INL/CON-25-87368

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

Sophia Zhu[1, 2], Congjian Wang[1], Jisuk Kim[1]

[1] Idaho National Laboratory, [2] University of California San Diego

Abstract

Digital instrumentation and control (DI&C) systems monitor and control parameters in nuclear power plants. Ensuring their safety is a critical part of ensuring overall plant safety. Nuclear power plant licensing generates thousands of safety documents that could be organized more effectively using a safety assurance case (SAC). We conducted a literature survey of SACs and created a SAC framework for DI&C software using Goal Structuring Notation (GSN). This framework focuses on four software development processes: management & assurance, pre-developed software (PDS) qualification, the Software Development Life Cycle (SDLC), and the Machine Learning Development Life Cycle (MLDLC). We organized our framework using a novel level structure that can be applied to other SACs to improve their clarity. Finally, we demonstrate how our framework can be incorporated as part of a SAC for a larger reactor system.

Objectives

- To organize safety arguments from the literature, U.S. Nuclear Regulatory Commission documents, and international standards
- To develop a SAC framework for DI&C software that is adaptable to any SDLC or MLDLC model

Safety Assurance Cases

- A SAC is a structured argument to demonstrate a product's safety to stakeholders [1, 2]
- **Functional** requirements: the system **performs required functions** [3]
- **Process** requirements: **quality of the system development** process [3]
- Software is complex – cannot ensure safety through test cases alone [3]
- Machine learning (ML) techniques can introduce even more uncertainty and complexity [4]
- Hence, process requirements are the focus of this framework (Goal G5)

Development Life Cycles

- The SDLC (G9) and MLDLC (G10) are a list of phases with defined activities.

Example SDLC model [5]

1	Conceptual design
2	System requirements
3	Detailed system design
4	Implementation
5	Testing
6	Installation & site acceptance testing
7	Operations & maintenance
8	Retirement

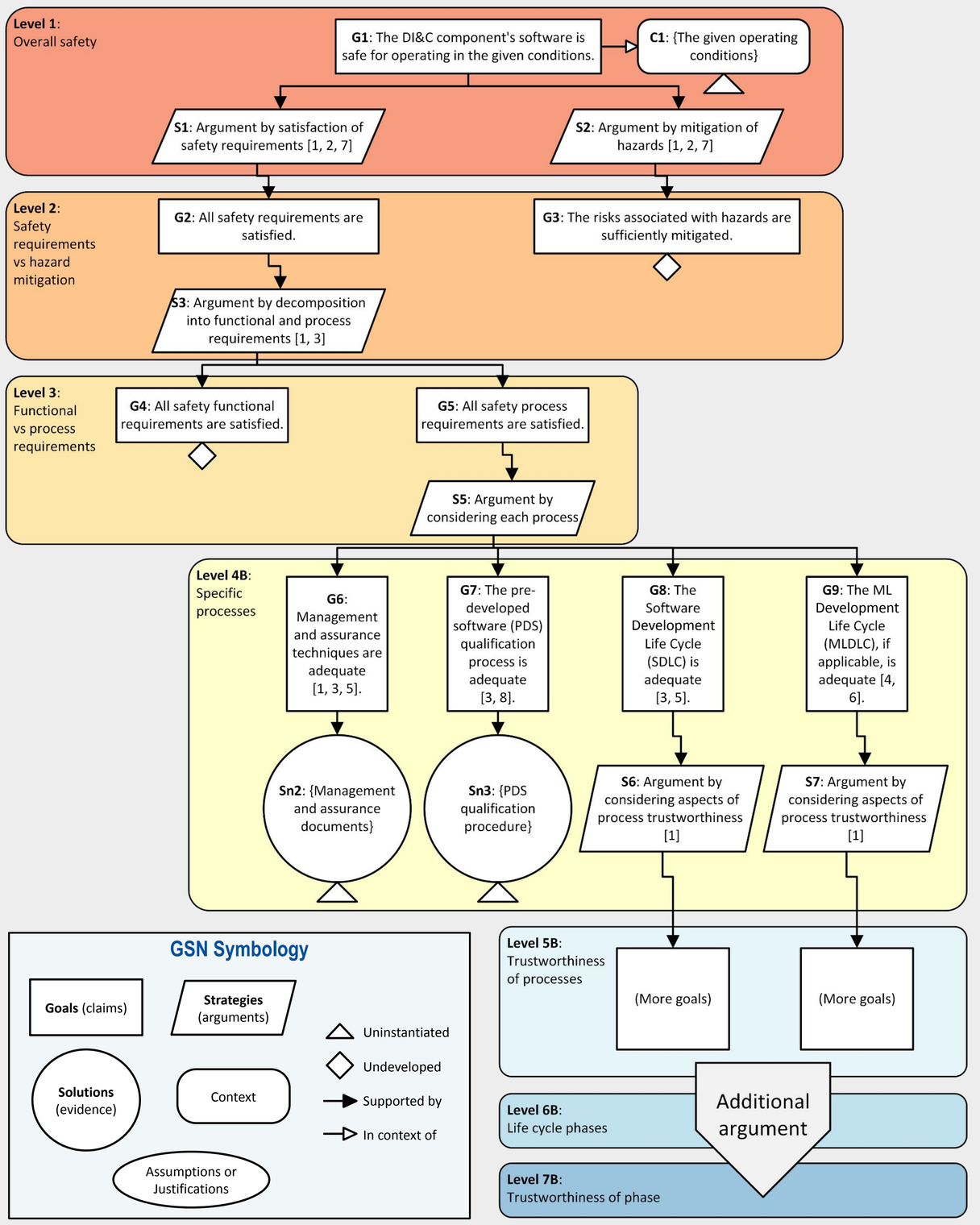
Example MLDLC model [6]

1	ML safety assurance scoping
2	ML requirements
3	Data management
4	Model learning
5	Model verification
6	Model deployment

Conclusion & Future Work

- **Conclusion**: We have developed a SAC framework for DI&C software and introduced a classification of levels to increase clarity and organization for safety management.
- **Future work**: Develop additional branches of the framework and demonstrate its usage via a case study on the Core Protection Calculator System of the APR1400's reactor trip system.

Proposed SAC Framework Overview



References

[1] I. Habli and T. Kelly, "Process and Product Certification Arguments: Getting the Balance Right," *SIGBED Rev.*, vol. 3, no. 4, pp. 1–8, Oct. 2006, doi: 10.1145/1183088.1183090.

[2] D. Rinehart, J. Knight, and J. Rowanhill, "Current Practices in Constructing and Evaluating Assurance Cases With Applications to Aviation," NASA, Jan. 2015. [Online]. Available: https://ntrs.nasa.gov/api/citations/20150002819/downloads/20150002819.pdf

[3] 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

[4] 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.

[5] *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.

[6] 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.

[7] K.-C. Kwon, J.-S. Lee, and E. Jee, "A Framework for the Safety Assurance of Safety Software in Nuclear Power Plants," Gyeongju, Korea, Nov. 2017. [Online]. Available: https://www.kns.org/files/int_paper/paper/ISOFIC_2017_10/ISOFIC-2017-Kee-Choon-KWON.pdf

[8] *Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Software Aspects for Computer-Based Systems Performing Category A Functions*, IEC 60880, 2006.