Report No. DOE-SG-13808

Security Hardened Cyber Components for Nuclear Power Plants

Phase I SBIR Final Technical Report

Grant No. DE-SC0013808
US Department of Energy
Office of Science, Chicago Office

Michael D. Franusich, Principal Investigator
SpiralGen, Inc.
201 S. Craig St., Suite 2E
Pittsburgh, PA 15213

March 18, 2016

Abstract: SpiralGen, Inc. built a proof-of-concept toolkit for enhancing the cyber security of nuclear power plants and other critical infrastructure with high-assurance instrumentation and control code. The toolkit is based on technology from the DARPA High-Assurance Cyber Military Systems (HACMS) program, which has focused on applying the science of formal methods to the formidable set of problems involved in securing cyber physical systems. The primary challenges beyond HACMS in developing this toolkit were to make the new technology usable by control system engineers and compatible with the regulatory and commercial constraints of the nuclear power industry. The toolkit, packaged as a Simulink add-on, allows a system designer to assemble a high-assurance component from formally specified and proven blocks and generate provably correct control and monitor code for that subsystem.

TABLE OF CONTENTS

LIST OF FIGURES

1 EXECUTIVE SUMMARY

Along with the alarming growth and magnitude of cybersecurity incidents there has been a rapid growth in technology and focus in response; however, the bulk of the focus has been on securing Information Technology (IT) systems and less so on the digital systems that control cyber-physical systems (CPS), such as power plants, refineries, and modern vehicles. A common belief is that IT cybersecurity strategies are effective for CPS security, but that has proven to be a weak assumption for several reasons, including the vast differences in system architectures and use, the different classes of attack surfaces, and goals and nature of attacks and failures. The risk to an IT system is primarily monetary, through loss of data or access, but the risk to a power plant additionally involves safety, including massive damage and large scale loss of life. Nuclear power plants (NPP) are an inviting target to some attackers, and they are particularly difficult to defend, with their intricate and sometimes arcane control systems spanning potentially decades of technical upgrades, the regulatory and business constraints, and the quantity and variety of potential attack surfaces and failure modes. Combining traditional IT cybersecurity with new CPS-focused security is a promising approach.

In 2015 SpiralGen, Inc., a Pittsburgh, PA company, was awarded a Phase I SBIR grant, DE-SC0013808, to investigate the applicability of technology from an ongoing DARPA program for NPP cybersecurity. The DARPA High-Assurance Cyber Military Systems (HACMS) program has been developing formal methods-based technology for designing and building safe and secure control code, with an emphasis on autonomous ground and air vehicles. As part of the HACMS program, SpiralGen, along with researchers from Carnegie Mellon University, have been extending the Spiral code generator from its original focus on high-performance math code to high-assurance control code. For the Department of Energy SBIR project, the main goal was to develop a prototype toolkit that control system engineers could use to build high-assurance NPP control software. The toolkit had to bridge the gap between the complexity of the new formal methods technology and its practical application in a production setting.

The two key pieces underlying the new toolkit are the KeYmaera X theorem prover for cyber-physical systems and the Spiral code generator. KeYmaera X proves a formal specification of a system and generates input for Spiral to produce a correct implementation of that system. Formally specifying and proving a real system requires a high level of training and a lot of time, which has been a major impediment to widespread adaption of this methodology. SpiralGen's toolkit tackles this problem by breaking down system specification and proof into small pieces that can be composed into a larger specification, with the proof of the larger system being a byproduct of the composition. The toolkit is packaged as a Simulink add-on that a designer can use to add high-assurance components to a larger design and generate both monitor and control code. A demonstration feedwater subsystem shows toolkit components detecting various anomalies in feedwater flow, condensate flow, and tank level indications. The proof-of-concept toolkit and demonstration have already spurred some strong interest and positive feedback from potential early adapters.

2 ACKNOWLEDGEMENTS

The author would like to thank the SpiralGen, Inc. team: Franz Franchetti, Jane Opgaard, Brian Duff, and Jason Larkin for their contributions, along with CMU researchers Tze Meng Low and André Platzer for their expert advice. Bill Mills and Ray Thomas from Nuclear Energy Consultants, Inc. provided essential domain-specific information needed to shape the project. Mike Bradley, Will Lutz, and Thad Welch helped greatly with the final toolkit tuning from their dual perspective of engineers who have also operated reactors.

3 INTRODUCTION

NPP Cybersecurity. Nuclear power plants (NPP), a crucial fifth of the United States' electricity supply, have for decades been a popular *bogeyman* of various activist groups, film and television thrillers, and the media. With the increase in high profile cybercrime incidents, storylines containing shadowy evil genius hackers threatening massive damage to NPPs have become almost *cliché*. Nevertheless, though not necessarily in the form portrayed in popular fiction, cybersecurity is a serious and ongoing concern for NPPs and other critical infrastructure. Power plants are *cyber-physical systems* (CPS), where the physical processes are monitored and controlled by the cyber components, and where the cybersecurity concerns are more about safety and continued operation than about privacy and data integrity [Weiss 2010]. The term *cybersecurity*, for the purposes of this discussion, has a broad meaning that encompasses all aspects of assuring that the cyber assets of a system perform safely and as expected. In an NPP this includes the traditional information technology (IT) security focus of defending against and responding to external attacks and malware, but it also pertains to such things as malfunctioning field devices, degraded circuits, algorithmic errors, and many other attack or failure modes that are typically beyond the view of IT security. As shown in Figure 1, the focus of this project is the inner layers of an NPP's control system. Problems that elude the outer security layers are the problems of interest.

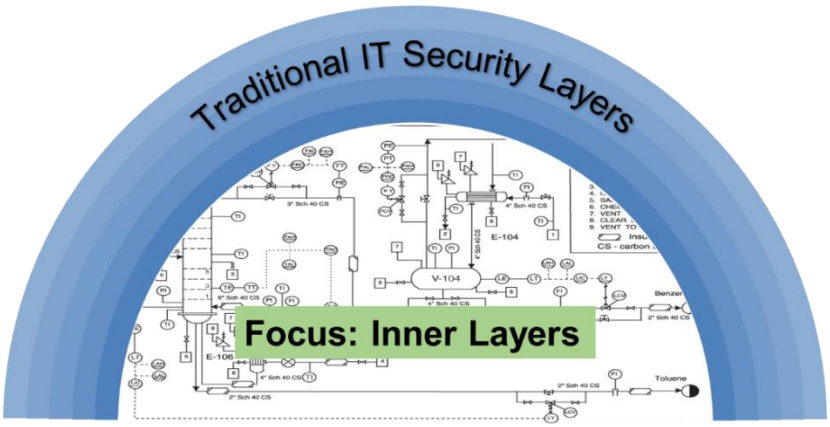

Figure 1. Focus is on Inner Layers. The outer layers handle network attacks and other known malicious behaviors. Stealthy attacks that penetrate the outer layers and other "unknown unknowns" require additional technology and strategies.

Formal Methods. The difficulty and inherent complexity in developing software is not a new topic [Brooks 1975], and this difficulty is a central factor in why it is cybersecurity is such a struggle. The typical development cycle of write-test-fix carries over into the regular patch cycles for deployed software, but that approach is not acceptable for control systems. The science of *formal methods*, which seeks to produce error-free algorithms and code with mathematical modeling and automatic code generation, has been an area of study for decades [Dijkstra 1972], but has only enjoyed niche acceptance, with perceived cost and difficulty in learning being key reasons for its slow adoption. In 2012, the Defense Advanced Research Projects Agency (DARPA) began the High-Assurance Cyber Military Systems (HACMS) program to find practical ways to apply formal methods to the cyber assurance gaps in CPSs, with emphasis on

unmanned ground and aerial vehicles. The HACMS research forms the basis for this project's technological contributions to NPP cybersecurity.

Project vision. The high level question behind this project is, "Does the formal methods technology advanced by the HACMS program have a practical application to NPPs?" The assumption behind this project is that the answer is "yes", provided that typical system designers can use the new technology without major disruption and if there is a way to deploy the products of the technology into an existing NPP within regulatory and commercial constraints. The concept of the project is to break down typical NPP control system components into small configurable modules, with the difficult formal specifications and proofs already built into those modules, which the designer can assemble and configure, then automatically generate code for high-assurance cyber components. The products of this project are a prototype toolkit and demonstration subsystem showing an example of a high-assurance monitor.

4 METHODS, ASSUMPTIONS, AND PROCEDURES

Task List. To meet the stated project goal of demonstrating the practical applicability of HACMS technology in the context of NPP cybersecurity, the Phase I statement of work has four main tasks:

1. Define an appropriate subsystem
2. Build a test environment
3. Build a prototype toolkit
4. Build a demonstration model of the subsystem using components from the toolkit

The research and development process followed the statement of work in an iterative fashion, with overlap between items 2, 3, and 4. The model subsystem has examples of the three proposed high-assurance components, a PID controller, a monitor, and sensor fusion, which is part of the monitor.

Defining the subsystem. At the beginning of the project the SpiralGen team leaders met with a nuclear energy consultant to discuss the project and find a good target subsystem. The desired subsystem would be in the feedwater system of a typical pressurized water reactor (PWR) and would be central and dynamic enough to be interesting. The consultant suggested the deaerator storage tank (DAST), which is a typical feature in a lot of PWRs and fossil plants, forming the boundary between the condensate coming from the turbine and the feedwater heading to the steam generators (or boilers in fossil plants). Searching the Nuclear Regulatory Commission (NRC) ADAMS online database produced enough records of DAST-related events to confirm it was a good choice. The consultants proceeded to provide details of the subsystem instrumentation and control sufficient to begin building a simplified demonstration model.

Test environment. Simulink offered a good foundation for building a project test environment. It only required a few customizations, such as dialogs for injecting sensor errors. The bulk of the environment was configured from standard Simulink features. The widespread use of Simulink by control system designers also influenced its choice over other options, because the familiarity would likely aid acceptance of the eventual toolkit.

Prototype toolkit. The proof-of-concept toolkit, packaged as a Simulink add-on, evolved along with the test environment and demonstration subsystem. The PID controller and companion monitor blocks contain formal specifications and linkage for calling Spiral to generate code.

Demonstration. The demonstration of the running subsystem, detailed in Section 5, shows how the behavioral monitor can catch anomalies. Subject matter experts, typically engineers with reactor operation experience, helped improve the toolkit demonstration through its development. The alpha-level feedback contributed to realism, and beta-level feedback tuned up the general appearance.

4.1 TECHNOLOGICAL FOUNDATION

CMU tools. The foundation technology for this project is the CMU HACMS tool chain, as shown in Figure 2. The KeYmaera theorem prover and the Spiral code generator form the backbone that processes a formal specification to code [Fulton 2015] [Püschel 2005]. The initial version of the CMU tool chain requires a high level of expertise and training, particularly for specifying and proving hybrid systems.

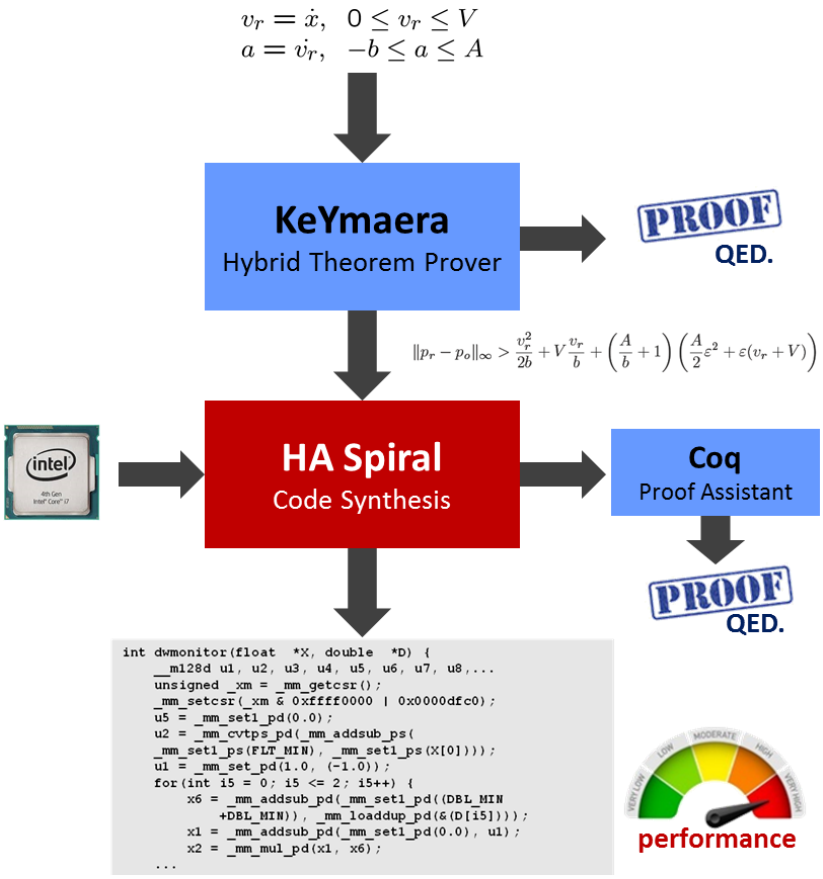

Figure 2. CMU HACMS Tool Chain. The KeYmaera theorem prover and the Spiral code generator form the backbone that maps a formal specification to code. The Coq proof assistant uses a code generation trace from Spiral to prove that the generated code correctly implements its specification.

Chain of evidence. Figure 3 illustrates the cascading chain of evidence produced at each step of transforming a specification to code. This could eventually become part of a process for certifying code from the tool chain.

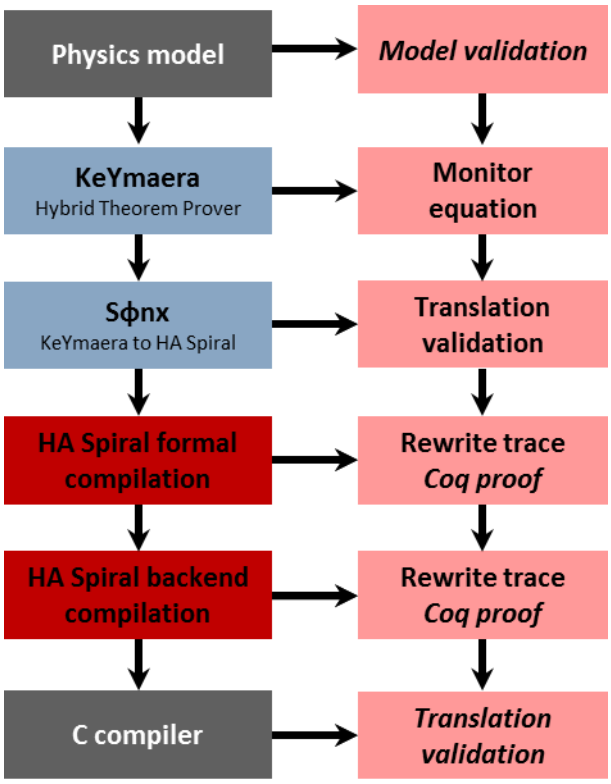

Figure 3. End-to-End Chain of Evidence. The left column shows the progression from specification to code through the subcomponents of KeYmaera and Spiral, and the right column shows the corresponding parts of the full proof and validation.

4.2 SPIRAL NPP TOOLKIT

Figure 4 is an overview of the project's approach and shows a monitor watching the deaerator tank subsystem. The volume of the tank must correlate with the net flow out and in.

Physics-based monitor. A feature of cyber-physical systems distinct from IT systems is that the laws of physics govern the behavior of the system. If the system appears to be doing something physically impossible, then there is a cyber-related problem. In the case of the deaerator tank subsystem, the physical *invariant* is that the relationship between flow out, flow in, and volume does not change regardless of flow rates, etc.

Proof composition. The ability to compose a complex formal specification and proof from smaller proven elements is what makes the Spiral NPP toolkit practical. The essence is that as long the guaranteed outputs of one block match the required inputs of another block, the two can combine into a proven composite. Code generated from the composite is also provably correct.

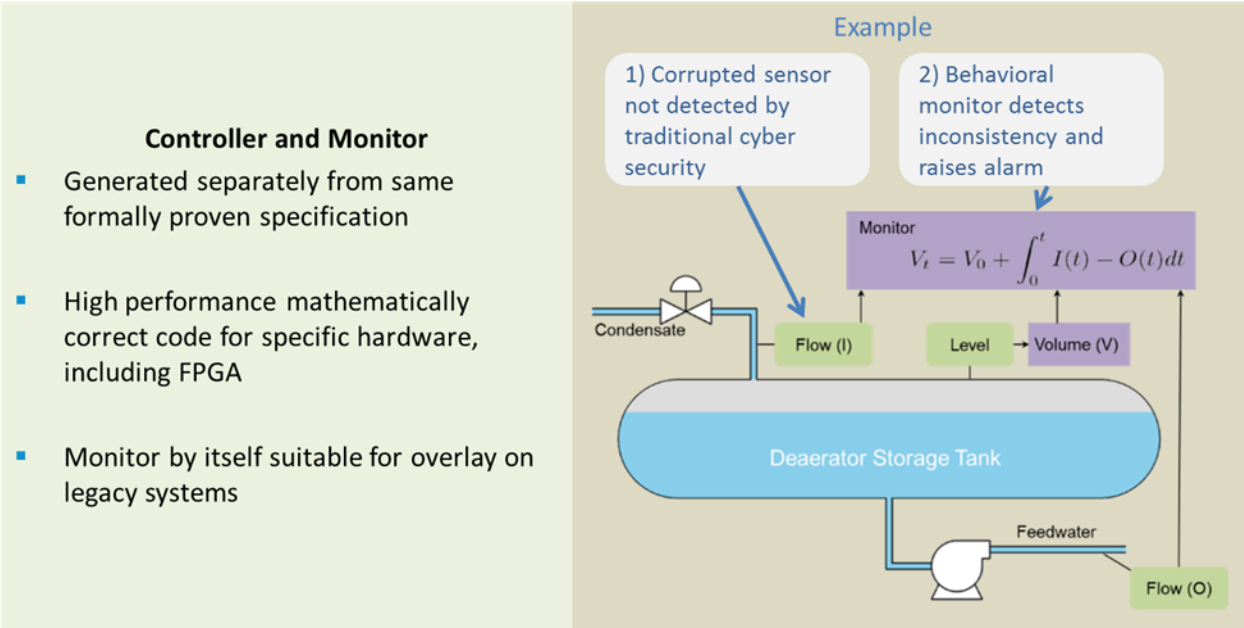

Figure 4. Overview of Project Approach. Formally specified, provably correct, behavioral monitor detects anomalies in the subsystem.

5 RESULTS AND DISCUSSION

5.1 DEMO WALK THROUGH

Figure 5 through Figure 10 are screen capture images from the toolkit demonstration. Side-by-side views show the key parameters as seen by the operator and control system along with a "ground truth" view of the tank that shows its actual level. Injecting an error into the tank level value causes the controller to let the tank level drop. When the monitor is running, it detects the problem and raises and alarm.

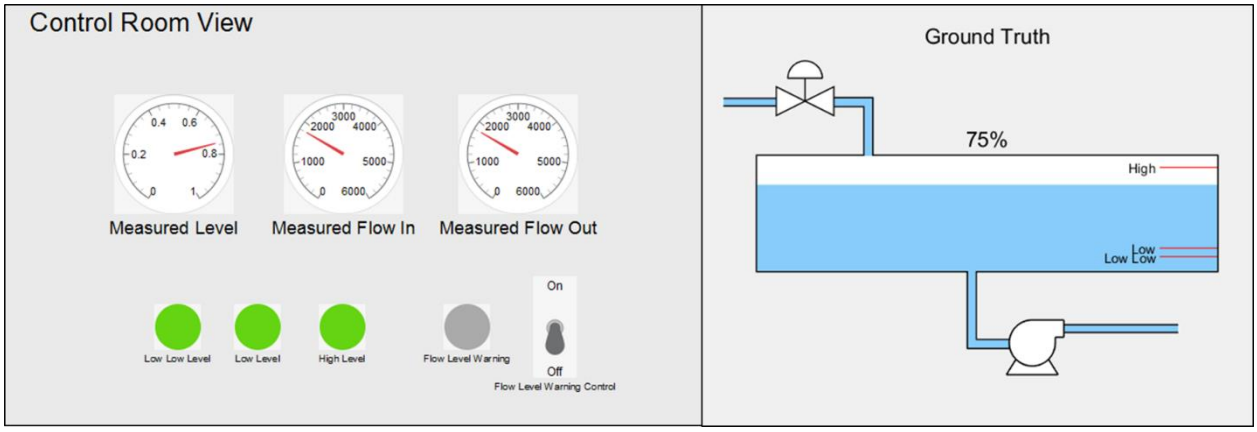

Figure 5. Control Room and Ground Truth Views. The control room view shows the measured/indicated values for the subsystem, and the ground truth view shows the actual tank level that is not seen by the operator or the control system. The red lines on the tank drawing are the setpoint levels for the three alarms.

.

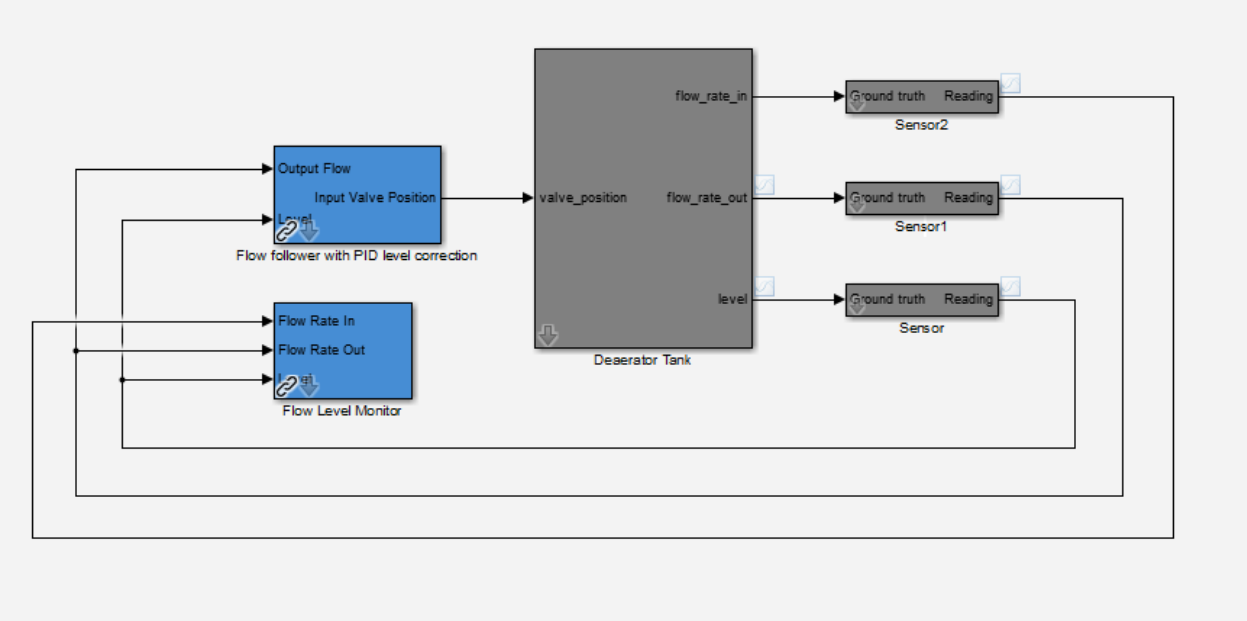

Figure 6. Simulink Model of Subsystem. The blue blocks are the PID controller and companion monitor from the SpiralGen toolkit, and the grey blocks are regular Simulink blocks.

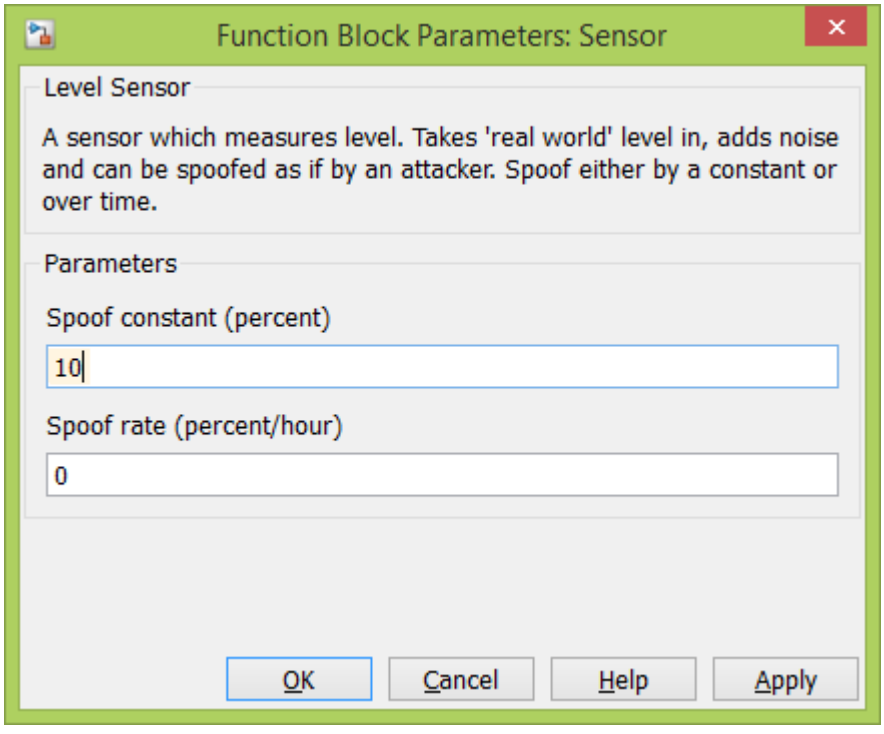

Figure 7. Sensor Spoof Dialog. A constant value simulates a calibration error, and a rate drifts the difference over time.

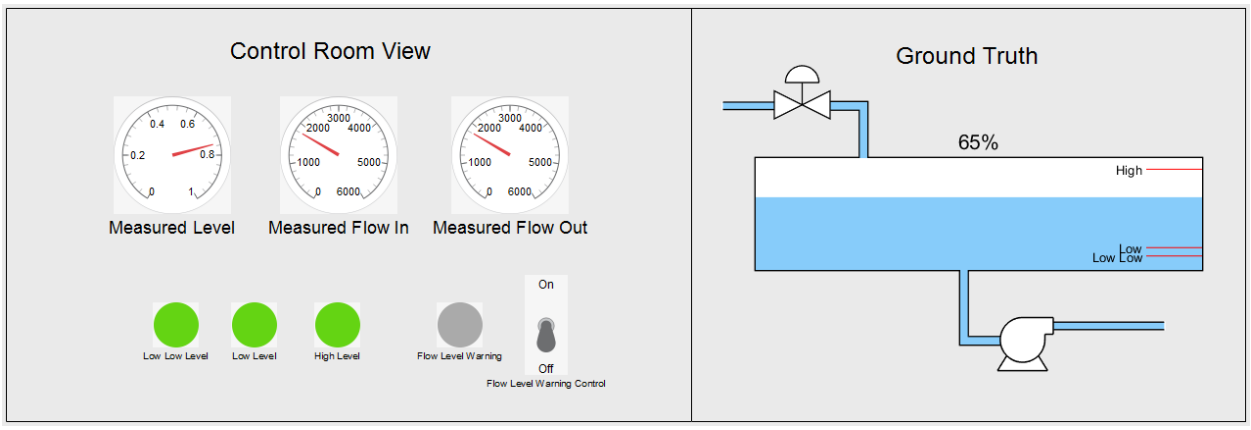

Figure 8. Level Drifted 10%, Monitor Not Running. Note the difference between the indicated tank level and the actual tank level. Also note that the monitor is toggled off. If a slowly developing inconsistency were discovered at this point, it's possible the problem could be resolved without tripping the plant.

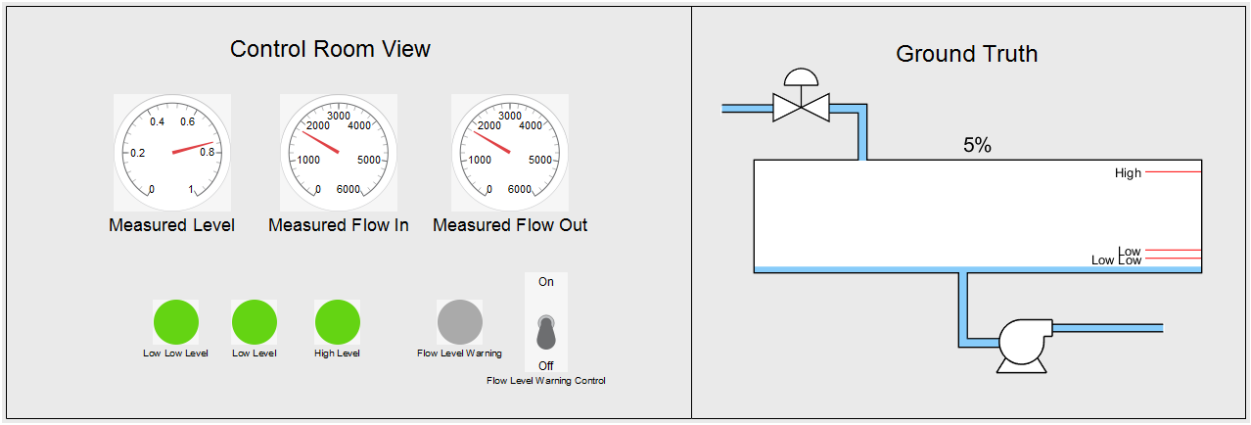

Figure 9. Tank Almost Empty, No Alarm. Under unspoofed conditions the feedwater pumps would have tripped from the tank low-low alarm, but here the control system is unaware of the actual level, allowing the feedwater pumps to be in imminent danger of damaging cavitation.

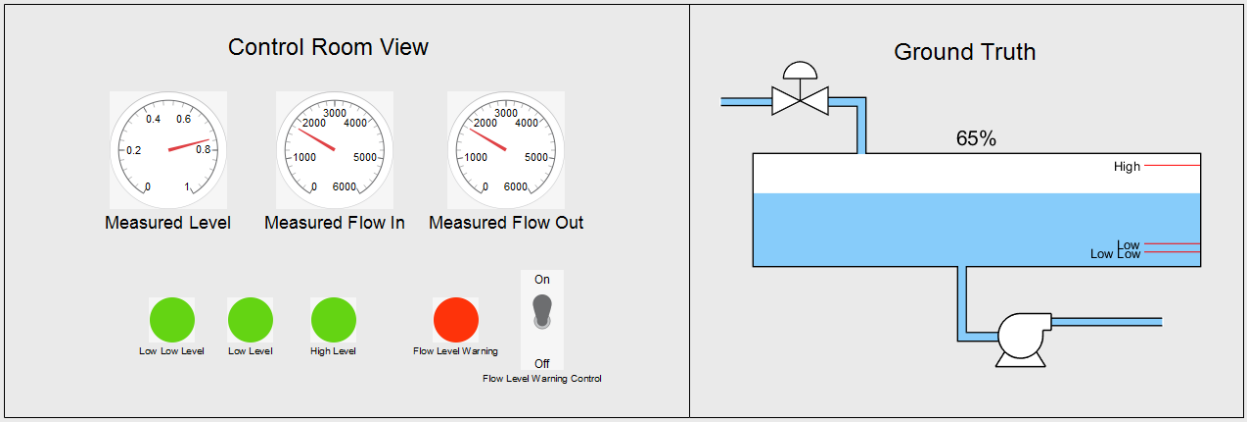

Figure 10. Monitor Detects 10% Inconsistency. Note the difference between the indicated tank level and the actual tank level. The toggle switch shows that the monitor is active, and the red alarm announces the inconsistency.

5.2 THOUGHTS ON DEPLOYMENT

10 CFR 50.59. For good reason new control hardware and software has to be thoroughly vetted before it ever sees the inside of an NPP, with the certification process often taking several years. There is no obvious short path to deploying new high-assurance controllers into a plant, no matter how much better the new technology. But there is a provision in the regulations, detailed in 10 CFR 50.59, that allows for rapid adoption of some new technology under specific constraints. High-assurance behavioral monitors that only watch and do not touch the controls should be allowable. A workable deployment strategy for the technology from this project would be to first get monitors in place and then put the new controllers into the qualification pipeline.

Alarm Response Procedures. Typical control system alarms tend to be specific, such as the low-low tank level alarm in the DAST model. An alarm from a behavioral monitor would likely be much less specific, along the lines of, “inconsistency in DAST subsystem”. It would be up to the operators to diagnose and ameliorate the problem. Writing good alarm response procedures for the behavioral alarms would be a key part of successful deployment.

6 CONCLUSIONS

This project successfully demonstrated the applicability of HACMS technology to enhancing NPP cybersecurity by producing a proof-of-concept Simulink add-on for building high-assurance components of larger systems, along with a demonstration showing a generated monitor detecting anomalies in that larger system. A major roadblock to using formal methods is the difficulty of formally specifying and proving a large system, and this project shows a novel way around that roadblock through pre-specifying and pre-proving small reusable system pieces, and then composing a larger proven specification from those pieces. The new layers of cybersecurity do not conflict with existing layers, nor are they dependent on any other cybersecurity technology. The abstraction and composition strategy has potential application far beyond NPPs, and with further development has significant commercial potential.

Having a working demonstration to show interested parties has already begun to generate encouraging interest from prospective partners and early adapters. SpiralGen, Inc. wants to continue this line of research and development, with hopes of making a significant and lasting contribution toward filling the gaps in cyber assurance.

7 REFERENCES

Weiss, J.: Protecting Industrial Control Systems from Electronic Threats, Momentum Press (2010)

Brooks, F.P.Jr.: The Mythical Man-Month, Addison-Wesley (1975)

Dijkstra, E.W.: The Humble Programmer. University of Texas at Austin, Austin, TX (1972)

Fulton, N., Mitsch, S., Quesel, J., Völp, M., Platzer, A.: KeYmaeraX: an axiomatic tactical theorem prover for hybrid systems. In: Felty, A.P., Middeldorp, A. (eds.) CADE-25, Berlin, Germany, August 1-7, 2015, proceedings. LNCS, vol. 9195, pp.527-538. Springer (2015)

Püschel, M., J. M. F. Moura, J. Johnson, D. Padua, M. Veloso, B. Singer, J. Xiong, F. Franchetti, A. Gacic, Y. Voronenko, K. Chen, R. W. Johnson, and N. Rizzolo,: SPIRAL: Code generation for DSP transforms, Proceedings of the IEEE, special issue on “Program Generation, Optimization, and Adaptation", vol. 93, no. 2, pp. 232-275 (2005)

8 DISCLAIMER

This work was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof, its contractors or subcontractors.