SAND2023-07082C

The Sliding Scale of Cybersecurity Applied to the Cybersecurity Analysis of Advanced Reactors

Lee T. Maccarone[1]*, **Michael T. Rowland**[1]

[1]Sandia National Laboratories, Albuquerque, NM

ABSTRACT

The Sliding Scale of Cybersecurity is a framework for understanding the actions that contribute to cybersecurity. The model consists of five categories that provide varying value towards cybersecurity and incur varying implementation costs. These categories range from offensive cybersecurity measures providing the least value and incurring the greatest cost, to architecture providing the greatest value and incurring the least cost. This paper presents an application of the Sliding Scale of Cybersecurity to the Tiered Cybersecurity Analysis (TCA) of digital instrumentation and control systems for advanced reactors.

The TCA consists of three tiers. Tier 1 is design and impact analysis. In Tier 1 it is assumed that the adversary has control over all digital systems, components, and networks in the plant, and that the adversary is only constrained by the physical limitations of the plant design. The plant's safety design features are examined to determine whether the consequences of an attack by this cyber-enabled adversary are eliminated or mitigated. Accident sequences that are not eliminated or mitigated by security by design features are examined in Tier 2 analysis. In Tier 2, adversary access pathways are identified for the unmitigated accident sequences, and passive measures are implemented to deny system and network access to those pathways wherever feasible. Any systems with remaining susceptible access pathways are then examined in Tier 3. In Tier 3, active defensive cybersecurity architecture features and cybersecurity plan controls are applied to deny the adversary the ability to conduct the tasks needed to cause a severe consequence. Earlier application of the TCA in the design process provides greater opportunity for an efficient graded approach and defense-in-depth.

Keywords: Tiered Cybersecurity Analysis; Secure by Design; Advanced Reactors

1. INTRODUCTION

Under the United States Nuclear Regulatory Commission (US NRC) Regulatory Guide 5.71 [1], licensees of light water reactors (LWRs) have been required to broadly apply a large set of technical and operational cybersecurity controls to all identified critical digital assets (CDAs). For advanced reactors (ARs), this prescriptive approach places a large time and resource burden on the licensee and does not allow the licensee the flexibility to prioritize the systems with the greatest potential for physical harm. The regulation that sets cybersecurity policy for ARs, Title 10 of Code of Federal Regulations (10 CFR) 73.110 specifies, "Technology neutral requirements for protection of digital computer and communication systems and networks," and is currently in draft review stages [2]. The draft rule proposes a graded approach to cyber security controls based on potential consequences of credible postulated attacks at each risk level.

*lmaccar@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

To address the requirements outlined in 10 CFR 73.110, the US NRC has presented "U.S.A. Regulatory Efforts for Cyber Security of Small Modular Reactors/Advanced Reactors," at the International Atomic Energy Agency (IAEA) Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors [3]. The presentation included a three-tier cybersecurity analysis approach proposed in the draft regulatory guide. The methodology is pre-decisional, but the concepts are referred to in this paper as the Tiered Cybersecurity Analysis (TCA).

This work examines the alignment of the TCA with the Sliding Scale of Cybersecurity. The Sliding Scale of Cybersecurity is a framework taught by the SANS Institute for describing the actions that contribute to cybersecurity [4]. Each category within the Sliding Scale can be described in terms of its security value and cost to identify the priority it should receive within a security program. It is critical that the Sliding Scale categories and TCA tiers are implemented at the correct phase of plant design in order to maximize cost efficiency. The phases of advanced reactor design maturity defined by the World Nuclear Association (WNA) are used in this work [5]. After examining the alignment between the Sliding Scale, the TCA, and the WNA design phases, a modified Sliding Scale of Cybersecurity for Advanced Reactors is presented.

2. THE SLIDING SCALE OF CYBERSECURITY

The Sliding Scale of Cyber Security is a framework for describing the actions that contribute to cybersecurity [4]. The definitions of the five categories in the Sliding Scale of Cybersecurity model are quoted below.

1. Architecture: "the planning, establishing, and upkeep of systems with security in mind" [4].
2. Passive Defense: "systems added to the architecture to provide consistent protection against or insight into threats without constant human interaction" [4].
3. Active Defense: "the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats internal to the network" [4].
4. Intelligence: "the process of collecting data, exploiting it into information, and producing an assessment that satisfies a previously identified knowledge gap" [4].
5. Offense: "direct action taken against the adversary outside friendly networks" [4].

Note that some categories of the Sliding Scale are related. For example, many security analysts consider the development of a secure architecture to be a passive defense (not considering the specific definitions above). Specifically, the development of a defensive cybersecurity architecture (DCSA) will be discussed in greater detail later in Section 3.

It is also noteworthy that the five categories of the Sliding Scale are not equally important. For example, architecture is the foundation of a secure system, whereas offense provides little benefit to cybersecurity (and would likely be illegal for an organization). The relationship between the utility of the categories and their costs is summarized in Figure 1.

Architecture is the most important category in the Sliding Scale and is also the least costly. Passive and active defenses build upon the foundation of architecture and incur additional costs. Finally, intelligence and offense are the most expensive categories and provide comparatively low value towards the overall cybersecurity posture. These relationships will be further examined through comparisons with the TCA.

3. TIERED CYBERSECURITY ANALYSIS FOR ADVANCED REACTORS

The TCA is a cybersecurity assessment methodology that aligns domestic standards, international standards, and technical guidance to select Secure-by-Design (SeBD) requirements to develop defensive network architectures and apply effective cybersecurity controls. The TCA is shown in Figure 2.

The TCA begins by considering unacceptable consequences (e.g., radiological release) and plant control actions that can lead to unsafe states. The process assumes that safety analyses pertinent to the consequences

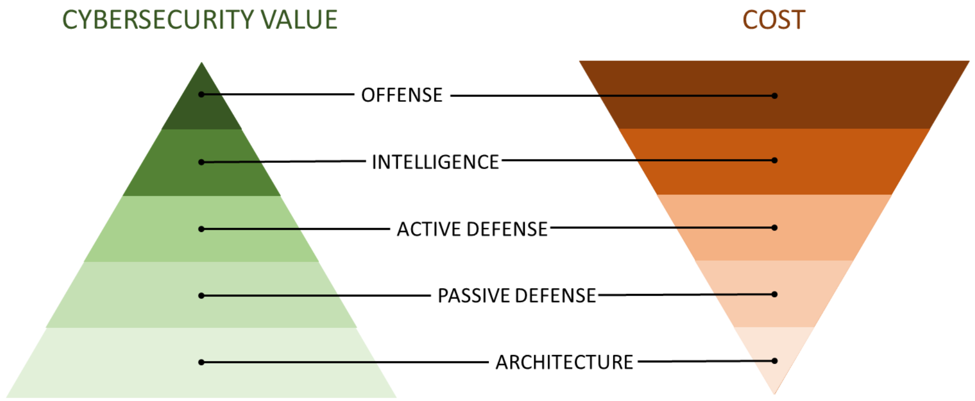

Figure 1: The Value and Costs of Categories of the Sliding Scale of Cybersecurity [4].

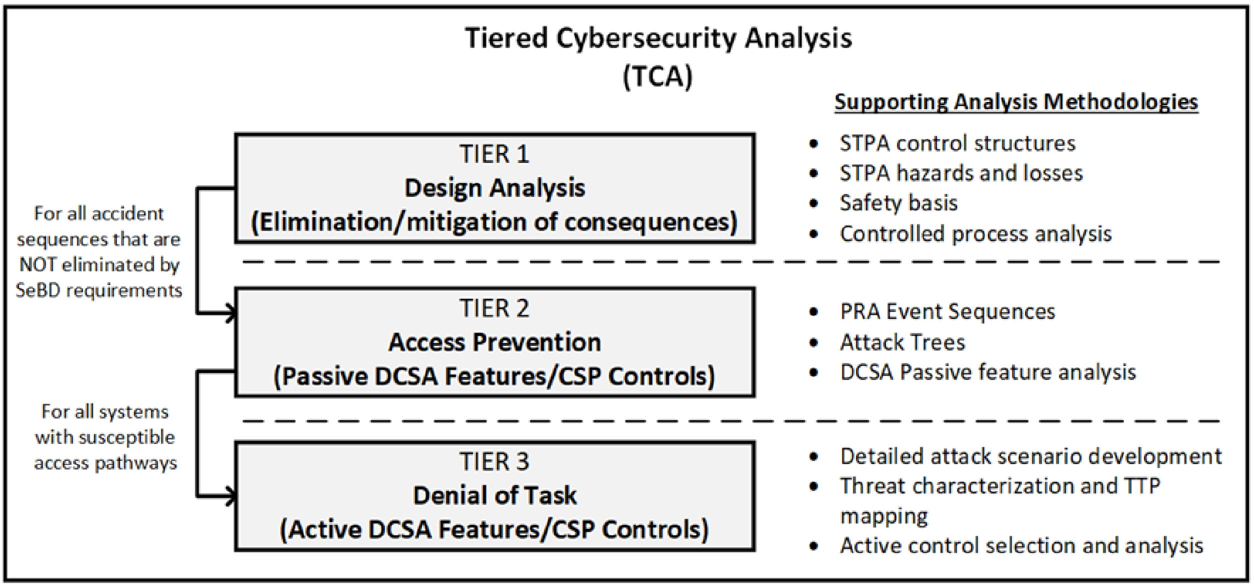
Tiered Cybersecurity Analysis
(TCA)
Supporting Analysis Methodologies
TIER 1
Design Analysis
(Elimination/mitigation of consequences)
STPA control structures
STPA hazards and losses
Safety basis
Controlled process analysis
For all accident sequences that are NOT eliminated by SeBD requirements
TIER 2
Access Prevention
(Passive DCSA Features/CSP Controls)
PRA Event Sequences
Attack Trees
DCSA Passive feature analysis
For all systems with susceptible access pathways
TIER 3
Denial of Task
(Active DCSA Features/CSP Controls)
Detailed attack scenario development
Threat characterization and TTP mapping
Active control selection and analysis

Figure 2: Tiered Cybersecurity Analysis (TCA) [6].

of concern have been performed prior. Tier 1 of the TCA is Design and Impact Analysis and is used to evaluate safe-by-design features. SeBD is an extension of safe-by-design. While safe-by-design considers how consequences of an accident or random failure can be mitigated or eliminated, SeBD considers the mitigation or elimination of consequences caused by an adversary.

If it is determined that SeBD elements and passive safety features are not able to fully eliminate the consequence, then Tier 2 (Denial of Access) is required for the functions that are in place to mitigate the consequence. This generally takes the form of accident sequences, and analyzes each function credited by safety with preventing accident conditions following an initiating event. Key considerations in the Tier 2 analysis are access pathways. A function may have supporting systems, networks, and components that represent access points for the adversary. The goal is to inform secure network architecture and passive security features at this level, or otherwise identify areas that require further control measures, and therefore further analysis in Tier 3 (Denial of Task). Tier 3 analysis is performed for all systems analyzed in

Tier 2 that require further control (i.e., systems for which passive safety features do not mitigate all access pathways). Tier 3 analysis is an assessment of more detailed scenarios and the active cybersecurity plan (CSP) elements that can be implemented to protect the system.

3.1. Tier 1 Analysis

The goal of Design and Impact Analysis is to evaluate the plant's safety design features and determine if they can be credited as SeBD features. Crediting the design features means that they would prevent an attack from leading to an unacceptable consequence, and therefore a more detailed analysis of the scenario is not required. To make this claim, the impact of an attack would need to be eliminated. Protective measures that would delay an attack are valuable to the security of the plant, but still require Tier 2 analysis of the function because the impact is not eliminated. Abstraction at the three tiers is best thought of as adversary capabilities. At Tier 1, the scenarios are developed considering an adversary that is limited only by the physical limitations of the plant design. This adversary is assumed to have access to any digital system, component, or network in the plant, and is assumed to be capable of implementing any control action within the capability of the system.

3.2. Tier 2 Analysis

The goal of Denial of Access Analysis is to evaluate adversary access vectors and implement passive measures to deny system and network access. At this tier of analysis, it is assumed that the adversary can achieve their objective if they gain access to the appropriate systems. Once again, safety analyses are taken as inputs and used to identify unsafe event sequences. One method to represent attack sequences and bound the scope of scenarios is to use traditional probabilistic risk assessment (PRA) event trees. Each plant function that must operate to mitigate an accident should be considered. This analysis should examine each system in the sequence of plant functions required for accident mitigation and identify available pathways for an adversary. The results of Tier 2 analysis are passive or deterministic defensive cybersecurity architecture (DCSA) or CSP elements.

The IAEA defines the features of DCSA in the Nuclear Security Series (NSS) publication 17-T [7]. Several key definitions are quoted below from NSS 17-T.

- Function: "a coordinated set of actions and processes that need to be performed at a nuclear facility" [7].
- Security Level: "a designation that indicates the degree of security protection required for a facility function and consequently for the system that performs that function" [7].
- Security Zone: "a logical and/or physical grouping of digital assets that are assigned to the same computer security level and that share common computer security requirements owing to inherent properties of the systems or their connections to other systems" [7].

A zone is a region bounded by logical and physical protections which contains at least one system. Communication between assets within a zone is trusted, while communication between different zones is restricted and controlled [7]. DCSA levels provide a framework for implementing security measures corresponding to the criticality of each level. Each plant function is assigned a level based on its criticality. The stringency of measures put in place for a given level is directly related to the significance of the function protected by the level. Levels allow flexibility in security requirements across the facility which allows designers to prioritize the areas of greatest risk. Each level includes one or more zones. Figure 3 provides an example of how DCSA zones and levels would be implemented.

3.3. Tier 3 Analysis

The goal of Denial of Task Analysis is to provide risk-informed control measures to unmitigated systems identified in Tier 2. In Tier 3, it is assumed that the adversary has obtained the access required to achieve their objective and control measures must be implemented to prevent the adversary from completing their objective. Generally, a body of controls may consist of baseline controls and risk-informed controls. Baseline controls apply broadly and provide information security assurance while risk-informed controls treat a

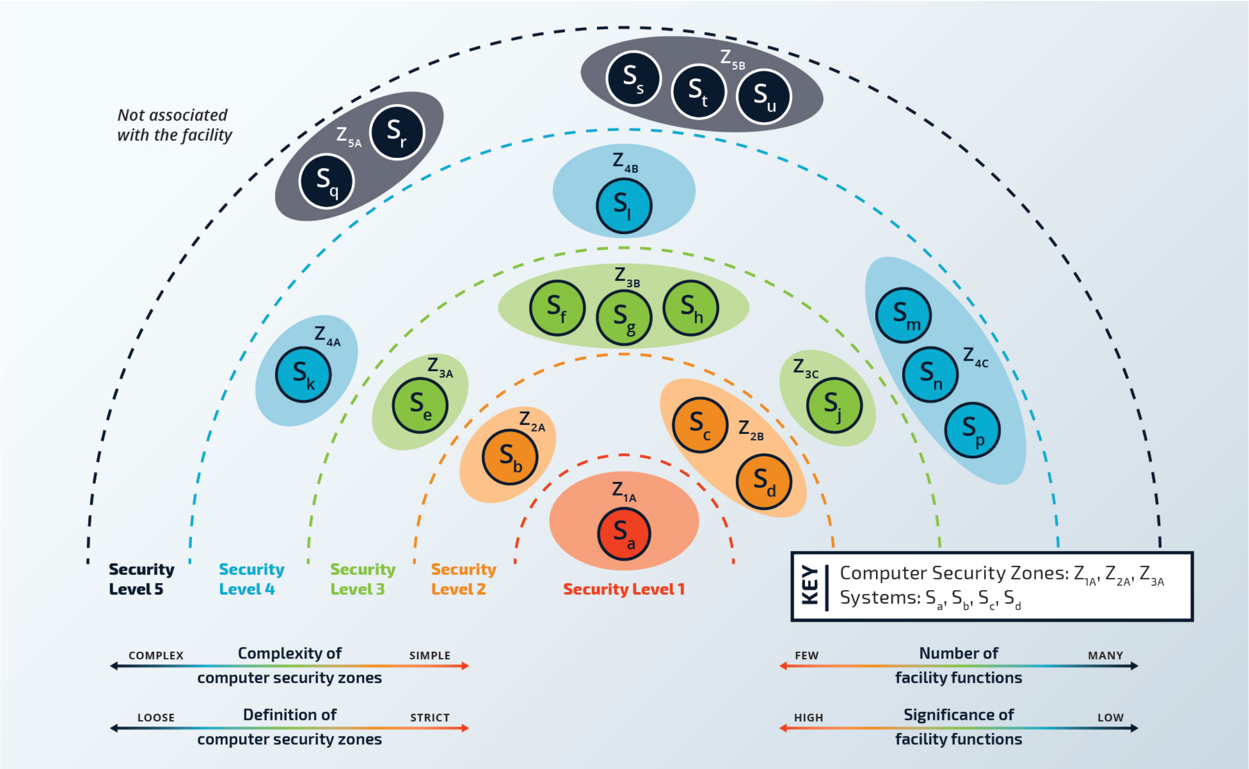

Figure 3: Conceptual DCSA Model [7].

specific identified risk. There are several methods that can be leveraged to identify applicable risk-informed controls (e.g., combining control action modeling using STPA and adversary sequence modeling using attack tree modeling).

4. PHASES OF DESIGN MATURITY

It is critical that the Sliding Scale categories and TCA tiers are implemented at the correct phase of plant design in order to maximize cost efficiency. The WNA defined a series of plant design phases of maturity for small modular reactors as shown in Figure 4. The first phase of design maturity is the conceptual phase where the reactor concept is developed. In Phase 1 critical questions are asked and major risks are identified. The second phase of design maturity is plant-level design. In Phase 2 the requirements and design parameters of key systems, structures, and components (SSCs) are defined. The third phase of design maturity is system-level design. In Phase 3 the requirements and design parameters of key SSCs are further refined and other plant systems are defined. Finally, the fourth phase of design maturity is component-level design. In Phase 4 the engineering details are finalized for SSCs to allow for manufacturing to begin [5,8].

5. ALIGNMENT OF THE SLIDING SCALE, TIERED ANALYSIS, AND DESIGN PHASES

Given the descriptions of the Sliding Scale and TCA provided in the previous sections, the alignment between the two constructs is readily apparent. These constructs can also be aligned with the WNA phases of design maturity to optimize their cost-efficiency. The relationship between the WNA phases of design maturity, the Sliding Scale, and the TCA is shown in Figure 5.

The architecture and passive defense components of the Sliding Scale clearly align with Tier 2 analysis. Tier 2 analysis corresponds to Denial of Access and the outcome is a DCSA with passive cybersecurity controls. Similarly, the active defense component of the Sliding Scale clearly aligns with Tier 3 analysis

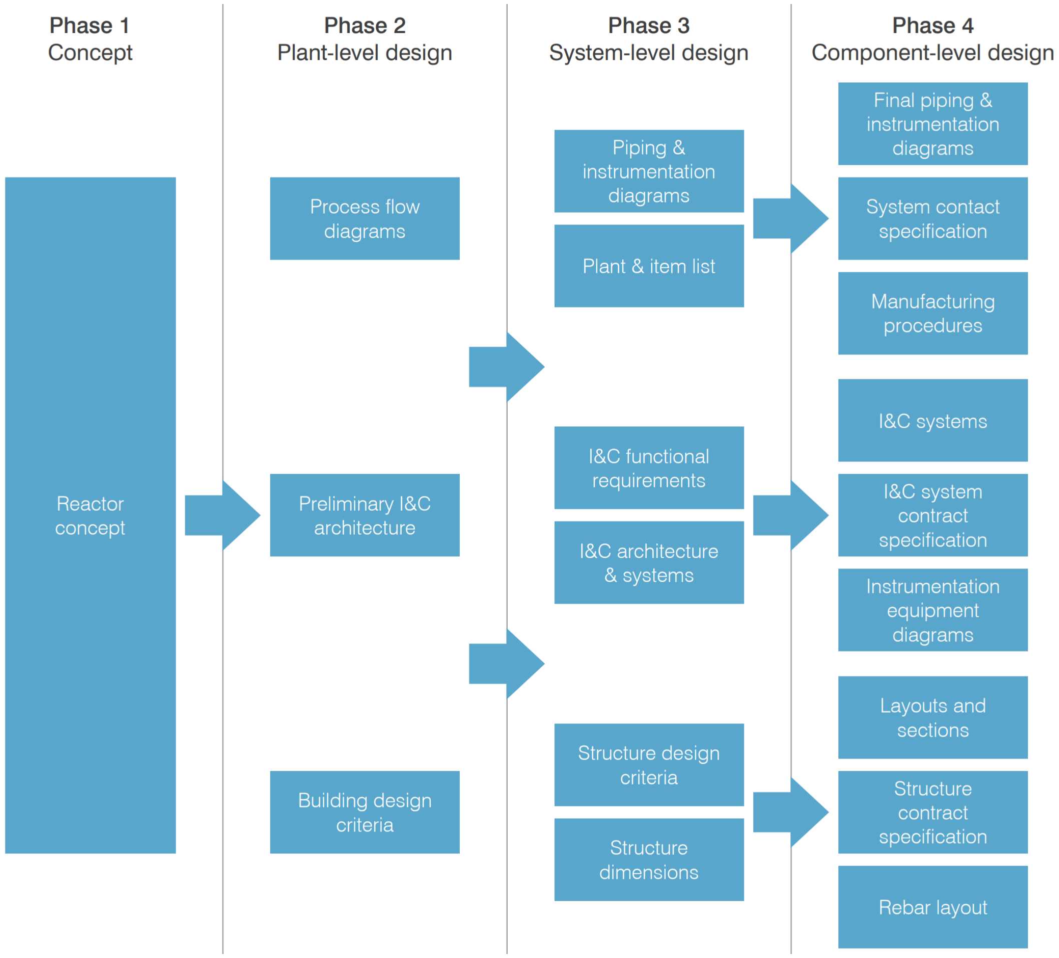
Phase 1
Concept
Phase 2
Plant-level design
Phase 3
System-level design
Phase 4
Component-level design
Reactor concept
Process flow diagrams
Preliminary I&C architecture
Building design criteria
Piping & instrumentation diagrams
Plant & item list
I&C functional requirements
I&C architecture & systems
Structure design criteria
Structure dimensions
Final piping & instrumentation diagrams
System contact specification
Manufacturing procedures
I&C systems
I&C system contract specification
Instrumentation equipment diagrams
Layouts and sections
Structure contract specification
Rebar layout

Figure 4: WNA Plant Design Phases of Maturity [5].

because Tier 3 corresponds to the assignment of active cybersecurity controls where passive controls were insufficient. The intelligence component of the Sliding Scale also aligns with Tier 3 analysis because the attack scenario development utilizes threat characterization and intelligence regarding adversary TTPs.

The concept and plant-level design phases align with Tier 1 of the TCA and do not directly align with any of the Sliding Scale components. Upon completion of these design phases, the impact of SeBD features can be analyzed. The system-level design phase aligns with Tier 2 of the TCA and with the corresponding architecture and passive defense components of the Sliding Scale. This alignment occurs because the system-level design phase results in the design of I&C functional requirements and architectures. The component-level design phase aligns with Tier 3 of the TCA and with the corresponding active defense and intelligence components of the Sliding Scale. This alignment occurs because the component-level design phase provides the level of detail required to create the attack scenarios required for Tier 3 analysis. Improper alignment of the TCA and Sliding Scale with the WNA design phases may result in increased cybersecurity costs.

It is noteworthy that the offense component of the Sliding Scale that does not align with the TCA. The offense component does not map to a TCA tier because offensive or retaliatory actions do not have a legal place in the cybersecurity program of a commercial power reactor. The offense component also has the greatest cost and lowest value of all of the Sliding Scale components, therefore inclusion of this component in the TCA should not be desired.

It is also noteworthy that Tier 1 analysis does not align with the Sliding Scale. Design Analysis relies on

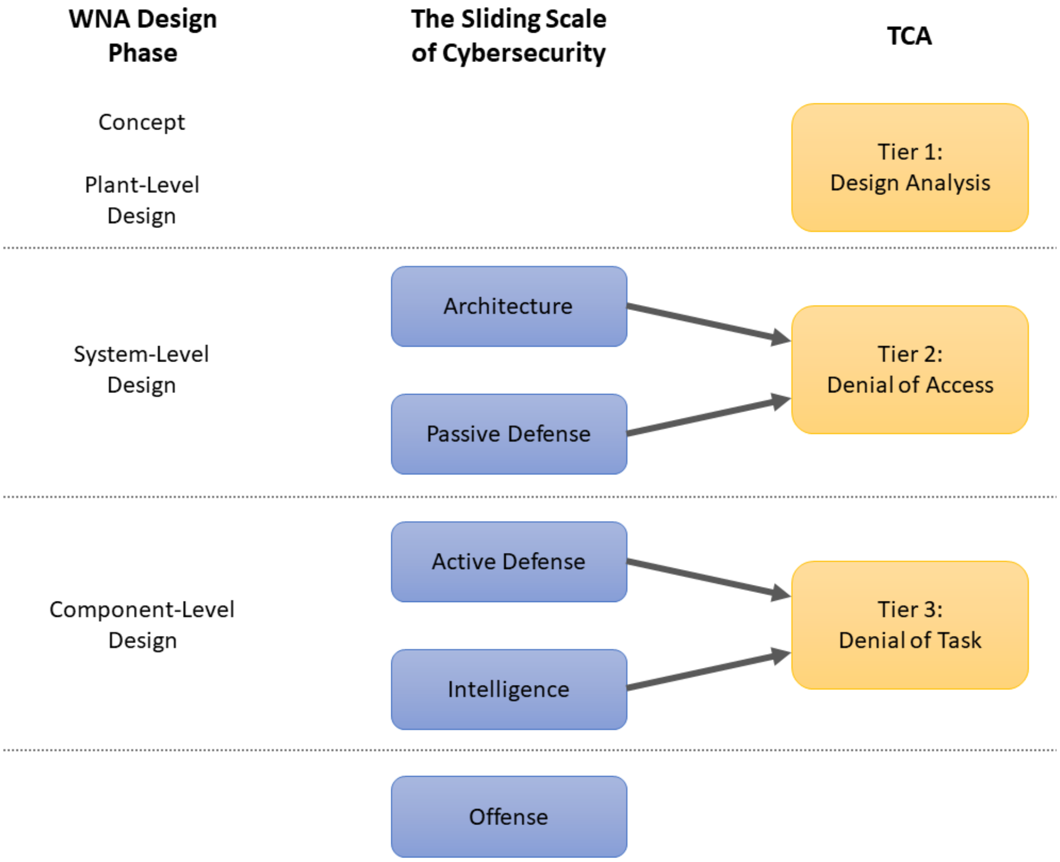

Figure 5: The Alignment of the WNA Phases of Design Maturity, Sliding Scale of Cybersecurity, and TCA.

SeBD features to eliminate or mitigate accident sequences caused by a cyber-adversary. While architecture is the foundation of the cybersecurity of traditional cyber-systems, the foundation of cybersecurity for ARs (i.e., cyber-physical systems) in the TCA is considered to be the plant physics. An AR design that maximizes the benefit of plant safety features for security applications may achieve greater value through SeBD than even the architecture component of the Sliding Scale, at lower cost.

A revised version of the Sliding Scale of Cybersecurity called the Sliding Scale of Advanced Reactor Cybersecurity summarizes the application of the Sliding Scale to AR applications through the TCA. The revised Sliding Scale removes the offense category and adds SeBD as the foundational category. The proposed value and costs of the components are shown in Figure 6. It is noteworthy that the costs of the components are predicated on their proper alignment with the phases of plant design.

6. CONCLUSIONS

In this work, we have demonstrated the alignment of the Sliding Scale of Cybersecurity with the proposed TCA for the cybersecurity of ARs. It was shown that the tiered approach strongly most strongly aligns with the architecture, passive defense, and active defense categories, and that the intelligence category also plays a role in the TCA. Notably, the offense category is not part of the TCA. This exclusion is justified given the high cost of offensive actions, low value towards security, and legal restrictions prohibiting retaliation. SeBD features are the foundation of the TCA, and are therefore the foundation of the Sliding Scale of

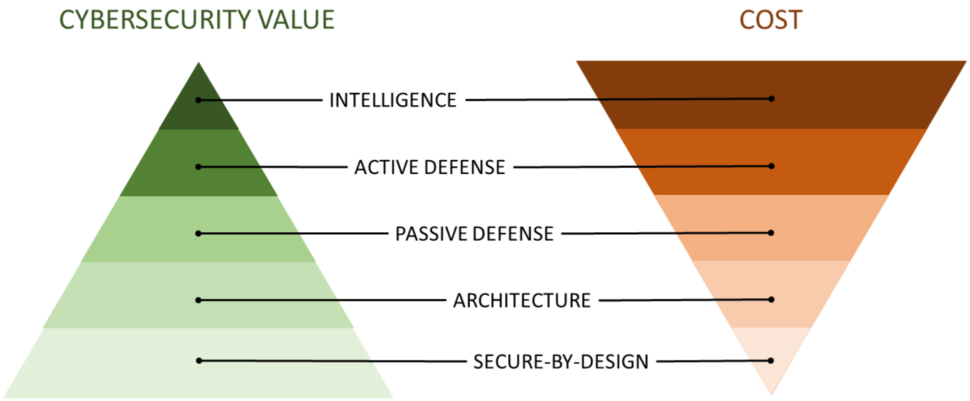

Figure 6: The Value and Costs of Categories of the Sliding Scale of Advanced Reactor Cybersecurity.

Cybersecurity for ARs. By leveraging SeBD features in the TCA, AR designers can reduce the scope and total cost of active cybersecurity measures. Through proper alignment of the TCA and Sliding Scale with the WNA phases of plant design, the total cost of cybersecurity programs may be optimized.

ACKNOWLEDGMENTS

This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan https://www.energy.gov/downloads/doe-public-access-plan.

REFERENCES

[1] U.S. Nuclear Regulatory Commission. “Regulatory Guide 5.71 - Cyber Security Programs for Nuclear Facilities.” (2010).

[2] U.S. Nuclear Regulatory Commission. “DRAFT 10 CFR Part 73, Section 10: Technology Neutral Requirements for Protection of Digital Computer and Communication Systems and Networks.” (2022).

[3] J. Jauntirans, I. Garcia, and M. Rowland. “U.S.A. Regulatory Efforts for the Cyber Security of Small Modular Reactors/Advanced Reactors.” In *IAEA Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors*. Vienna, Austria (2021).

[4] R. M. Lee. “The Sliding Scale of Cyber Security.” Technical report, SANS Institute, North Bethesda, MD (2015).

[5] World Nuclear Association. “Design Maturity and Regulatory Expectations for Small Modular Reactors.” Technical report, London, United Kingdom (2021).

[6] J. James, J. Mohmand, L. Maccarone, D. R. Sandoval, A. Haddad, M. T. Rowland, and A. J. Clark. “Consequence Modeling and Simulation of Hazardous Events for Advanced Reactors.” Technical report, Sandia National Laboratories, Albuquerque, NM (2023).

[7] International Atomic Energy Agency. *NSS-17T: Computer Security Techniques for Nuclear Facilities*. IAEA, Vienna, Austria (2021).

[8] L. T. Maccarone, J. R. James, D. R. Sandoval, A. W. Haddad, and M. T. Rowland. “An Efficient Graded Approach for the Design of Secure Instrumentation and Control Systems.” In *Proceedings of the 2023 30th International Conference on Nuclear Engineering (ICONE30)*. Kyoto, Japan (2023).