INL/CON-25-87368

October 14, 2025

Sophia Zhu
Undergraduate Intern

Congjian Wang
Modeling/Simulation Professional

Jisuk Kim
Computational Scientist

Safety Assurance of Software and ML Development for Nuclear Instrumentation and Controls

For the 2025 San Diego Undergraduate Tech Conference

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

Introduction

- Nuclear power plants are safety-critical
- Instrumentation and control (I&C) equipment monitors and controls reactor processes
  - Shift to digital (DI&C)
- Challenges with software:
  - Complex — cannot test every case [1]
  - ML & AI introduce uncertainty [2]
- Focus on having a high-quality process of developing the software [1]

Approaches to Safety Assurance

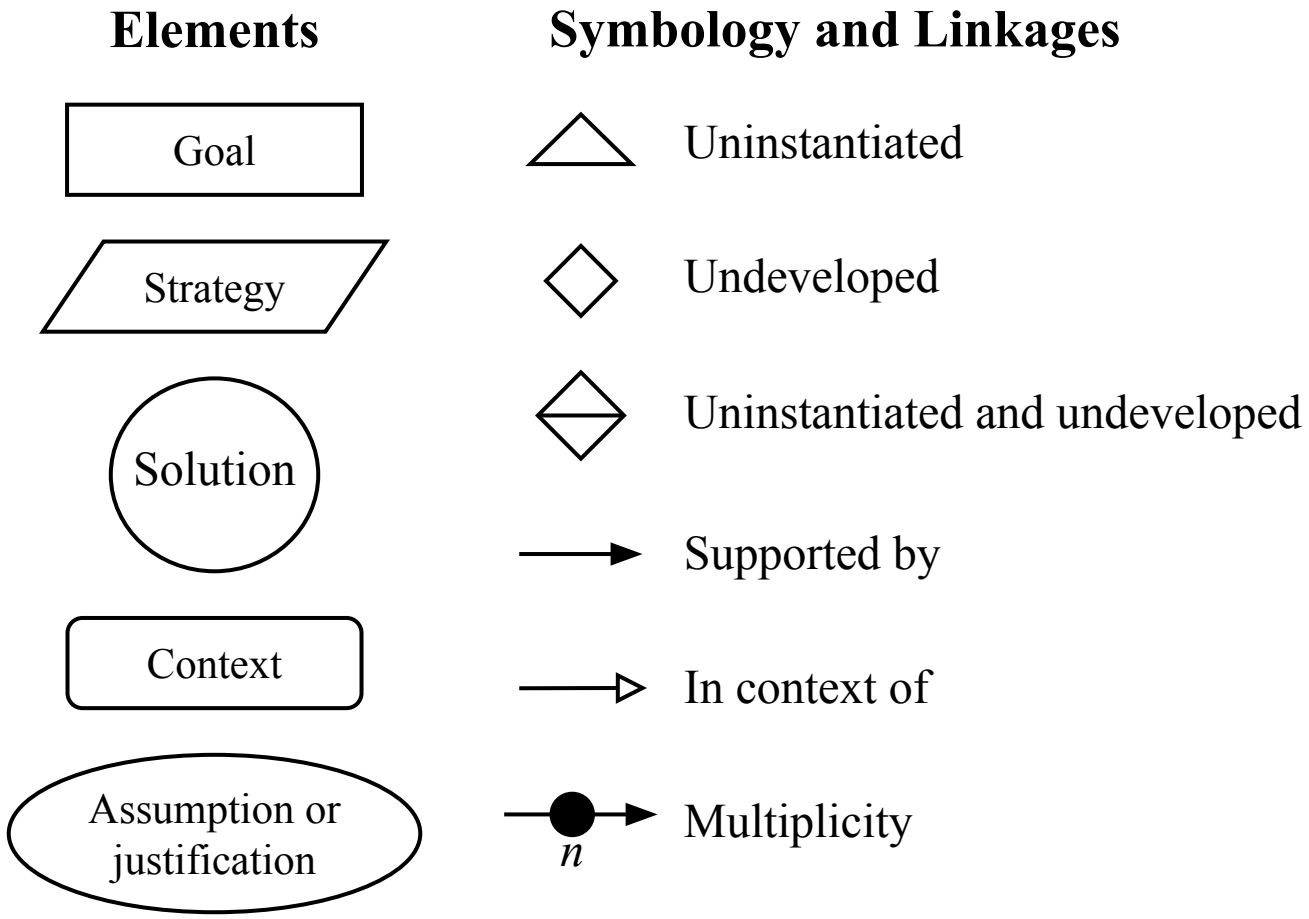
- Traditional U.S. NRC approach
  - Applicants submit hundreds of documents demonstrating safety of their reactor design
- Alternative: Safety assurance case (SAC)
  - Structured safety argument with supporting evidence [3]
  - Argument can be illustrated using diagram [3]

Research Objectives

- Identify software-related safety arguments through literature survey
  - Research papers
  - NRC regulations
  - IEEE and IEC standards
- Generate a SAC framework for DI&C software
  - Illustrate using Goal Structuring Notation (GSN)

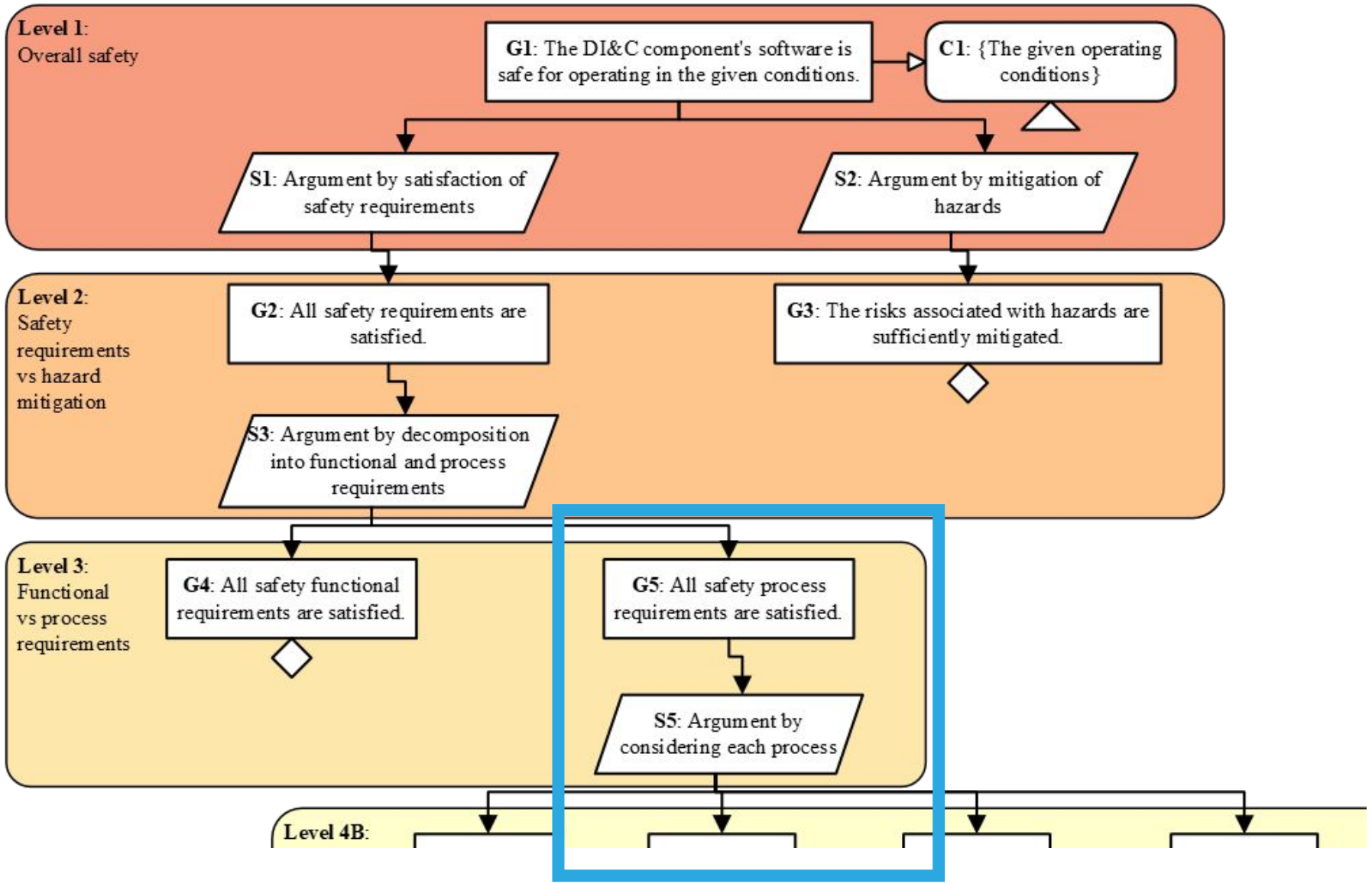
GSN Symbology

From the GSN Community Standard [4]



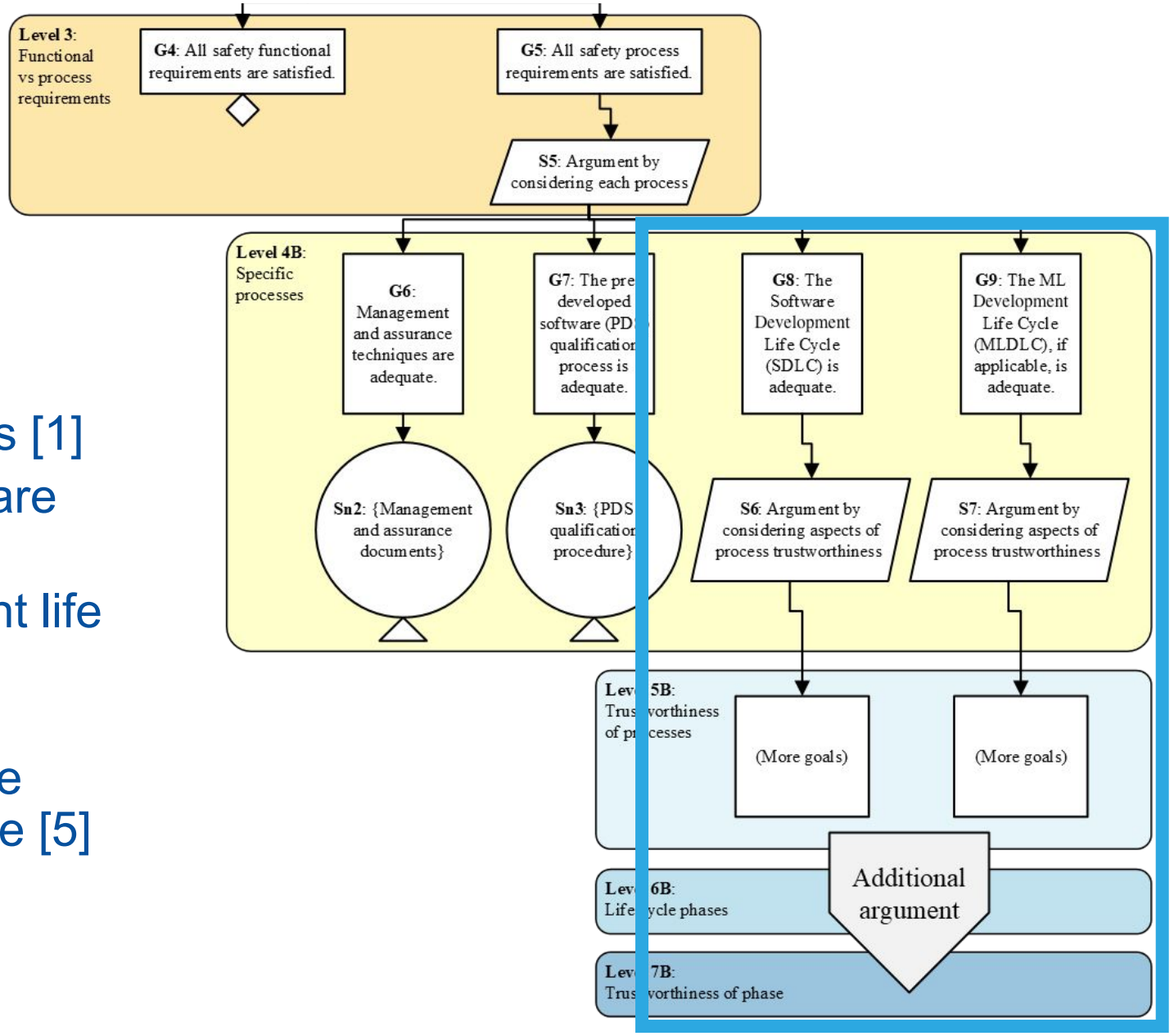
Upper Levels of Framework

- Every 2 rows forms a level
- Focus on G5: safety process requirements



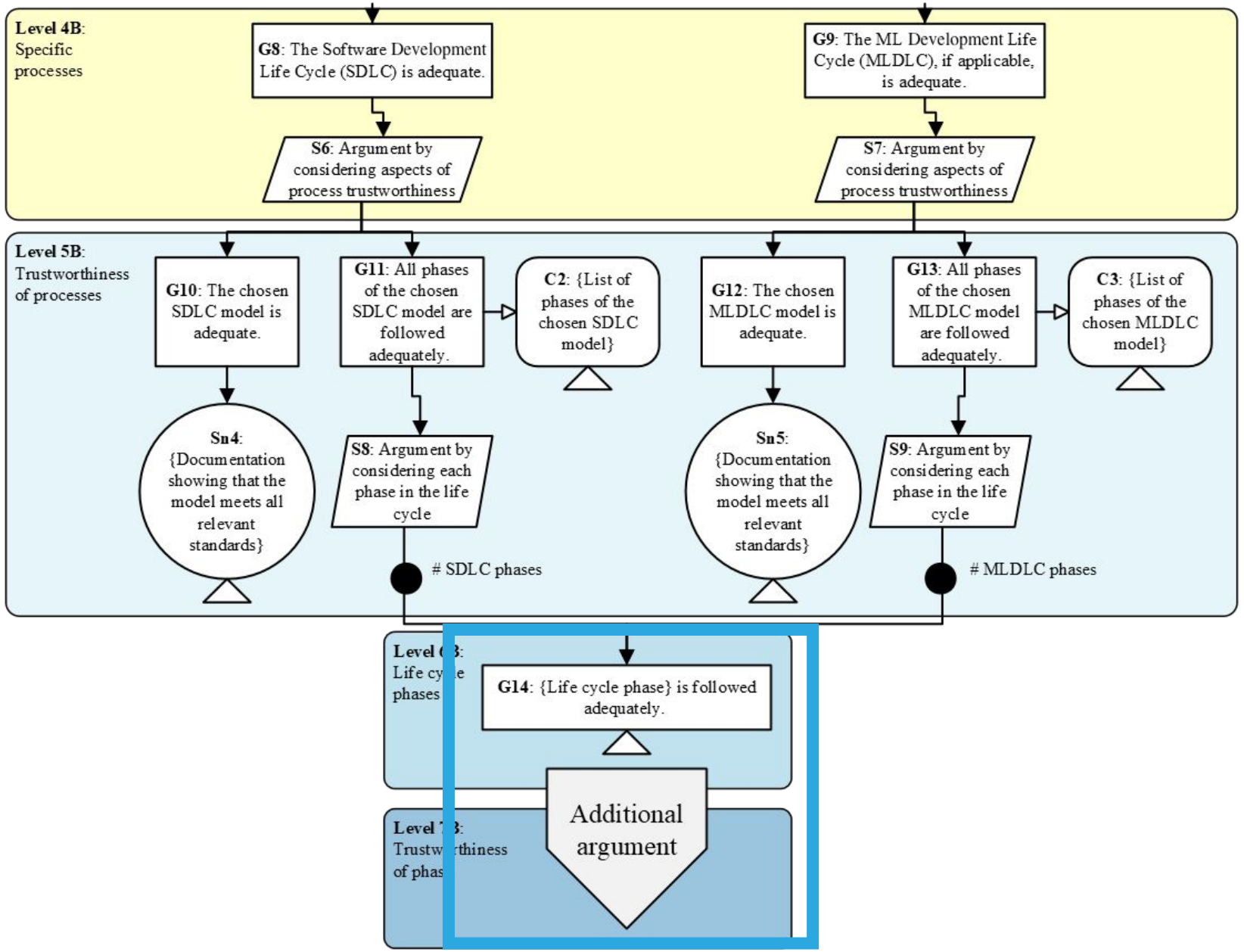
Lower Levels of Framework

- Identified four main processes
  - Management and assurance techniques [1]
  - Pre-developed software qualification [1]
  - Software development life cycle (SDLC) [1]
  - Machine learning development life cycle (MLDLC), if applicable [5]



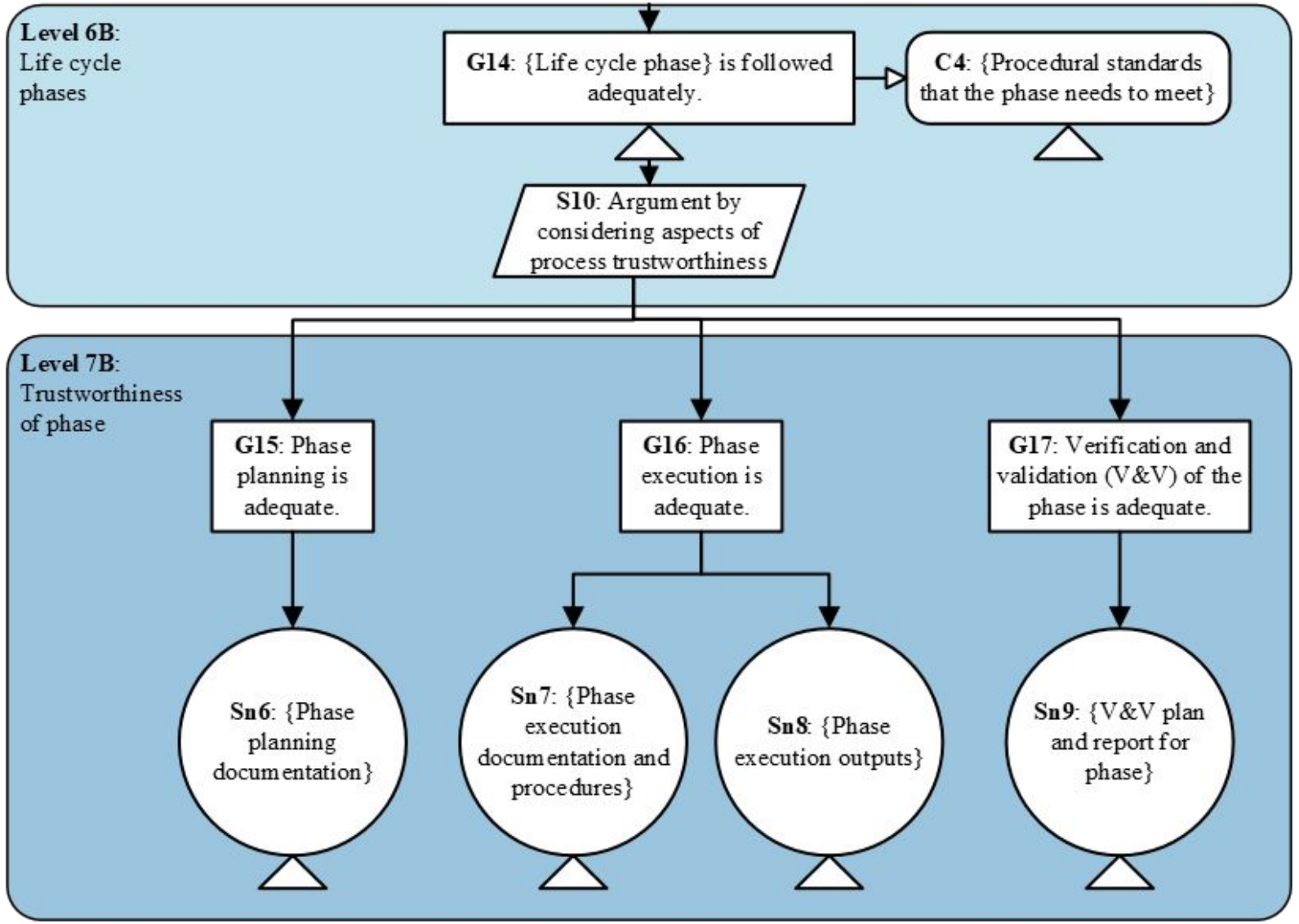
Development Life Cycles (Software and Machine Learning)

- Must select suitable development life cycle model and follow all phases adequately [6]



Life Cycle Phase

- Demonstrate each life cycle phase is adequately followed
- Involves proper planning, execution, and verification & validation (V&V) [7]



Conclusion and Future Work

- Our framework organizes safety assurance arguments for software development processes in DI&C components.
- Work in progress
  - Developing the rest of the SAC framework (functional requirements, hazard mitigation branches)
  - Conducting a case study on the APR 1400 reactor

References

[1] Nuclear Regulatory Commission, “Appendix 7.0-A: Review Process for Digital Instrumentation and Control Systems,” in *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition*, NUREG-0800, Aug. 2016. [Online]. Available: https://www.nrc.gov/docs/ML1601/ML16019A085.pdf

[2] H.-Y. Hsieh and P. Tsvetkov, “Advancements and challenges of machine learning and deep learning in autonomous control of nuclear reactors,” *Annals of Nuclear Energy*, vol. 223, p. 111643, Dec. 2025, doi: 10.1016/j.anucene.2025.111643.

[3] M. Sivakumar et al., “The Last Decade in Review: Tracing the Evolution of Safety Assurance Cases through a Comprehensive Bibliometric Analysis.” arXiv, Nov. 13, 2023. doi: 10.48550/arXiv.2311.07495. [Online]. Available: http://arxiv.org/abs/2311.07495

[4] *GSN Community Standard*, Version 3, The Assurance Case Working Group, England, May 2021. [Online]. Available: https://scsc.uk/index.php/gsn-standard

[5] C. Paterson, R. Hawkins, C. Picardi, Y. Jia, R. Calinescu, and I. Habli, “Safety assurance of Machine Learning for autonomous systems,” *Reliability Engineering & System Safety*, vol. 264, p. 111311, Dec. 2025, doi: 10.1016/j.ress.2025.111311. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832025005125

[6] *IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations*, IEEE 7-4.3.2, Aug. 2016, doi: 10.1109/IEEESTD.2016.7552419.

[7] R. Youngblood III, H. Everett, and H. Dezfuli, “Application of Objectives-Drive Assurance Cases to System Development in an Evolving Acquisition Model,” Oct. 2022. [Online]. Available: https://www.osti.gov/biblio/2403507

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.