DESCRIPTION OF THE RESEARCH PROJECT FOR THE 2020 SUMMER RET SITE

Project 5: Software and Systems Security in Model-Driven Engineering

Area Coordinator:
Dr. Nan Niu
Associate Professor
Department of Electrical Engineering and Computer Science
College of Engineering and Applied Science
University of Cincinnati
Cincinnati, OH 45221-0030
Office: 832 Rhodes Hall
E-Mail: nan.niu@uc.edu
Phone: (513) 556-0051

Sub-Area Coordinator:
Dr. Boyang Wang
Assistant Professor
Department of Electrical Engineering and Computer Science
College of Engineering and Applied Science
University of Cincinnati
Cincinnati, OH 45221-0030
Office: 806A Rhodes Hall
E-Mail: boyang.wang@uc.edu
Phone: (513) 556-4785

Graduate Research Assistant:
Mr. Xuanyi Lin
Ph.D. Candidate in Electrical Engineering and Computer Science
Office: 527 Engineering Research Center
E-Mail: linx7@mail.uc.edu
Phone: (518) 779-0898

Project Summary

This research topic is inspired by the safety and security concerns in developing cyber-physical systems, and linked to the ***big idea*** of meeting the critical requirements in model-driven engineering (MDE). Many industries, such as defense, manufacturing, finance, transportation, telecommunication, healthcare, and energy, use MDE to develop and maintain safety-critical and mission-critical capabilities. The systems modeling language (SysML) [1] has become a *de facto* standard for modeling the requirements, structure, and behavior of a complex system, and received increasing attention from various industrial sectors [2].

Figure 1 shows a SysML state machine diagram (SMD) of the water distiller intended to be used in remote, undeveloped regions where water is generally available but seldom safe to drink. A distiller unit purifies water via heating; however, an actual solution must consider broad issues like environmental protection, energy conservation, installation cost, and functional safety. In particular, IEC 61508 [4] defines *functional safety* as part of the overall safety relating to the equipment under control (e.g., the water distiller shown in Figure 1). The goal is to ensure that any safety-related system must work correctly or fail in a predictable, safe way.

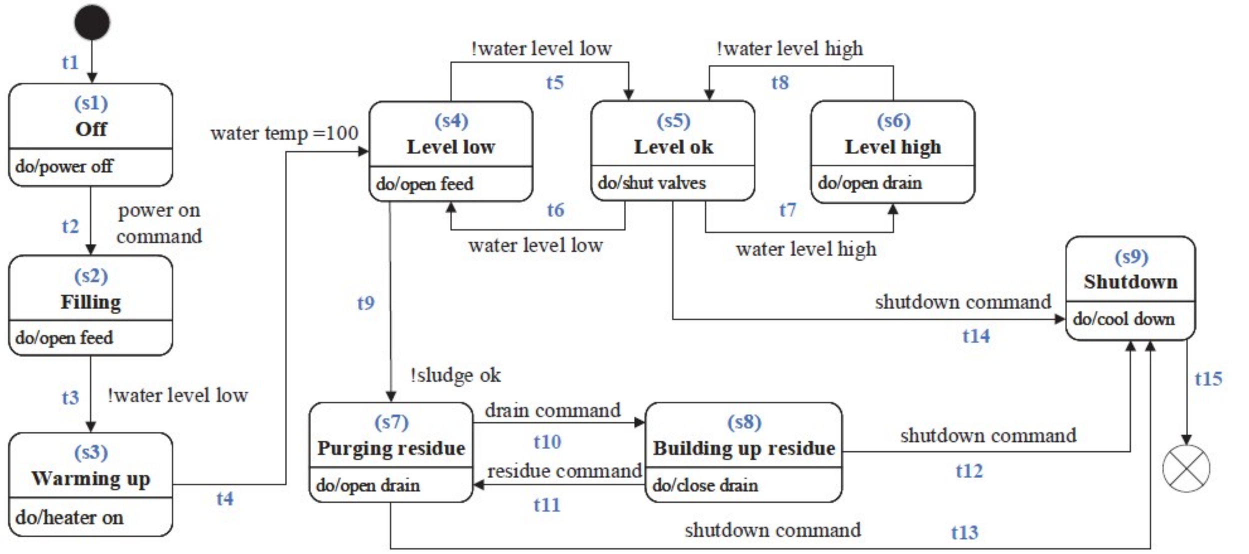


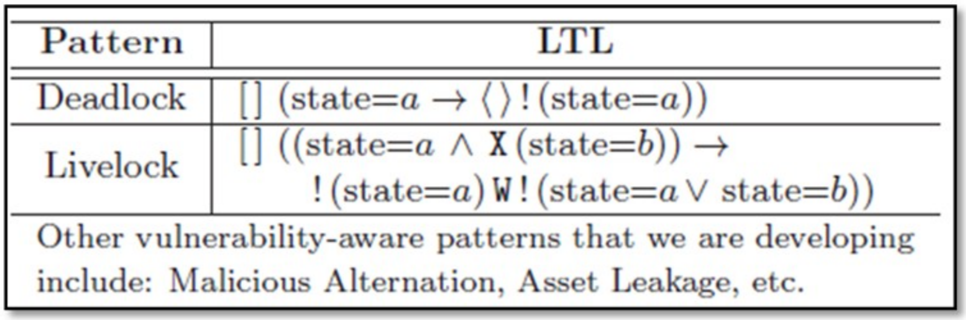
Figure 1 SysML state machine diagram (SMD) of the water distiller example (adapted from [3]).

In the example of Figure 1, a fault of leakage or explosion, and a functional safety requirement mitigating the fault can implement the proper safeguards to prevent the water level from staying low. However, specifying such safety requirements and reasoning about their satisfactions is challenging for large-scale and complex SysML models. Thus, the ***guiding questions*** of the research project are to address the main ***challenge*** of formally specifying safety and security requirements and reasoning about their satisfactions in SysML models.

The ***guiding questions*** of the research project are to address the main ***challenge*** of discovering vulnerabilities in large-scale and evolving web applications, such as the first-order and second-order XSS vulnerabilities illustrated above. Teachers will engage in ongoing research in modeling test paths based on requirements, user interface interactions, and data flow dependencies. The real-world application of Scholar@UC and their development processes and practices will be used throughout the project to ensure the relevance and usefulness of the research.

Training Provided

Teachers will first learn the state-of-the-practice standards, such as the SysML specifications [1] and IEC 61508 [4], and extract instances of safety and security patterns from them. These patterns are created and codified by the research team, and expressed in linear temporal logic (LTL). Figure 2 illustrates a couple of patterns. Referring to the water distiller of Figure 1, the LTL formula: [] ((state== “Level low” → ! (<> (state==“Level low”)))), states that, “it is always ([]) the case once the water level is low it will eventually (<>) not be low”. The teachers will also learn how to use the state-of-the-art model checker to verify the safety and security properties expressed in LTL formulas. Finally, they will be trained to leverage process mining tools (e.g., ProM) to discover the circumstances and conditions where the SysML models may fail to satisfy the critical requirements thereby uncovering defects in the systems design and offering explainable insights and improvements to the MDE process.



Pattern	LTL
Deadlock	$[]\ (\text{state}{=}a \rightarrow \langle\rangle\ !\,(\text{state}{=}a))$
Livelock	$[]\ ((\text{state}{=}a \wedge \mathtt{X}\,(\text{state}{=}b)) \rightarrow$ $!\,(\text{state}{=}a)\ \mathtt{W}\ !\,(\text{state}{=}a \vee \text{state}{=}b))$
Other vulnerability-aware patterns that we are developing include: Malicious Alternation, Asset Leakage, etc.	

Figure 2 Safety and security patterns express in linear temporal logic (LTL) forms.

Research Facilities

The teachers will be conducted in the Software Engineering Research Laboratory (ERC 527). Currently, the lab has six desktops with 3.4 GHz Intel i3 processor and one server with 2.60 GHz Intel Xeon dual-core processor. RET participants’ research will be tool-driven and computational in nature, enhanced with hands-on experience and informed by empirical findings. Consequently, the work will be carried out on computers and whiteboard in our lab. The list of software includes No Magic SysML modeling tool, ProM process mining tool, and the LTL model checker. Additionally, the RET research will be connected to the Ohio Cyber Range at the University of Cincinnati (OCR@UC) where three nodes (virtual machines) built in an on-campus network will be available for the RET researchers to better experiment the tools and to develop their scalable solutions in a distributed setting.

Industrial Partner

Glen Horton, project manager of the Scholar@UC project, has agreed to directly interact with the team. The majority of his work has been in agile and open-source software development. Meanwhile, he has expertise and experience in MDE. He has been a very close collaborator of our lab for many projects. For example, in the summer of 2018, he helped to transfer our recent research findings in security vulnerability discovery to the broader open-source development community (https://github.com/samvera/hyrax/issues/3187). Glen is willing to share the artifacts, processes, and documentations with the RET researchers who are also invited to observe and participate in the scrum meetings and other project meetings of Scholar@UC.

Ideas for Classroom Implementation

The software and systems security project offers a wide variety of classroom applications built around using the state-of-the-practice tools and the state-of-the-art modeling methods to ensure that critical needs are met in large-scale and evolving systems. Existing research on Scholar@UC system and the emerging findings ensure that the teachers will build upon valid results for their learning. A classroom unit will constitute the study of Scholar@UC or other safety-critical and mission-critical applications to develop effective and efficient approaches to assuring that the system must work correctly or fail in a predictable, safe way.

References Cited

[1] Object Management Group, "Systems Modeling Language (SysML)," https://www.omg.org/spec/SysML/1.6/Beta1/PDF Last accessed: February 2020.

[2] W. Schäfer and H. Wehrheim, "The Challenges of Building Advanced Mechatronic Systems," In *Future of Software Engineering (FOSE)*, Minneapolis, MN, USA, 2007, pages 72-84.

[3] S. Friedenthal, A. Moore, and R. Steiner, "Water Distiller Example Using Functional Analysis," In *A Practical Guide to SysML (Second Edition)*, S. Friedenthal, A. Moore, and R. Steiner (Eds.). The MK/OMG Press, 2012, pages 393-429.

[4] International Electrotechnical Commission, "Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems (IEC 61508)," https://www.iec.ch/functionalsafety/ Last accessed: February 2020.