ORNL/TM-2023/2850

Oak Ridge National Laboratory Security by Design: A Plant Design and Component–Based Approach to Technical Solutions to Insider and Outsider Threat

Scott Nelson
Prashant Jain
Alex Huning

May 2023

OAK RIDGE National Laboratory

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

ORNL/TM-2023/2850

Nuclear Energy and Fuel Cycle Division
International Nuclear Security

SECURITY BY DESIGN: A PLANT DESIGN AND COMPONENT–BASED APPROACH TO TECHNICAL SOLUTIONS TO INSIDER AND OUTSIDER THREAT

Scott Nelson
Prashant Jain
Alex Huning

May 2023

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

This page is intentionally left blank.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ALARA	as low as reasonably achievable
ARIS	Advanced Reactor Information System
CFR	US Code of Federal Regulations
CSV	comma-separated value
DBT	design basis threat
FSAR	final safety analysis report
HDF5	hierarchical data format
HRC	high radiological consequences
HWR	heavy water reactor
IAEA	International Atomic Energy Agency
IEMO	Initiating Events of Malicious Origin
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
LWR	light-water reactor
NEI	Nuclear Energy Institute
NES	Nuclear Energy Series
NPP	nuclear power plant
NRC	US Nuclear Regulatory Commission
NSS	Nuclear Security Series
O&M	operations and maintenance
ORNL	Oak Ridge National Laboratory
PPS	physical protection system
PRA	probabilistic risk assessment
SaSID	safety and security interface database
SeBD	security by design
SMR	small modular reactor
TTCD	time-to-core-damage
SQL	structured query language
SRP	standard review play
VAI	vital area identification
VTK	visualization toolkit

ABSTRACT

Security costs for nuclear reactors increase over a nuclear facility's lifecycle as new threats, security weaknesses, and the plant's generic threat profile change over time. This report reviews current technological gaps in security by design (SeBD) based on an analysis of available literature and provides details to close those gaps through proposed technological constructs and processes that can integrate safety and security into the design process of a plant, with a primary focus on small modular reactor technology. Under the new modular and mass manufacturing approach, plants are designed to reduce costs through economies of scale and modular construction. The current SeBD definitions focused on state-level regulators are not adequate for this approach because the licensing stage is often too late in the design process to allow for integration of true SeBD cost savings. This document proposes a new approach to allow for continuous implementation of security alongside development of the plant's safety concept. If this approach is adopted as part of the design process, then the resulting technological ecosystem will imbed security concepts into the plant's physical design components.

1. INTRODUCTION

To properly develop and test methodologies to address the security of small modular reactors (SMRs), especially methodologies focused on an insider threat, it is important to develop the SMR design framework, the security by design (SeBD) concept, the general theory of security against insider threat, and the method for combining design and security throughout the plant's entire lifecycle. This approach is necessary to maintain the parameters against which a plant's security paradigm, equipment, technical solutions, and security culture can be tested for performance at all stages.

To accomplish this, a series of assumptions must be made, and various security protocols must be defined and tested. First, the term *small modular reactor* must be defined. Second, a study must be conducted to determine the similarities and differences in the various SMR technologies as defined in the public domain. These similarities and differences must be defended across a wide spectrum of international locations and differing threat profiles. Once the groundwork is established and the existing SMR designs are defined, then the approach for applying SeBD can be developed.

The International Atomic Energy Agency (IAEA) developed the Nuclear Security Series (NSS)[1] for guidance on implementing nuclear security and safeguards by design in the IAEA Nuclear Energy Series (NES).[2] However, guidance is minimal for SeBD. Within the IAEA/nuclear lexicon, *safeguards* refers to nonproliferation or resistance to proliferation of nuclear material, as well as theft or dispersal of special nuclear materials, and *security* is defined as the means for protecting a facility. Security is related to safeguards in that security fulfills a necessary role in protecting a facility and preventing the occurrence of incursions, theft, sabotage, and/or other malicious events. However, security does not deal with proliferation or tracking of special nuclear material in terms of theft or dispersal and thus is beyond the scope of this paper. A clear definition of SeBD is key when determining whether the appropriate steps have been taken and the proper equipment and tools have been used to ensure that security was considered as part of plant design. Clear definition of SeBD metrics is also necessary for testing. The primary goal of this paper is to develop a technical methodology that, if followed during a nuclear plant's design process, can ensure that a plant has met the SeBD principles as established herein.

Once SeBD, SMR features, and security and safety processes are clearly defined, specific insider threat timelines and mitigation techniques can be determined and tested. Once testing is complete, the

[1] IAEA Nuclear Security Series (NSS) ISSN: 1816-9317.
[2] IAEA Nuclear Energy Series (NES) ISBN 978-92-0-101018-6 STI/PUB/1806.

methodology will be reviewed, and the plant design stages within the methodology will be applied to ensure that this methodology allows designers to include secure features into plant safety.

This methodology will be applied to future nuclear design projects to ensure that communication between safety, security, and safeguards is effective and continuous. SeBD will also provide a framework for development and testing of future designs to ensure their security from both insider and outsider threats.

2. SMALL MODULAR REACTORS

2.1 DEFINITION OF SMALL MODULAR REACTOR

Although the definitions of *small modular reactor* (SMR) have some similarities across various nuclear agencies, there are notable differences between definitions from regulatory and industry entities such as the US Nuclear Regulatory Commission (NRC), the Nuclear Energy Institute (NEI), the World Nuclear Association, and nuclear designers. The most encompassing definition of the term is from industry representatives, who define SMRs as advanced reactors that produce ≤300 megawatts of electricity and utilize components that can be factory built.[3][4]

IAEA defined *small modular reactor* at the nuclear reactor's forum as a nuclear reactor having the following features:

- Typically produces <300 MWe or <1,000 MWt per reactor
- Designed for commercial use (not test or research reactors)
- Designed to allow for multiple reactors in close proximity using the same infrastructure
- Light or non–light-water cooled reactors
- Uses novel designs not widely analyzed or licensed by regulators[5]

One of the most restrictive definitions is the NRC's, which stipulates that all SMRs are light-water reactors (LWRs), whereas other reactors that are not considered SMRs are defined as *advanced reactors* (non-LWR designs).[6]

This report uses the IAEA's definition of *small modular reactor*, as presented below:

- Produces less than 300 MWe
- For commercial use only (no test or research reactors)
- May be one of multiple reactors in close proximity on site using the same infrastructure
- Must be light-water or non–light-water cooled (differs from NRC)

---

[3] NEI, "Small Modular Reactors," accessed Feb. 23, 2023. https://www.nei.org/advocacy/build-new-reactors/small-modular-reactors#:~:text=What%20Are%20Small%20Modular%20Reactors,quality%20and%20reducing%20construction%20schedules.

[4] World Nuclear Association, "Small Nuclear Power Reactors," accessed Feb. 23, 2023. https://www.world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/small-nuclear-power-reactors.aspx#:~:text=Small%20modular%20reactors%20(SMRs)%20are,production%20and%20short%20construction%20times.

[5] Small Modular Reactor (SMR) Regulators' Forum, "Terms of Reference," March 2022, accessed Feb. 23, 2023. https://www.iaea.org/sites/default/files/22/04/smr_rf_tor_april_2022.pdf

[6] NRC, "Small Modular Reactors (LWR Designs)," accessed Feb. 23, 2023. https://www.nrc.gov/reactors/new-reactors/smr.html,

- May have modular design with modules manufactured off site and delivered; may be typically assembled on site for large nuclear plants

Based on this definition, designs presently under detailed design or licensing review according to the Advanced Reactor Information System (ARIS) Database were reviewed. In addition, reactors meeting any of these criteria that have been awarded government grants to continue development were also prioritized in the SMR review. The goal of this review is to determine a set of typical traits common to SMRs.

2.2 TYPICAL SMR TRAITS

Plants were selected for the review based on four criteria:

- Plants labeled in the ARIS Database as "Detailed Design," indicating that they have proceeded past the conceptual level
- Plants that have received public funds for development within the last three years
- Plants that have signed agreements with a state to conduct research and development
- Plants for which there are large amounts of data available in the public space (i.e., design developed publicly by a national lab or other public entity)

With these criteria established, the following nine reactors were selected, and their high-level systems and components were reviewed, as shown in Table 1.

Table 1. SMR trait review table

Component	NuScale	4S	SMART	KLT-40S	HTR-PM	HAPPY200	ThorCon	SmAHtr	IPHWR-220
Reactor core	P	P	P	P	P	P	P	P	P
Encased fuel	P	P	P	P	P	P	N	P	P
Non-encased fuel	N	N	N	N	N	N	P	N	N
Primary reactor coolant pumps	N	P	IR	IR	P	P	P	IR	BR
Pressurizer	IR	N	IR	P	N	P	N	N	BR
Steam generator/primary heat exchanger	IR	P	IR	BR	BR	BR	BR	IR	BR
Turbine generator	P	P	P	P	P	P	P	P	P
Chemical control system including purification	P	P	P	P	P	P	P	P	P
Enclosed containment building	P	P	P	P	P	P	P	P	P
Online fuel loading system	N	N	N	N	P	N	U	N	P
Spent fuel pool/tank	P	N	P	N	P	P	P	P	P
Spent fuel recirculation pumps	P	N	P	N	U	P	U	P	P
Coolant towers UHC	N	P	N	N	U	U	P	P	P
Coolant pond UHC	P	N	N	N	U	U	P	N	P
Pressurizer spray valves	P	N	N	N	N	P	N	N	P
Condenser	P	P	P	P	P	U	P	P	P
Off gas system	P	U	P	U	P	U	P	U	U

IR = Integral to reactor pressure vessel
P = present
N = not present
U = unknown
BR = boundary to reactor pressure system

The reactor designs presented in Table 1 share many common traits at a high level. SMR designs typically maintain encased fuel, forced convection, and turbine generators. Also, components typically located outside the primary pressure vessel for large scale PWRs are now located within the SMR pressure vessel boundary. This facilitates a modularized, reduced facility footprint, which is of key interest to many potential nuclear customers.

NuScale, Happy200, and ThorCon, which average of 3,646 MW/m^2, list their footprints on as 1.4E4 m^2, 6.0E4 m^2, and 2.5E5 m^2, respectively. Current US LWRs[7] generate 2.742E-4 MW/$m^2$with footprints averaging 3.367E6 m^2. Although the exact footprint can vary widely based on many factors, this comparison shows that the NuScale, Happy200, and ThorCon footprints are reduced by factors of 319, 74 and 18, respectively—a significant decrease in facility size. When considering the smaller footprint along with the power density of the facility, one finds 2.13E-1, 6.67E-3, and 1.60E-3 MW/m^2 for NuScale, Happy200, and ThorCon designs, respectively. The increases in site-based power densities for these reactors—781, 24, and 6 MW/m^2, respectively—should be offset by additional safety features built into

[7]Landon Stevens et al., *The Footprint of Energy: Land Use of US Electricity Production*. Strata, 2017.

their designs. However, smaller footprints may present security risks, such as limitations on the ability to delay threats, or the likelihood that an mutual SMR could be in close proximity to each other because multiple systems in close proximity could be tampered with more easily.

SMRs present several SeBD challenges, such as maintaining security around target sets when facilities are tightly packed together, operating with less staff while maintaining the necessary redundancy against potential insiders, delaying potential insider and outsider threats to a smaller space and area, and allowing for the ability to upgrade security to manage new threats as they evolve within the SMR's limited space. Examples of threats that could evolve in the plant's 40+ year licensed lifetime include events such as the September 11 terrorist attacks on the World Trade Center, the bombing of the USS Cole, and the impending widespread usage of drones or other technologies. All of these challenges must be addressed in time, due to the ever evolving threats to security. Because of the small size and compact nature of these facilities, the margin for error is narrow if a plant's security is compromised. Such a compromise would result in unanticipated costs. Furthermore, it may not be possible to make the necessary upgrades to address security concerns. SMRs cannot readily absorb the costs of adding on-site security posts, delay mechanisms, or other security measures after the finalized design because of their small electrical output. Therefore, incorporating and reducing security risks within the design of the plant itself is paramount, thus necessitating implementation of a true SeBD process.

2.3 ECONOMICS OF SMALL MODULAR REACTORS

The plan for NuScale is to reduce the number of operation staff onsite—not to eliminate the staff entirely, as a microreactor designer might prefer. Current nuclear plants require skilled, highly trained staff to be present onsite, including certified operators, maintenance personnel, engineers, and managers. The current staffing level for a 1,000 MWe plant is approximately 1,000, or approximately one person per MWe.[8] A one-to-one comparison of these numbers based on the VOYGR NuScale reactor design would result in a maximum of 924 staff members for a 12-module plant reaching 924 MWe. Current NuScale licensing documents specify that two senior reactor operators and one reactor operator must be present in a single control room for safe operation of the 12-module plant. This differs from the typical LWR staffing, which would require two senior reactor operators for a two-unit plant and four reactor operators. However, these staffing levels can vary based on plant design and licensing restrictions.[9] According to ZipRecruiter, the average US nuclear power plant (NPP) salary is $98,094 as of September 1, 2022. A one to one estimation of labor costs based on these assumptions is not accurate however since the general movement of SMR technology is to reduce costs and on site personnel a one to one assumption should provide a conservative ceiling on labor costs that is likely very high compared to actual costs. Thus this ceiling based on a 924 MWe plant would be 90 Million USD per year.

Multi-module SMR overnight cost estimates were analyzed based on publicly available data for reactors within a range of 3,600 to 3,900 $/kWe[10]. Table 2 presents an[11] analysis of base overnight costs of new electricity generation in the United States for various reactor types.

[8] S. R. Greene, G. F. Flanagan, and A. P. Borole, *Integration of Biorefineries and Nuclear Cogeneration Power Plants – A Preliminary Analysis*, ORNL/TM-2008/102 (ORNL/GNEP/LTR-2008-047), March 9, 2009.
[9] NEI, "Control Room Staffing for Small Reactors," 2011, accessed Feb. 23, 2023. https://www.nrc.gov/docs/ML1206/ML120690009.pdf.
[10] W.R. Stewart and K. Shirvan, "Capital Cost Estimation for Advanced Nuclear Power Plants," https://doi.org/10.1016/j.rser.2021.111880, *Renewable and Sustainable Energy Reviews* 155 (2022) 111880.
[11] Statista, "Base overnight costs of New Electricity Generating Stations in the United States in 2021, by Major Technology," accessed Feb. 23, 2023. https://www.statista.com/statistics/519118/power-plant-base-overnight-costs-in-the-us-by-technology/#statisticContainer

Table 2. United States construction overnight costs of various power plants

Plant type	Overnight costs $/kW
Solar thermal	7,895
Nuclear - SMR	6,861
Nuclear - LWR	6,695
Wind offshore	4,833
Hydropower	3,083
Geothermal	3,076
Wind	1,718
Solar photovoltaic	1,327

Statistica also provides estimates of fixed and variable costs for operation and maintenance of new US power plants as of 2021:

LWR

- 127.35 $/kW yr fixed,
- 2.48 $/kW yr variable

SMR

- 99.46 $/kW yr fixed,
- 3.14 $/kW yr variable

Abdulla[12] produced ranges for SMRs and LWRs based on expert opinion, as follows:

LWR

- One 1,000 MWe unit = $2,600 – $6,600 / kWe

SMR

- One 45 MWe Unit = $4,000 – $16,300 /kWe
- Five 45 MWe (225 MWe) units = $3,200 – $7,100 /kWe

As a simple study of data from a few industry papers indicates here, the estimated costs can vary widely without proprietary information from the vendor/manufacturer. However, the expert estimates put the $/kWe costs in ranges similar to those of LWRs, indicating that potential cost overruns or security upgrades may be difficult for a smaller plant to recoup over its lifetime. Therefore, SeBD must be implemented at the onset, when the cost of implementing changes can be factored into the plant design. This approach is justifiable to regulators because it will prevent costly upgrades in the future. LWRs have not been built to this concept, resulting in increased costs for security and emergency response over the course of their lifetimes.

[12] A. Abdulla, I. L. Azevedo, and M. G. Morgan, "Expert Assessments of the Cost of Light Water Small Modular Reactors," PNAS, Vol. 110, 24, accessed Feb. 23, 2023. https://doi.org/10.1073/pnas.1300195110

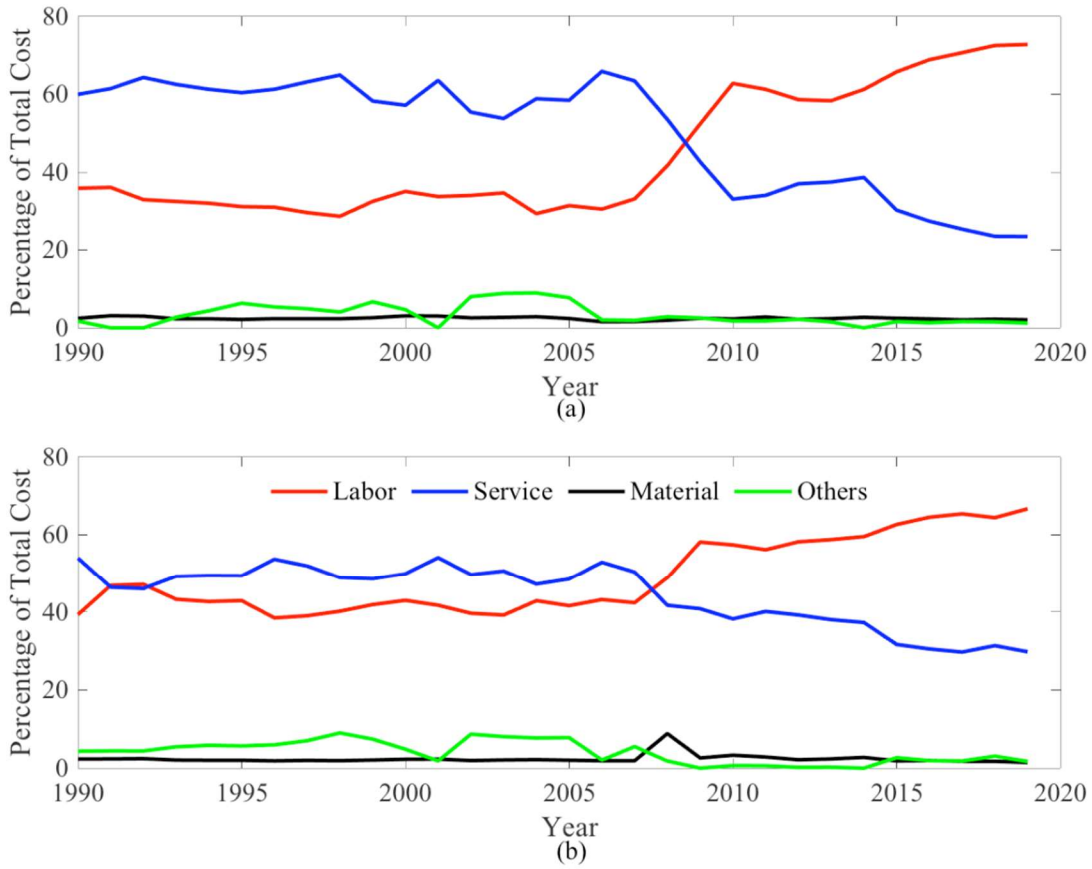


Figure 1. Percentage of total cost for the four types of physical security costs from 1990 to 2019: labor, service, material and others at (a) single-unit NPPs and (b) duel-unit NPPs.[13]

As shown in Figure 1, physical security costs have increased between 2008 and 2019, with an increase in personnel physical security costs, which is a yearly cost as opposed to a capital cost. For SMRs with lower MWe output, recurring personnel costs should be avoided.

Assuming a 924 MWe plant with a cost of 99.46 $/kW yr, the total fixed cost for an SMR would be 91 million $/yr in fixed operations and management (O&M) costs, with an overnight cost of over $6 billion. Estimated typical security costs for large LWRs are 6% of total O&M costs.[13] Based on this assumption, the total security costs for an SMR with a full complement of reactor modules is greater than $5 million. Therefore, adding one or two posts can add up to $1 million (20% increase in security costs and 1% increase in O&M costs). Although it is flawed to use overnight costs for many estimates, and no SMRs to date have been built, these assumptions provide a large margin of error, as demonstrated by the estimates presented above. Finally, assuming a 20-year return on investment without inflation adjustments, capital expenditures, or unknown costs, the total necessary return per year would be $391 million per year. Because the cost for security officers and posts does not decrease for the smaller facility, it is even more important that security be right sized for the reactor during the design phase. SeBD principles should be applied to eliminate as many costs as possible, because implementing changes later can add significantly to a small reactor's bottom-line margins.

[13] B. D. Middleton, G. A. Reyes, T. J. Harrison, P. Burli, A. Foss, A. Huning, V. Yadav, and T. Drennen, *Security by Design Economics Analysis for Advanced Reactors and Small Modular Reactors*, SAND2021-15544, Project Interim Report for FY2021.

The IAEA estimated a significant cost associated with extracting design defects discovered later in the design cycle, as illustrated in Figure 2.

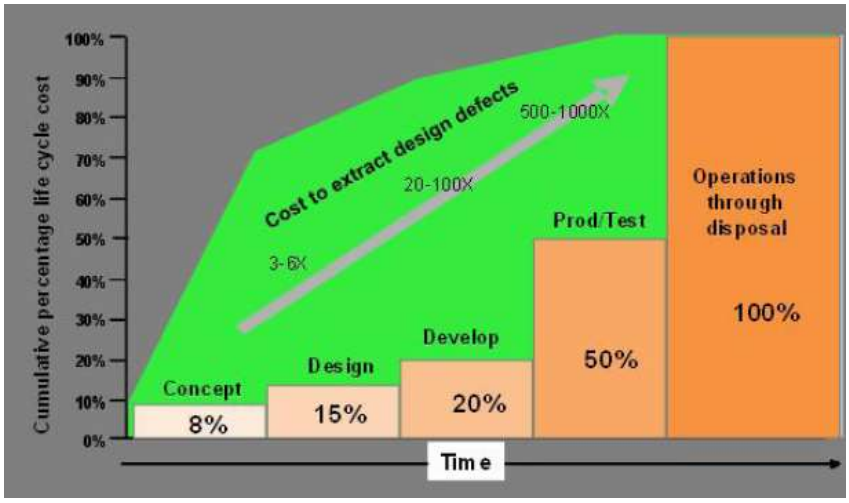


Figure 2. Cumulative life cycle costs as a function of time.[14]

The cost of personnel rises or remains fairly constant, whereas threat profiles change, and reactor designs become smaller and more compact, leading to an increased impact of additional security posts.

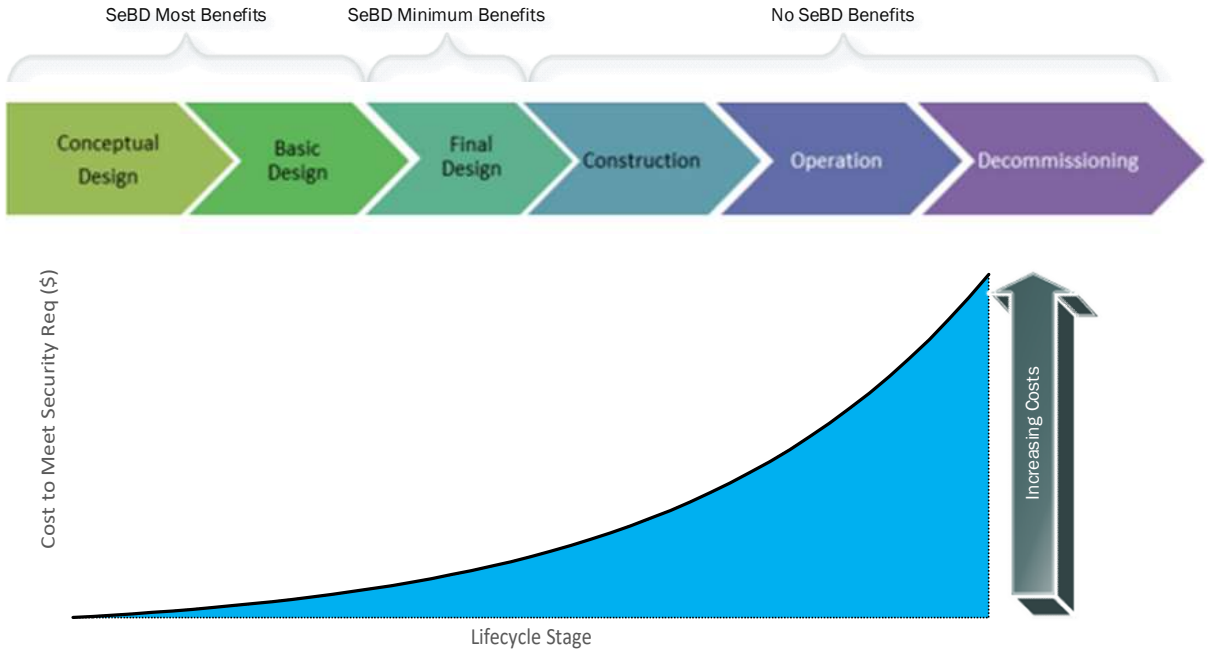


Figure 3. Costs of not implementing SeBD principles early in the design phase.

[14] IAEA, *International Safeguards in the Design of Nuclear Reactors*, IAEA Nuclear Energy Series No. NP-T-2.9, IAEA, Vienna, 2014.

Study results from Middleton et al.[15] illustrate that labor costs account for 60% of the total physical security budget and have continued to rise since 2008. All of this leads to a key conclusion: the technology must be applied early to keep operation and maintenance costs in check during the full life of the plant. SeBD principles must be introduced at the outset and maintained consistently to ensure that security is built in to the reactor as much as possible and maintained throughout the plants lifecycle. These early efforts will prevent future increases in security costs, and they will allow for the ability to evaluate new threat profiles, to demonstrating the plant's continuing security to regulators and the public.

3. SECURITY BY DESIGN

3.1 REVIEW OF SECURITY BY DESIGN

3.1.1 Insider Threat

An *insider threat* is defined as "an individual with authorized access to [nuclear material], associated facilities or associated activities or to sensitive information or sensitive information assets, who could commit, or facilitate the commission of criminal or intentional unauthorized acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities or other acts determined by the State to have an adverse impact on nuclear security."[16] The Nuclear Security Series also specifies that the insider threat has various combinations of the following attributes that must be considered.

Abilities:

- Access
- Authority
- Knowledge

Motivations:

- External motivation
  - Money
  - Revenge
  - Coercion

- Internal motivation
- Mental health issue
- Ideology
  - Self-indoctrination

[15]Bobby D. Middleton, Gustavo A. Reyes, Thomas J. Harrison, Pralhad Burli, Andrew Foss, Alexander Huning, Vaibhav Yadav, Thomas Drennen, *Security by Design Economics Analysis for Advanced Reactors*, 2021.
[16] IAEA, *Objective and Essential Elements of a State's Nuclear Security Regime*, IAEA Nuclear Security Series No. 20, IAEA, Vienna, 2013.

Adversary categories are illustrated in Table 3.

Table 3. Insider threat categories

Adversary	Provides info	Has intent and motivation	Performs active malicious acts	Uses physical force
Unwitting insider adversary	✓			
Aware passive insider adversary	✓	✓		
Aware active insider: nonviolent	✓	✓	✓	
Aware active insider: violent	✓	✓	✓	✓

The NuScale Final Safety Analysis Report (FSAR), Chapter 1, Table 1.9-2, specifically states that insider mitigation programs are not applicable because this program will be based on a combined license (COL) applicant or licensee responsibility. Additionally, Table 1.9-3 of the FSAR states that the design only partially conforms with Standard Review Plan (SRP) 14.3.12 in that the COL applicant will be responsible for addressing all physical security hardware Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) outside the nuclear island and structures.

3.1.2 Definitions of SeBD

The SeBD handbook[17] defines the SeBD concept as follows: "the system-level incorporation of the physical protection system (PPS) into a new nuclear power plant or nuclear facility resulting in a PPS design that minimizes the risk of malicious acts leading to nuclear material theft; nuclear material sabotage; and facility sabotage as much as possible through features inherent in (or intrinsic to) the design of the facility."[17]

The general assumption for SeBD as laid out in the handbook is similar to the approach put forth in the IAEA NSS.[18,19] The state develops the national infrastructure and defines the necessary requirements. As such, "SeBD is best implemented through a structured approach by which a state's nuclear security objectives are fully integrated throughout the life of the project."[17]

This has a fundamental flaw: state review, construction, or inspection of a nuclear facility design is often too late in the process for incorporation of SeBD concepts into fundamental plant systems. Changes implemented at this stage often have dramatic impacts on safety, security, safeguards, and cost that can preclude plant construction. Section 4.1 provides more details about shift from the site-by-site construction of disparate, highly diverse NPPs—such as many of the US-based LWR fleet—to a more standardized approach of modular, certified designs licensed by the NRC or another licensing body and then deployed at multiple sites using the design certification as a reference for construction permits. Therefore, instead of each site undergoing its own review, a standard plant design could be accepted many years prior to the building of the fleet, and once the state or licensing body is involved, the safety and design of the plant would already be approaching completion. A key objective for SMRs is for modules to be built assembly-line style and delivered to countries worldwide with standardized features, thus realizing economy of scale and reducing overall costs. This SMR approach could mean that a state's

[17] M. K. Snell, C. D. Jaeger, and C. Scharmer, *Security by Design Handbook*, SAND2012-0038, 2013.
[18] IAEA, *Milestones in the Development of a National Infrastructure for Nuclear Power*, Nuclear Energy Series No. NG-G-3.1, Vienna, 2007.
[19] IAEA, *Evaluation of the Status of National Nuclear Infrastructure Development*, Nuclear Energy Series No. NG-T-3.2, Vienna, 2008.

involvement to ensure SeBD would result in a *security cost adder* in which additional security features are incorporated late in the process at their highest cost to impact instead of earlier in the process, when the costs of incorporating security are significantly less.

In the new modular reactor design and licensing age, plants would receive a standard design certification. These plants would already be developed, and efforts would be under way to deploy them in other countries, thus invalidating some of the assumptions included in SeBD methods. The SeBD Handbook[17] states, "Note that if the DBT [design basis threat] is only in place when the plant is ready to be commissioned, then the security system design for the plant would have to be postponed past the early phase of the lifecycle where the real value of SeBD can be achieved." The general direction of regulatory authorities within the United States and elsewhere regarding the standard design certification invalidates this base assumption and thus reduces the possibility of SeBD to affect SMR development. Consequently, for modular or generically licensed SMR designs, the proposed SeBD approach must be altered to provide a more generic, and modular design method. This method is presented in Section 4.

3.1.3 Definition Safeguards by Design

NPPs have been implementing safeguards by design for some time through methodologies that differ from the concept of SeBD. IAEA guidance specifies the following state-level safeguards objectives:[20]

- *to detect undeclared nuclear material or activities in the State as a whole,*
- *to detect undeclared production or processing of nuclear material in declared facilities or locations outside facilities,*
- *to detect diversion of declared nuclear material in declared facilities or locations outside facilities*

This definition differs from the concept of security in that it focuses primarily on material theft, diversion, and nondeclaration of nuclear material. The focus here is on the nuclear material itself. However, threats to nuclear infrastructure do not have to be wholly intended for theft and removal of nuclear material. A threat can focus instead on destruction of the facility for other purposes. This threat and its solutions are therefore very different than those targeted to prevent theft or removal of nuclear material. For example, an insider threat could be carried out as manipulation of data or instruments, or it could involve circumvention of detection systems to facilitate stealing material from a facility and dispersion on or off site. Furthermore, the threat may include potential damage to the facility's infrastructure, ultimately leading to core damage. Safeguards typically focus on designing a plant so that the material on site is less attractive to an insider or outsider threat, but this method does not deter an insider/outsider threat with the intent to damage the facility or disperse material from the facility. Therefore, different methods are employed in SeBD: the objective must focus on deterrence from damaging components that could lead to core damage.

3.2 INHERENT SAFETY BY DESIGN

3.2.1 Passive Safety

Over the past several decades, the concept of passive safety, in which the natural laws of nature are used to prevent core failure, has been incorporated into an ever-increasing number of designs. SMRs are well suited to this concept because of their small footprint, small thermal output, and modular designs. The

[20] IAEA, *International Safeguards in the Design of Nuclear Reactors*, IAEA Nuclear Energy Series No. NP-T-2.9, IAEA, Vienna (2014).

general idea is that the reactors remain safe because of these factors, and their designers have painstakingly analyzed the reactor's natural conditions to credit passivity in the safety case. The general consensus is to "fail to safe" conditions or to focus the reactor's failure modes to a condition in which the plant is most likely to survive the event. For instance, loss-of-coolant accidents coincident with loss of offsite power, as well as sudden reactivity insertion events, are of prime concern in the aging LWR fleet. New designs have not only focused on eliminating these primary accidents as a potential failure mode; they have also allowed for these failures in the current designs so that the plants can easily survive these events through passive safety features that function automatically when such failures occur.

3.2.1.1 Passive Safety and Inherent, Self-Protecting Security

In this section, the key fundamentals of *passive safety* are established and applied to security to examine the correlations. Passive safety for reactors typically states no action is required of the operators during an event for up to three or more days.[21,22,23] Passive safety relies on physics and its well-known natural laws (such as natural convection, radiative heat, conduction, and gravity) to explain how fission product barriers prevent release of radiation to the public. Thus, the refined definition of passive safety is to cool reactors by applying the natural laws of physics without requiring any action to initiate.

Creating a series of items in the security space that are analogous to a passive safety system seems difficult at the outset because there are no clear natural laws that would prevent sabotage. However, at a minimum, the physical protection system and security elements are established to detect, delay, respond, and recover. These four active initiators are inherent in the definition of *security*. *Detection* requires active systems and personnel who are constantly monitoring these systems. *Delay* requires that staff members or components take active measures to prevent a sabotage threat from progressing. *Response* requires offsite or onsite personnel or equipment to actively engage with a sabotage threat. *Recovery* requires personnel and equipment to recover lost, stolen, or damaged equipment or material. Thus, this definition by its very nature is all active. So how does one create a passive method of security when all measures that are considered taken to achieve security are active? One approach is to define *passive security* as *inherent security* as a self-protecting strategy. The objective is to force the insider or outsider threat into the most detectable category of violent active insider or outsider, with mitigation designs requiring a person to be a violent, active insider or outsider willing to sacrifice their health and wellbeing for an obtainable goal. Plant design would include two or more redundant, harmful systems (example would be highly radioactive) that must be enacted in separate areas so that one person would not be able to harm both locations at once. This approach would drastically reduce threat risk and would be an inherently secure design.

Design nuclear systems that are inherently secure could cause safety problems. For example, a valve that would prevent an insider from turning it and damaging the plant would be a safety hazard for normal plant operation and maintenance, and it would also present a response hazard and a recovery hazard for security issues. The probability of someone operating this hypothetical valve incorrectly in normal conditions and causing harm would be much higher than if they were operating a normal valve. Requiring two personnel to operate a component is useful, but it could interfere with maintenance operations and would require more personnel than typically estimated for SMRs.

---

[21] GE Hitachi Nuclear Energy, "ESBWR Passive Safety," accessed Feb. 24, 2023. https://nuclear.gepower.com/content/dam/gepower-nuclear/global/en_US/documents/product-fact-sheets/ESBWR%20Passive%20Safety%20Fact%20Sheet.pdf

[22] Westinghouse, "Westinghouse AP1000® Nuclear Power Plant: Coping with Station Blackout," accessed Feb. 24, 2023. https://www.westinghousenuclear.com/Portals/5/Other%20PDFs/Coping%20with%20Station%20Blackout.pdf

[23] https://www.nuscalepower.com/-/media/nuscale/pdf/fact-sheets/smr-fact-sheet.pdf

Self-protection has been defined as *"*the incapacitation inflicted upon a recipient from inherent radiation emissions in a time frame that prevents the recipient from completing an intended task."[24] This approach requires that a radiological dose limit be ensured, and it only applies to theft or dispersion of nuclear material. If sabotage from an outsider or insider threat is the ultimate goal with no concern for self-protection, then the person imposing the threat may not need to exit with the material, so there would be ample time to damage the plant before becoming incapacitated. However, in order to sabotage the facility, an insider or outsider must be within the category of *insider threat* that is least likely to occur. The person imposing a violent action threat is willing to sacrifice their life in order to inflict the damage. Therefore, the definition of a safeguards system for self protection would be the following: "The design of a system, component, or object that upon the attempt to sabotage one part of a redundant system would cause grave bodily harm or incapacitate the target and thus force the necessity to be an aware, active, insider/outsider, with a willingness to incur grave or deadly injury to sabotage a particular asset." In this example a vital location that is so highly radioactive that it would prevent anyone entering would provide challenges to repair and maintenance and thus requiring remote systems which opens up additional vectors of attack and potentially eliminates the harm deterrent completely.

Plant design must consider the active violent insider and thus have an established PPS to address this scenario. The proposed definition includes independent redundant systems, each of which must be taken offline, and both of which would incapacitate or otherwise harm and delay an adversary. Although this concept may be useful, it could present issues by making the design difficult to execute and adding expense, which advanced reactor and SMR designs must avoid. Because it may be impossible to include these features after the design is complete, these types of designs must be incorporated during the design phase. The ultimate goal of this type of system is to credit the theory associated with restricting access to suicide hotspots that will not cause a shift at other locations,[25,26] meaning that the combination of self harm and restricted access could significantly reduce certain mental states conducive to harm. If the plant design must be changed, then the true goal should be shifted to eliminating the particular vulnerability using SeBD principles and methods like those set forward in Section 4.

4. METHODOLOGY FOR SECURITY BY DESIGN INSIDER AND OUTSIDER THREAT MITIGATION

4.1 INTRODUCTION TO LICENSING: A MODULAR APPROACH AND THE IMPACTS TO SEBD METHODOLOGY

Today, nuclear reactors can be developed in many ways. In the United States, reactors can be built through various pathways to licensing and construction as set forth in 10 US Code of Federal Regulation (CFR) Part 50, 52, and Part 53. These methods are either site-based or standard design–based. The site-based method follows 10 CFR Part 50 and the early site permit whereas 10 CFR Part 52 follows a standard design process in which a standard design certification is referenced in the NRC's combined licensing review. The standard design method licenses a generic design, whereas the combined license review process references the generic design and ensures that there are no unjustified and/or unacceptable deviations from that design for a specific deployment. The process is illustrated in Figure 4.

[24] A. Glaser & F. von Hippel, "Thwarting Nuclear Terrorism," Scientific American, Feb. 2006

[25] C. Law, , J. Sveticic, and D. De Leo. "Restricting Access to a Suicide Hotspot Does Not Shift the Problem to Another Location: An Experiment of Two River Bridges in Brisbane, Australia." *Australian and New Zealand Journal of Public Health* 38.2 (2014): 134–38.

[26] A. Leenaars et al. "Controlling the Environment to Prevent Suicide: International Perspectives." *The Canadian Journal of Psychiatry* 45.7 (2000): 639–644.

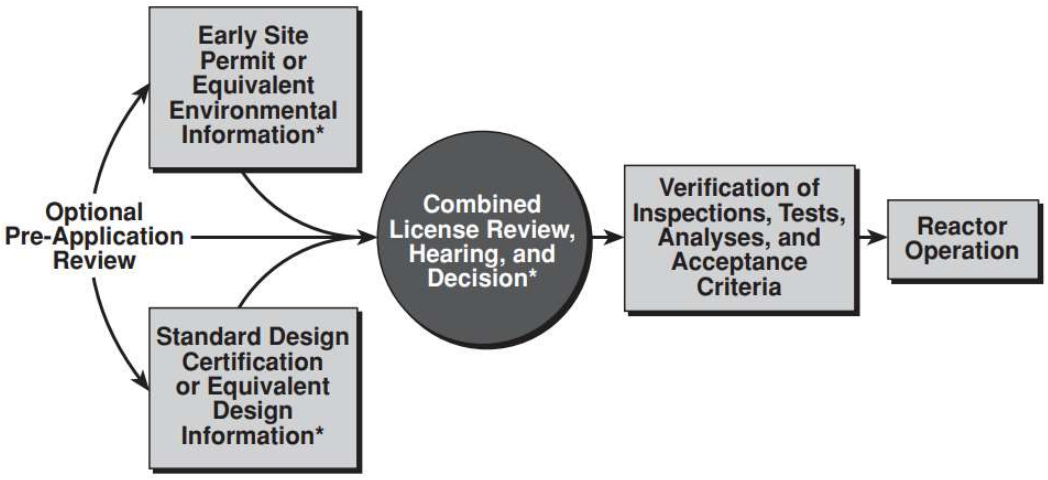


Figure 4. NRC licensing process under 10 CFR Part 52 for new reactor deployment.[27]

Based on SMR deign principles—particularly the modularity of design and the economies of scale required to mass produce modules—the obvious preferred method for these plants in the United States and worldwide is to license a single or series of generic designs and then deploy those modules worldwide without change or customization. It should also be noted that larger LWR designs like the AP1000 reactor have advertised modular construction. Furthermore, deployment of 4-, 6- or 8-unit SMRs and the ability to scale to a 6-, 8- or 12-unit SMR is a potential advertised design features. Adding another module would present licensing difficulties. Following a standard design licensing methodology would benefit the economic business case for the SMR design, but from a security standpoint, DBTs and insider threat profiles, as well as facility locations, can change dramatically between the various states where the modular reactor is deployed. Therefore, it becomes increasingly important to tie the design to data associated with SMR safety and to design security into those features compared to other plants and other licensing methods.

Based on these factors, a true SeBD method must ensure that component safety and security are developed using a bottom-up approach, and a singular identifiable repository must be used for cross checking and maintaining the security posture as the facility's detailed design evolves. Publications addressing SeBD take the approach that security experts must be "in the room" at the beginning of a plant's design phase. However, experience has shown that during the development and building of all current reactors worldwide, design changes occur during all stages of reactor deployment, including during the construction and operation phases. Having security evaluations at the beginning, middle, and end of development is not equivalent to a true SeBD approach. Rather, a predetermined level of security effectiveness must be maintained from the conceptual design through construction, for the designer and operation to decommission, for the owner operator, to qualify as SeBD. This requires a handoff and maintenance of SeBD design to the owner/operator until the plant is decommissioned. The following sections lay out the design approach, identify the tools to be developed and utilized for plant security

[27] NUREG/BR-0298, Revision 2, "Nuclear Power Plant Licensing Process," ML042120007.

design, and specify the items that must be deployed specifically to prevent insider threats commensurate with generic DBTs and insider threats.

4.2 SYSTEM INTEGRATION FOR COMPONENT BASED SEBD APPROACH

When a new plant design is in the conceptual phase, the temptation is to include a security expert with the safety experts to discuss the various systems and what could lead to core damage. Although inclusion of security experts at the beginning of the design process is key to creating an SeBD concept plant, this alone does not ensure that the plant meets SeBD requirements. The general principle of integrated project teams has been implemented in safety requirements for many years.[28] Security strategy concepts should be put into place in the early design stages as safety aspects are being considered, but ideally, design documentation and data must be established to construct a plant. Various items must be established or have a high probability of being in place to construct an NPP. Metrics against which items can be continuously monitored and analyzed to ensure that security criteria are met should be the overriding goal during the initial design phases. The following items must be established in some form to construct a physical plant.

- Safety case
- Inspection criteria
- Testing criteria
- Analysis and documentation
- Final acceptance criteria.
- Construction drawings
- System diagrams
- Piping and instrumentation diagrams
- Probabilistic risk assessment
- Floorplan and blueprints
- Physical protection system diagrams

Several of these items are specified in the IAEA Nuclear Security Series, which discusses identification of vital areas from safeguards and sabotage from the operator's perspective. However, in the modular approach for SMRs, this is too late in the process for SeBD to be applied:

"Typically, an operator is responsible for identifying the vital areas, and the State's regulatory body is responsible for validating the [vital area identification] (VAI) process."[29]

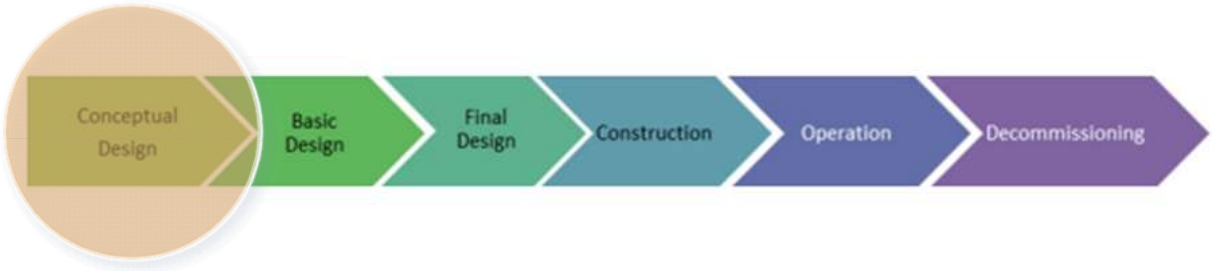
The first stage of the SeBD process is to identify a single location or a small set of locations for maintaining the necessary data to be used to design a protection system against insider and outsider threats. During this first stage, a general assumption must be made on what the acceptance criterion will be for a PPS and insider threat mitigation system. Within this acceptance criterion must be an evolving prescriptive assumption on what the DBT is that must be mitigated and what the corresponding insider threat will be that must be mitigated. Note that at this point it is important to not have the PPS or insider threat defense principles defined. The reason for this is so that the plant design can dictate the PPS and insider threat defense principles, and then those can feed back into the design to reinforce a plant with security built into the fundamental safety systems. This establishes a self-reinforcing cycle of safety and security feedback to assist in communication. This process should be implemented as part of the conceptual design phase. The cost for adding security measures at later stages of plant design could

[28]DOE, *Integration of Safety into the Design Process*, DOE-STD-1189-2008, March 2008.
[29] IAEA, *Identification of Vital Areas at Nuclear Facilities*, IAEA Nuclear Security Series No. 16, 2012.

increase exponentially, depending on the stage at which the SeBD is implemented, especially given that adding security personnel is a yearly expense that must be absorbed each year by an operating reactor.

Insider and outsider threat mitigation strategies will follow the same basic process; however, designs of the physical protection system and the insider threat mitigation system may use very different strategies to mitigate threats.

4.3 CONCEPTUAL DESIGN SEBD PROCESS.



When a plant design is at the conceptual or basic design phase the process unfolds into three basic stages.

Stage 1 involves the development and documentation of high-level safety concepts (passive safety features, integral modules, natural convection driven, innovative removal of specific failure modes), plant systems at the highest level (reactor vessel, heat exchangers, ultimate heat sink, turbine, decay heat removal systems), security concept (PPS requirements, response assumptions, equipment considerations, technically available solutions, innovative security solutions for the specific plant concept), and the safety and security interface database (SaSID): the touch point between safety and security. This method description is based specifically on identifying and establishing this item. In the NSS series on VAI,[29] IAEA accomplishes this task, but it is not directly related to SeBD; nor is it identified as a key interface and aspect of the SeBD method. Instead, the VAI documentation is the primary objective:

"The vital area concept is used to define a boundary around the vital equipment, systems, or devices, or nuclear material to which physical protection can be applied. The objective of the VAI process is to identify a set of areas of a facility containing the equipment, systems, structures, components, devices, or of operator actions that, if adequately protected, will prevent HRCs [high radiological consequences]."

IAEA categorizes initiating events of malicious origin IEMOs as related to high radiological consequences (HRCs) and frames this in a state-driven framework, not a standard design framework centered around data, assumptions, threat profile, and adaptive design change. Therefore, the process is inflexible, and it occurs too late during the design finalization stage (licensing) and can even be delayed until the construction phase in certain licensing paradigms. Although other SeBD concepts focus on overall procedures from a state, regulatory, site, or guidance perspective, the method presented here focuses on (1) establishing the interface and automatic checks of safety design as related to security design that can be maintained throughout the lifecycle of the plant, and (2) tracking of the assumptions that went into the database. In essence, this is a data-driven approach to security based on safety designs and security input that is applied to mitigate issues with appropriate protection strategies. This approach no longer relies on expert opinions and traditional security approaches. In the present approach, the safety design changes can be made to address security during development, preferably very early development.

IAEA guidance uses the probabilistic risk assessment (PRA) approach to determine target sets. This approach provides a wealth of data and information to inform not only the safety case of a plant, but also

all the target sets and vulnerabilities of the plant. At the beginning of the conceptual design phase, the system design will be very high level, so the PRA model will be simplified. However, as the design becomes more complex, the systems and analysis for safety will also become more detailed and complex. PRA provides a resource to document changes to plant design. Other potential areas of communication between security and safety are identified in Section 4.2 as key items that must exist in some form to build a nuclear plant. If a PRA is not used when designing a nuclear plant, other items may be used, such as piping and instrumentation diagrams or software and database solutions to document change notifications.

Stage 2 is based on engagements with states or regulators and involves defining assumptions to be included in the safety and security interface database (SaSID). Within Stage 2, security takes the lead and incorporates assumptions for a DBT and insider threat profile for the facility based on expert knowledge and engagement with the deployment country if possible. This further augments the security concepts and links to the SaSID. Security defines mitigating effects on systems, rooms, and components in abstract of those individual systems and identifies mitigation techniques that can be linked to a physical protection system (PPS). At this point, the PPS is not being designed in full, but the strategies and tools that will be used for particular aspects and vulnerabilities of a plant will be thought out, defined, and potentially tested to verify key safety components.

Once Stage 2 is complete, the initial setup for the basis will be in place for a component-based strategy to build a PPS to mitigate insider and outsider threats. The goal is to create a component from the ground up using a component-first mitigation strategy linked relationally via a system or database to the PRA or other key document model. This approach allows the data to be used to determine the best mitigations and to identify when design changes may lead to additional vulnerabilities, and it also allows for removal of vulnerabilities during the design process in near live updates. The ground-up component-based process is illustrated in Figure 5.

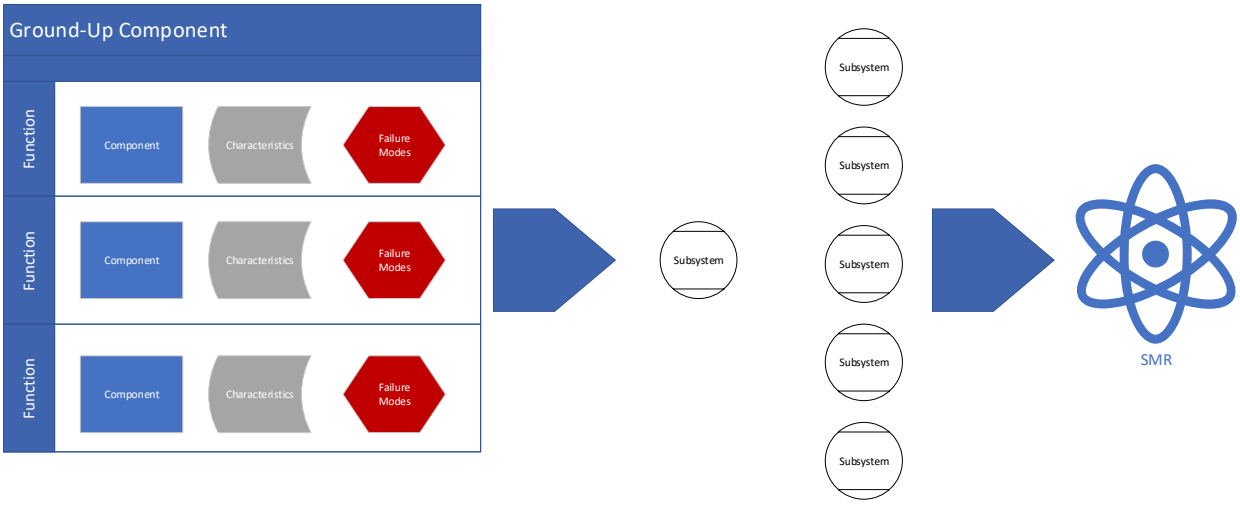


Figure 5. Component to System buildup of SMR Facility.

During the conceptual design phase or the basic design phase, a high assurance evaluation process should be initiated.[30] The process is illustrated below, augmented to include the feedback between safety and security, as well as the Sigma One process.

[30]James E. Vaughn, Nuclear Power Plant Security Assessment Guide, United States Nuclear Regulatory Commission, ML13122A181, April 2013.

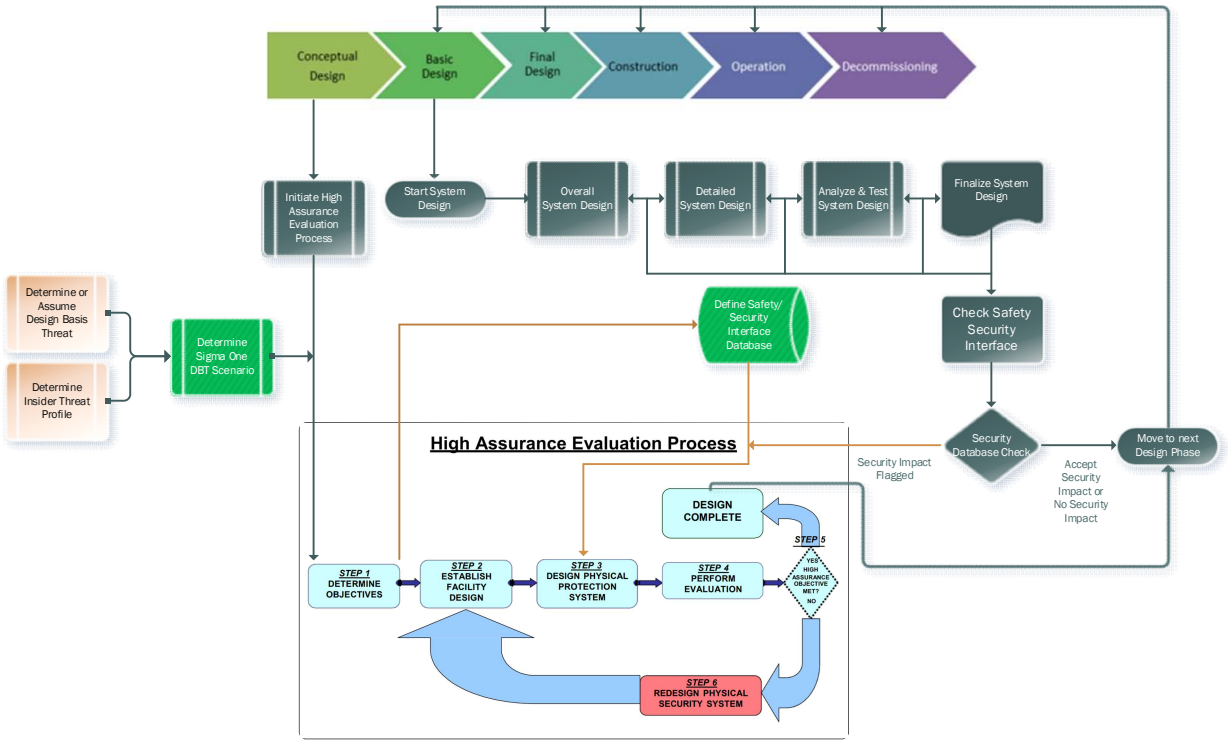


Figure 6. Process for implementing SeBD and SaSID database concept.

The conceptual design phase will include items such as the reactor fuel, power production concept, target electrical output, control schema, any novel reactor concepts and finally the business case for such a reactor design. It is at this phase that a security consultant should be engaged with the reasoning and understanding that an assumed DBT will be made with large uncertainty bands around the various predictions and determine the overall security objectives. In the conceptual design phase only a building conceptual design should be imagined as the facility with the full expectations of dramatic design changes in the future. Each of the outcomes of the safety and security concepts should be documented as design assumptions at the highest level that will have more detail defined as the nuclear facility design process goes to basic design and final design. Documenting and relating these safety and security assumptions together in a integrated fashion makes it easier in future refinements to check the validity of the safety and security assumptions initially established and test those assumptions against the changes being made in the plant. This basic method is what is shown in Figure 6. The conceptual design phase of a new nuclear plant focus primarily on an economic evaluation of profitability and return on investment and more detail will be added at later stages in an iterative fashion. The interface is now established and assumptions laid out in a way such that they can be tested against as the safety design progresses. Now the designers can move to the next stage.

At Stage 3, the conceptual safety case and generic security case have been developed, and the conceptual design is complete. At this point, the DBT and the insider threat profile are established, and then the high assurance evaluation process is initiated. Information to inform the DBT and the insider threat profile is typically provided by the state where the facility is being licensed for future construction. DBTs may not be well defined at this time, depending on the level of established nuclear infrastructure. Therefore, the vendor should engage and determine the DBT in several states and determine what is being proposed as the Sigma One DBT scenario. The purpose of this determination supports the design of the PPS and the insider threat mitigation based on two factors: (1) the DBT within the country where the plant is being developed, and (2) DBT discussions with nations in which a facility may wish to deploy the reactor. In

this scenario, the Sigma One DBT case will be determined by taking the known DBTs and designing a stepped physical protection system based on assumptions for future deployments until the maximum Sigma One DBT assumption is reached. The stepped process is then inserted into the SaSID and checked against designs as they are updated for the plant. With the generic layout and design in hand, the PPS and insider threat security basis can be made.

The advantage of taking this type of approach is fourfold:

First, security is incorporated at the early phase of the reactor design, when the most security cost reduction can be realized for the life of the plant. Second, the SaSID serves as a central repository as designs for individual systems are developed; they can be checked and enhanced, and requirements and assumptions between safety and security are documented. Third, the key aspects of the plant's safety case can be generically analyzed and protected to maintain the safety case during an insider or outsider attack. Fourth, security can be constantly checked and increased or decreased as designs evolve.

Once detailed subsystems and components are added to the design and are assigned locations within the plant structure layout, the base security design and Sigma One security design can be analyzed against these updates and alterations. See Section 5.1 for more details on how data can be organized to allow for data monitoring and analysis to be merged to determine weaknesses, vulnerabilities, and mitigations.

As these components become part of the safety case, they must be connected to security, so the data must be in a consumable form for both safety and security to create the SaSID. To create a truly integrated SeBD process, safety design and security design should both incorporate the items required for a plant to be licensed or constructed. For example, one cannot build a skyscraper without some form of building blueprint and documentation stating how it will meet regulations. As stated above, several items must exist for a plant to be constructed. The SaSID identifies the item early in the conceptual design phase and serves as the interface between safety and security. The item may be the piping and instrumentation diagrams for the plant, various system diagrams or system integration diagrams, or the PRA. Although it can cost millions to properly develop a PRA or a dynamic PRA model, the value to the safety and security of a plant can be vast and can often save millions of dollars in the design. Additionally, because the PRA is extensive and expensive, it typically contains a vast amount of data associated with the safety case that can be used for the security design and justification of the PPS and insider threat mitigation techniques. More details on PRA are discussed below. Multiple sources that can be used for this interface, but the primary components of the interface remain the same.

4.4 DEFINITION OF THE SAFETY AND SECURITY INTERFACE DATABASE

As noted above, the primary source of this information is from plant layouts and PRAs, but certain mitigation effects and component-based buildup of security requirements are involved. As part of the initial security objectives, the key components relied upon for safety as part of the conceptual design safety case should be mitigated through technological, design, layout, personnel, or other security mitigation techniques.

As described in Section 4.3, integration of safety and security is accomplished through the creation of the SaSID database. The method for identifying the necessary design documentation can be implemented to link the security and safety together into a single evolutionary process in a symbiotic manner. The database is used to determine component vital areas, target sets, and time-to-core-damage (TTCD), all of which will evolve throughout the design process. This section discusses design formulation and integration, maintenance of the SaSID, and establishment of the basis to the SaSID.

To address insider and outsider threats, the security, safety, and culture of the facility must be analyzed. The security designs of plants differ depending on their locations, ideally they are compliant with the Sigma One security design basis and the process described above.

The SaSID should fulfill four key roles.

First, it must provide the relational safety information necessary for the design of the PPS and insider threat mitigation, and it must also provide the relational security information necessary for safety analysis and design. The information must be a form that can be consumed and readily interpreted by both groups.

Second, it must organize the data in a standard way so that changes in the PPS and insider threat mitigation techniques will (1) flag the safety designs already in place for potential exposure to risk and (2) notify security experts of updates to plant designs that could lead to exposure to additional vulnerabilities. Further discussion and examples are provided in Section 5.1.

Third, the SaSID must provide the correct amount of information to allow for the appropriate analysis of the PPS and insider threat mitigation techniques using tools necessary to validate the designs, such as exercises, path analysis tools, and others.

Fourth, and finally, the SaSID must maintain the necessary security for the database itself. Establishing the specifications of a security component to be used to mitigate a particular threat should clearly not be broadly distributed to all designers. The specifics of the technologies selected as part of the PPS and how they will mitigate various vulnerabilities must be held secure. Therefore, safety personnel do not need to know the particular technologies or items incorporated into the PPS to mitigate a particular threat. They only need to know that a vulnerability is potentially mitigated though system design or particular security measures.

4.5 USE OF THE SaSID WITHIN A DESIGN FRAMEWORK

Figure 6 shows a process focused on design of a nuclear reactor's safety concept as linked to security designs. The process depicted does not define how the SaSID should be formatted, the form it should take, or how it would be integrated into the system. Unfortunately, there cannot be a one-size-fits-all SeBD program. The highly diverse designs of nuclear reactors, the different regulatory regimes, the different threat profiles in deployment countries, and the different vendor processes would make such a system impossible to develop. However, the process used to develop the database can be generalized based on typical design and security data sets, analyses, and choices that must be made during a typical design process.

This process will be structured around three areas of nuclear reactor design:

- Safety – design, analysis, testing, and approval of safety systems, structures, and components.
- Security – design, analysis, response, mitigation, testing, and approval of security systems, structures, and components
- Culture – establishment of a nuclear safety and security culture for nuclear designers and security up and down an organization.

Safety and the safety concept are the driving forces for nuclear reactor design to appropriately license and sell a reactor, whereas security is a part of this design concept for licensing. Security is typically separate from safety design changes, so it must be well integrated into the safety data flow.

The overall safety case must be integrated into the design through a series of high-level designs at the beginning of the plant's physical layout. This will take the form of the highest level of a PRA and the generic piping and instrumentation diagrams for the plant. The diagram and PRA would be developed at the system level only. Simple diagrams would be created such as that shown in Figure 7.

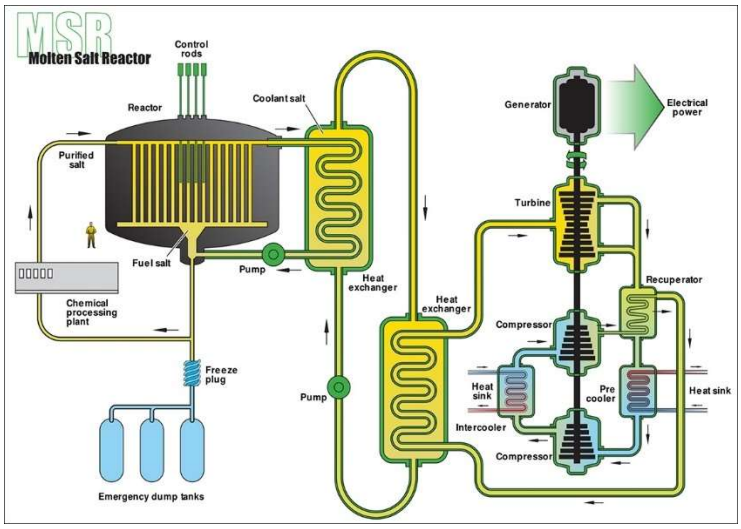


Figure 7. Example of a conceptual level NPP system diagram.[31]

From this stage, schematics for the safety, fire, and flood PRA, piping and instrumentation diagrams, and other schematics can be integrated by translating the common cause failures and time-to-core damage into the security database, where the plant overview will be more fully developed with detailed systems and diagrams. Even if the PRA is deemed unnecessary because of the large capital investment required to properly conduct a PRA for a complex nuclear reactor, the database can still be populated as development continues. A connector must be established to delineate the facility's layout and the location of the system. The database only needs to be a listing of components and generic locations, similar to a bill of materials. More fidelity would be needed when security measures are applied; this would be handled primarily through metadata of components as each system is designed in more detail. Appendix A contains a list of certain component types and locations for a licensed SMR that would represent the first and highest level of design that would be expected during the conceptual stage. This data is useful for safety, but they must undergo data translation, which often includes removing probabilities of failure, scaling, and adding desirability, as discussed further below. The data must be incorporated into the design of the PPS, which will establish the security items applied to the buildings within the design space. Safety component location must be mapped to the PPSs and their mitigation systems. If certain areas include more security doors, monitoring, or security features than others, then the fidelity of the model to the room must be ensured. In this data translation and linking, the safety requirements define the target sets and vital areas, whereas the security requirements highlight the weaknesses, assumptions, and key mitigations needed for certain areas. The security and safety sections of this database can be encrypted separately so that data are only exchanged with those with the correct clearances; The database can also only note that a change to the safety system may have invalidated one of the security items held within that section. This would apply in cases such as when running a pipe that was once contained within one building into another building. Once this change is entered into the SaSID, the database would show that security evaluations have changed because of the change in location of a potential target set, or it would flag a new weakness through a common cause failure mode (e.g., the pipe failing now will cause a

[31] IAEA, "Molten Salt Reactors: IAEA to Establish New Platform for Collaboration, accessed March 1, 2023. https://www.iaea.org/newscenter/news/molten-salt-reactors-iaea-to-establish-new-platform-for-collaboration

secondary failure in a safety system that was previously isolated). Maintaining this interface and emphasizing the need of such an interface does relies on a strong security culture that is accepted within the safety culture of the design team. Such a shift within a workforce is not trivial but should be given attention by a design organization. Such examples would be parallel and similar to safety advocates that often are incorporated in design meetings for safety and having regular security briefings related to safety work as part of a normal training paradigm.

The culture present within a nuclear organization is heavily emphasized as a safety culture but is not typically communicated in terms of security or the establishment of a security culture. Constant discussion at US and international nuclear facilities focuses on nuclear safety culture; however, very little effort is made to incorporate a security culture. Because the psychology of an active insider factors into many detection and mitigation methods, security culture must be considered. Vendors and regulators both hold key roles in security culture, but a vendor's influence typically ends when startup testing is complete or sooner, when the plant is fully passed to the facility owner. The vendor's role is summarized in procedures and training for operations and maintenance personnel. The guidance given to the operator must include a strong safety and security culture, but at this point in reactor design, the focus is on the final as-built diagrams, software, reports, testing, and licensing documentation, as well as with the physical facility. The state can maintain vigilance and impact the safety and security culture later in the SeBD process, because the culture must be established through training, but it must be maintained and fostered throughout the life of the plant though various means. Security culture should be an integral part of the training included in the sale of the nuclear facility.

The diagram below presents several categories and related analyses and construction items necessary to complete the safety basis and build a nuclear plant, to be included in the database in the three areas of interest.

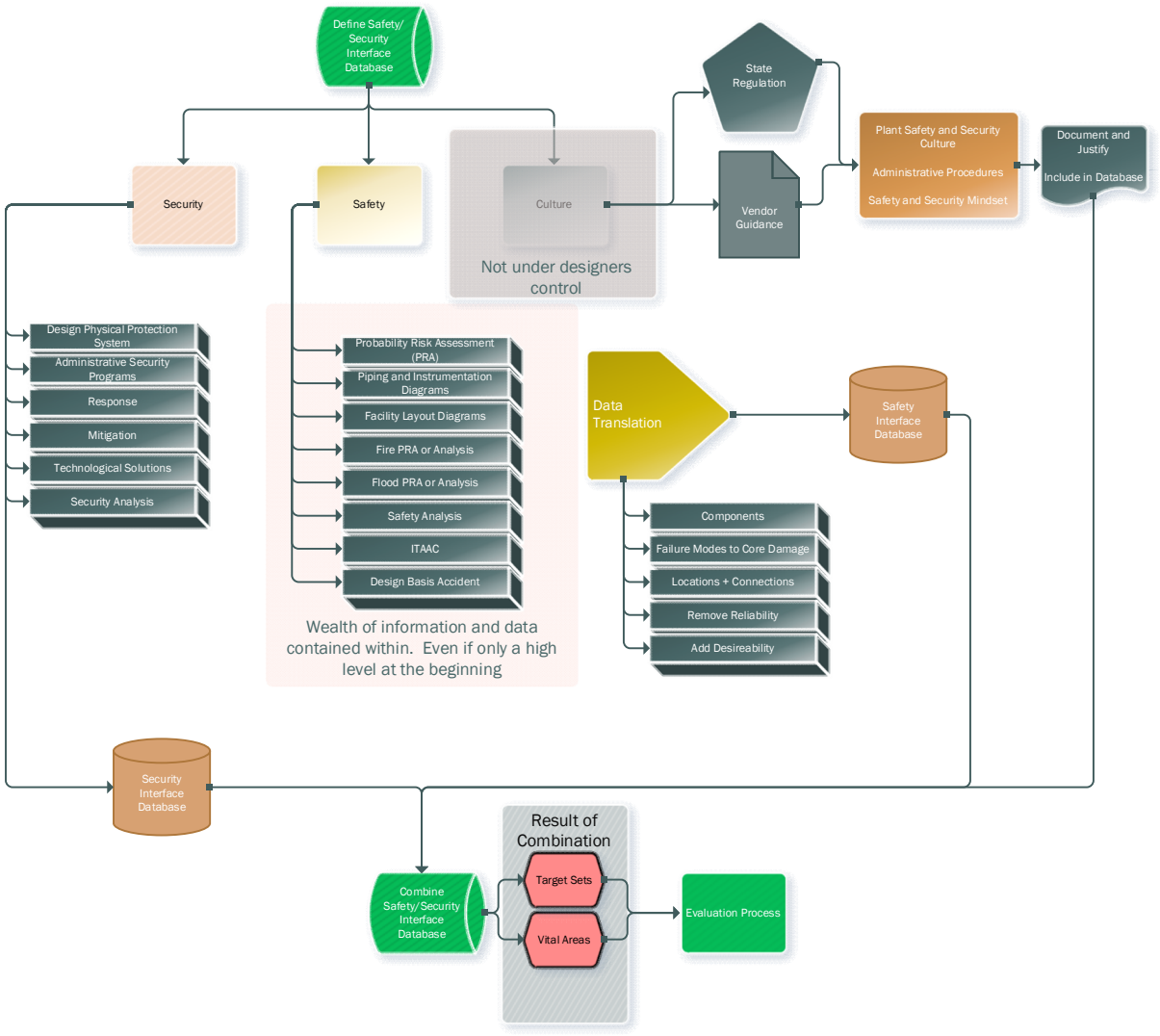


Figure 8. Process for defining the SaSID.

As seen in Figure 8, the safety and security items are held within their respective areas, but then they are merged into the final product, where external data analysis tools can pull the necessary information from the overall database as needed for the particular analysis. This data combination serves as the connection for automation of SeBD between plant safety designs and plant security designs to facilitate constant communication. The two differing fields of expertise can then be overlayed, evaluations can be conducted, and the necessary triggers can be implemented to further evaluate the security systems when design decisions are made or when changes occur. Dividing the database into two separate parts can allow for encryption of results between security and safety, thus meeting security protocols for compartmentalization of security mitigation techniques. In this setup, the tools can flag safety changes that impact the security analysis or assumptions, and the security toolsets contain the decryption algorithms to allow for viewing or utilizing the analysis tools on the database.

These diagrams show the generic process of how an SaSID system could be created and used, but thus far, the form this would take has not been determined. Section 4.1 discusses the licensing environment and how safety is typically incorporated within a design in absence of security tracking, testing, or incorporation. Section 4.2 discusses the security by design system as it currently stands and the

environment of safety design in which this type of methodology must co-exist. Section 4.3 lays out the concept of SeBD and describes the concepts for how to incorporate security into your safety design process, while alluding to an automation scheme to alleviate the extra costs and burden of safety having to take into account security within their design. Section 4.4 details the integration of the SaSID in current processes for security and safety design. Finally, Section 4.5 relates the areas of potential data and interfaces with current processes used for security while setting up the SeBD and SaSID as a salable product that can maintain a high level of certainty that the previous security and safety analysis conclusions are still met after changes are made.

Because the form the database can take could be varied and defined solely based on the type of plant being built or the company structure that is creating the design, the database can be highly variable. The next section lays out a model that can do the automation for such a system to alleviate the additional cost burden that comes from adding security in the early stages of a plant design and reduce the overall cost of designing a security system for the plant.

5. IMPLEMENTATION

5.1 DATA FORMATTING AND INTEGRATION OF SaSID INTO ANALYSIS

To create a buildup from component to system and then from system to plant, it is useful to take a software design perspective of accepted industry standards for storing, presenting, and analyzing data. The diagram below illustrates two key components that should be established to properly create and maintain the SaSID.

First is an inheritance-based approach to organizing the metadata and inheriting the data between systems.

Second is a data management standard similar to that found in other databases used for storing scientific data, such as comma-separated values (CSVs), hierarchical data format (HDF5), visualization toolkit (VTK), structured query language (SQL), or no-SQL database files. A basic illustration of object-oriented programming is shown in Figure 9.

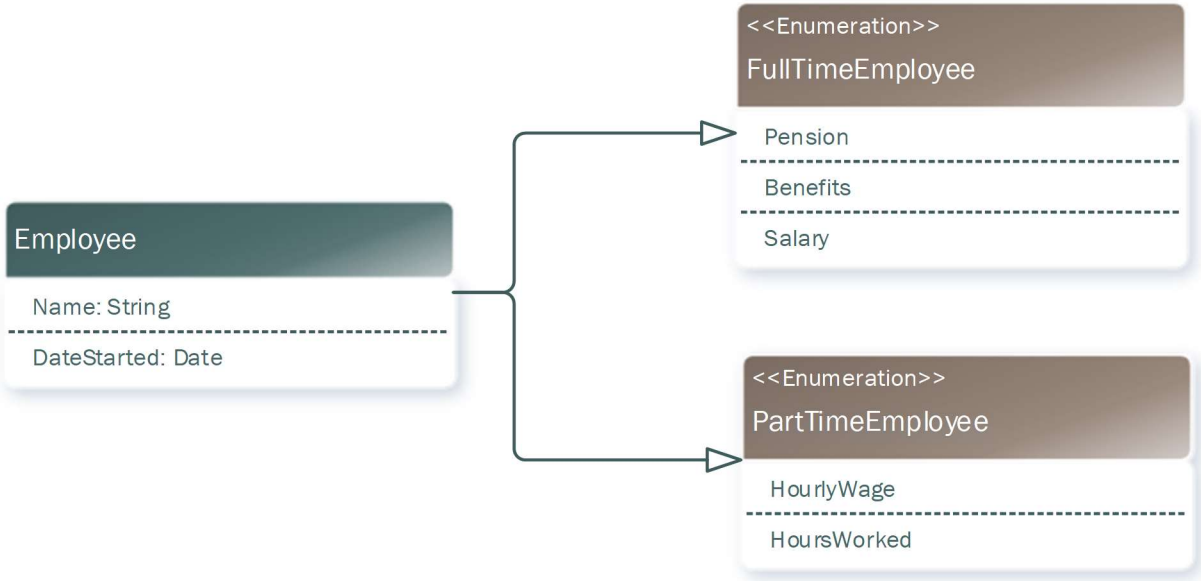


Figure 9. Object-oriented programming illustration.

In this illustration, a virtual class is created for employees. This class is then enumerated into several different objects: one for full-time employees, with a set of data associated with that object, and part-time employees, with a separate set of data. For a more practical application, see the example illustrated in Figure 10.

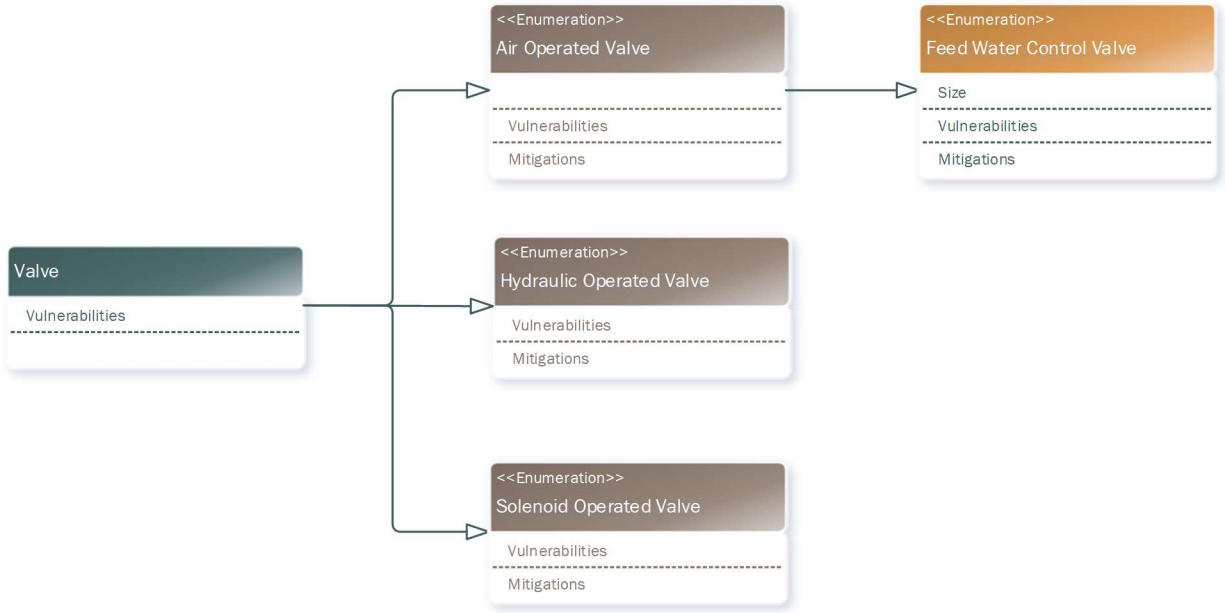


Figure 10. Valve object-oriented data construct.

This figure presents the class, valves, and a certain type of vulnerability is associated with a valve. A simple construct is a potential threat that damages the valve, incorrect operation of the valve, incorrect operation of the valve with malicious intent, or a faulty valve. Beyond these constructs are the various enumerations of this class into objects that can represent valve types, such as air-operated valves, hydraulic valves, or solenoid valves, which will inherit the basic valve vulnerabilities and include their own more descriptive weaknesses. This provides a component-up build of vulnerabilities to be paired with the PRA, system diagrams, and systems at the component level, and then it is paired with the top-down building, room, hallway, and the door analysis conducted for pathway and security analysis. In this setup, the PRA is brought forth again, because each component will have a failure mode reviewed and a data change linking what occurs when the valve fails to the methods that can cause it to fail. This becomes the security vulnerability analysis.

The following items are necessary for the SaSID from safety.

1. Component listings that can lead to core damage
2. Time to core damage
3. Component locations
4. Component connections
5. Component susceptibility to fire at location
6. Component susceptibility to flood at location (internal flood only)
7. Common cause failure modes

Note that the probability of failure is excluded from this database. This is because the failure rates and probabilities are of no concern to security, as a knowledgeable assailant will know exactly how to defeat a component, so the failure rate is 100% in that case.

The items needed for security are as follows.

1. DBT and insider assumptions
2. Sigma One DBT
3. Component vulnerabilities
4. Security components
5. Security component area of applicability
6. Mitigation components and criteria
7. Response criteria

This database contains the items used to mitigate the various potential threats. These could be physical assets such as doors, locks, security checks, patrols, or procedural items such as dual access criteria and compartmentalization of knowledge. Basic objects are created, and then more detailed instances of those objects are created that include more detailed mitigations and weaknesses. Once the database is complete, the two can be combined with the physical layout of the plant, and expert knowledge can be included to create not only target sets and vital areas, but also the mitigation's present down to the exact room if necessary.

Although the SaSID is referred to as a database here, it could take other forms. The general concept is to translate the knowns from the safety case into target sets and vital areas based on their initiating events and then merge and cross reference them with the mitigations present in the security design. When the safety component data, which often takes the form of the safety PRA, is overlayed with the system locations within the plant, the final result is a set of targets and vital areas that can be screened based on various mitigation and response measures to create an overall picture of the facility's security outlook. Next, two additional measures will be added to the overall system—fire and flood safety information. This is often in the form of a fire and internal flood PRA. These two items add two key aspects to the system, because the failure of a component could be impacted by internal flooding from another failed component, or a fire hazard could impact another component. When the data from these other two sources are overlayed on top of the standard PRA, it is possible to obtain a set of failure modes for key components based on location data rather than a failure tree. These items will then combine these target sets with the desirability rankings established by security during the initial plant layout. Once completed, a set of target sets sorted and listed by the shortest time to core damage will result. The final sets will then be iterated upon to prove that the ranking systems did not overly bias the PRA results and to show the sensitivities of the final results. Figure 11 shows how the evaluation process can utilize the information contained in the SaSID.

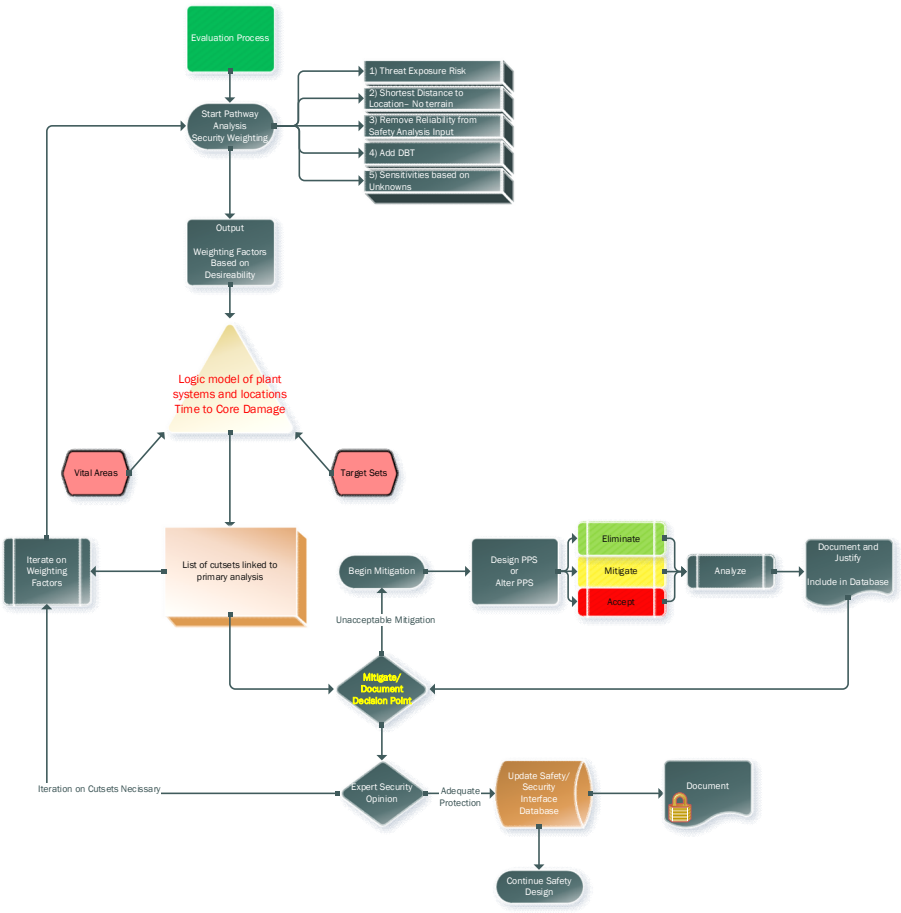


Figure 11. Evaluation stage using the SaSID database.

Appendix A lists he NuScale NPP's design information that is publicly available regarding systems, valves, and buildings. While SMRs and advanced reactor designs include novel approaches to their safety concepts, designs, and build methodologies, dividing these plants into to their basic components, as seen in the survey of components and systems for the NuScale design, it can be seen that the novel approaches still use the same basic component designs as the LWRs and heavy water reactors (HWRs) designed in the 50s and 60s now in operation. This means that, although a component-based approach is still monumental in its potential scale, the designs for reactors will likely still draw from the same list of components seen across the nuclear plant spectrum, with little need for novel component additions based on a single facility. Therefore, once a template of these components is made, it can be used across SMR and advanced reactor concepts in the future. If two or more different designs are to implement such a template it would need to be in a format that can translate easily between potentially highly different systems and thus must be standardized.

To best facilitate the communication of this information, a standard should be established to facilitate efficient communication between security and safety tools. In this case, using the HDF5 standard to illustrate an example shows how the data can be organized to facilitate and object-oriented approach to handling these data sets.

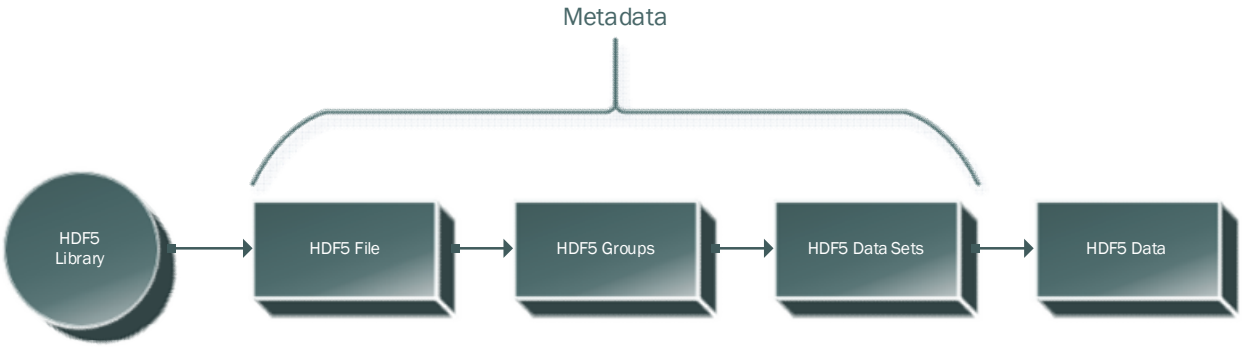


Figure 12. HDF5 data construct example.

As shown in Figure 12, a typical HDF hierarchy can meet the basic design scheme of the component's inheritance model by using metadata to link and allow for basic, widely used public tools to facilitate communication of a standard.

With a formatted structure, a series of matrices can be overlayed and built for each component type into a vulnerability and mitigation matrix, a failure consequence matrix, and a failure cause matrix.

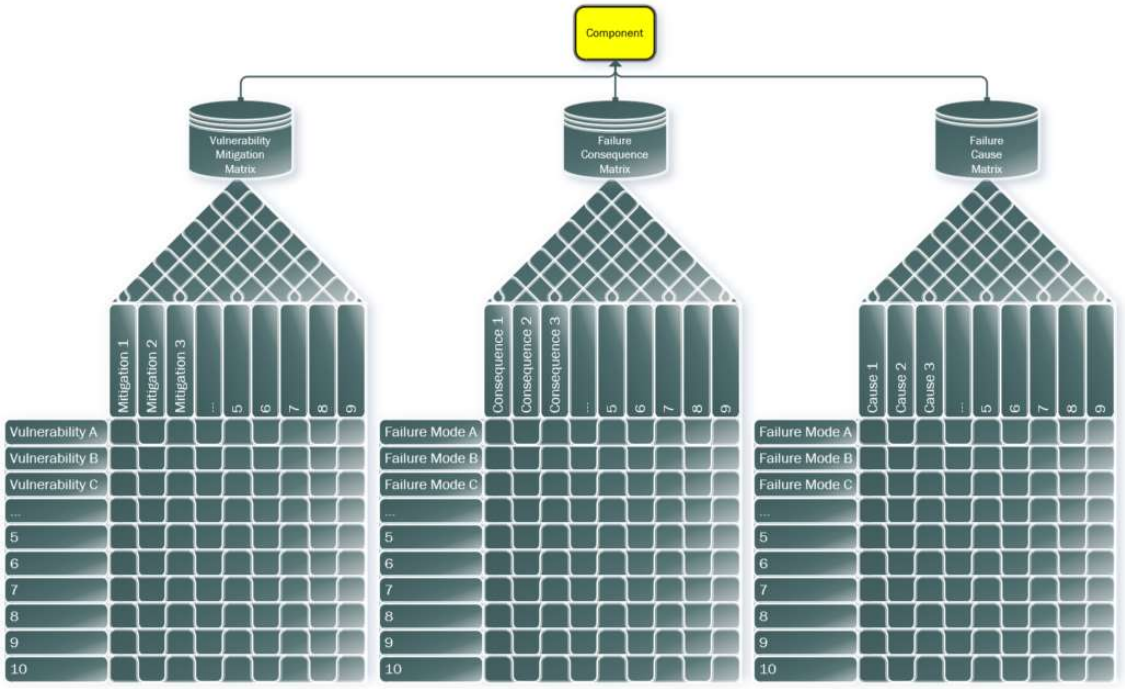


Figure 13. Example component data matrix for inheritance buildup model.

Each matrix stores the various data aspects for a given component. This component is then combined with other components to create the final system.

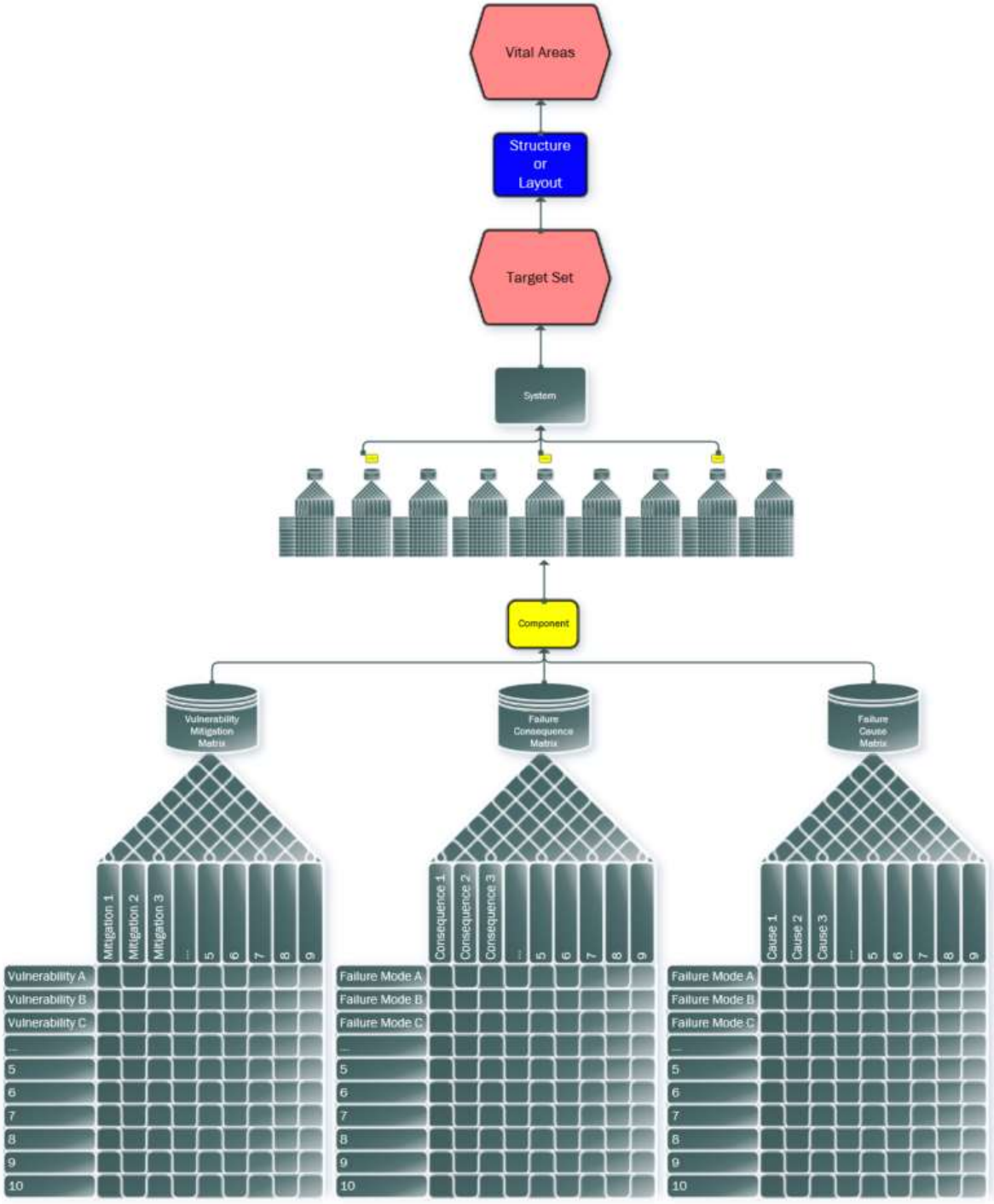


Figure 14. Component data rollup into target sets and vital areas.

With the data from the PRA, piping and instrumentation, and for each component in the system, the data can be rolled up to system and plant levels, as shown in Figure 15, to provide target sets and vital areas and to provide the necessary data for security tools to analyze the database. With the data stored and key items defined, the results can be simplified into cutsets that are categorized by the fastest time to core damage and iterated upon by security experts. A mitigation technique can be added to the structure,

system, or component within that area to change the output to the desired output, where hopefully the time-to-core-damage is greater than that of a cutoff threshold, and the damage incurred is now recoverable for the facility.

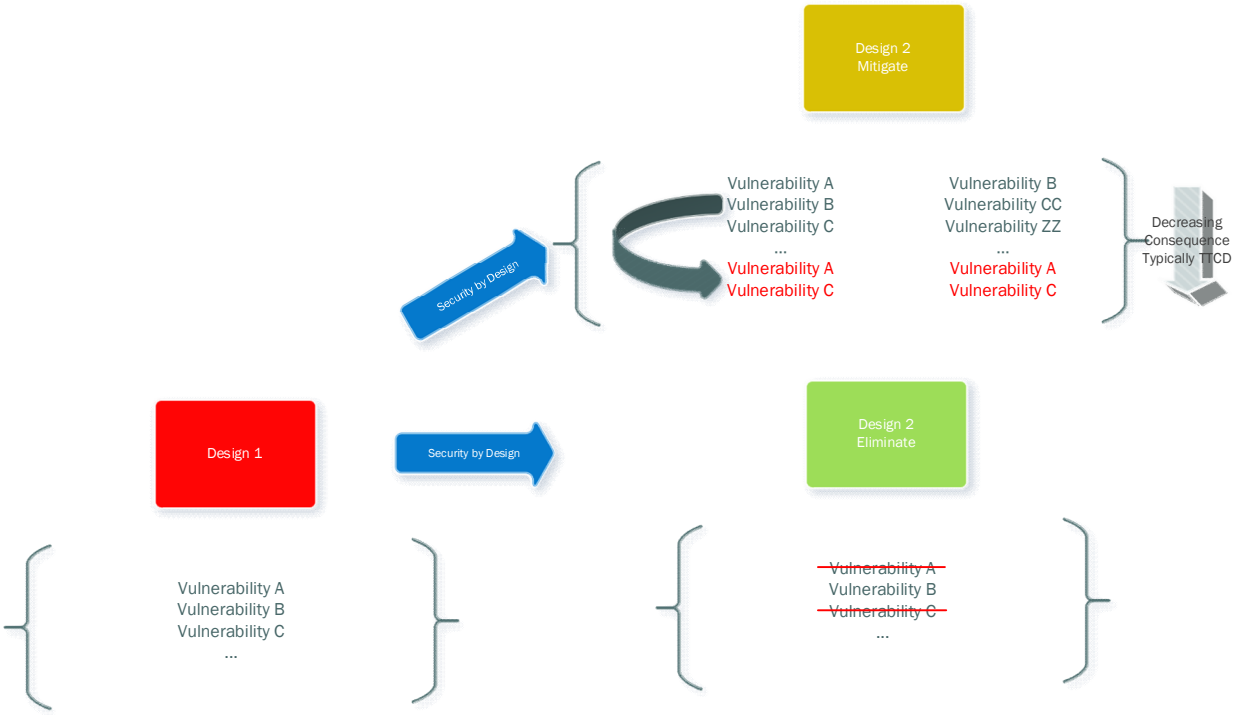


Figure 15. Example iteration on the design to eliminate or mitigate a discovered vulnerability.

PRAs are expensive, and they take the perspective that failure modes are probabilistic, but they are very useful from the security perspective.

5.2 PRA METHODS FOR SECURITY BY DESIGN

The PRA is being explored as a potential tool for security risk assessment and SeBD applications. *PRA* is a broad term that encompasses a variety of technical elements for both nuclear and non-nuclear applications. Fundamentally, PRA asks and attempts to find answers to engineering systems about (1) what can go wrong? (2) what is the likelihood? and (3) what are the consequences? These three questions were explored in the context of how a PRA can support security assessments and documented in an Oak Ridge National Laboratory (ORNL) report,[32] which includes the following observations:

- Both NRC and IAEA guidance on security assessments identify security design as a process step occurring after facility design and before any security evaluations.

- Process hazard assessment methodologies, like master logic diagram approaches and/or events tree methods, could be beneficial in establishing a more systematic and technical basis for the selection of DBT scenarios.

[32] A. J. Huning, and T. J. Harrison, *Methods for the Enhancement of Security Probabilistic Risk Assessments*, Oak Ridge National Laboratory, ORNL/TM-2021/2034, 2021.

- Mechanistic consequence modeling would be beneficial in terms of both sabotage, with connection to safety analysis, and theft/diversion, where radiological material may pose significant health hazards to individuals and the public in contact or near the displaced material.

- Security-related event-initiating event frequencies would be difficult to assess using probabilistic models. Analysis of the likelihood of threats may continue to require strong insights and collaboration with intelligence resources.

Based on these observations, a dynamic PRA for security assessment combines many of these recommendations into a framework that includes some experience in the nuclear safety analysis community. Dynamic PRA is often used to describe any probabilistic model coupled directly with time-dependent physics models or event simulations. In the context of security assessment, dynamic PRA consists of dynamic event trees in which possible scenarios are modeled with event states, and in which branches are determined through security effectiveness evaluations of various postulated positions and event variables. ARES performed a PRA using a similar approach in their optimization of the physical security system at South Texas Project.[33]

A similar approach or methodology could be utilized for new and advanced reactors using conceptual design information. This would allow for possible improvements and feedback prior to construction and operation. The potential cost savings of such analysis may be strongly beneficial for concepts such as microreactors, which include features such as autonomous operation, limited site personnel, generic siting, and rapid mobility and deployment.

6. TECHNICAL SOLUTIONS FOR INSIDER THREAT

This paper thus far has focused on developing the method in which the specific technical solutions for an insider threat can be applied while being a technical solution itself for SeBD. The purpose of all protective measures for malicious acts is to design to detect, delay, and respond to all potential threats. However, these items are reactive in nature, so they typically occur after the act has occurred. Preventative measures are used to reduce the number of insiders and to reduce their ability to reach and conduct a malicious act.[34] The natural response to this is to add additional personnel and technology. This added redundancy, as discussed by Sagan,[35] could lead to a reduction in security if implemented incorrectly. Instead, the design process of a plant should addresses each of these items, and if tracked, the process can ensure that as the design matures, elements such as “the ability to reach a target” or “the ability to conduct a malicious act” become more expensive and difficult to achieve through an outsider or insider threat.

The nuclear industry has several advantages and disadvantages for mitigation of an insider threat. Disadvantages include the complexity, size, slow adoption of new technologies, and consequence of damaging nuclear facilities, because they require a large amount of personnel to operate and conduct maintenance. New technology must be proven and licensed at times to adopt, and failures could have significant consequences. Advantages are high levels of regulation requiring due diligence in terms of security, training, and monitoring of employee health and well being. If technologies are implemented to

[33] J. Raines, K. Rowth, and J. Edwards, “Using AVERT Physical Security (AVERT-PS) to Optimize Physical Security Effectiveness at the South Texas Project Electric Generating Station,” *Proceedings of the INMM & ESARDA Joint Virtual Annual Meeting*, August 23–26 & August 30 – September 1, 2021, 2021.
[34] IAEA, *Preventive and Protective Measures against Insider Threats*, IAEA Nuclear Security Series No. 8-G, IAEA, Vienna, 2020.
[35] Scott D. Sagan, “The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security,” *Risk Analysis* 24, No. 4, 2004.

avoid the disadvantages while highlighting the advantages, then those technologies are more likely to provide real, usable solutions to meet the insider threat mitigation challenge.

As illustrated in Section 3.1.1 there are psychological components to evaluating an insider threat and various methods to address such items, such as reporting certain behaviors, monitoring social media, noticing out-of-work trends, or other similar items. These types of solutions also require training and reinforcement in ensure that vigilance is maintained. However, these administrative tools do not remove insider threat. They rely heavily on people to make decisions that can impact coworkers. Thus, it is possible that such administrative procedures are self-defeating because of human nature and a lack of willingness to report someone's behavior as out of the ordinary or the tendency to question oneself prior to reporting. Thus, technological solutions must be brought to bear. In essence, the key issue is to be able to determine a signal out of human variability or noise and thus to find the signal-to-noise for a potential insider threat. A few technological theories can be applied to facilitate the selection of technologies to mitigate insider threats. One such theory would be to require a critical component could fail to secure. This would ensure that if a single failure is caused, then once the degraded system has failed, then the system's failed state would cause another critical system to be incapable of allowing an insider to cause a failure. However, this is especially difficult due to the possibility of discontinuous timelines in which someone degrades one system and then another system at different points to facilitate the failure of both systems from two discontinuous actions. This approach has its drawbacks, because an insider increases their detection probability by taking more actions over more time, but this must still be considered when selecting any technology. Other areas under consideration are through automated and monitoring systems.

Restrict or otherwise impair ease of access.

"Why is that guy up on a ladder by himself?"

SMRs attempt to become cost competitive by having small footprints, modular designs, simple designs, and a small workforce. Having two employees working on a system at all times is a standard requirement within the nuclear industry. Therefore, seeing an individual working alone is considered an off-standard event. Technology could be introduced if the design of a plant is such that it can maintain line of sight to flag when a person is alone and near a component of interest. Additionally, technology could be used during plant design to ensure that a single individual acting maliciously would be obvious to security and personnel when that person is in a location where they should not be doing something they should not be doing. In both cases, technology could be introduced to recognize these items through optics, sensors, or design criteria to identify these items and mitigate or eliminate them.

Expose safety and security adder.

From a cultural standpoint, the nuclear industry focuses largely on a safety culture through training, human performance monitoring and improvement, financial compensation, and procedures. Most of these are accomplished through administrative means, relying on a person to act to accomplish the safety goal. However, one method that takes the form of phycological effects is the idea of identifying the "nuclear adder." For example, consider a welder working at a welding shop, industrial facility, or in a home garage A welder working at a nuclear facility typically earns more money than working at other locations based on three factors. The requirement for the quality of the work is high, the requirement for the method of the work to be conducted, and the requirement that the results be safe and relied upon for safety, and the requirement that the welder be subjected to security monitoring and checks to ensure that they are not a threat to the nuclear facility. Each of these areas is a typical adder to this person's necessary skillset and should be compensated above work in other facilities without these requirements. A safety culture could be adapted into a quality-safety-security culture in which the specifics of the salary and benefits adders on a person's salary is specifically called out during each review cycle. This would reinforce that the welder

is being paid not only to weld a pipe, but also to weld that pipe to a high standard of quality in a safe manner (while also looking out of the safety of others) as part of a secure facility and culture. Thus, itemizing promotions or benefit increases according to these areas of expertise illustrates that one can have an impact on all of these areas that are beneficial to a plant and thus bring security into the standard culture on par with the areas of quality and safety.

Safety movement mapping for security analysis.

Technologies have been developed that can track personnel within a facility and flag people and their paths through a facility in both real time and for delayed analysis. Such tools could provide the data necessary to conduct algorithmic, machine learning, or full artificial intelligence analysis upon the path and actions to detect a person's out-of-ordinary actions. This is a valuable monitoring item as part of the security infrastructure, but people rarely consent to being monitored as they work. Union rules and issues of privacy are also a concern for employees. However, the nuclear industry is unique regarding these types of devices. Nuclear facilities implement multiple types of radiation monitoring, badge monitoring, bioassay monitoring, and general surveillance as part of the standard and not the exception. Although many personnel would still be resistant to utilizing specific movement monitoring hardware on their persons, they are already required to do so for radiation detection and monitoring. If tracking and monitoring items are incorporated into radiation detectors, then randomized which personnel are tracked, key coding them to a person's badge and identifiable password, then the data provided would not only serve as an easy tool for security monitoring, but also a tool for radiation protection monitoring. The concept of maintaining exposure to radiation as low as reasonably achievable (ALARA) is a central concept in the nuclear industry. During an outage, radiation maps with thousands of data points are taken by radiation protection, and maps of the facility are created showing the various hot spots or areas of high radiation that often change during the outage. However, tracking and implementing security and radiation protection software algorithms and hardware would allow for tracking a person's location and radiation levels at a specific location. This would allow for radiation protection personnel to actively monitor a facility's radiation maps while providing security with the data needed to protect against an insider threat. This would all fit well into the current US nuclear facility culture and potentially around the world while providing a general benefit to employees to reduce and visualize their positions and the routes they should take to avoid unnecessary dose. Finally, this approach can also be used to monitor and detect if someone is alone and thus more likely to conduct a malicious act or to detect whether someone is often with another specific employee for an operation, pointing to an increased likelihood of collusion.

Finally, the best was to prevent insider and outsider threats is through the removal or creation of reactor designs that prevent, limit, or eliminate insider and outsider threats, and if those threats succeed, then to allow a time-to-core-damage of such length that mitigation actions are still available once the threat is eliminated. To accomplish this, a system must be created to track the design of a reactor and the security of the reactor from concept through the operational handoff to the reactor operator and beyond to decommissioning is necessary. This potential security design method presented in Section 4.

7. CONCLUSIONS

The cost of security through the lifecycle of a plant has been shown to rise over time and requires investment in technical solutions, analysis, and licensing proof to realize cost savings for an operating plant without sacrificing security. Therefore, it is expected that as SMRs are deployed and operate and the threat profile around the world evolves to include more sophisticated or unanticipated threat paradigms, a system focused on the tracking and continuous analysis of plant safety and security and the assumptions made will be necessary. This approach is necessary because the economy of scale and electrical output of these facilities are smaller, so potential profit margins are lower and may not be counterbalanced by other savings. The plant footprint is also smaller, leading to less available territory for delay, although there is a

smaller area to cover for insider and outsider threat. The solutions for the advanced SMR and other reactors under development and deployment must be multifaceted, innovative, and most importantly, adaptive. Security systems must be constantly monitored and evaluated as changes occur from forces external to the nuclear operation of a plant (change in threat profile). Security systems must also adapt from internal changes to a plant as the safety, operation, maintenance, and decommissioning of facilities occur. Further research into the collaborative space linking security and safety in a standard consensus-based system can allow for future technologies to be applied to present designs quickly and efficiently to either highlight weaknesses in a plant's design or to demonstrate that the current design choices of a plant prevent or mitigate new threats, thus allowing a plant to maintain its predicted operational cost with high levels of effective security.

APPENDIX A. COMPONENT SURVEY OF NUSCALE SMR SAFETY ANALYSIS REPORT

Abbreviation	Description	Abbreviation	Description
ABS	auxiliary boiler system	LWMS	liquid waste management system
ABVS	Annex Building HVAC system	MCS	module control system
AFWS	auxiliary feedwater system	MHS	module heat up system
BAS	boron addition system	MSS	main steam system
BPDS	balance-of-plant drain system	NSSS	nuclear steam supply system
BPSS	backup power supply system	OHLHS	overhead heavy load handling system
BRVS	battery room ventilation system	PACS	priority actuation and control system
CARS	condenser air removal system	PCS	plant control system
CAS	compressed air system	PCUS	pool cleanup system
CES	containment evacuation system	PLDS	pool leakage detection system
CFDS	containment flooding and drain system	PLS	plant lighting system
CFWS	condensate and feedwater system	PPS	plant protection system
CHRS	containment heat removal system	PSCIV	primary system containment isolation valves
CHWS	chilled water system	PSCS	pool surge control system
CIS	containment isolation system	PSMS	power supply monitoring system
CNTS	containment system	PSS	process sampling system
COMS	communication system	PVMS	plant-wide video monitoring system
CPRS	condensate polisher resin regeneration system	PWS	potable water system
CPS	condensate polishing system	RBVS	Reactor building HVAC system
CRDS	control rod drive system	RCCWS	reactor component cooling water system
CRHS	control room habitability system	RCS	reactor coolant system
CRVS	normal control room HVAC system	RMS	fixed area radiation monitoring system
CSS	containment sampling system	RPCS	reactor pool cooling system
CVCS	chemical and volume control system	RPS	reactor protection system
CWS	circulating water system	RTS	reactor trip system
DAS	distributed antenna system	RWBVS	Radioactive waste building HVAC system
DAS	diverse actuation system	RWDS	radioactive waste drain system
DCS	distributed control system	RWMS	radioactive waste management system
DGBVS	Diesel Generator Building HVAC system	RWSS	raw water supply system
DHRS	decay heat removal system	SAS	service air system
DSS	digital safety system	SBVS	Security Building HVAC system
DWS	demineralized water system	SCS	secondary sampling system
ECCS	emergency core cooling system	SCWS	site cooling water system
EDNS	normal DC power system	SDIS	safety display and indication system
EDSS	highly reliable DC power system	SDS	site drainage system
EFDS	equipment and floor drainage system	SFPCS	spent fuel pool cooling system
EHVS	13.8 kV and switchyard system	SFSS	spent fuel storage system
ELVS	low voltage AC electrical distribution system	SGS	steam generator system
ERDS	emergency response data system	SICS	safety information and control system
ESAS	emergency safeguards actuation system	SMS	seismic monitoring system
ESFAS	engineered safety features actuation system	SPS	security power system
FDS	fire detection system	SRWS	solid radioactive waste system
FPS	fire protection system	SSCIV	secondary system containment isolation valve
FWS	feedwater system	SSS	secondary sampling system
FWTS	feedwater treatment system	SWMS	solid waste management system
GRWS	gaseous radioactive waste system	SWYD	switchyard system
HVDS	feedwater heater vents and drains system	TBS	turbine bypass system
IAS	instrument air system	TBVS	Turbine Building HVAC system
ICIS	in-core instrumentation system	TGS	turbine generator system
ICS	integrated control system	TGSS	turbine gland sealing system
IOTBS	inadvertent opening of the turbine bypass system	TLOSS	turbine lube oil storage system
LRWS	liquid radioactive waste system, liquid radwaste system	UWS	utility water system

Abbreviation	Description
AOV	air-operated valve
CIV	containment isolation valve
FWIV	feedwater isolation valve
FWRV	feedwater regulating valve
HOV	hydraulic-operated valve
MOV	motor-operated valve
MSIBV	main steam isolation bypass valves
MSIV	main steam isolation valve
MSSV	main steam safety valve
PORV	power-operated relief valve
POV	power-operated valve
PRV	pressure relief valve
PSCIV	primary system containment isolation valves
RRV	reactor recirculation valve
RSV	reactor safety valve
RVV	reactor vent valve
SOV	solenoid-operated valve
SRV	sump recirculation valve
SSCIV	secondary system containment isolation valve
VRLA	valve-regulated lead-acid

Abbreviation	Description
AB	annex building
ABB	auxiliary boiler building
CRB	control building
CUB	central utility building
DGB	diesel generator building
FWB	fire water building
FWPB	fire water pump building
RWBCR	radioactive waste building
RXB	reactor building
SCB	security buildings
TGB	turbine generator building
WB	warehouse building
WTB	waste treatment building