First of a Kind Use of an Assurance Case in NEI 20-07 to Address Common Cause Failure

Andrew Nack, University of Tennessee, Knoxville, TN, USA
Simon Diemert, Critical Systems Labs Inc., Vancouver, BC, Canada
Alan Campbell, Nuclear Energy Institute, Washington, DC, USA

First of a Kind Use of an Assurance Case in NEI 20-07 to Address Common Cause Failure

Andrew Nack [1,2], Simon Diemert [3], Alan Campbell [4]

[1] University of Tennessee, Knoxville, TN, anack@vols.utk.edu
[2] Rivermist Engineering LLC, Knoxville, TN, andrew.nack@rivermistengineering.com
[3] Critical Systems Labs Inc., Vancouver, BC, simon.diemert@cslabs.com
[4] Nuclear Energy Institute, Washington, DC, adc@nei.org

ABSTRACT

The latest revision of US NRC Branch Technical Position 7-19 and SRM-SECY-22-0076 opened a pathway to the use of risk-informed approaches to addressing common cause failure. NEI 20-07 has been developed to implement this type of methodology. Risk-informed and performance-based methodologies are relatively new to the US commercial nuclear power industry. Prescriptive (i.e. deterministic) methods are still most common and most familiar to the US NRC. Risk-informed and performance-based methodologies hold great promise to provide freedom in design of technology solutions, but one drawback is that compliance with requirements can be more difficult to demonstrate. The use of an assurance case within NEI 20-07 is meant to address this drawback. IEC/IEEE 15026-2 defines an assurance case as an "auditable artefact that provides a convincing and sound argument for a claim on the basis of tangible evidence under a given context". Assurance cases are commonly in use in non-nuclear safety-critical industries and in the UK nuclear industry, but NEI 20-07 is the first instance of the use of an assurance case in the US NRC regulatory environment. This paper describes this initial instance at its current status and how the approach can be enhanced in the future.

Keywords: Common Cause Failure, Assurance Case, Performance-Based, Risk-Informed

1. INTRODUCTION

The latest revision of US NRC Branch Technical Position 7-19 and SRM-SECY-22-0076 opened a pathway to the use of risk-informed approaches to addressing common cause failure. NEI 20-07 has been developed to implement this type of methodology. The Nuclear Energy Institute is utilizing the assurance case methodology within NEI 20-07. This is a first of a kind approach in the US nuclear industry but is a common practice to several other safety-critical industries. The NEI 20-07 document is titled, "Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems" and is intended to provide guidance for addressing common cause failure in a risk-informed and performance-based (RIPB) manner. Since this guidance is intended for use for high safety significant systems, it is assumed that the single failure criterion applies as a prescriptive and qualitative approach to address system reliability. Common cause failure (CCF) is a concern because it defeats the underlining concept of the single failure criterion [1]. Historically, CCF has been regulated by prescriptive (i.e. deterministic) requirements that drive the use of a specific defense in-depth approach to ensure the single failure criterion is maintained. This paper is not focused on the details of the novel logical argument presented in NEI 20-07 but on the novel use of a structured, graphical assurance case.

2. MOVING TO RISK-INFORMED AND PERFORMANCE-BASED

Currently, there is a desire in the US nuclear power industry to migrate away from prescriptive (i.e. deterministic) requirements and towards risk-informed and performance-based requirements. There are two main reasons for this. First, increased freedom is needed in the designs of reactors and reactor systems. Second, it is necessary for the level of rigor to scale to the risks involved in a particular reactor design and in each of its associated systems. The traditional requirements are too restrictive and cause unnecessary hindrances to the industry.

To utilizing the more desirable style of requirements, NEI 20-07 utilizes the following overall RIPB requirement, "Vulnerabilities to digital CCF have been adequately identified and addresses commensurate with the risk significance of the proposed digital I&C system." Within an assurance case, this overall requirement is used as the top-level claim that is to be proven by the supporting argument. The selection of this top-level claim was very intentional to ensure the assurance case accomplishes all the goals of the NEI 20-07 document. Note that this requirement does not specify how it must be met by the digital I&C system. This is what makes it performance-based and not prescriptive. Additionally, the word "adequately" and the phrase "commensurate with the risk significance" were specifically included to highlight the risk-informed aspect. The requirement is also specific to the context of the "proposed digital I&C system". This context clarifies what the scope is concerning "vulnerabilities to digital CCF". The assurance case is focused on digital CCF vulnerabilities within the proposed digital I&C system. With the top-level claim defined, the argument portion of the assurance case can be developed.

3. ASSURANCE CASE USE IN NEI 20-07

An assurance case, at the most basic level, involves the top-level claim, evidence that should prove the top-level claim, and the logical argument that explains why the evidence proves the top-level claim. During the effort to draft the NEI 20-07 document, the Claims-Arguments-Evidence (CAE) [2], [3] notation was utilized to develop the assurance case. This is one of the notations defined in IEC/IEEE 15026-02 [4]. The assurance case (as of draft E of NEI 20-07) is shown in Figure 1.

For this first of a kind approach, not only did the logic of the argument have to be developed but also the methodology for using the assurance case needed to be identified. The methodology that was developed divided the assurance case into three tiers. Tiers 1 and 2 address the four points that come from SRM-SECY-22-0076 and are intended to be generically approved by the US NRC so that they can be utilized for all instances of the use of the guidance. Tier 3 of the assurance case is intended to be developed specifically for each application, but the expectation is that this development will be simple in practice since tiers 1 & 2 will already be approved. For demonstration purposes, examples of what the tier 3 sections of the assurance case could look like have been developed using The Socrates – Assurance Case Editor [5] and are included as Figures 2, 3, 4, & 5.

The status of this effort is that the NEI needs to address the US NRC's comments and re-submit an updated draft for another review. The NEI's effort is currently delayed by logistical and external factors, such as a soon to be released revisions to EPRI guidance that the NEI 20-07 document depends on.

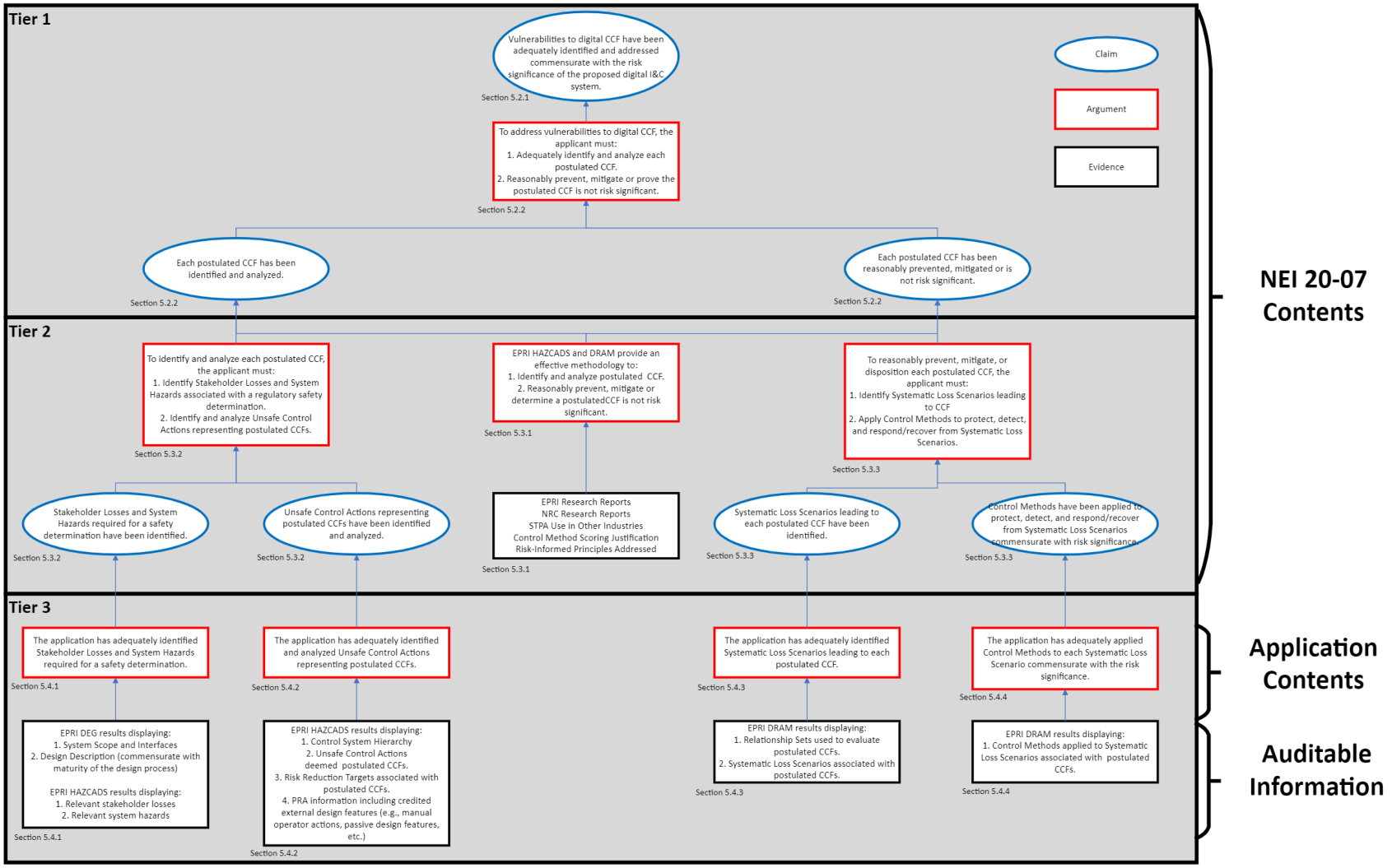

Figure 1. Assurance Case from NEI 20-07 Revision 0 Draft E.

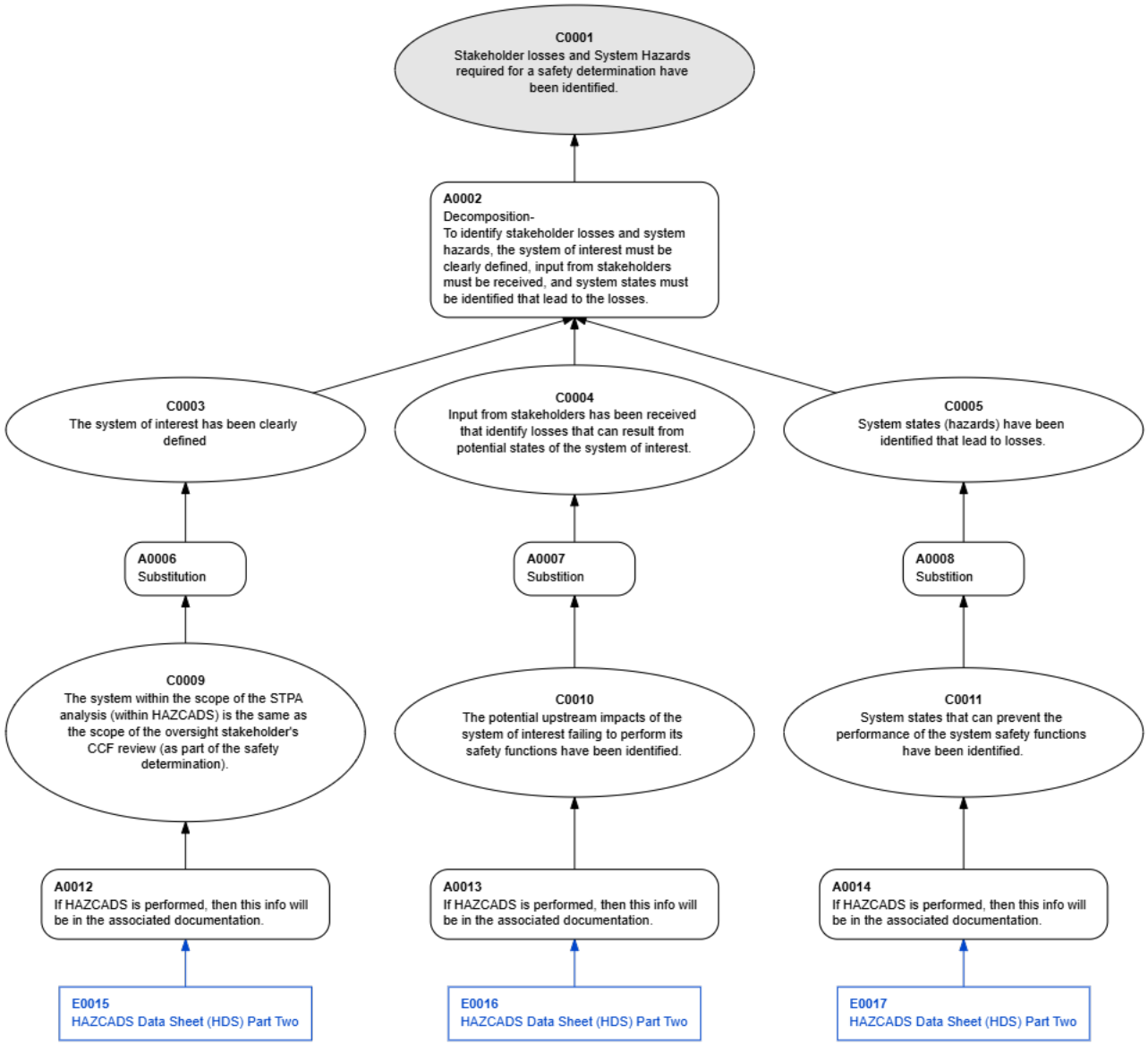

Figure 2. Example of Tier 3 Assurance Case for Tier 2 Sub-claim 1.

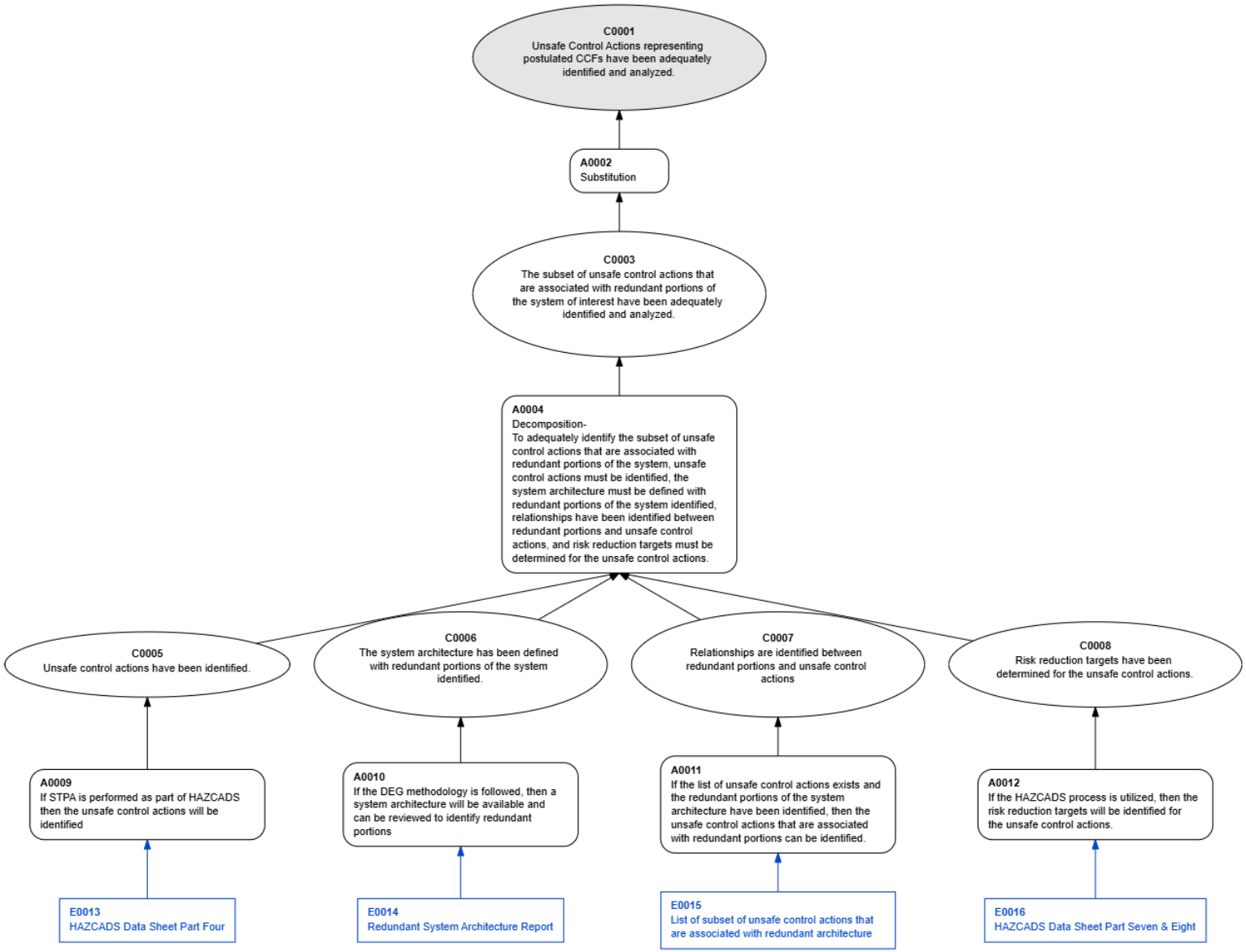

Figure 3. Example of Tier 3 Assurance Case for Tier 2 Sub-claim 2.

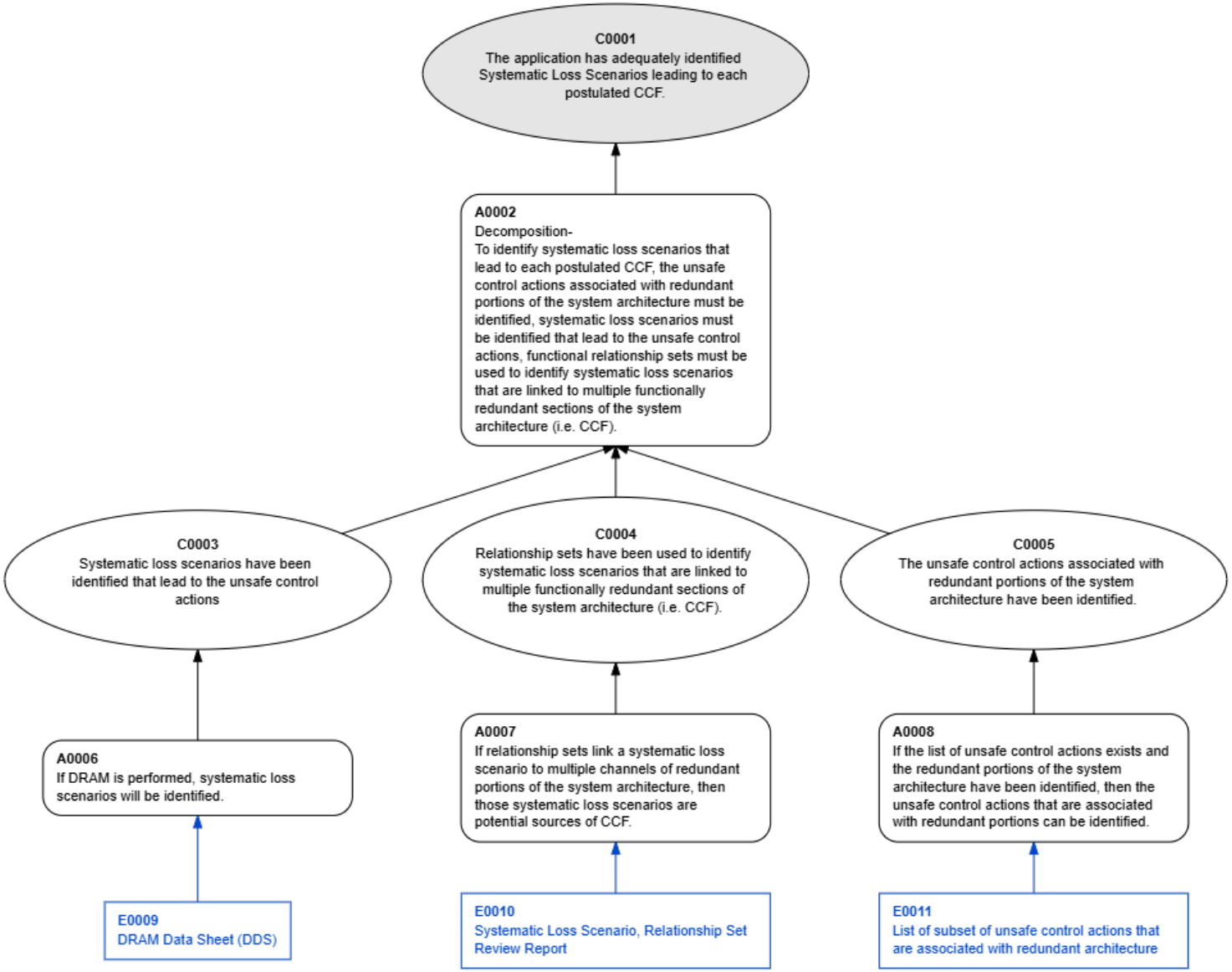

Figure 4. Example of Tier 3 Assurance Case for Tier 2 Sub-claim 3.

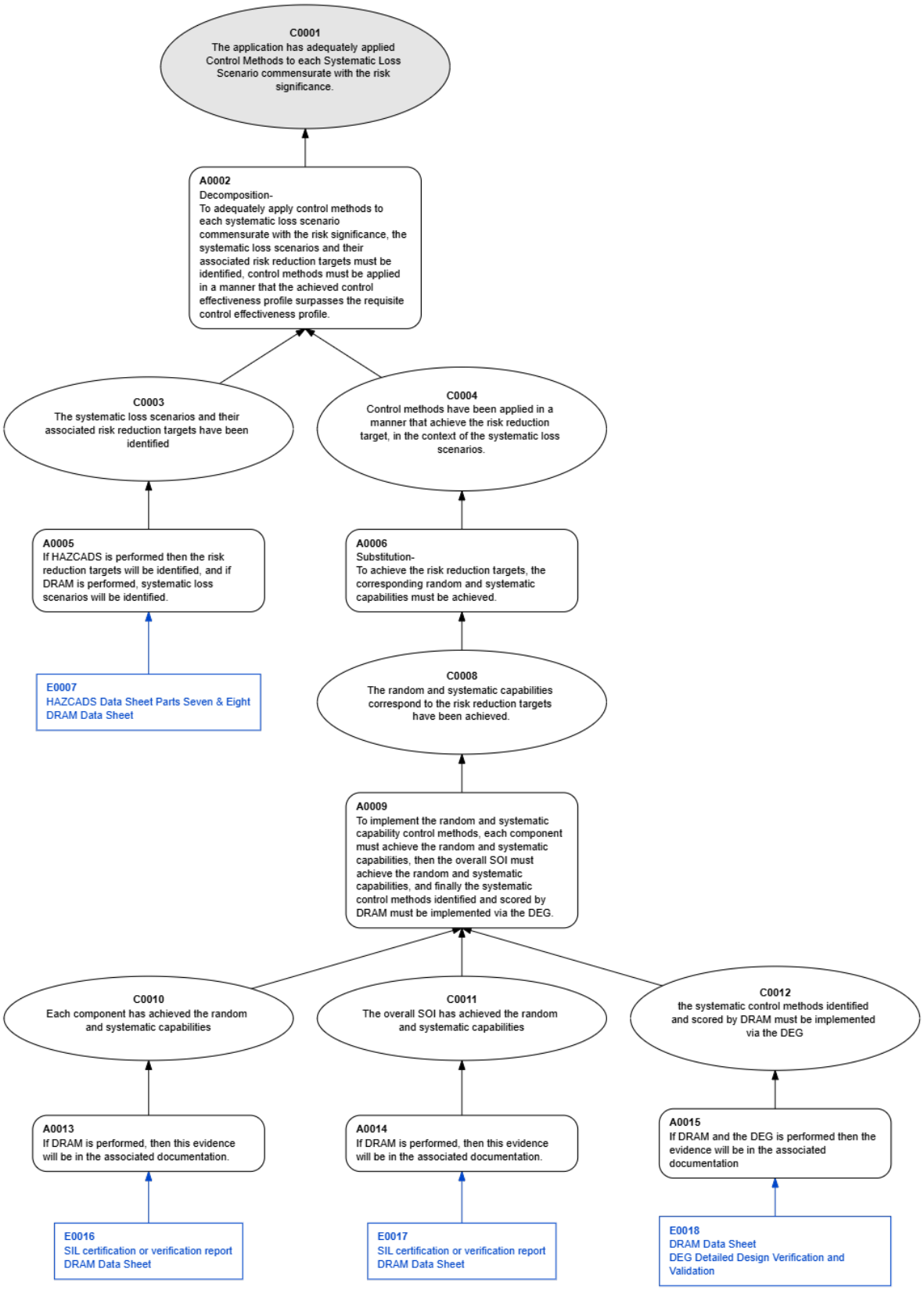

Figure 5. Example of Tier 3 Assurance Case for Tier 2 Sub-claim 4.

4. AN OPTION FOR NEXT STEPS

Since the NEI is delayed by external factors in starting the next engagement with the NRC, there is an opportunity to take a step back and evaluate if there is a way to utilize the developed assurance case to facilitate a novel approach to interacting with the NRC to improve the process of achieving approval. Up to this point, the approach has been for the NEI to develop a case and then submit it to the NRC. Maybe there would be benefit from engagement with the NRC to further refine the assurance case in joint meetings.

Using structured argumentation, expressed through CAE or similar notations such as GSN or EA, provides an opportunity for stakeholders such as the NRC to review a concise, evidence-based, argument about the safety of a system. The templates proposed in NEI 20-07 provide a starting point for such an argument. However, additional dialogue between stakeholders is required to establish that the argument(s) in NEI 20-07, if fulfilled by a license applicant, are sufficient to demonstrate that safety-critical functions in a nuclear system are acceptable for use. This additional dialogue should focus on both the depth ("is enough technical detail elicited in the template?") and breadth ("have all relevant topics been considered in the argument?") of the argument template.

The Eliminative Argumentation (EA) method may be used to facilitate dialogue between stakeholders. EA is a method of building safety arguments that uses "doubt" to drive critical thinking [6]. EA has been used to prepare safety case arguments in several industries [7], [8], including nuclear control systems for the CERN Large Hadron Collider [9]. Importantly, the expression of doubt in the EA method helps to mitigate confirmation biases due to authors of the safety case selecting only evidence that supports the overall safety claim they wish to "prove".

Using the EA method, authors or reviewers of a safety case capture doubts in the case as "defeaters" in the argument or about the supporting evidence. Once defeaters are identified, there are three potential avenues. First, further argumentation or evidence may be provided in the argument template to resolve the defeaters, with the potential for new defeaters to be introduced in the process. Defeaters that are resolved at this level may be either entirely removed or left in the argument, but "struck out" to denote they were considered and resolved. Second, defeaters that remain unresolved are marked as "residual" and must be accepted by stakeholders as contributing to the overall doubt in the safety argument. Finally, defeaters might reveal gaps in information that cannot be addressed at the level of a generic argument pattern or template, and so addressing those defeaters may be deferred to the creation of the concrete safety argument by license applicants.

In practical terms, tool support for performing the EA method is important, especially when working with multiple stakeholders. Such a tool must be collaborative in nature, provide features for applying the EA method, provide features for decomposing complex argument structures, allow for multiple stakeholders to concurrently access the safety case argument, provide support for patterns or templates, and be usable by a wide range of users with different levels of expertise in structured methods for describing safety cases. The Socrates – Assurance Case Editor [5] product provides these, and other features, that would allow the NEI and NRC to engage in a collaborative dialogue, using the EA methodology, to further develop the patterns described in NEI 20-07.

5. CONCLUSION

At this point, the NEI supports this plan of action. After the NRC has a chance to become more familiar with the technical details of the underlining methodologies involved with NEI 20-07, plans will be made to organize an interaction as recommended by this paper. This is expected to occur during the second half of 2025.

REFERENCES

[1] R. Alvarado and S. A. Arndt, "MODERNIZING APPROCHES TO ADDRESS COMMON CAUSE FAILURE IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS".

[2] Adelard (Firm), *ASCAD /az-kad : Adelard safety case development manual.* Adelard, 1998.

[3] R. Bloomfield and J. Rushby, "Assurance 2.0: A Manifesto," Jan. 14, 2021, *arXiv*: arXiv:2004.10474. doi: 10.48550/arXiv.2004.10474.

[4] "ISO/IEC/IEEE International Standard - Systems and software engineering–Systems and software assurance–Part 2: Assurance case," *ISOIECIEEE 15026-22022E*, pp. 1–30, Nov. 2022, doi: 10.1109/IEEESTD.2022.9938452.

[5] "Socrates – Critical Systems Labs." Accessed: May 10, 2024. [Online]. Available: https://criticalsystemslabs.com/socrates/

[6] J. B. Goodenough, C. B. Weinstock, and A. Z. Klein, "Eliminative Argumentation: A Basis for Arguing Confidence in System Properties." Accessed: Feb. 06, 2025. [Online]. Available: https://insights.sei.cmu.edu/library/eliminative-argumentation-a-basis-for-arguing-confidence-in-system-properties/

[7] S. Diemert and J. Joyce, "Eliminative Argumentation for Arguing System Safety - A Practitioner's Experience," in *2020 IEEE International Systems Conference (SysCon)*, Aug. 2020, pp. 1–7. doi: 10.1109/SysCon47679.2020.9275852.

[8] C. Hobbs, S. Diemert, and J. Joyce, "Driving the Development Process from the Safety Case," 2024, Accessed: Feb. 06, 2025. [Online]. Available: https://criticalsystemslabs.com/resources-hub/2024SCSCHobbs/2024SCSCHobbs.pdf

[9] L. Millet *et al.*, "Assurance Case Arguments in the Large: The CERN LHC Machine Protection System," in *Computer Safety, Reliability, and Security*, Springer, Cham, 2023, pp. 3–10. doi: 10.1007/978-3-031-40923-3_1.