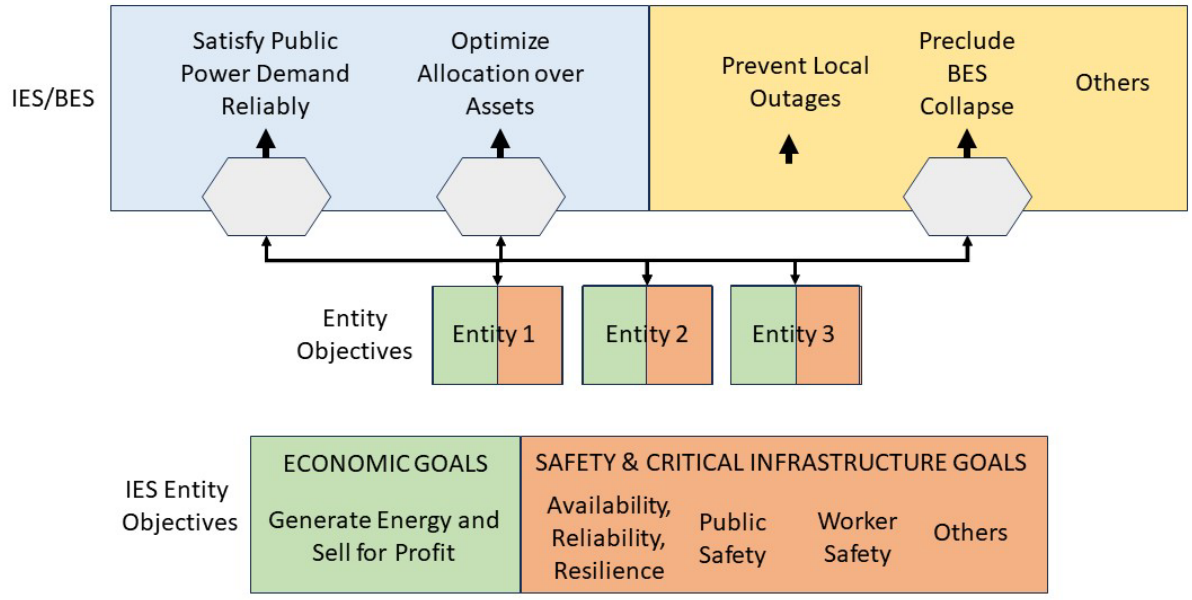

Figure 11. Example objectives for IES energy supplier entities and their relationship with the IES/BES.

3.2.2 Internal Stakeholders

Internal stakeholders are those directly involved in the nuclear engineering project as well as those within the various organizations with project responsibilities. In large projects, such as the design of new reactors or the design of integrated energy systems, there are typically multiple design teams. In digital engineering projects, separate teams may be responsible for designing specific systems, hardware, and/or software. There may be different teams for integration, validation and verification, quality assurance, and operations. There may also be groups functioning in oversight roles, such as project management, safety, regulatory, security, supply chain, and organizational management roles. Additionally, teams and personnel may be located in multiple organizations and/or multiple locations. For example, NuScale, an

early SMR vendor, has approximately 550 employees, with offices and test facilities in six locations as well as partners across the world.[i]

As there are competing objectives in nuclear digital engineering projects, there are competing needs within and between teams and project personnel. Internal stakeholder groups can be differentiated by their varying dependencies and risk responsibilities potentially affected by decisions made in the system engineering process. Nuclear engineers responsible for reactor physics will likely have different priorities than chemical engineers designing piping or control engineers designing I&C systems. All of these groups likely have different priorities than cybersecurity engineers. And, while many organizations may use a formal model-based systems engineering (MBSE) methodology to support processes throughout the systems engineering lifecycle, they often do not incorporate digital risk or security considerations into the MBSE approach.

Implementation teams vary according to project scope and complexity and will evolve over the systems engineering lifecycle. Developing and maintaining secure-by-design practices from the onset of the project will provide project teams with the skills to identify adverse impacts due to risks associated with digital systems. While CIE is focused primarily on lowering adversarial cyber risk, its principles of consequence-focused design, engineered controls, secure architecture, design simplification, and resilient layered defenses, can also be effective in lowering unintentional, non-adversarial digital risk. Other engineering practices used for design of safety systems, such as eliminating the potential for one single failure to cause loss of a function through use of redundant, diverse, and separated SSCs, can also be highly beneficial in reducing digital risk.

The challenge is that most employees and project teams are generally unfamiliar with digital risk. Hardware engineers are focused on developing a device to perform a function; software engineers are focused on developing an application to perform a task; safety engineers are focused on ensuring the design cannot cause radiological release. Engineers are often trained in analyzing failure modes, such as component failure. Control engineers are also often trained to evaluate I&C issues, such as common cause failures or equipment drift. But they are usually not trained in identifying adverse impacts to digital I&C systems from other threats, such as unintentional or malicious human actions. Since digital threats may arise from people, process, or technology, internal stakeholders must be trained to recognize these threats.

There are multiple cyber risk analysis methods, none of which cover adequate scope, are readily adoptable, or are repeatable [58]. One method for modeling digital risks is system-theoretic process analysis (STPA) [59]. While not an ideal method for NPPs since it is cumbersome to implement in an entire facility, this technique views accidents as resulting from unsafe control actions, corresponding to flaws in, or failures of, a control structure that leads to violations of constraints that enforce design intent. The term unsafe is understood to refer generally to actions whose effects are adverse to design intent; thus, the term unsafe, as used in STPA, includes safety but is not limited to safety. The more detailed functional requirements that emerge in the subsequent stage of the systems engineering lifecycle can arise from consideration of the constraints that need to be imposed on the design, including the control structure, in order to satisfy those stakeholder requirements.

Thus, since nuclear digital systems should be designed to be functional, safe, and secure, personnel should be trained in understanding how interconnected systems and subsystems may be impacted from digital degradation, failure, or compromise. If information flow is degraded, disrupted, or distorted between systems or subsystems, what happens? If an unsafe control action occurs, what happens? Further, as teams evaluate needs and concepts, identify stakeholder and functional requirements, and begin high-level design, digital risk must be a part of the discussion. As competing priorities arise from internal stakeholders, the risk analysis and decision-making process should be documented, with risk treatments identified and residual risk understood by all impacted stakeholders.

[i] https://www.nuscalepower.com

Figure 12 shows a simplified, notional IES in which the nuclear steam supply system (NSSS) of an SMR is located in the upper left, supplying steam. Examples of information flowpaths are overlaid in dashed lines. In this example, high-pressure steam is routed to the turbine and/or thermal storage depending on the setting of the bypass valve. Ultimately, if steam is supplied to the turbine, then electricity is supplied to the BES. In this example, the BES is also supplied by other energy suppliers and the setting of the bypass valve is informed by both current grid demand and the status of the thermal storage plant. The control knob shown on the NSSS block implies that there are influences on reactor power other than just grid demand and the thermal storage plant. Figure 12 also shows NSSS status information being conveyed to the grid for planning purposes (e.g., planned or forced outages). Despite this example's simplicity, the information flow needs to be carefully considered. Once the information flowpath is determined, a hazard analysis should be performed to identify any necessary constraints to be addressed by functional requirements.

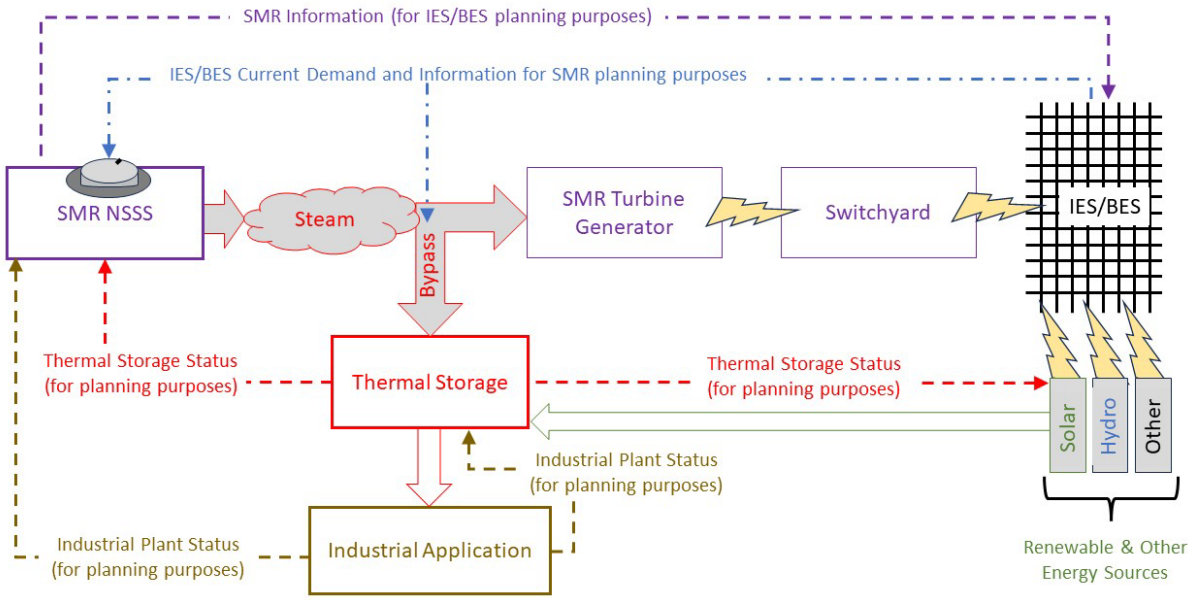

Figure 12. Information flow for a notional IES, both between SMR and IES entities, and within the SMR.

Given the example of the Northeast blackout, the importance of achieving balance between load and demand is clear, and constraints on design are needed to assure this balance. However, since there may be both adversarial and non-adversarial events, one set of constraints might not be adequate to preclude adversarial events. The flowpaths in Figure 12 involve a range of time scales. A trip can take a plant offline quickly, potentially creating a need for the balancing authority at the ECC to quickly recover the balance between load and supply on the BES, and potentially asking energy suppliers to rapidly ramp up generation. Of course, a planned shutdown will proceed more slowly. Demand may also have varying time responses—usually in a foreseeable way, but potentially unexpectedly. For instance, the industrial facility may go offline or want to ramp up production. Market forces, contractual obligations, and economic decisions may impact both supply and demand.

4. CONCEPT OF OPERATIONS FOR AN SMR-DRIVEN IES—SIMPLIFIED EXAMPLE

As shown in Figure 5, thermal and electrical subsystems from generating sources can be interconnected to industrial applications in an IES. The purpose of this simplified example is to explore digital risks and early design phase considerations for an SMR-driven IES. Since an SMR generates heat and electricity which can then be transferred to physically and digitally interconnected applications, there may be early design phase digital I&C decisions that positively affect performance but negatively influence security. For example, if I&C is designed to monitor and control the SMR and integrated industrial applications from one system in one central location, the tighter coupling may lead to improved communications and system performance, but the cyber risk of the SMR and associated facilities may increase due to additional attack vectors into the facilities.

The SMR under consideration in this example can be installed in multiple configurations with a varying number of modules. This SMR is designed to safely shut down and remain self-cooled indefinitely with no operator action, additional water, or electrical requirements; therefore, it has a simplified I&C protection system when compared to existing light water reactors. Similar to other reactors under design, the SMR modules in this project use field-programmable gate arrays (FPGAs) in the reactor protection system. I&C for normal operations is based on a typical distributed control system (DCS) architecture to monitor plant parameters and control plant SSCs.

The modules are designed with a high-pressure steam bypass prior to the turbine and a low-pressure steam bypass after the turbine to enable use in industrial applications, such as H_2 production and water desalination, respectively. The high-pressure steam is directly routed to a high-temperature steam electrolysis (HTSE) system to dissociate steam into a clean source of hydrogen and oxygen in an H_2 facility. The low-pressure steam is directly routed to a multi-effects distillation (MED) system to provide the thermal requirements for desalination. The condensate from the HTSE and MED systems is recombined with condensate in the module prior to entering the feedwater system. Due to energy diversity, reliability, and clean energy concerns, the SMR is also interconnected with an electric grid supplied with renewable energy sources with the goal to maximize electricity from renewables whenever possible.

Depending on the coupling of a SMR-driven IES (e.g., tightly, thermally, loosely), there may be different objectives and CONOPS. Appendix B contains an example of a CONOPS annotated outline developed by NASA that describes the type and sequence of information that it should contain.[j] The remainder of this section presents a simplified example of a CONOPS using this template for a thermally coupled SMR-driven IES. This CONOPS is for demonstration of digital engineering security decision analysis only. This example is purposefully not detailed, complete, or precise. It is not intended to provide low-level design details of the SMR, H_2 facility, desalination facility, or renewable energy sources. However, it is intended to provide enough detail in this example to understand how mission-level, facility-level, and systems-level decisions can impact or influence digital engineering and security considerations. Additionally, a CONOPS may be a living document—as more information is learned during the systems engineering lifecycle this document will be updated. An actual CONOPS will be validated and verified by an engineering/project team throughout the lifecycle to ensure it contains detailed and accurate information.

[j] https://www.nasa.gov/seh/appendix-s-concept-of-operations

4.1 Introduction

4.1.1 Project Description

The objective of this project is to thermally couple an SMR facility to process heat applications and renewable energy sources.

4.1.1.1 Background

Due to ongoing concerns with energy diversity, reliability, and sustainability there is a transformational shift underway to develop integrated systems to connect power plants and other renewable energy sources to non-traditional heat and electricity demands for industrial, commercial, and residential applications, such as district heating, electric vehicle charging, water purification, and H_2 production. Additionally, there is strong motivation to use the thermal and electrical energy from NPPs to improve the economic viability of both existing and new reactors.

The integration of an SMR facility with process heat applications improves its economics by enabling use of bypass steam to these applications when electricity demand is low. Additionally, an SMR's load following capabilities and integration with renewable energy sources, such as wind and power, enables grid operators to take one or more reactor modules ("module") offline when there is sustained output from renewables. When a module is not connected to the BES, its full steam capacity can be used for process heat applications. The SMR's flexibility enables each module to be dedicated or used for different purposes.

The SMR is a multi-module pressurized water reactor (PWR) that uses standard PWR fuel assemblies. The modules are passively safe—they do not require operator action, AC or DC power, or additional water to safely shutdown and maintain long-term safe shutdown. For the purposes of this report, the SMR uses standard PWR technology with FPGA-based protection systems and standard digital I&C systems for the remainder of the facility.

Figure 13 illustrates the SMR facility with eight modules. Modules 1 and 2 are interconnected to the H_2 facility via a high-pressure bypass line prior to the steam generator. To supply superheated steam to the HTSE, electricity is sent from the SMR switchyard to an external heat exchanger to raise the pressure and quality of the steam for higher process efficiency. Module 1 is the primary module for H_2 production. Module 2 is a backup module intended for use when Module 1 is offline, in maintenance, or unable to send the required amount of steam to the H_2 facility. The normal mode for Module 2 is solely to provide electricity to the interconnected renewables grid.

Modules 4-8 are connected to the water desalination facility which uses MED technology. Similar to [60], 100 percent of the turbine exhaust steam is sent to the reboiler coupled to an MED system to maximize the steam for desalination while still enabling electricity generation. Since this project is still in early design stages, it is possible that with a co-located SMR and water desalination facility near a seawater source, the normal SMR condenser cooling water output could be used directly in the MED system instead of low-pressure steam and a secondary seawater inlet [61]. Modules 5-8 are the primary modules for the desalination facility. Module 4 is a backup module intended for use when any of Modules 5-8 are offline, in maintenance, or unable to send the required amount of steam to the desalination facility. The normal mode for Module 4 is solely to provide electricity to the interconnected renewables grid.

Module 3 is primarily dedicated to electrical generation. It is currently anticipated that one module will be shutdown for a maintenance and refueling outage at all times. This enables continued outage rotation and planning cycles for the facility.

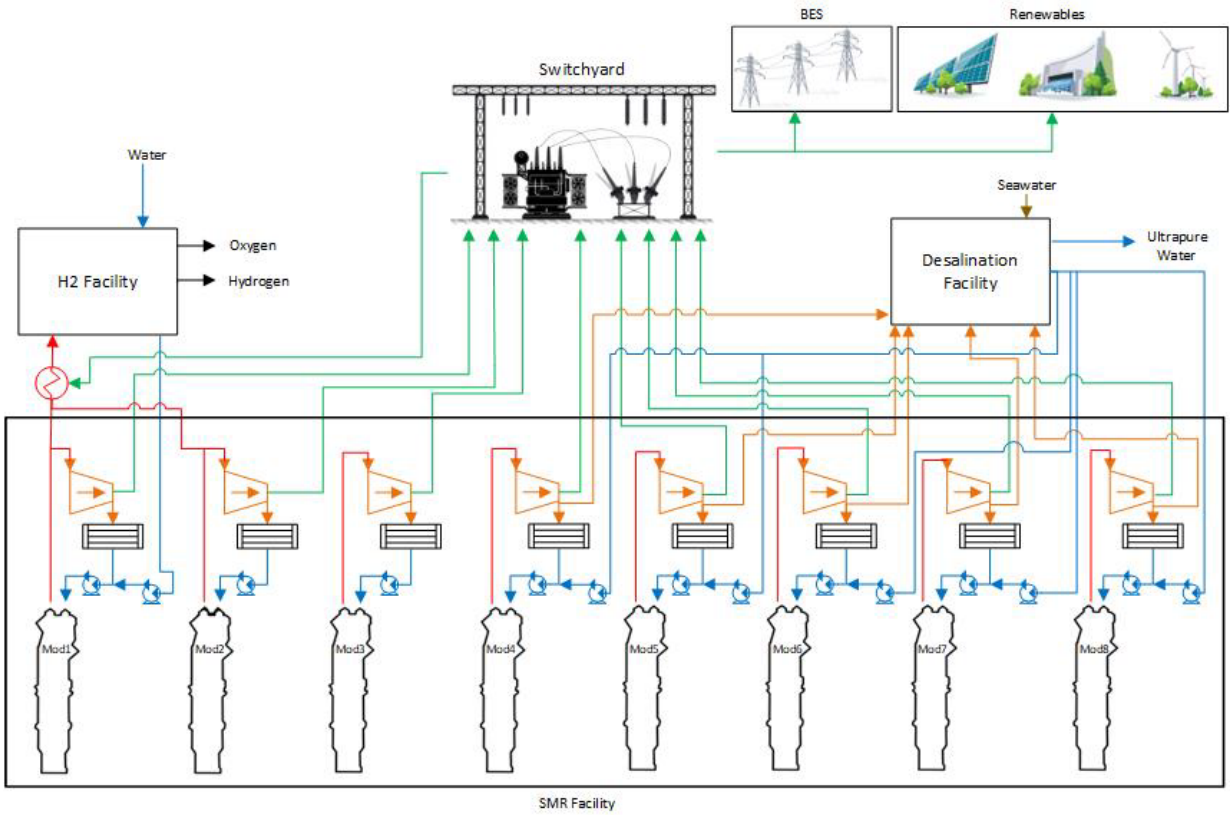

Figure 13. Simplified drawing of an SMR facility interconnected with an H_2 facility, water desalination facility, and BES with renewables.

4.1.1.2 Assumptions and Constraints

Current assumptions include the following:

- The economics of using process heat from the SMR facility for industrial applications are favorable.
- Industrial facilities will partner with the SMR facility, i.e., there will be a market for clean nuclear energy to power industrial applications.
- Renewable energy sources will be available for interconnection.
- For the H_2 production facility, there will be a market for clean hydrogen upon SMR startup.
- Load-following capability by using up to 100 percent turbine bypass will not adversely affect reactor components. Additionally, ramp rates are acceptable for both the load-following approach and the reactor design.
- The design will provide separation between the systems such that radionuclides will not be transferred from the primary reactor coolant loop to the ultrapure water output of the water desalination facility.
- Nuclear and energy regulators (e.g., NRC, Federal Energy Regulatory Commission, NERC) will approve the design.
- Chemical and other required regulators (e.g., Environmental Protection Agency) will approve the design.

- The use of low-pressure steam bypass for the MED cycle is more efficient and cost-effective than use of the condenser's cooling water outlet, which could use this heated seawater as the MED system inlet.

Current constraints include the following:

- Regulatory siting constraints and exclusion zone for an NPP located in close proximity to interconnected industrial facilities.
- Regulatory approval constraints with physically and digitally connecting the SMR to external industrial applications. These constraints may include safety and security considerations.

4.1.2 Overview of the Envisioned System

4.1.2.1 Overview

In a thermally coupled IES, thermally and electrically connected subsystems are tightly coupled with the steam supply from an SMR module as previously illustrated in Figure 5. The location of the industrial facility is primarily determined by the steam quality required for the application. Figure 14 illustrates the simplified process flow for one module and turbine generator set connected to an H_2 production facility via a high-pressure steam bypass line. In this project, the thermal storage in Figure 5 is the HTSE in the H_2 facility; there is currently no plan for thermal storage in this project. Figure 15 illustrates the simplified process flow for one module connected to an MED-based water desalination facility via a low-pressure steam bypass line. A more detailed description is provided in CONOPS Section 4.3.

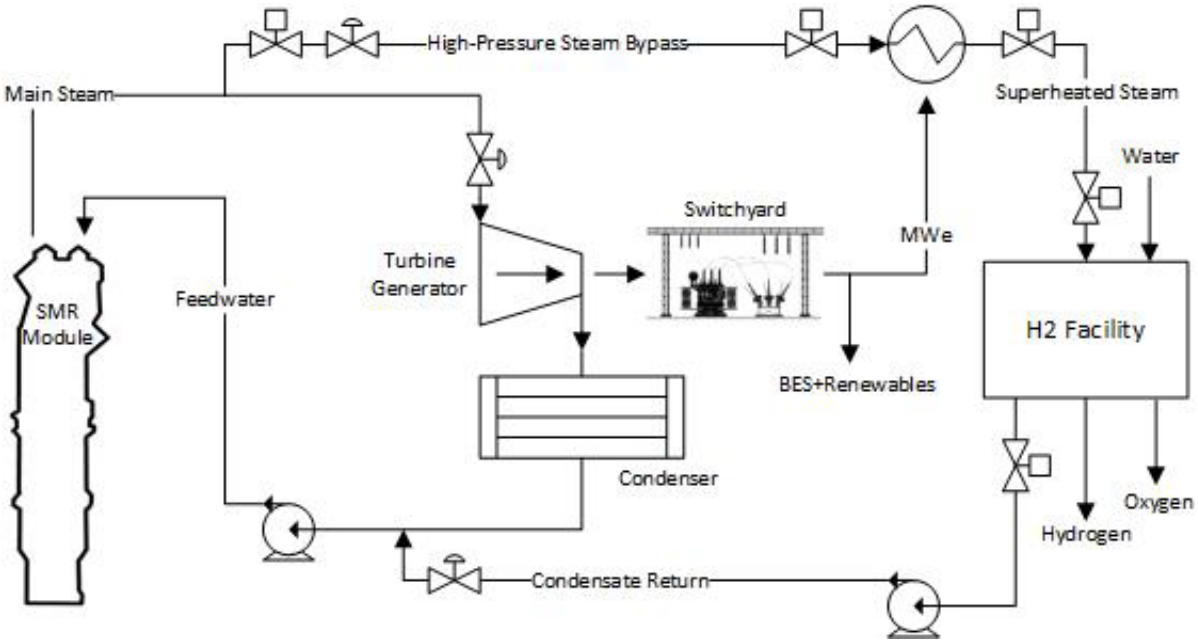

Figure 14. Simplified SMR-driven process flow for an HTSE-based H_2 production facility using high-pressure steam bypass.

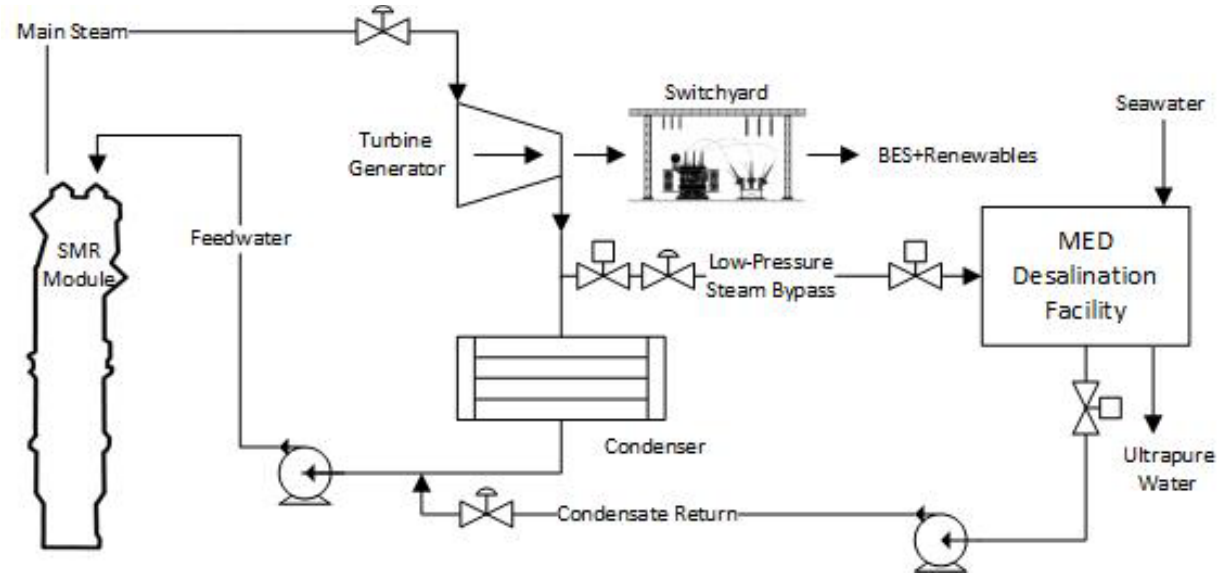

Figure 15. Simplified SMR-driven process flow for an MED-based water desalination facility using low-pressure steam bypass.

4.1.2.2 System Scope

Each module in the SMR facility has a dedicated turbine generator. This configuration provides flexibility to use dedicated process steam from one module to one destination, which enables different modules to provide steam to different industrial applications. Additionally, this flexibility enables the following modes of operation for process steam from each module:

- 100 percent steam supplied to the industrial application.
- 100 percent steam supplied to the turbine generator for electricity generation.
- Steam supplied simultaneously to the industrial application and turbine generator based upon demand.

The planned overall project scope is to interconnect process steam from the SMR modules to industrial applications, including a H_2 production facility and water desalination plant. The SMR electrical generation will also be configured for load following in an integrated BES with renewable energy sources. Interfaces include:

- Connection of a high-pressure steam bypass line from two modules to a H_2 facility.
- I&C system for monitoring and control of process steam to the H_2 facility.
- Connection of a low-pressure steam bypass line from five modules to a water desalination facility.
- I&C system for monitoring and control of process steam to the desalination facility.
- Connection of the integrated reactor control and turbine generator output for each module for load following purposes in the integrated BES.
- Automated load following digital I&C system using AGC.
- Entities operating the H_2 production facility, desalination facility, and ECC.

The construction and operation of the SMR and external industrial applications is outside the scope of this project to the extent they are not listed in one of the above interface items.

4.2 Nuclear Digital Engineering Documents

For the purposes of this CONOPS example, this section is omitted for readability. Some relevant references for similar projects are listed in Section 7, References.

4.3 Description of Envisioned Digital I&C System(s)

While the scope of the overall project is to interconnect reactor module SSCs to external facilities that requires physical components and digital components, the primary focus of this CONOPS is on the digital I&C requirements for the interconnected systems. Note that Module 3 does not have interconnections with external facilities and is solely used for electrical generation.

4.3.1 Needs, Goals, and Objectives of Envisioned System

4.3.1.1 Module 1 and 2 connections to an H_2 production facility

- Capabilities: Provide superheated process steam from two SMR modules to an H_2 facility for continuous, controlled H_2 production.
- Behavior: Control bypass steam flow by opening/closing control valves on high-pressure steam bypass line and on H_2 facility isolation line. Provide superheated steam as needed at HTSE inlet by providing electricity to an inline heater from the SMR switchyard [62]. Module 1 is the primary source for the H_2 facility. Module 2 is a backup module that can be used when necessary.
- Operations: Module 1 will provide continuous high-pressure steam via the bypass control valve based on demand signal from the H_2 facility. Based upon control signals from the automated load-following control system, any excess steam will either be sent to the turbine generator for electricity or dumped to the condenser. Electricity from the switchyard will be controlled to the heat exchanger to raise the pressure and temperature of the steam to provide superheated steam to the H_2 facility. SMR facility operators will monitor the system on a human-machine interface (HMI) in the control room. Manual override capabilities will exist. Module 2 is normally connected to the grid. In the event Module 1 is taken offline or is unavailable to provide the necessary quantity of steam, operators (or potentially automatically by the I&C system) can switch the lineup to Module 2 during a planned evolution. Once connected to the H_2 facility, operations for Module 2 will mimic those indicated for Module 1.

4.3.1.2 Modules 4-8 connected to a water desalination facility

- Capabilities: Provide low-pressure process steam from five SMR modules to a MED-based water treatment facility for continuous, controlled desalination of seawater.
- Behavior: Control bypass steam flow by opening/closing control valves on low-pressure steam bypass lines and on the desalination facility isolation line. Due to loss of feedwater preheating capabilities from heat loss in the desalination facility reboiler, overall thermal efficiency of the module will decrease. Modules 5-8 are the primary source for the desalination facility. Module 4 is a backup module that can be used when necessary.
- Operations: The MED-connected modules will provide continuous low-pressure steam via bypass control valves on demand signal from the desalination facility. Based upon control signals from the automated load-following control system, high-pressure steam from the steam generators will either be sent to the turbine generator for electricity or dumped to the condenser. SMR facility operators will monitor the system on an HMI in the control room. Manual override capabilities will exist. Module 4 is normally connected to the grid. In the event Module 5, 6, 7, or 8 is taken offline or is unavailable to provide the necessary quantity of steam, operators (or potentially automatically by the I&C system) can switch the lineup to Module 4 during a planned evolution. Once connected to the desalination facility, operations for Module 4 will mimic those indicated for Modules 5-8.

4.3.1.3 Automatic load-following control of module

- Capabilities: The modules connected to process heat applications will first supply baseload steam to their respective applications (e.g., high-pressure steam to H_2 facility and low-pressure steam to MED system). Each module will be able to provide constant minimum or maximum steam flow as determined by the needs of the integrated application. The remaining energy will automatically load follow based upon command and control from the integrated I&C system(s), BES SCADA system, and requirements of the balancing authority in the ECC. The integrated I&C system(s) demand signal will incorporate any min/max steam requirements into its control logic as well as any electricity demand signal from the interconnected renewable generation sources.
- Behavior: Open/close bypass valve(s) and industrial application isolation valve(s) and ramp up/down power to control steam flow and electricity generation, as needed.
- Operations: AGC will be used to adjust generation setpoints based on commands from the BES SCADA system via ICCP. In addition to the normal AGC calculations, the SCADA system will maximize energy production from renewables on the BES. Additionally, the allowable energy (MWe) for each of the five modules normally interconnected to process heat facilities will be calculated by the module's DCS. This calculation will use the demand signal from the connected facility (e.g., high-pressure steam demand for HTSE facility and low-pressure steam demand for MED system) along with the module's thermal heat balance calculation and actual main steam flow to calculate the MWe available for BES use. This available MWe for each module will be transmitted to the SCADA system.

4.3.2 Overview of Digital Systems and Key Digital Elements

For the interconnected systems, there will be digital process instrumentation for monitoring system parameters, such as pressure, temperature, level, radiation, and flow sensors. The design will also include programmable logic controllers, DCS(s), HMIs, and the necessary OT interconnecting all together in a secure architecture. The actual components and design have not yet been determined. This section will be updated as the design progresses.

4.3.3 Digital I&C Interfaces

This section describes the digital interfaces of the SMR facility with external entities. This includes digital process instrumentation as well as the control system(s) for monitoring and process control. HMIs are also considered. Since the project is still in the early design phase, this information is only conceptual and will be updated as the low-level design is completed. A hazard analysis for the digital I&C design will be performed as part of this early design and then repeated throughout the project. The objective of this analysis is to understand the impacts of unsafe control actions as well as distorted, disrupted, and destroyed information flows. This analysis should also include human factor considerations with regard to operator actions and the possibilities for error due to different module configurations. What are the adverse impacts, if any, to the SMR, H_2 facility, desalination facility, and integrated energy grid? Digital I&C interfaces considered in this CONOPS include:

- I&C components and interfaces for the high-pressure steam bypass line to the H_2 facility.
- I&C components and interfaces for the low-pressure steam bypass line to the MEDs.
- I&C components and interfaces for the automatic load-following system(s).

4.3.4 Modes of Operations

4.3.4.1 Module connected to H_2 Facility

Table 3 lists the modes of operation for Module 1 (or Module 2 if swapped) interconnected to the H_2 facility. The amount of MWe sent to the grid is dependent on the amount of steam available for the turbine and the load demand from the SCADA system on the renewable-connected grid. The last column in Table 3 indicates the MWe available to the grid, not necessarily what will be sent to the grid. If additional electricity is not needed on the grid, then the excess steam will be dumped to the condenser in accordance with module design limits.

The normal mode during module power operation (e.g., Mode 1) is for the module to send the necessary amount of high-pressure steam through the bypass line to the H_2 facility by opening the block valves and modulating the steam control valve to support 100 percent operation for H_2 production. The required MWe output from the switchyard will also be sent to the preheat heat exchanger (PHE) to superheat the steam (e.g., PHE breaker closed) prior to entry into the HTSE.

During module startup and shutdown, the H_2 facility will be isolated by closing the block valves and steam control valve; no steam will be provided for H_2 production. The breaker to the PHE will be opened.

During planned module reactivity evolutions, the interconnected system should continue to supply 100 percent steam demand to the H_2 facility, if possible. The PHE breaker will remain closed. The steam control valve may be modulated as needed.

During unanticipated module downpower or module trip, the block valves to the H_2 facility should close and the PHE breaker should open, stopping flow of steam and PHE electricity to the H_2 facility.

During planned H_2 facility shutdown or unplanned H_2 facility trip, the H_2 facility will be isolated by closing the block valves and steam control valve; no steam will be provided for H_2 production. The breaker to the PHE will be opened.

During H_2 facility startup, the steam flow will be ramped up by opening the block valves and slowly opening the steam control valve, as needed.

During H_2 production output changes, the steam flow will be modulated by open/closing the steam control valve as needed. MWe available to the grid will change as this valve is controlled.

Analysis will be performed to determine if hot swap-over from Module 1 to Module 2 (or vice versa) to the H_2 facility is possible (e.g., Module 2 remains in Mode 1 at lower power with either steam sent to the turbine or dumped to the condenser until valve lineup is completed). Otherwise, module swap will occur with both modules shutdown in hot standby or lower mode.

Table 3. Modes of operation for Module 1 (or Module 2) interconnected to H_2 facility.

Mode	Block Valves	Steam Control Valve	PHE Breaker	PHE MWe	Grid MWe Available
Normal, Module in mode1 (power operation)	Open	Open/Modulating	Closed	100%	0
Module Startup/Shutdown	Closed	Closed	Open	0	0
Module planned reactivity changed	Open	Modulating	Closed	Modulated	Modulated
Module unplanned downpower or trip	Closed	Closed	Open	0	0
H_2 shutdown or trip	Closed	Closed	Open	0	100%
H_2 startup	Open	0-100% open	Open to Closed	0-100%	100-0%
H_2 output change	Open	50-100% open	Closed	Modulated	Modulated
Testing	As needed	0-100% open	As needed	Modulated	As needed
Primary module unavailable	Perform controlled evolution to swap over to backup module.				

4.3.4.2 Modules connected to water desalination facility

Table 4 lists the modes of operation for Modules 5, 6, 7, and 8 (or Module 4 if swapped) connected to the water desalination facility. The amount of MWe sent to the grid is dependent on the amount of steam available for the turbine and the load demand from the SCADA system on the renewable-connected grid. The last column in Table 4 indicates the MWe available to the grid, not necessarily what will be sent to the grid. If additional electricity is not needed on the grid, then the excess steam will be dumped to the condenser in accordance with module design limits. Recall that use of low-pressure steam for desalination will lower thermal efficiency of the reactor and will result in less MWe output. As less steam is used for desalination, both MWth and MWe will increase.

The normal mode during module power operation (e.g., Mode 1) is for the module to send the necessary amount of low-pressure steam through the bypass line to the MED system in the desalination facility by opening the block valves and modulating the steam control valve to support 100 percent operation for desalination requirements.

During module startup and shutdown, the MED system will be isolated by closing the block valves and steam control valve; no steam will be provided for desalination.

During planned module reactivity evolutions, the interconnected system should continue to supply 100 percent steam demand to the MED system, if possible. The steam control valve may be modulated as needed.

During unanticipated module downpower or module trip, the block valves to the MED system should close, stopping flow of steam.

During planned desalination facility shutdown or unplanned desalination facility trip, the MED system will be isolated by closing the block valves and steam control valve; no steam will be provided for desalination.

During desalination facility startup, the steam flow will be ramped up by opening the block valves and slowly opening the steam control valve, as needed.

During desalination output changes, the steam flow will be modulated by open/closing the steam control valve as needed. MWe available to the grid will change as this valve is controlled.

Analysis will be performed to determine if hot swap-over from a backup to primary module to the desalination facility is possible (e.g., backup remains in Mode 1 at lower power with either steam sent to the turbine or dumped to the condenser until valve lineup is completed). Otherwise, module swap will occur with both modules shutdown in hot standby or lower mode.

Table 4. Modes of operation for Modules 5, 6, 7, and 8 (or Module 4 when swapped) interconnected to the water desalination facility.

Mode	**Block Valves**	**Steam Control Valve**	**Grid MWe Available**
Normal, Module in mode1 (power operation)	Open	Open/Modulating	All available
Module Startup/Shutdown	Closed	Closed	0
Module planned reactivity changed	Open	Modulating	All available
Module unplanned downpower or trip	Closed	Closed	0
MED system shutdown or trip	Closed	Closed	All available
MED cycle startup	Open	0-100% open	All available
MED output demand change	Open	50-100% open	All available
Testing	As needed	0-100% open	As needed
One of four primary modules unavailable	Performed controlled evolution to swap over to backup module.		

4.3.4.3 Automatic load following

Table 5 lists the potential examples of modes of operation for automatic load following of the interconnected facilities tied to a grid supplied from renewable energy sources. Since there are numerous configurations possible with eight modules, five of which are normally connected to external applications, only several high-level examples are listed. These are examples of load-following scenarios that will need to be designed and tested throughout the project. As these modes are designed, a digital risk analysis should be performed to evaluate how the function, facility safety (SMR, H_2, desalination), and security are balanced in the overall system. It is currently anticipated that one module will be shutdown at all times due to rotation through planned refuel outage and maintenance schedules.

Table 5. Potential examples of modes of operation for automatic load following.

Module Status	**H_2 Facility Status**	**Desalination Facility Status**	**Renewables**	**Load Following Mode**
7 modules in mode 1	100% operation	100% operation	100% available	Use 100% available from renewables. Maximize MWe from Modules 2-4. Lower MWe from Modules 5-8 as needed to balance grid.
7 modules in mode 1	100% operation	100% operation	<100% available	Maximize MWe from Modules 2-4. Balance load using MWe from Modules 5-8 as needed.
Transfer from primary to backup H_2 connected module	Transfer	100% operation	100% available	Load from renewables maximized. Modules 3-5 ramped as needed to balance load.
Transfer from primary to backup MED connected module	100% operation	Transfer	100% available	Load from renewables maximized. Modules 2-4 ramped as needed to balance load.
6 modules in mode 1 (Module 1 offline)	Shutdown	100% operation	100% available	Load from renewables maximized. Modules 2-8 ramped as needed to balance load. External energy generation may be needed.
7 modules in mode 1	100% operation	Shutdown	100% available	Load from renewables maximized. May need to downpower Modules 5-8 as needed to balance load.

4.3.5 Proposed Digital Capabilities

Refer to the prior paragraphs in this section for the detailed capability needs. It is anticipated that these needs will be met through engineering design. The interconnected digital I&C systems for the H_2 facility and water desalination facility will be designed to monitor and control the applications as noted in the modes of operation in Table 3 and Table 4. Additionally, the requirements for the design of the automatic load-following I&C systems (or system of systems) are listed in Table 5.

There are no special capabilities needed during decommissioning or disposal.

4.4 Physical Environment

The environment external to the facilities will be dependent on the site chosen for construction. The internal facility environment (e.g., turbine building) will be typical of SMR and industrial facilities; as these spaces are generally not conditioned, they will also be dependent on the external environment. Operator HMIs, DCS servers, and similar sensitive electronic components will likely be located in a conditioned space. Sensors should be rated, as a minimum, to the pressure and temperature ranges of the monitored process. Digital I&C components should be rated for continuous ambient temperature between -40°C to 85°C. If mounted in an external environment, the component must be waterproof. Class 1E ratings or radiation tolerance are not needed for these applications. If the component rating does not meet the anticipated installation environment, then measures must be taken to create that environment.

4.5 Support Environment

This section describes how the envisioned systems will be supported after being fielded. It will be updated as details are determined throughout the systems engineering lifecycle.

As mentioned, it is anticipated that one module will always be shutdown. This enables rotating maintenance schedules on the I&C equipment supporting the shutdown module; including the capability for personnel to apply patches and updates when devices are not needed for operation. One consideration, however, is maintaining the modules in alignment, so care must be taken to ensure configuration control is properly managed to maintain proper inventory of digital assets, including make, model, version, and configuration of the assets across the systems and modules.

It is currently planned to implement a Software Bill of Materials (SBOM) program with corresponding integrated vulnerability and risk management processes during the project for transfer to the SMR facility once constructed. This will enable both project and facility personnel to have in-depth knowledge into the high-level and low-level components used in the installed digital assets such that personnel can rapidly identify if a newly discovered vulnerability is present so that they can quickly respond to and mitigate the exposure.

4.6 Operational Scenarios and Use Cases

This section takes key scenarios or use cases and discusses what the envisioned system provides or how it functions throughout that single-thread timeline.

4.6.1 Nominal Conditions

This section will outline scenarios, or use cases, to cover how the envisioned system will operate under normal circumstances where there are no problems or anomalies taking place.

Normal modes of operation are listed in CONOPS Section 4.3.4. Detailed scenarios will be developed and updated as the design progresses.

4.6.2 Off-Nominal Conditions

This section will outline scenarios, or use cases, to cover how the envisioned system(s) will perform when conditions cause operations to deviate from normal. This covers failures, low performance, unexpected environmental conditions, or operator errors. It is anticipated that these scenarios reveal any additional capabilities or safeguards that are needed in the system.

The project team will perform a digital risk analysis to systematically review the digital I&C systems and interconnections to identify consequences from disruption, distortion, or destruction of information flow and/or unsafe control actions. The intent is to identify the consequences from both adversarial and non-adversarial/unintentional (e.g., software failure, human error) incidents on the system and to analyze how to harden or redesign the system to remove or mitigate the vulnerabilities that could enable the incident to occur. This risk analysis may be performed in conjunction with a safety PRA, but it is not intended to be a safety PRA.

While this section will be updated throughout the systems engineering lifecycle, examples to consider include those related to the digital engineering design of the interconnected facilities and systems, such as:

- Desalination facility rapid shutdown/trip. What are the impacts on the reactivity and operation of the four connected modules? How is the additional thermal energy controlled?
- H_2 facility rapid shutdown/trip. It is anticipated a trip of the H_2 facility would cause the connected reactor module to trip, similar to the effects of a turbine trip on a reactor. What are the impacts on reactivity and operation of the connected module?
- H_2 connected module reactor trip. What are the impacts on the H_2 facility?
- Desalination facility connected module reactor trip. What are the impacts on the desalination facility?
- Radioactivity alarms in the MED system or ultrapure water output. What are the facility responses?
- What are the impacts from: (1) higher/lower steam flow, temperature, pressure; (2) higher/lower condensate flow, temperature, pressure; (3) automatic command to reduce MWe to grid?

How could adversarial or unintentional actions cause these events? Can these risks be eliminated, mitigated, or transferred through secure-by-design principles? When can the organization accept the residual risk (e.g., what level of risk is considered acceptable)?

4.7 Impact Considerations

This section describes the potential impacts, both positive and negative, on the environment and other areas.

4.7.1 Environmental Impacts

A positive environmental impact of the overall project is the use of clean nuclear energy to provide capabilities to turn seawater into drinking water. Since the SMR is passively safe and requires no operator action during an abnormal event, the emergency planning zone is reduced, and it is anticipated that there will be no possibility of radiological release past this zone. However, this capability is dependent on the SMR's final design and safety analysis and is regulated by the NRC. The SMR modules will generate spent nuclear fuel and radiological waste that will be handled in accordance with all regulations. It is currently anticipated that an independent spent fuel storage installation will be constructed on site for longer-term storage of used nuclear fuel.

The H_2 facility and water desalination facility are regulated by the Environmental Protection Agency (EPA). They will be designed and constructed to EPA regulations and standards. However, the design and operation of these facilities in accordance with EPA regulations does not preclude the occurrence of an incident or explosion and it is anticipated there will be site exclusion zones around the H_2 facility. Additionally, while there will be several coolant loops between the reactor coolant system and the MED cycle, plus a distillation process to separate the seawater into ultrapure water, risk analysis should be performed to evaluate the likelihood of radionuclides entering the ultrapure water stream. If the likelihood, or risk, is unacceptable, the design will be modified to ensure an acceptable level of risk.

4.7.2 Organizational Impacts

The use of digital technology to interconnect an SMR facility with external applications is likely new to the engineering design and project teams. The performance of risk analysis, such as a hazard and operability analysis, that considers all potential hazards (e.g., public health and safety, worker safety, financial, reputation, etc.) and that considers all digital risk (e.g., adversarial compromise, common cause failure, unintentional human performance error, etc.) is necessary during early design phases. It is important to include as many project personnel as possible since many have a poor understanding of digital risk. Training the project team and performing risk analysis exercises as the design is under development will help build safety, security, resiliency, and reliability into the design from the beginning.

Additionally, it is anticipated that this integrated SMR facility will be designed and constructed at the same time operators and personnel are trained. Care must be taken to train these operators such that they understand the security and digital implications of connecting a reactor to external technologies. Training must provide specific details on the I&C operation so that issues can be detected and corrected. Since one module will be connected to a H_2 facility, four modules will be connected to a water desalination facility, three modules will only be connected to the grid, and all modules will potentially load-follow to maximize operation of renewable energy sources, operators, engineers, and plant personnel must be trained to understand system interactions and behavior. They must also be trained to recognize anomalies and to recognize when these anomalies are due to normal operations, equipment degradation, or a digital-related incident, either intentional or adversarial.

4.7.3 Scientific/Technical Impacts

The successful design, construction, and operation of an SMR facility connected to a water desalination facility that enables load following with the BES will demonstrate the capabilities of clean energy use to provide clean drinking water for communities across the world. Additionally, the successful demonstration of SMR use to provide clean H_2 as an energy source provides economic benefits to the nuclear industry, which will promote the continued operation and development of nuclear energy to enable continued energy diversity and security.

4.8 Risks and Potential Issues

Risk analysis to identify threats, vulnerabilities, and consequences of digital I&C systems and components will occur throughout the project lifecycle. Since this section is specific to risks and potential issues associated with the development, operations, or disposal of the envisioned system, as well as concerns/risks with the project schedule, staffing support, or implementation approach, this section will be updated throughout the project.

5. DIGITAL ENGINEERING DECISIONS DURING EARLY DESIGN PHASES OF THE SMR-DRIVEN IES

5.1 Digital Engineering Decision Analysis for Security Considerations

Many decisions are made throughout an engineering project's lifecycle. Mission-level, facility-level, and system-level decisions can impact the security of digital assets even if the decision is unrelated to digital I&C systems. For instance, a management decision to control multiple facilities from one location may require remote communication incorporating the secure use of digital I&C systems. It is important to evaluate these decisions from a cybersecurity perspective due to inherent interdependencies and interrelations within the overall project.

Additionally, the rationale behind the decision must be documented and periodically reviewed since some rationales are conditionally valid while others may be based on beliefs that have not yet been explicitly evaluated and tested. As the application context or conditions change, decisions may become invalid, thereby impacting the security and safety of the system or system of systems. It is essential to trace these security interdependencies and conditions that make the design decisions valid throughout the entire systems engineering lifecycle. The project team should identify triggers, or changes, that require reevaluation of the underlying security decisions and/or assumptions. This continuous process for security-related design decisions in engineering projects is illustrated in Figure 16.

Figure 16. Continuous process for digital engineering decision analysis.

Appendix D provides an adaptation of the U.S. DOE Office of Cybersecurity, Energy Security, and Emergency Response (CESER) *Cyber-Informed Engineering Implementation Guide* for use during the early phases of nuclear digital engineering projects. The purpose of the *CIE Implementation Guide* is to describe the CIE principles and provide questions for engineering teams to consider during each phase of the systems engineering lifecycle. Considering Appendix D and the CONOPS example, there are a series of questions and decisions that must be considered early in the project. Examples of these questions are provided in the following sections.

5.2 Examples of Mission-Level Decisions

5.2.1 Interconnected entities

5.2.1.1 Design decision

As described in the CONOPS, this project will interconnect an SMR with a hydrogen facility and water desalination facility. Two modules will be physically connected to an H_2 facility to supply high-pressure steam to an HTSE for hydrogen generation. One module is dedicated full-time to the H_2 facility with a backup module on standby in case the primary module is unavailable. The SMR switchyard will also connect to the H_2 facility to raise the steam pressure and temperature to superheated steam at the HTSE inlet. The SMR-H_2 process will be monitored and controlled by an interconnected digital I&C system(s).

Five modules will be physically connected to an MED system at a water desalination facility. Four modules are dedicated full-time to the water desalination facility, with one additional module available as backup in the event one of the four primary modules is unavailable. This SMR-desalination process will also be monitored and controlled by an interconnected digital I&C system(s). Additionally, all eight modules will be interconnected with an IES containing renewable energy sources to provide electricity as able and needed. Note that while high-pressure steam is available for electrical generation from the four desalination modules, it is on a downgraded basis due to thermal efficiency losses.

5.2.1.2 Digital engineering, security implications, and interdependencies

Selecting the type and number of entities to include in an IES is primarily driven by economic and clean energy objectives. Since the SMR is digitally interconnected to all entities in this project, any changes in this overall strategy will directly impact all aspects of the digital engineering design and security considerations. Adding or removing an entity may impact competing objectives in the overall project as well as the competing requirements of external and internal stakeholders. As the decision to add or remove an entity is an overarching project decision, implementing this change in early design phases would cause ripples throughout the entire project affecting many activities and lower-level decisions, such as those identified in Section 5.3.1. If an entity is added or removed, the entire digital engineering and security strategy should be reevaluated with all changes included in a follow-up risk analysis.

Of note, since it is possible that entities may be disconnected and/or that new entities may be connected to the SMR at a future date, a design that enables this flexibility from both physical and digital interconnectivity perspectives is ideal. If this flexibility is desired, the engineering design should ensure that security strategies, such as defense in depth, secure architecture, and active defense, are established early in the design to enable an easier "plug and play" capability. This would require engineering, safety, and regulatory analysis early in the design as well. These competing objectives will need to be documented and periodically reviewed to ensure they are implemented and maintained as required.

5.2.2 Participation in energy markets

5.2.2.1 Design decision

While it is required by regulations to operate the SMR safely, a mission-level objective for this project is to also maximize profitability by participating in energy markets. To a certain extent, the decision on which energy market to participate in is dependent on where the SMR is located and the market options available in that area. The goal for this project is, however, to operate two modules as baseload generation with four modules also providing electricity to the local IES on a continuous basis while also maximizing the electrical generation from the interconnected renewable energy sources and providing electricity by other carbon-based peaking power plants as needed to compensate for any load shortages on the larger BES.

The communications architecture of the IES should be designed to ensure secure communication to/from its control-center communications hub with other utilities, power pools, regional transmission organizations (RTO), independent system operators, and other grid-integrated devices. Accordingly, this project should be implemented so that energy market communications are consistent with the IEC 62325 standard as outlined in Background Section 2.5.2. There are different energy markets that exist to ensure that an aspect of the electric grid's operation is reliable. An RTO will generally operate ancillary services markets, capacity markets, and energy markets (day-ahead or real-time).[k] While NPPs typically supply baseload generation, the flexibility of this project enables the SMR to participate in the ancillary services market. SMR and IES can assess the economic viability of participating in the real-time energy market as

[k] https://www.ferc.gov/sites/default/files/2020-06/energy-primer-2020_0.pdf

opposed to the ancillary market by considering various factors (e.g., ancillary service market values, dispatch frequency, ramp rate, historical real-time wholesale electricity prices).

5.2.2.2 Digital engineering, security implications, and interdependencies

While the decision of which energy market to participate in will be justified with a detailed cost-benefit analysis, the safety, reliability, and security also must be considered in this analysis. The energy market decision drives the selection of software, firmware, and hardware systems necessary to ensure cyber-secure energy market communications in accordance with IEC 62325. Of course, the choice of digital engineering solution will be very important for the cyber-secure operation of the IES. The low-level design should incorporate redundancy, modularity, limited external network connectivity, and minimal internal network connectivity among the IES's sub-systems.

Interdependencies include energy market communication between the IES entities. It may also affect facility-level decisions on the BES responsibility and load balancing. The selection of energy markets will be documented in the CONOPS and overall project plan. The CONOPS should document how this decision impacts digital engineering activities and the basis for security decisions. An activity in the project plan should be added to flag a reevaluation of these security decisions if the energy market decision is modified.

5.3 Examples of Facility-Level Decisions

5.3.1 BES responsible entity and entity priority

5.3.1.1 Design decisions

While the decision on which entity is the economic priority in an IES and which entity is the BES responsible entity are two separate decisions, they are discussed together in this section since they have similar security implications. For this example, the SMR is selected as the responsible entity. Additionally, entity priorities for the project are the following:

- The renewable energy sources on the IES are the highest priority for sending electricity to the IES.
- Module 1 is fully dedicated to sending high-pressure steam to maintain continuous H_2 production. The H_2 facility has priority for this module. Module 2 is a backup module.
- The H_2 backup module is fully dedicated to generating electricity for the grid, as needed based on renewable energy generation on the IES.
- Modules 5-8 are fully dedicated to sending low-pressure steam to maintain continuous water treatment at the desalination facility. Module 4 is a backup module.
- The desalination backup module is fully dedicated to generating electricity for the grid, as needed based on renewable energy generation on the IES.
- When operating, Module 3 is fully dedicated to generating electricity, as needed based on renewable energy generation on the IES.
- The primary desalination modules will generate electricity for the grid as the lowest priority energy supplier. Due to thermal efficiency degradation from loss of low-pressure steam, they will have less MWe available.

5.3.1.2 Digital engineering, security implications, and interdependencies

This BES responsible entity design decision requires the SMR facility to have at least one control system that calculates and balances the steam requirements for the interconnected H_2 and desalination facility as well as the electrical generation available from all operating modules. This requires

independent digital interfaces (e.g., between the SMR and H_2 facility, and between the SMR and desalination facility) in which the demand for high-pressure steam for H_2 generation and the demand for low-pressure steam for the MED system is sent by each interconnected facility's control system to the SMR. Additionally, the SMR will communicate directly with the ECC, which will balance the BES demand based upon consumer demand, SMR electrical output availability, renewable generation, and other energy sources.

The addition of these external digital interfaces increases the overall attack surface at all three facilities (e.g., SMR, H_2 facility, and desalination facility). Not only are there additional digital assets within the facilities, an inter-facility communication pathway will be external to the facilities. These internal and external pathways create a need for establishment of security boundaries and segmented secure architecture to limit propagation (or access) of both adversarial and unintentional incidents (or people) between and within facilities. As much as possible, the I&C system(s), components, and network architecture design should be simplified and hardened to limit the attack surface while retaining functionality and reliability. Communication flow requirements should be analyzed during design to determine if it is possible to limit flow using boundary devices and/or data diodes to reduce likelihood of propagation or infiltration.

Using the activity maps in Appendix A as a starting point, the project plan should be updated to include action items for analyzing, prioritizing, and treating digital risk. Additionally, as the CONOPS matures, the stakeholder requirements and functional requirements should identify the digital I&C needs and objectives. The high-level and low-level design decisions should capture the risk analysis and the design traceability matrices to identify and test the security decisions. As risk analyses and design iterations will likely create modifications in I&C architecture and control logic, all changes should be reevaluated to ensure that functionality, safety, performance, and security has not been adversely impacted.

5.3.2 Load balancing

5.3.2.1 Design decision

As described in the CONOPS, load balancing is done through AGC with the SMR as the responsible entity (see Section 5.3.1). AGC will adjust generation setpoints based on ICCP commands from the BES SCADA system, renewable generation availability, and available MWe for each module connected to the IES. The MWe availability calculations for each module will include demand signals from the interconnected industrial facility (e.g., H_2 and desalination facilities) and will consider the reduced thermal efficiency of the modules. Based on demand, the power level and MWe output of each module will be set with the goal to maximize H_2 generation, water desalination throughput, and IES renewable energy.

5.3.2.2 Digital engineering, security implications, and interdependencies

AGC is the preferred load balancing method because it allows generation control to dispatch according to ACE and the electricity wholesale market. However, if incorporating AGC does not increase profits or improve overall grid reliability it may be possible to switch to PFC. The choice of load balancing methodology impacts the design of the monitoring and control systems, including information flowpaths. The current U.S. nuclear fleet raises or lowers power to supply electricity to the BES based on manual control, which is often initiated by a telephone call from the ECC to the NPP.

Since AGC is an automatic control method, there will be additional external communication flowpaths between the ECC and/or IES control center to the SMR facility. Additionally, changes in IES/BES demand will automatically result in reactivity evolutions on one or more modules. Since the

safety function of the control rods in each module is to drop into the core on a reactor trip signal, the lowering and raising of control rods for reactivity control is considered non-safety. Despite this classification, the external communication pathway expands the attack surface and raises the risk of an adversarial or unintentional event that could directly impact reactor operation.

The internal and external stakeholders must remain aware of this increased digital risk. Risk analyses of the digital infrastructure of this communication pathway and the interconnected digital I&C control systems at the SMR facility level and the module level must be performed at all stages of design, from conceptual high-level design to low-level design. If hazards are identified as a result of unsafe control actions or compromised information flow, the project team (including internal and external stakeholders) should attempt to engineer out the risks or to include security controls in the design.

The decision to use AGC for load balancing will result in some level of residual risk. This risk must be well understood by all stakeholders, especially at high managerial levels (e.g., project management, facility owners, regulatory authorities). Final design, risk assessment, and decision making must be documented and periodically reviewed for applicability and regulatory compliance.

5.4 Examples of Systems-Level Decisions

In addition to mission-level and facility-level decisions, there are many systems-level and systems-of-systems-level decisions. These decisions include design questions, such as:

- What are the physical and digital connections between entities and within entities for monitoring and control based on the CONOPS?
- Where are the I&C components located? How are they physically protected?
- What is the I&C/OT architecture within a module, within a facility, and between facilities?
- What is the tradeoff if I&C designs are simplified and SSCs are hardened?
- How is the steam bypass controlled to the HTSE and MED systems?
- How is the electricity controlled for the HTSE steam superheat requirements?
- Where is the human-in-the-loop with all I&C requirements? How and where is operator control performed?
- What are the module/facility behaviors on abnormal events?
- How are safety systems impacted from the interconnection of facilities?

Each of these questions have digital engineering, risk, and security considerations. As the project moves from the conceptual design to high-level design, to low-level design stages, the answers to these questions directly impact digital risk. Appendix C provides a series of questions adapted from the *CIE Implementation Guide* that teams should consider throughout the systems engineering lifecycle.

Similar to previous sections, the project team must evaluate digital risk with each decision. A risk analysis, such as a hazard and operability study, can identify unsafe control actions and hazards resulting from unanticipated process events. These risk analysis teams must include stakeholders within the various interdisciplinary project teams, including those from reactor physics and reactor design teams, industrial application teams, digital I&C teams (hardware, firmware, software). In the event the safety and digital risk is determined to be too high, the teams should consider redesigning the system(s), such as by simplifying the design, modifying system architecture, hardening SSCs, and/or adding diversity and redundancy to reduce the risk. Of course, since these options may seem to be in direct opposition to each

other (i.e., simplify vs. add redundancy), the teams should evaluate and document how the chosen modification lowers overall digital risk.

6. CONCLUSIONS

This report provides an approach for integrating all forms of digital risk into nuclear engineering projects. As illustrated by the activity maps in Appendix A, project workflows can be designed to incorporate both adversarial and unintentional digital risk to better integrate digital engineering decision analysis. A primary goal of this report is to identify how organizations can avoid creating silos between cybersecurity and everything else; cybersecurity must be evaluated along with all the other design inputs to balance functionality, safety, performance, reliability, and security.

An example of a simplified CONOPS for an SMR-driven IES project early in its systems engineering lifecycle is provided to demonstrate how mission-level, facility-level, and systems-level design decisions affect competing objectives and competing stakeholder requirements, including both physical and cyber security considerations. Considering a broad range of consequence types (or performance metrics) is necessary to fully evaluate digital risk; however, given the range of scenario types and consequence types (see Figure 2) that need to be considered, and the lack of design detail at early stages of design, it is necessary to apply suitable combinations of risk and hazard analysis methods to develop useful understanding of the risks that are present in a given CONOPS. Analyzing this digital risk and applying risk treatments to reduce the risk, including making it more difficult for an adversary to successfully achieve their attack objectives, must be performed throughout the systems engineering lifecycle. These design decisions and risk treatments should be documented and revisited whenever the underlying context or higher-level decision is modified. Project plans should be updated to include specific actions to flag this reanalysis. Ultimately, the goal is to maintain an awareness of digital risk throughout the project in order to effectively reduce this risk while balancing competing objectives and requirements.

7. REFERENCES

[1] DOE, "National Cyber-Informed Engineering Strategy from the U.S. Department of Energy," U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response, 2022, Available: https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf.

[2] INCOSE, "SEBoK, Guide to the systems engineering body of knowledge," INCOSE, 2021, Available: www.sebokwiki.org.

[3] IEEE, "IEEE 308-1971 - IEEE standard criteria for class 1E electric systems for nuclear power generating stations," Institute of Electrical and Electronics Engineers, 1971.

[4] *10 C.F.R. § 50 Appendix A, Domestic Licensing of Production and Utilization Facilities,* U.S. Nuclear Regulatory Commission, 2007.

[5] IEEE, "IEEE 279-1971 - Criteria for safety systems for nuclear power generating stations," Institute of Electrical and Electronics Engineers, 1971.

[6] IEEE, "IEEE 603-1991 - IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1991.

[7] NRC, "Regulatory Guide 1.152, Revision 3, Criteria for use of computers in safety systems of nuclear power plants," U.S. Nuclear Regulatory Commission, 2011, Available: https://www.nrc.gov/docs/ML1028/ML102870022.pdf.

[8] IEEE, "IEEE 7-4.3.2-2003 - IEEE standard for digital computers in safety systems of nuclear power generating stations," Institute of Electrical and Electronics Engineers, 2003.

[9] IEC, "IEC 61513:2011, Nuclear Power Plants - Instrumentation and Control Important to Safety - General Requirements for Systems, Rev 2.0," International Electrotechnical Commission, 2011, Available: https://webstore.iec.ch/publication/5532.
[10] IAEA, "Specific Safety Requirements No. SSR-2/1, Safety of Nuclear Power Plants: Design (Rev 1)," International Atomic Energy Agency, Vienna, STI/PUB/1534, 2016, Available: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1534_web.pdf.
[11] IAEA, "Specific Safety Guide No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants," International Atomic Energy Agency, Vienna, 2016, Available: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1694_web.pdf.
[12] IEC, "IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems (Parts 1 -7)," International Electrotechnical Commission, 2010.
[13] IEC, "IEC 61511, Functional safety - Safety instrumented systems for the process industry sector (Parts 1-3)," International Electrotechnical Commission, 2016.
[14] IEC, "IEC 60880:2006, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions," International Electrotechnical Commission, 2006.
[15] IEC, "IEC 62138:2018, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions," International Electrotechnical Commission, 2018.
[16] ISO/IEC/IEEE, "ISO/IEC/IEEE 24748-1, Systems and software engineering-Life cycle management-Part 1: Guidelines for life cycle management," 2018.
[17] ISO/IEC/IEEE, "ISO/IEC/IEEE 15289:2019, Systems and software engineering — Content of life-cycle information items (documentation)," 2019.
[18] ISO/IEC/IEEE, "ISO/IEC/IEEE 15288:2023, Systems and software engineering — System life cycle processes," 2023.
[19] EPRI, "Digital engineering guide: Decision making using systems engineering," Electric Power Research Institute, 2021.
[20] INPO, "NISP-EN-04, Standard digital engineering process (EB-17-06 digital supplemental), Revision 2," Institute of Nuclear Power Operations, 2021.
[21] INPO, "IP-ENG-001, Standard design process," Institute of Nuclear Power Operations.
[22] *10 C.F.R. § 73, Physical Protection of Plants and Materials*, 2023.
[23] *10 C.F.R. § 73.54, Protection of Digital Computer and Communication Systems and Networks*, 2009.
[24] EPRI, "Cyber security technical assessment methodology, risk Informed exploit sequence identification and mitigation, Revision 1," Electric Power Research Institute, 2018.
[25] IAEA, "Nuclear Security Series No. 17, Computer security at nuclear facilities," International Atomic Energy Agency, Vienna, 2011, Available: https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities.
[26] IAEA, "Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," International Atomic Energy Agency, Vienna, 2011, Available: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1481_web.pdf.
[27] IAEA, "NSS 17-T, Rev 1, Computer Security Tecniques for Nuclear Facilities," International Atomic Energy Agency, Vienna, 2021, Available: http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1921_web.pdf.
[28] IAEA, "NSS 42-G, Computer security for nuclear security," International Atomic Energy Agency, Vienna, 2021, Available: http://www-pub.iaea.org/MTCD/Publications/PDF/PUB1918_web.pdf.
[29] IAEA, "NSS 33-T, Computer security of instrumentation and control systems at nuclear facilities," International Atomic Energy Agency, Vienna, 2018, Available: http://www-pub.iaea.org/MTCD/Publications/PDF/P1787_web.pdf.

[30] ISA, "ISA-TR84.00.09-2017, Cybersecurity Related to the Functional Safety Lifecycle," International Society of Automation, 2017.
[31] NIST, "SP 800-30, Revision 1: Guide for conducting risk assessments," National Institute of Standards and Technology, 2012.
[32] NIST, "SP 800-53 Revision 5. Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, 2017.
[33] Stouffer, K., V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "SP 800-82, Revision 2: Guide to industrial control systems (ICS) security," National Institute of Standards and Technology, 2015.
[34] IEC, "IEC 62443-3-2, Security risk assessment and system design " International Electrotechnical Commission, 2020, Available: https://webstore.iec.ch/publication/30727.
[35] IEC, "IEC 62443-4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements," International Electrotechnical Commission, September, 2016 2017.
[36] IEC, "IEC 62645:2019, Nuclear power plants - Instrumentation, control and electric power systems - Cybersecurity requirements," International Electrotechnical Commission, November, 2019, Available: https://webstore.iec.ch/publication/32904.
[37] IEC, "IEC 62443-2-4, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers," International Electrotechnical Commission, 2017.
[38] ISO/IEC, "ISO/IEC 27005:2018, Information technology - security techniques - information security management systems - Information security risk management," International Organization for Standardization/International Electrotechnical Commission, 2018.
[39] IEC, "IEC 62325-301:2018, Framework for Energy Market Communications – Part 301: Common information model (CIM) extensions for markets,," International Electrotechnical Commission, 2018.
[40] IEC, "IEC 62325-452:2021, Framework for Energy Market Communications – Part 452: North American style market profiles," International Electrotechnical Commission, 2021.
[41] IEC, "IEC 62325-550-2:2021, Framework for Energy Market Communications – Part 452: Common Dynamic Data Structures for North American style Market Profiles," International Electrotechnical Commission, 2021.
[42] NERC, "NERC Critical Infrastructure Protection (NERC-CIP) Standards," North American Electric Reliability Corporation, Available: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx.
[43] NASA, "NPR 8000.4C, Agency risk management procedural requirements," 2022, Available: https://nodis3.gsfc.nasa.gov/displayDir.cfm?Internal_ID=N_PR_8000_004C_&page_name=AppendixA.
[44] NASA, "Risk review template," NASA Independent Verification and Validation Program, 2014, Available: https://www.nasa.gov/sites/default/files/atoms/files/ivv_t2006_-_ver_g.pdf.
[45] NRC, "WASH-1400, NUREG-75/014, Reactor safety study: An assessment of accident risks in US commercial nuclear power plants," U.S. Nuclear Regulatory Commission, Washington D. C., 1975.
[46] Farmer, F.R., "Siting criteria - A new approach," in *Symposium on the Containment and Siting of Nuclear Power Plants*, Vienna, Austria, 1967.
[47] Eggers, S. *et al.*, "Cyber-Informed Engineering case study of an integrated hydrogen generation plant," in *ANS 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (NPIC&HMIT)*, Online Virtual Meeting, 2021: American Nuclear Society.
[48] NRC, "51 FR 30028. Safety goals for the operations of nuclear power plants. Policy statement.," 1986.

[49] Wyss, G.D. and A.D. Williams, "Possible Does Not Mean Useful: The Role of Probability of Attack in Security Risk Management," *Nuclear Science and Engineering,* vol. 197, no. sup1, pp. S80-S94, 2023.
[50] Wyss, G.D., "Risk-Informed Managementof Enterprise Security: Method and Example Applications," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2014.
[51] Arvanitidis, A.I., V. Agarwal, and M. Alamaniotis, "Nuclear-Driven Integrated Energy Systems: A State-of-the-Art Review," *Energies,* vol. 16, no. 11, p. 4293, 2023.
[52] Glover, J.D. and M.S. Sarma, "Power System Analysis," *Brooks/Cole Thompson Learning,* 2002.
[53] NERC, "BAL-001-2, Real Power Balancing Control Performance," North American Reliability Corporation, 2015, Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/BAL-001-2.pdf.
[54] NERC Resources Subcommittee, "Balancing and frequency control," North American Reliability Corporation, 2011, Available: https://www.nerc.com/comm/OC/BAL0031_Supporting_Documents_2017_DL/NERC%20Balancing%20and%20Frequency%20Control%20040520111.pdf.
[55] Ram Babu, N., S.K. Bhagat, L.C. Saikia, T. Chiranjeevi, R. Devarapalli, and F.P. García Márquez, "A comprehensive review of recent strategies on automatic generation control/load frequency control in power systems," *Archives of Computational Methods in Engineering,* vol. 30, no. 1, pp. 543-572, 2023.
[56] NRC, "Regulatory Guide 5.71 revision 1, Cyber security programs for nuclear facilities," U.S. Nuclear Regulatory Commission, 2023.
[57] NRC, "Regulatory Guide 5.81 Revision 1, Target set identification and development for nuclear power reactors," U.S. Nuclear Regulatory Commission, 2019.
[58] Eggers, S. and K. Le Blanc, "Survey of cyber risk analysis techniques for use in the nuclear industry," *Progress in Nuclear Energy,* vol. 140, 2021.
[59] Williams, A.D., "System Theoretic Process Analysis (STPA): Overview of Sandia Uses to Address National Security Problems," presented at the Conference: Proposed for presentation at the Boiling Water Reactor Owners Group Meeting held June 3-21, 2019 in Albuquerque, NM, United States., United States, 2019. Available: https://www.osti.gov/biblio/1645411
[60] Ingersoll, D., Z. Houghton, R. Bromm, and C. Desportes, "NuScale small modular reactor for Co-generation of electricity and water," *Desalination,* vol. 340, pp. 84-93, 2014.
[61] Al-Othman, A., N.N. Darwish, M. Qasim, M. Tawalbeh, N.A. Darwish, and N. Hilal, "Nuclear desalination: A state-of-the-art review," *Desalination,* vol. 457, pp. 39-61, 2019.
[62] Boardman, R., M. McKellar, D. Ingersoll, Z. Houghton, R.B. , and C. Desportes, "Extending nuclear energy to non-electrical applications," presented at the Conference: The 19 pacific Basin Nuclear Conference (PBNC2014),Hyatt Regency Hotel Vancouver British Columbia,Canada,08/24/2014,08/28/2014, United States, 2014. Available: https://www.osti.gov/biblio/1169226
[63] DoT, "Systems engineering guidebook for Intelligent Transportation Systems, Version 3.0," U.S. Department of Transportation, 2009.
[64] Wright, V.L. *et al.*, "Cyber-Informed Engineering Implementation Guide," United States, 2023, Available: https://www.osti.gov/biblio/1995796.
[65] Eissa, D., "Concept generation in the architectural design process: A suggested hybrid model of vertical and lateral thinking approaches," *Thinking Skills and Creativity,* vol. 33, p. 100589, 2019.

Page intentionally left blank

Appendix A
Nuclear Digital Systems Engineering Lifecycle Activity Maps

Nuclear Digital Systems Engineering Lifecycle Activity Maps

Figure 1 illustrates a v-model of the systems engineering lifecycle showing a progression through five phases from concept exploration to decommissioning or disposal. Each of these phases has separate independent stages. The early design phases can be broken into separate activity maps to enable project personnel to understand the specific activities needed for nuclear digital engineering design. These activity maps, adapted from the Department of Transportation Systems Engineering Guidebook for Intelligent Transportation Systems [63], indicate inputs and outputs for each set of activities, as well as constraints and enablers for nuclear digital systems engineering.

As digital engineering incorporates balancing multiple objectives, such as functionality, safety, reliability, and security, these activity maps incorporate all necessary activities, not only those related to cybersecurity. The intent is to bring all of these design requirements together instead of building a separate silo for cybersecurity. An additional concept included in these maps is that the project team should be concerned about ALL digital risk, including unintentional (e.g., software errors, common cause failures, inadvertent human performance errors, environmental hazards) and intentional or adversarial threats, as well as all consequences (e.g., public health and safety, equipment failure, lost generation, reputation damage).

The following figures provide a list of suggested activities, inputs, outputs, constraints, and enablers in a simple format for use during the early design stages. Most of the activity descriptions can be found in other systems engineering and nuclear digital engineering guidance documents and are not repeated here. Sample input and output formats are also typically found in these documents. Using these maps can ensure that key activities in both digital engineering and cybersecurity are not omitted as the team moves through the lifecycle.

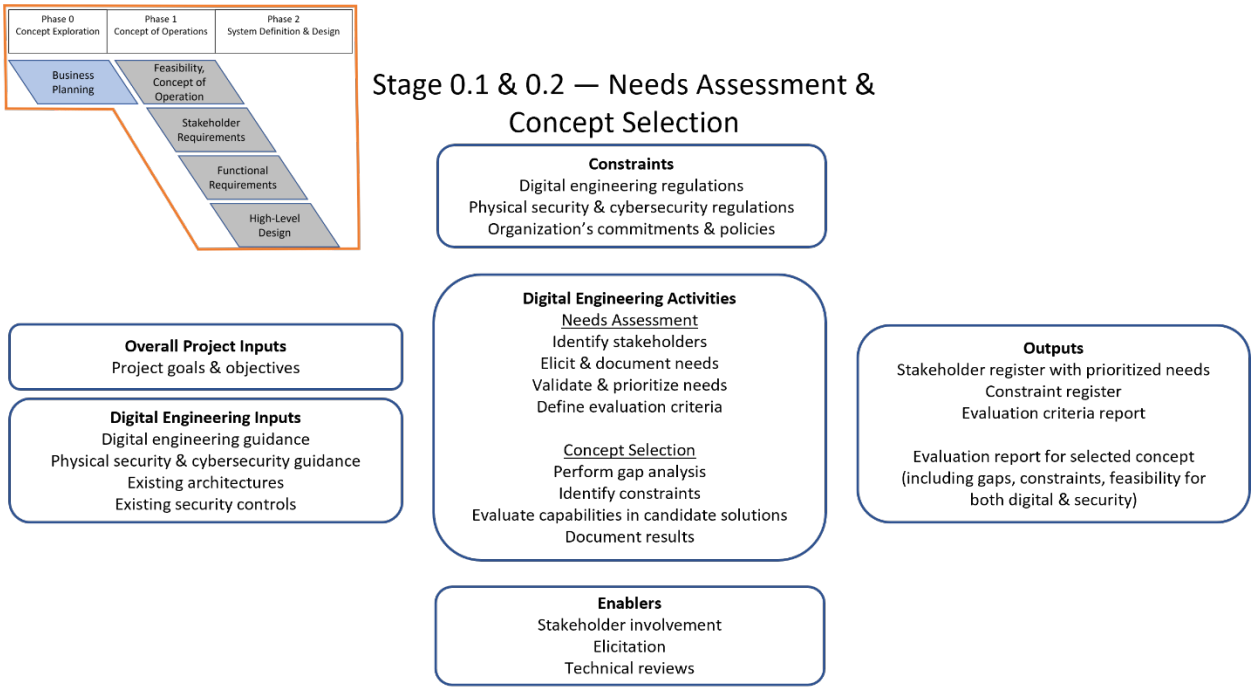

Figure 17. Nuclear digital engineering activity map for the concept exploration phase.

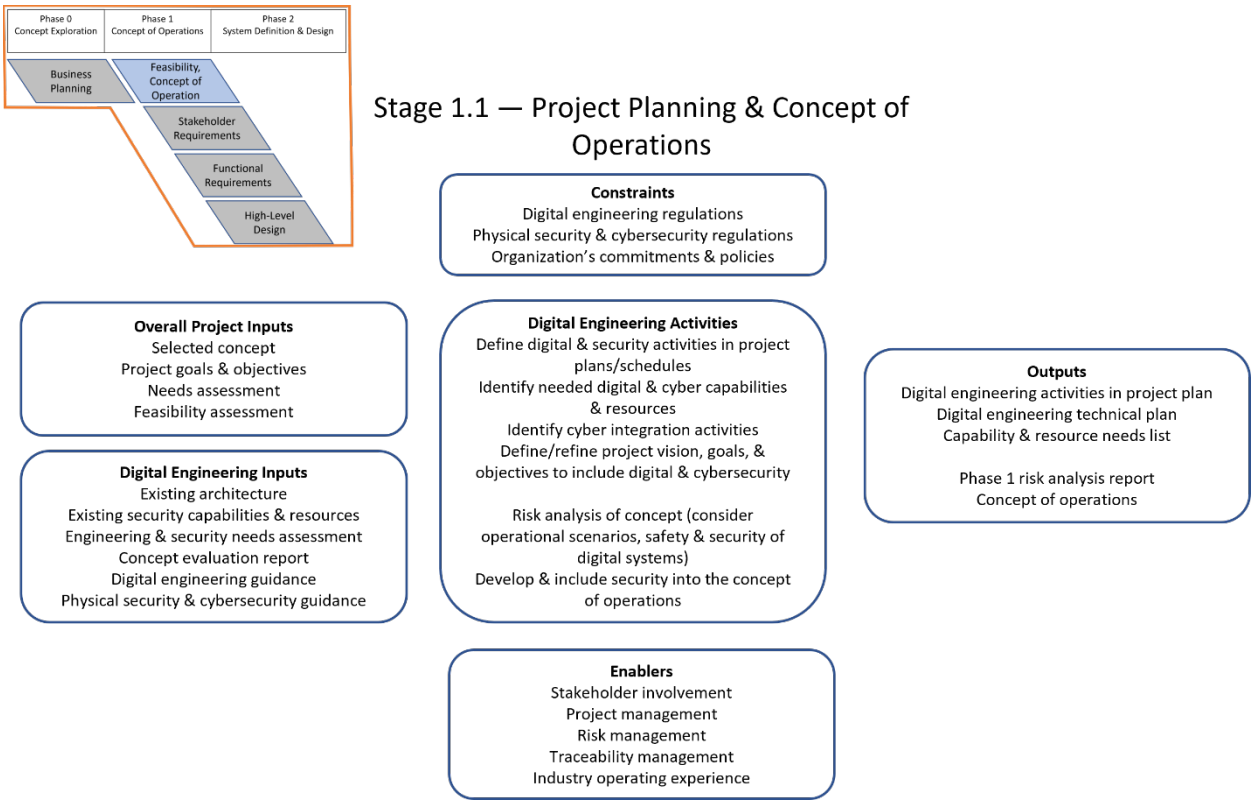

Figure 18. Nuclear digital engineering activity map for the concept of operations phase.

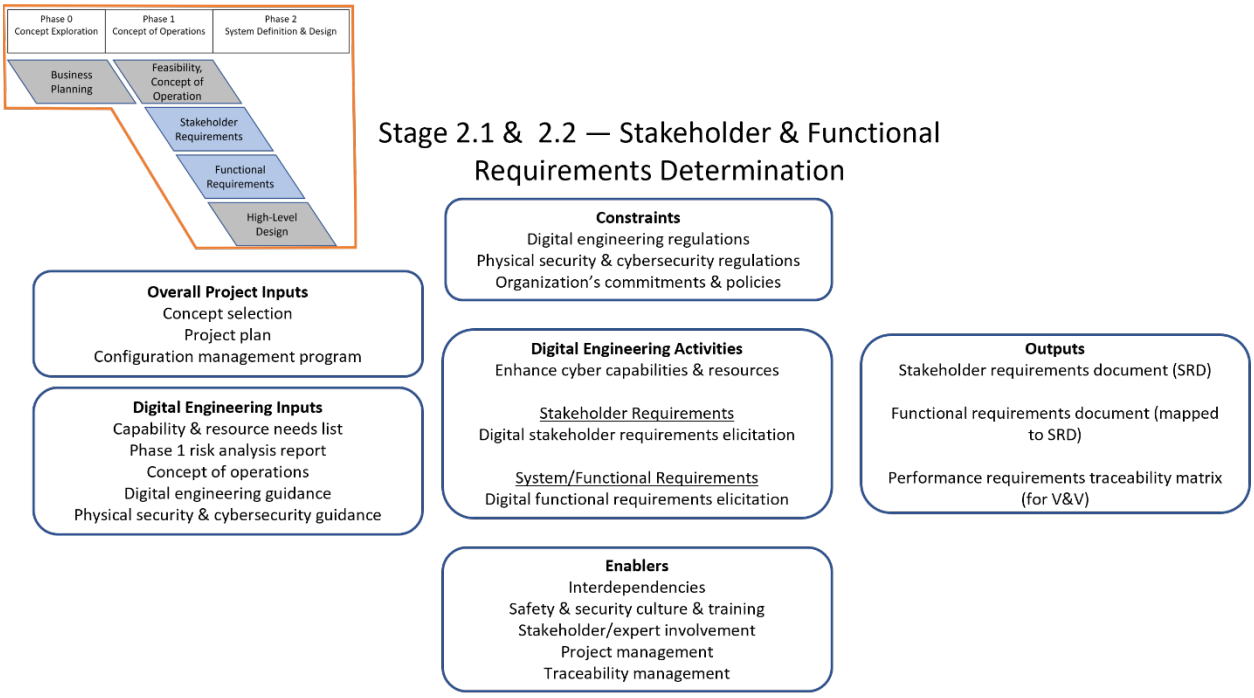

Figure 19. Nuclear digital engineering activity map for the stakeholder and requirements determination stages.

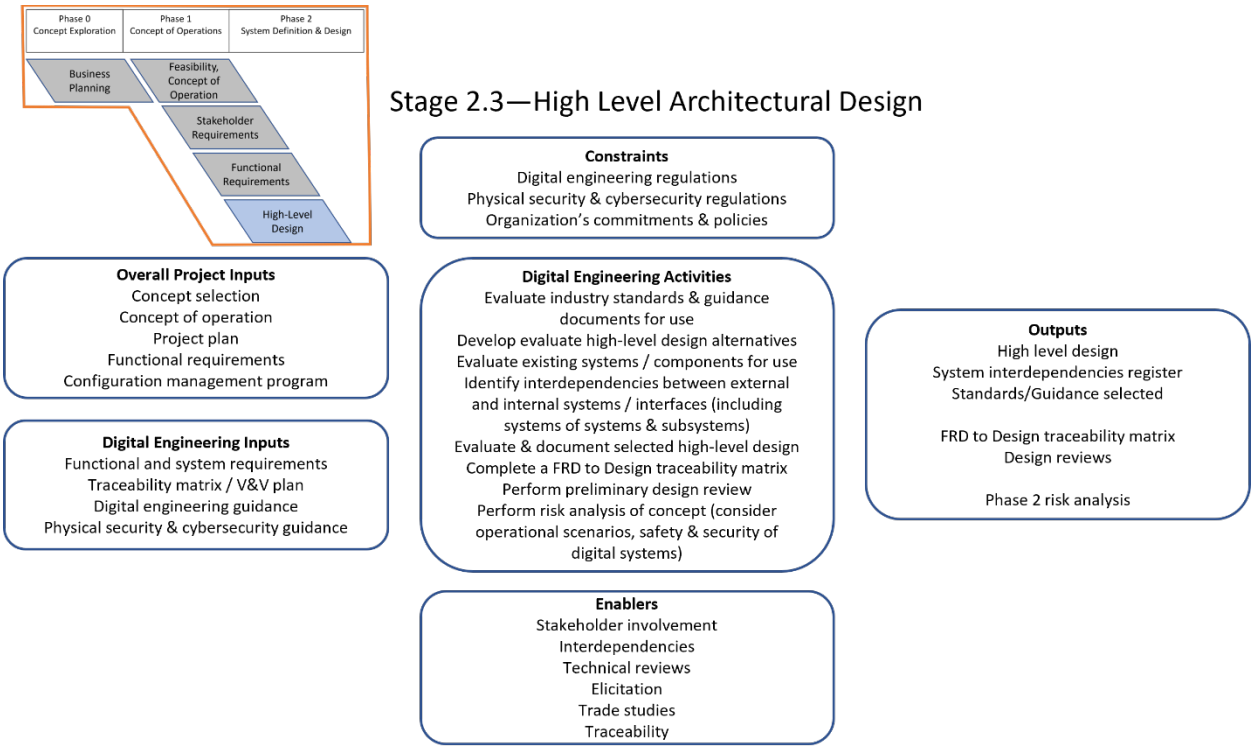

Figure 20. Nuclear digital engineering activity map for the high-level design stage.

Appendix B
NASA CONOPS Annotated Outline

NASA Concept of Operations Annotated Outline[1]

Cover Page

Table of Contents

1.0 Introduction

1.1 Project Description

This section will provide a brief overview of the development activity and system context as delineated in the following two subsections.

1.1.1 Background

Summarize the conditions that created the need for the new system. Provide the high-level mission goals and objective of the system operation. Provide the rationale for the development of the system.

1.1.2 Assumptions and Constraints

State the basic assumptions and constraints in the development of the concept. For example, that some technology will be matured enough by the time the system is ready to be fielded, or that the system has to be provided by a certain date in order to accomplish the mission.

1.2 Overview of the Envisioned System

This section provides an executive summary overview of the envisioned system. A more detailed description will be provided in Section 3.0

1.2.1 Overview

This subsection provides a high-level overview of the system and its operation. Pictorials, graphics, videos, models, or other means may be used to provide this basic understanding of the concept.

1.2.2 System Scope

This section gives an estimate of the size and complexity of the system. It defines the system's external interfaces and enabling systems. It describes what the project will encompass and what will lie outside of the project's development.

2.0 Documents

2.1 Applicable Documents

This section lists all the documents, models, standards or other material that are applicable and some or all of which will form part of the requirements of the project.

2.2 Reference Documents

This section provides supplemental information that might be useful in understanding the system or its scenarios.

3.0 Description of Envisioned System

[1] https://www.nasa.gov/seh/appendix-s-concept-of-operations

This section provides a more detailed description of the envisioned system and its operation as contained in the following subsections.

3.1 Needs, Goals, and Objectives of Envisioned System

This section describes the needs, goals, and objectives as expectations for the system capabilities, behavior, and operations. It may also point to a separate document or model that contains the current up-to-date agreed-to expectations.

3.2 Overview of System and Key Elements

This section describes at a functional level the various elements that will make up the system, including the users and operators. These descriptions should be implementation free; that is, not specific to any implementation or design but rather a general description of what the system and its elements will be expected to do. Graphics, pictorials, videos, and models may be used to aid this description.

3.3 Interfaces

This section describes the interfaces of the system with any other systems that are external to the project. It may also include high-level interfaces between the major envisioned elements of the system. Interfaces may include mechanical, electrical, human user/operator, fluid, radio frequency, data, or other types of interactions.

3.4 Modes of Operations

This section describes the various modes or configurations that the system may need in order to accomplish its intended purpose throughout its life cycle. This may include modes needed in the development of the system, such as for testing or training, as well as various modes that will be needed during its operational and disposal phases.

3.5 Proposed Capabilities

This section describes the various capabilities that the envisioned system will provide. These capabilities cover the entire life cycle of the system's operation, including special capabilities needed for the verification/validation of the system, its capabilities during its intended operations, and any special capabilities needed during the decommissioning or disposal process.

4.0 Physical Environment

This section should describe the environment that the system will be expected to perform in throughout its life cycle, including integration, tests, and transportation. This may include expected and off-nominal temperatures, pressures, radiation, winds, and other atmospheric, space, or aquatic conditions. A description of whether the system needs to operate, tolerate with degraded performance, or just survive in these conditions should be noted.

5.0 Support Environment

This section describes how the envisioned system will be supported after being fielded. This includes how operational planning will be performed and how commanding or other uploads will be determined and provided, as required. Discussions may include how the envisioned system would be maintained, repaired, replaced, it's sparing philosophy, and how future upgrades may be performed. It may also include assumptions on the level of continued support from the design teams.

6.0 Operational Scenarios, Use Cases, and/or Design Reference Missions

This section takes key scenarios, use cases, or DRM and discusses what the envisioned system provides or how it functions throughout that single-thread timeline.

The number of scenarios, use cases, or DRMs discussed should cover both nominal and off-nominal conditions and cover all expected functions and capabilities. A good practice is to label each of these scenarios to facilitate requirements traceability, e.g., [DRM-0100], [DRM- 0200], etc.

6.1 Nominal Conditions

These scenarios, use cases, or DRMs cover how the envisioned system will operate under normal circumstances where there are no problems or anomalies taking place.

6.2 Off-Nominal Conditions

These scenarios cover cases where some condition has occurred that will need the system to perform in a way that is different from normal. This would cover failures, low performance, unexpected environmental conditions, or operator errors. These scenarios should reveal any additional capabilities or safeguards that are needed in the system.

7.0 Impact Considerations

This section describes the potential impacts, both positive and negative, on the environment and other areas.

7.1 Environmental Impacts

This section describes how the envisioned system could impact the environment of the local area, state, country, world, space, and other planetary bodies as appropriate for the systems intended purpose. This includes the possibility of the generation of any orbital debris, potential contamination of other planetary bodies or atmosphere, and generation of hazardous wastes that will need disposal on earth and other factors. Impacts should cover the entire life cycle of the system from development through disposal.

7.2 Organizational Impacts

This section describes how the envisioned system could impact existing or future organizational aspects. This would include the need for hiring specialists or operators, specialized or widespread training or retraining, and use of multiple organizations.

7.3 Scientific/Technical Impacts

This subsection describes the anticipated scientific or technical impact of a successful mission or deployment, what scientific questions will be answered, what knowledge gaps will be filled, and what services will be provided. If the purpose of this system is to improve operations or logistics instead of science, describe the anticipated impact of the system in those terms.

8.0 Risks and Potential Issues

This section describes any risks and potential issues associated with the development, operation, or disposal of the envisioned system. Also includes concerns/risks with the project schedule, staffing support, or implementation approach. Allocate subsections as needed for each risk or issue consideration. Pay special attention to closeout issues at the end of the project.

Appendix A: Acronyms

This part lists each acronym used in the ConOps and spells it out.

Appendix B: Glossary of Terms

The part lists key terms used in the ConOps and provides a description of their meaning.

Appendix C
Adaptation of DOE CESER CIE Implementation Guide for Early Design Phases in Digital Engineering

Adaptation of DOE CESER CIE Implementation Guide for Early Design Phases in Digital Engineering

The U.S. DOE CESER *Cyber-Informed Engineering Implementation Guide Version 1.0* outlines questions that engineering teams should consider at various phases of a system's life cycle [64]. This guide aims to extend the secure-by-design concept for all system design aspects. It is worth noting that some questions appear redundant, for example, the question related to "purpose" is in multiple places (e.g., 1A.1, 1A.2, 2E.1, 3A.1b, 3A.1d, 4B.1a, and 12A.1a). While this redundancy is helpful to provide a theoretical basis, in practice performing redundant and repetitive work may be cumbersome for designers, engineers, and developers. Simplification and ease of use are often preferred.

To simplify the guide and make it more user friendly, a high-level outline was created by reviewing each question, merging related questions, and simplifying the content. Documentation is required throughout the systems engineering lifecycle to provide a basis for risk acceptance decisions. A deep understanding of the overall system also facilitates design explorations. As it is critical to first understand the overall system, the following paragraphs describe the structure of this analysis.

Overall System

The overall system incorporates all decomposition and dimensional aspects throughout the product lifecycle. The *DOE CESER CIE Implementation Guide* uses the concept of the product lifecycle, so the general categories are similar. In the iterative process of restructuring, merging, and simplifying, we summarize the overall system description into four categories: compositions, functional purposes, rationale/assumptions, and operational conditions, as shown in Figure 21.

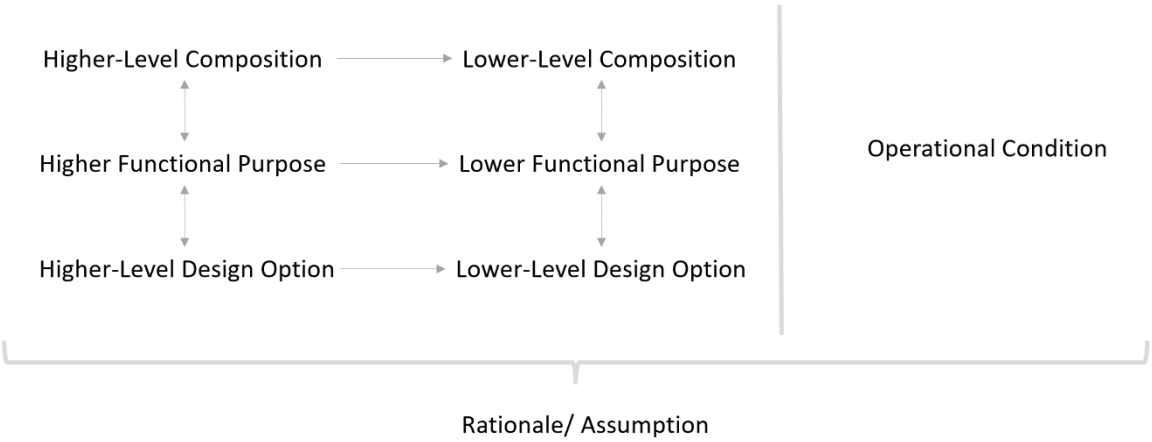

Figure 21. Compositions, functional purposes, rationale/ assumptions, operational conditions, and their interrelations.

Composition

A composition represents a set of items that support the functional purpose(s) of the overall system. Compositions can range from broad entities or organizations to specific components and personnel. While personnel functions are not always explicitly specified in system design and product life cycle documents, the CIE implementation guide includes personnel-related questions (e.g., 2A.3, 6F.6a, 7D.3, 12F.1). In a work domain, each person serves specific values and functionalities for the entity or organization. During the design phase, the overall functional purposes of the entity or organization are decomposed into systems, sub-systems, sub-subsystems, and so on, down to the lowest level. Thus, each composition has its functional purposes, including:

- Entity/ Organization
- System
- Subsystem
- Component
- Subcomponent
- Digital asset
- Interdependency, interconnectivity, and network
- Personnel (e.g., employee, user, worker).

Functional Purpose

Several terms (e.g., value, purpose, function, goal, subgoal, intent) have been used to describe the concept of functional purpose. These terms may have slight differences between them. For instance, goals are often related to specific ways of executing values. In such cases, "value" may refer to a higher level of decomposition, whereas "goals" may apply to a lower level of decomposition. To simplify terminology, we categorize these terms together. The consideration of functional purpose encompasses:

- Priority, trade-off, and acceptability. Multiple functional purposes often serve the highest level of decomposition given the diversity of human and social values. While achieving all functionalities would be ideal, there are situations and contexts where these functional purposes may compete. Understanding their priorities is crucial to making effective trade-off decisions and judgments. Assessing low-probability and high-consequence events can sometimes be challenging and may depend on various individual factors (e.g., education), so finding out the acceptability offers another way to explore trade-offs.
- Decomposition. Functional decomposition is a key process throughout the product design life cycle. During this process, designers and developers determine the functionalities of each composition and the flow of information processing and logical interdependencies. On the one hand, this structure can be viewed as fixed, with higher-level functional decomposition determining lower-level functional decomposition. On the other hand, modifying higher-level functional decomposition can sometimes expand the available options for achieving goals. There might be simpler and more straightforward solutions. Insights can be from conscious and unconscious thinking, but they are always rooted in an understanding of theories, methods, and challenges that individuals encounter. On a broader scale, developing a comprehensive and simplified understanding of each interconnected domain can facilitate lateral thinking, which does not only select but opens other alternative approaches, inspiring the discovery of new design options [65].
- Design options. Each functional decomposition can be associated with multiple design options. These design options can be related to the concept of operations, system requirements, methods, techniques, processes, logic, algorithms, etc. There are various ways to achieve the ultimate functional purposes, which is why stakeholders often explore multiple approaches.

Rationale/ Assumption

Understanding the rationale and assumptions behind major decision-making during the design process is critical. There is always a rationale behind the decisions made by project managers, designers, and developers. Some rationales are based on theories, while others may result from experiments, testing, guidelines, regulations, and previous system setups. Some assumptions are unintentionally made through reasoning, inference, or personal understanding. That is to say, some decisions are conditionally valid,

meaning they are applicable to specific conditions. When external conditions deviate from the design assumptions, previous conclusions may no longer hold true. Assumptions nested within assumptions can be risky because they can propagate, and individuals who did not design and build them may struggle to identify the entire hierarchy. Therefore, documenting the rationale and assumptions behind each decision is important. Rationale can be broken down into the following three categories:

- Valid
- Conditional valid
- Unclear.

Operational Condition

Operational conditions are associated with the functional decomposition. Representativeness and generalizability are critical factors to consider. Different types of interdependencies may require varying levels of detail to study their effects. Functions at each decomposition level have interrelated operational conditions. Ideally, the overall system should be designed to accommodate all operational conditions. Operational conditions can include:

- Normal
- Compromise
- Failure
- Unexpected conditions.

Questions to Facilitate Design Explorations

This session contains questions relevant to design options explorations. We have condensed questions from the *DOE CESER CIE Implementation Guide's* concept phase and requirements phase, excluding those more relevant to other product design phases (e.g., operation and maintenance). Here are the questions that facilitate design explorations.

1. Understand the overall system

- What are the compositions, functional purposes, rationale/ assumptions, operational conditions, and their interrelations?
- What common personal digital systems do individuals use or carry at work?
- What deliberate functional misuses of the subsystem, component, subcomponent, software application, personnel, and their interdependencies can lead to high-consequence events and functional purpose loss?
- What the common events and misuses can trigger multiple abnormal operational conditions happening concurrently, potentially resulting in high consequences?

2. Explore the conceptual and engineering design options

Research and analyze the latest methods and best practices, while understanding the theories and reasoning. Analyze the system:

- What are the necessary interdependencies and interconnectivities?
- Is it necessary to use digital assets to serve the functions?
- Based on theories, can we change the design (e.g., concept of operation, system, process, controller logic, function) to ensure that critical functions are not affected by digital assets?
- Can we isolate digital assets with physical barriers?
- What additional redundancy is required in the event where digital assets within the same physical barriers are simultaneously compromised and misused?
- How long would it take to repair, reconfigure, or restore these functions considering the worst case?
- Can the public and consumers accept such temporary loss or misuse of functions? Would it lead to severe irreversible losses?
- Can additional engineering controls and mitigations be put in place to shorten the restoration?
- Can engineering controls and mitigations result in unforeseen consequences?

3. Explore the interdependencies and interconnectivities design options:

When developing digital assets, there is a tendency to assume that everything is interconnected. Some interconnections and dependencies may be unnecessary to establish. Another way to think about design options is to start with the assumption that nothing is interconnected and ask:

- What interconnectivities need to be established?
- What is the flow of information processes for each system/subsystem/component function?
- Is it possible to modify the design to segment the system and minimize the use of digital assets and network?
- Can alternative local or nondigital measurements and devices be used to achieve the function?