Modeling and Testing in Cyber Physical Systems

ITEC 503-951

Jeff Miller

Graduate Student

School of Information Systems and Applied Technology

Southern Illinois University

Carbondale, IL

Southern Illinois University

August 1st, 2021

Modeling and Testing in CPS

Introduction

We have learned throughout our CPS course that a high degree of reliance on software defined functionality and the wide availability of network connectivity are two of the biggest transformations across the industry. Software development plays an ever more significant role in the overall device safety. In the medical field this means that instead of standalone devices that can be designed, certified, and used independently of each other to treat patients; networked medical devices will work as distributed systems that simultaneously monitor and control multiple aspects of the patient's physical state. Patient safety will always be a primary concern when considering MCPS development. Regulatory procedures are in place to require approval of their use for treating patients. The FDA has to approved devices and the process is becoming more lengthy for developers to comply. What challenges exist when designing these systems correctly? We see though research that designing for security and patient safety is one and the same. It requires modeling and testing to ensure that objectives of overall patient safety is achieved. In other industries, we also see modeling and the construction of cyber physical testbeds in order to achieve a secure environment. Modeling is also used for IDS, and has a valuable application in the power infrastructure industry. This lecture could be used to demonstrate the importance of modeling to IST students in a modern systems analysis and design class.

Practical Modeling

"The Unified Modeling Language (UML) provides a standard, graphical-based formalism for capturing system models. UML is very flexible but lacks the semantical content required in most application domains" (Villar, Eugenio & Posadas, Hector & Henia, Rafik & Rioux, L, 2020). With the goal of safety defined in the introduction, we can take a look at model based development. Model-based development techniques provide one way to ensure the safety of a system. Increasingly, model-based development is embraced by the medical devices industry. Even so, the numerous recalls of medical devices that have occurred in recent years demonstrate that the problem of device safety is far from being solved. (Rajkumar, Niz & Beebe, 2016).

Students beginning any modern information technology program will be introduced to UML in their first database design and processing class, furthermore UML and object oriented systems analysis and design has become the industry standard. "Typically, the process of creating a UML model involves, first, creating models of the individual elements of the system (e.g. components) and then, combining these elements to specify the system. It is usual to spend more time in the modeling of the components than in the modeling of their interactions, due to the different parameters and details to be configure within the component models" (Villar, et al., Rioux, 2020). The time involved will be discussed later, but this is a result of factors such "As commented above, the main challenges to be faced by a CPSoS modeling methodology are the increasing complexity of the integrated circuits, its growing heterogeneity and the increasing complexity of the system behavior and structure, composed by a number of distributed embedded systems, eventually connected to the cloud. From the analysis of the state of the art, it is possible to conclude that there is a lack of powerful-enough system modeling methodologies able to scale to cyber-physical systems composed by a variety of embedded systems" (Villar,

Eugenio & Posadas, Hector & Henia, Rafik & Rioux, L, 2020). “In a CPS, the embedded system has to operate inside a physical environment ruled by strict physical equations” ” (Villar, Eugenio & Posadas, Hector & Henia, Rafik & Rioux, L, 2020).

Development Time

Generating a complete model of a large system (i.e. a CPSoS) is a time-consuming task, as explained in a 2020 *article Mega-Modeling of complex, distributed, heterogeneous CPS systems.* To address the time needed, we can “focus on proposing solutions capable of reduce this effort by improving model reuse, as shown in section 5. These improvements are presented for the S3D modeling methodology, but they could be applied to other methodologies, especially due to the fact that they are based on standards, not on specific profiles” (Villar, Eugenio & Posadas, Hector & Henia, Rafik & Rioux, L, 2020). “little research to date has focused on testing and validation for CPS within health care, smart transportation, power grids and safety support, where suitable testing method can arguably have profound impact in preventing costly and possibly fatal system failures. Compositional verification and testing methods should be adapted for the heterogeneous CPS models” (Abbaspour Asadollah, Inam & Hansson, 2015). Reusability is one of the key factors in all modeling systems, in the smallest real world application, all the way to complex power grid infrastructure applications.

Cyber Physical Testbeds

"Cyber Physical Systems (CPSs) are an integral part of modern society; thus, enhancing these systems' reliability and resilience is paramount. Cyber–physical testbeds (CPTs) are a safe way to test and explore the interplay between the cyber and physical domains and to cost-effectively enhance the reliability and resilience of CPSs" (Vaagensmith, Bjorn & Singh, Vivek & Ivans, Robert & Marino, Daniel & Wickramasinghe, Chathurika & Lehmer, Jacob & Phillips, Tyler & Rieger, Craig & Manic & Milos, 2021). Based on enabling execution techniques, the architecture of testbeds can be divided into three categories according to the corresponding implementation enabling technique: hardware-based, simulation-based, or hybrid platform. (Zhou, Xin & Gou, Xiaodong & Huang, Tingting & Yang, & Shunkun, 2018)

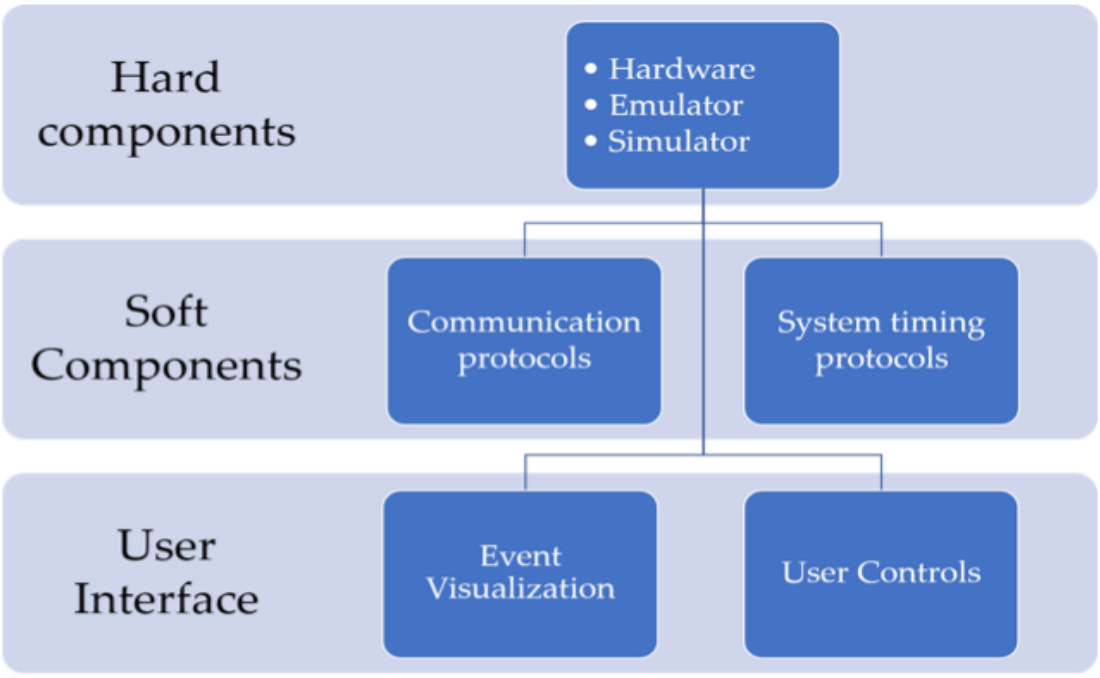

Figure 1. Three levels of consideration for cyber physical testbed construction (Vaagensmith, et al., Milos, 2021).

IDS Modeling

"Signature-based IDS relies on network traffic to detect different classes of data- integrity attacks based on the defined attack-signature database. Several IDS tools, including BRO, Snort, Firestorm, and Spade can be applied in developing signature-based IDS in real-time in a cyber–physical test bed environment" (Vaagensmith, et al., Milos, 2021). Anomaly-based IDS detects intrusions based on deviations from the normal behavior of the distribution system. It includes different types, such as model-based IDS, machine-learning-based IDS, multi-agent-based IDS. These are discussed below. Model-based IDS utilizes the current grid information, historical measurements, and other relevant information to develop a baseline model and detects attacks based on the statistical and temporal correlation analysis of incoming grid measurements" (Vaagensmith, et al., Milos, 2021). It is suggested in other research that the use of models will replace expert systems and rules. "The main research objective is to build a reliable model or a set of reliable modes that can be used for intrusion detection. We also wish to establish if supervised or unsupervised learning methods work best to build models used in intrusion detection. The research would allow us to establish which machine learning or pattern recognition algorithms work best for problem of intrusion detection" (Lochner, Elric & Arendse, & Connan, James & Omlin, Christian, 2021).

Conclusion

In cyber physical systems and information technology in general, object oriented modeling will be an indispensable tool. Students can use Microsoft Visio or create a free account at Lucidchart to begin modeling systems such as ERD's for database applications and many

other types of modeling. “Model based development has emerged as a means of raising the level of assurance in software systems. In this approach, developers start with decorative models of the system and perform a rigorous model verification with respect to safety and functional requirements; they then use some systematic code generation techniques to derive code that preserves the verified properties of the model” (Rajkumar, Niz & Beebe, 2016). Developing models that are reusable can help save time, this is a great discussion item when reviewing the existing Microsoft suite of applications available to most students.

References

Abbaspour Asadollah S., Inam R., Hansson H. (2015) A Survey on Testing for Cyber Physical System. In: El-Fakih K., Barlas G., Yevtushenko N. (eds) Testing Software and Systems. ICTSS 2015. Lecture Notes in Computer Science, vol 9447. Springer, Cham. https://doi.org/10.1007/978-3-319-25945-1_12

Lochner, Elric & Arendse, & Connan, James & Omlin, Christian. (2021). Constructing Intrusion Detection Systems Models.

https://www.lucidchart.com

https://www.microsoft.com/en-us/microsoft-365/visio

Vaagensmith, Bjorn & Singh, Vivek & Ivans, Robert & Marino, Daniel & Wickramasinghe, Chathurika & Lehmer, Jacob & Phillips, Tyler & Rieger, Craig & Manic, Milos. (2021). Review of Design Elements within Power Infrastructure Cyber-Physical Test Beds as Threat Analysis Environments. Energies. 14. 10.3390/en14051409.

Villar, Eugenio & Posadas, Hector & Henia, Rafik & Rioux, L.. (2020). Mega-Modeling of complex, distributed, heterogeneous CPS systems. Microprocessors and Microsystems. 78. 103244. 10.1016/j.micpro.2020.103244.

Zhou, Xin & Gou, Xiaodong & Huang, Tingting & Yang, Shunkun. (2018). Review on Testing of Cyber Physical Systems: Methods and Testbeds. IEEE Access. 6. 1-1. 10.1109/ACCESS.2018.2869834.