Proceedings of the Annual General Donald R. Keith Memorial Conference
West Point, New York, USA
May 4, 2023
A Regional Conference of the Society for Industrial and Systems Engineering

Model-Based Systems Engineering Cybersecurity of Field Programmable Gate Arrays for Future Weapons Systems

Shea Burcham[1], Andrew Cabo[1], Caden Kotter [1], Christopher Von Haasl[1], Keith Bearden[2], Chad Tossell[1], and James Walliser[1]

[1]Department of Operations Research
United States Air Force Academy
Air Force Academy, Colorado 80840

[2]The Aerospace Corporation
El Segundo, California 90245

Corresponding author's Email: james.walliser@afacademy.af.edu

Disclaimer: The views expressed herein are those of the authors and do not reflect the position of the United States Air Force Academy, the Department of the Air Force, or the Department of Defense.

Author Note: Cadets Burcham, Cabo, Kotter, and Von Haasl are all cadets at the United States Air Force Academy (USAFA) majoring in systems engineering. They thank Lieutenant Colonel James Walliser for providing us with the opportunity to work with the Long Range Stand Off (LRSO) nuclear acquisition System Program Office (SPO). Additionally, they thank the LRSO SPO for guiding them throughout this project and particularly Dr. Keith Bearden for his endless mentorship and access to resources.

Abstract: Field Programmable Gate Arrays (FPGAs) are an essential component of many technologies including DoD aerospace systems. Because of their reprogrammable features, designers can implement algorithms and mitigate radiation-induced failures cost-effectively and efficiently. However, this can also render FPGAs vulnerable to potentially catastrophic cyber consequences. In order to evaluate the probability and consequences of cyber risks (including the potential mission impact), the goal of this paper is to understand the vulnerabilities and potential attack vectors that adversaries might exploit. We use Model-Based System Engineering to design a cyber-threat assessment tool to this end. The resulting tool considers threats throughout an FPGA's lifecycle and produces a risk matrix encompassing all assessed threats. In this report, we describe the scope of the project, the development process, and potential applications to government acquisition programs. We conclude with a discussion of the criticality of cyber-risk assessment highlighting the need for more research in FPGA cybersecurity.

Keywords: Cybersecurity, Model-Based Systems Engineering, Aerospace Systems

1. Introduction

Field-Programmable Gate Arrays (FPGAs) are a type of integrated circuit (IC) that allows designers to configure and customize digital circuits. Unlike traditional ICs, such as Application-Specific Integrated Circuits (ASICs) which are hardwired to perform specific functions, FPGAs can be programmed and reprogrammed in theater to perform different tasks (Farooq et al., 2012). FPGAs have numerous applications in digital signal processing, communications, aerospace, automotive, and industrial control systems (Piggin 2016). Furthermore, FPGAs offer many advantages over traditional ICs, such as higher flexibility, faster time-to-market, and lower development costs (Cloud, 2022). The United States has raised concerns about obtaining microchips developed in foreign countries due to the potential security threat (as they are used in major systems across the Department of Defense and the American civilian infrastructure; Matheny 2022). Because of this cyber risk, our primary customer, the Air Force Lifecycle Management Center (AFLCMC) Armament Division, Long-Range Stand Off (LRSO) program, asked us to quantify the risk associated with differing types of FPGAs and differing manufacturers to better determine FPGA procurement and lifecycle processes. To this end, we model a novel, complex aerospace system to inform decision-making within these processes to ensure overall cybersecurity and, thus, broader cybersecurity for broader DoD missions and enterprises.

Model-Based Systems Engineering (MBSE) can serve as a powerful tool in modeling the system architecture and

requirements of an FPGA-based system. It can encompass hardware components, software components, and the interfaces between them, enabling designers to identify potential problems, test different scenarios, and optimize the system design before committing to implementation. By utilizing MBSE to describe the system architecture, designers can gain a comprehensive understanding of the system and identify potential flaws or limitations in the design. This approach allows for more informed decision-making and can improve the efficiency and effectiveness of the overall system design process. Through models, designers can explore various design alternatives, predict system behavior, and validate system requirements, leading to a more reliable and optimized system design. To model the FPGA design, including the logic functions, interconnections, and other components of the FPGA, system designers and developers can identify potential issues, optimize the design for specific use cases, and test the performance of the FPGA before implementation. Our primarily focus on this project was on the hardware trojan horse (HTH) threats potentially implemented within the procurement process though we hope the resulting model will be useful for broader cybersecurity analysis as well.

1.1 Client Organization

The primary stakeholder on this project was the AFLCMC LRSO program office. They provide acquisition oversight of the LRSO Cruise Missile under development to eventually provide a long range survivable standoff weapon capable of delivering lethal nuclear effects on strategic targets. LRSO will replace the currently-fielded Air Launched Cruise Missile (ALCM) and will be integrated on both legacy and future bomber aircraft. The LRSO weapon system will be capable of penetrating and surviving advanced Integrated Air Defense Systems (IADS) from significant standoff ranges to prosecute strategic targets in support of the Air Force's global attack capability and strategic deterrence core function. It is a roughly $10 billion dollar acquisition program. Given the Office of the Secretary of Defense has provided guidance for the Air Force to increase their use of digital acquisitions, the LRSO program office is pioneering the way forward for use of model-based Systems Engineering (MBSE) in the acquisition of this system. The LRSO program is aided by Aerospace Corporation and MITRE engineers to ensure a smooth transition to MBSE; as experts in this field, they provided significant mentorship and oversight in this project.

1.2 Goals

This project's objective was to develop a comprehensive analysis tool that enables Subject Matter Experts (SMEs) to assess the risks associated with FPGAs from various manufacturers across distinct phases of their lifecycle. The tool will provide a user-friendly graphical output in the form of a standard DoD risk cube and facilitate the analysis of multiple threats within a single phase. The complexity and programmability of FPGAs have made them an integral part of various systems, including DoD, aerospace, and computer systems, but have also made them vulnerable to cyber threats, which can have catastrophic consequences. The analysis tool developed in this project will enable SMEs to assess the likelihood and potential impact of various cyber threats and produce a comprehensive risk matrix. This tool will be instrumental in enhancing the security of FPGAs and mitigating the risks associated with their usage.

1.3 Related Work

Use of MBSE in the design of FPGAs in systems development is rare. Recently, Ibrahim and Jung (2016) propose a systems engineering approach for implementing hardware cybersecurity controls for non-safety data networks. The authors present a framework that integrates system requirements, design, and testing to ensure that the cybersecurity controls are effective and meet the system requirements. The framework includes several stages, including the identification of the system requirements, development of the design, and testing and validation of the cybersecurity controls. More closely related to our project, Kim and Jung (2018) presented an approach to developing FPGA-based cybersecurity equipment for nuclear power plants. The authors proposed a methodology that includes requirements analysis, design, and verification and validation to ensure the effectiveness of the cybersecurity equipment. The authors emphasized the importance of systems engineering in the development of cybersecurity equipment to ensure that the equipment meets the requirements and specifications of the system. Digital twin-enabled MBSE testbeds are also gaining increasing attention as a means of prototyping and evaluating complex systems, particularly in the aerospace industry. Madni et al. (2021) present a digital twin-enabled MBSE testbed for prototyping and evaluating aerospace systems. The authors demonstrated the effectiveness of the testbed in identifying design flaws and optimizing system performance. The authors highlight the value of digital twin-enabled MBSE in system development, particularly in identifying and mitigating cybersecurity vulnerabilities. In another paper, Elakrat and Jung (2018) proposed the development of a field programmable gate array (FPGA)-based encryption module to mitigate man-in-the-middle attacks for nuclear power plant data communication networks. The encryption module, which includes requirements analysis, design, and validation stages, demonstrated the effectiveness of the encryption module in mitigating cybersecurity threats and improving

the security of nuclear power plant communication networks.

Our work is unique in that it produces models that will be used to analyze risks of FPGAs across the lifecycle phases in the acquisition of a DoD system. Our stakeholder required a comprehensive understanding of the applications of FPGAs incomplex systems and the associated risks. Still, prior to modeling, the previous research helped us understand the role of FPGAs in different systems and the potential vulnerabilities they may have. This research provided valuable insights into the phases of the FPGA lifecycle and the primary locations of procurement. By understanding these aspects, the developed tool incorporated threat analysis capabilities and effectively analyzed risks associated with multiple manufacturers and types of FPGAs throughout their lifecycle. This research-driven approach ensured that the tool could provide a holistic assessment of the risks involved with FPGAs and help stakeholders make informed decisions to mitigate potential threats.

1.4 Types of Threats

Even though there are a wide variety of threats applicable to the FPGA, we scoped our project to focus on the Hardware Trojan Horse (HTH) based on related work and our stakeholder's requirements. The modeling efforts can extend to multiple threats under the same modeling framework. However, there are over 259 HTH threats and analyzing these threats can provide utility in broader cybersecurity contexts.

1.4.1 Hardware Trojan Horse

HTH threats refer to the presence of malicious code or parts integrated into circuitry that can negatively impact system operation or collect sensitive data. Such threats are common and highly detrimental to FPGA systems, especially those used in high-level defense systems and manufactured in certain locations. HTH threats can occur at any phase of the FPGA lifecycle, but not all types of FPGA systems or manufacturers are equally vulnerable. The goal of an HTH is to compromise the FPGA's functionality or security by altering its behavior in ways that benefit the attacker. This can include leaking confidential data, disabling encryption, or providing unauthorized access to the FPGA. Detecting HTHs can be challenging since they are inserted at the hardware level and may not manifest themselves until long after deployment.

Designers can mitigate the risk of HTHs by implementing various security measures such as using trusted foundries and suppliers, enforcing supply chain management protocols, performing regular security audits, and using advanced verification techniques to detect and isolate Trojan activity (Salmani et al., 2012). Additionally, encryption and secure boot mechanisms can help protect the FPGA from unauthorized access and manipulation. We analyze 106 HTH threats as part of this project.

2. Data and Use of Equations

The process outlined in Table 1 was used in defining the risk to the system, in this case the risk that hardware trojan horse has on an FPGA. The severity of risk (S_i), ease of obfuscation (EO), willingness to invest in time and resources to develop attack (WTR), technical knowledge gap (TKG), perceived impact due to timeframe (PIT), and perceived impact on resources (PIR) were assigned by a SME in each area. Similarly, technical likelihood was assigned by a SME, however, this value is scored on a Likert scale making the domain $\{0,1,3,9\}$. This methodology was provided in a document quantifying FPGA threats and countermeasures (Sadhasivan, 2023).

ISBN: 97819384964-4-8

Table 1. Equations for Risk Cube Analysis

Device Threat Profile Number	$Dev_{TPN} = \frac{number\ of\ threats\ in\ play\ (n)}{total\ number\ of\ threats}$	(1)
Baseline Occurrence	$O_j = \frac{\sum(EO,\ WTR,\ TKG,\ PIT,\ PIR)}{5}$	(2)
Threat Aggregate Residual Risk Potential	$ARP_j = \frac{E_j x O_j}{2} x S_j$	(3)
Geometric Mean of Considered Threats Residual Risks	$Dev_{iRR} = (\prod_{i=1}^{n} ARP_i)^{\frac{1}{n}}$	(4)
Device's Final Residual Risk Number	$Dev_{RR} = Dev_{iRR}^{(1+Dev_{TPN})}$	(5)

After defining risk, the focus shifted to the countermeasures (CM) quantification for threat mitigation. The mitigation effect of a CM (E) and the degree of difficulty of CM implementation (D) are assigned by a SME according to a Likert scale, again making the domain of values within $\{0,1,3,9\}$. This culminates in a Final Threat Residual Risk Value that program leadership can use to determine whether to accept this level of risk or to apply additional countermeasures. This methodology was provided in a document quantifying FPGA threats and countermeasures (Sadhasivan, 2023).

Table 2. Equations for Mitigation Analysis

Total Effectiveness of each CM	$TE = \sum ARP_i \times E$	(6)
Effectiveness to Difficulty Ratio	$ETD = \frac{TE}{D}$	(7)
Average Cumulative Mitigation Effect	$\frac{\sum E}{Number\ of\ CMs\ applied}$	(8)
Final Threat Residual Risk Value	$ARP_{RRj} = ARP_j \times (1 - \frac{E_{Avg}}{10})$	(9)

3. Methodology

Throughout the project, an agile project management application was employed, providing a platform for feedback and review to take place. The project was divided into four epics, each spanning two months, and concluded with a review briefing delivered to the LRSO program advisor. This process ensured a specific and useful product was delivered to the customer within the project's scope. A product backlog was maintained, and an agile heartbeat was established to facilitate efficient project management.

The modeling methodology employed Block Definition Diagrams (BDD), Internal Block Diagrams (IBD), and hierarchical representations of the system to create a structured model. Behavior diagrams were subsequently developed to model the interactions between the various parts of the system, serving as the first step to analysis. Once behavioral diagrams were established, simulations were executed using MATLAB integration as a part of a Simulation Configuration Diagram, with Graphical User Interfaces (GUI) developed to provide user-friendly functionality. Using Excel, equations 1-7 were iterated for each of the 106 threats across 13 phases for FPGA type Xilinx. The CATiA model was utilized to pass the desired threats and phases to MATLAB. MATLAB, in turn, is related to severity of risk and likelihood values, creating a risk cube, and returning the FPGA's final residual risk number to CATiA. This modeling methodology allowed for a comprehensive and accurate analysis of the system, producing reliable results that can be used in a variety of applications.

ISBN: 97819384964-4-8

4. Modeling

4.1 Structure

The entirety of the modeling process was conducted in Magic Systems of Systems – CATiA (referred to as CATiA), employing a SysML modeling approach. We initiated the modeling phase by creating high-level block definition diagrams, which allowed us to establish a baseline for the interactions and definition of relevant parts and parameters. Subsequently, we decomposed the structure further within internal block definition diagrams to facilitate the integration of flows within the model. These structure diagrams served as the foundation for establishing the behaviors required for simulation purposes. Through this approach, we were able to capture the complexity of the system and its interactions, allowing for a comprehensive analysis and evaluation of the model's performance. Moreover, the use of SysML modeling approach ensured that the model was accurately represented, minimizing any discrepancies and errors that may have arisen during the design phase. The resulting model offers a reliable and effective tool for simulating and analyzing complex systems, with the potential for use in a wide range of applications.

4.2 Behavior

After creating all the structural diagrams, we proceeded to develop behavior diagrams such as Use Case and Activity Diagrams. These diagrams were instrumental in displaying and connecting relevant components of the model for further integration and simulation application. Specifically, behavior diagrams helped us manipulate the functionality of CATiA and provide additional features required for the project. For instance, state machines diagrams depict the procurement process which can be integrated into future simulation aspects of the model. Similarly, activity diagrams enabled the model to input and analyze multiple threats simultaneously within a single phase and visually depict selected processes. These behavior diagrams offer a detailed and systematic representation of the model's various functionalities, aiding in its effective use and future development.

4.3 Simulation

To simulate the risk assessment process of the Field Programmable Gate Arrays (FPGAs), we developed a Graphical User Interface (GUI) within the CATiA model. The GUI integrates the parametric diagram functionalities of the model with MATLAB code, resulting in a risk cube visualization, as shown in Figure 1. The risk cube represents selected threats specific to a manufacturer and particular phase of the lifecycle. This approach provides a scalable output of information and data based on the level of risk involved. The model currently supports up to 106 different threats, but only 13 can be displayed simultaneously to maintain usability. Once the user selects appropriate mitigation measures, a second risk cube can be generated to assess the effectiveness of the mitigations and the residual risk that remains. Overall, this method offers a practical and efficient means of evaluating risks associated with FPGAs, accommodating multiple manufacturers and design phases.

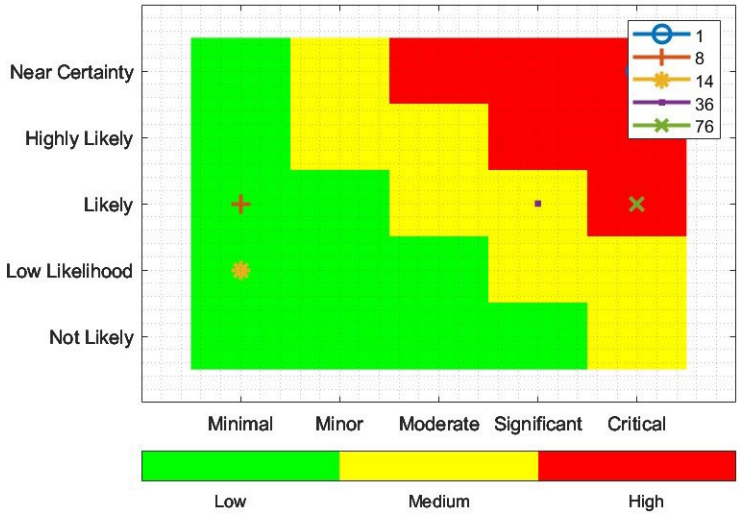

Figure 1. Risk Analysis Output (Risk Cube)

ISBN: 97819384964-4-8

5. Future Work

A new group comprised of cadets has already been selected to continue the partnership with the LRSO program office. Their focus will be on integrating intellectual property theft and tampering threats into the model and improving its usability. Currently, each simulation is stand-alone and assumes all mitigations will be taken to lower the risk. Allowing for a selection of which mitigation techniques to apply would increase the capability of this tool. This will allow for program offices to optimize their selection in the FPGA they will use and how much time, money, and effort they will put toward mitigating the threats they are interested in. Another improvement would be to allow for multiple risk cubes to be generated if the type or phase is different to allow for analytical comparison.

6. Conclusion

The DoD has embraced MBSE as a means of improving the efficiency and effectiveness of system development while reducing costs and increasing quality. MBSE digital tools, including the UML-extended language SysML, offer engineers a unique advantage in understanding cybersecurity considerations at every stage of system development. By modeling cybersecurity requirements and tracing them throughout the system implementation, engineers can automate the process of identifying design conflicts and minimize risk. This report demonstrated the value of MBSE and SysML in the design of a DoD system, and how it can be leveraged to improve cybersecurity and system performance. Indeed, MBSE was used to contribute to FPGA security by providing the framework for the procurement process of the FPGAs in a digital format. MBSE was shown to be useful in modeling the system architecture and security requirements of the FPGA procurement and lifecycle process and providing a living model capable of becoming more robust over time. By modeling the system architecture structure, the model identified potential vulnerabilities and security risks and develop strategies to mitigate them. In addition to modeling the security requirements of the system, the output analyzed the threats associated within specific phases of the procurement process and providing a useful output in the form of a risk cube. Early SME and leadership feedback from our primary DoD revealed it will be useful now and in the future to make informed data driven decisions. More importantly, stakeholders will leverage our model to ensure that the FPGA-based system meets the necessary security standards and complies with relevant regulations.

ISBN: 97819384964-4-8

7. References

Intel. (2022). Cloud services, 5G. *FPGA or Structured ASIC: Which Is Right for You?* Retrieved from https://www.intel.com/content/www/us/en/products/programmable/fpga-vs-structured-asic.html.

Elakrat, M. A., & Jung, J. C. (2018). Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network. *Nuclear Engineering and Technology, 50*(5), 780-787.

Farooq, U., Marrakchi, Z., Mehrez, H. (2012). *FPGA Architectures: An Overview. In*: *Tree-based Heterogeneous FPGA Architectures*. Springer, New York, NY. https://doi.org/10.1007/978-1-4614-3594-5_2.

Ibrahim, A. S., & Jung, J. (2016). A Systems Engineering Approach to Implementing Hardware Cybersecurity Controls for Non-Safety Data Network. *Journal of the Korean Society of Systems Engineering, 12*(2), 101-114.

Kim, J. S., & Jung, J. C. (2018). Systems Engineering Approach to develop the FPGA based Cyber Security Equipment for Nuclear Power Plant. *Journal of the Korean Society of Systems Engineering, 14*(2), 73-82.

Madni, A. M., Erwin, D., & Madni, C. C. (2021, March). Digital twin-enabled MBSE testbed for prototyping and evaluating aerospace systems: Lessons learned. In *2021 IEEE Aerospace Conference (50100)* (pp. 1-8). IEEE.

Matheny, J. (2022). The U.S. Has a Microchip Problem. Safeguarding Taiwan Is the Solution. *The Atlantic*, Atlantic Media Company. Retrieved 3 Oct. 2022, from https://www.theatlantic.com/international/archive/2022/10/taiwan-microchip-supply-chain- china/671615/.

Piggin, R., & Sampson, C. (2016). Security and safety of FPGAS in nuclear safety systems: benefits and challenges. *11th International Conference on System Safety and Cyber-Security (SSCS 2016), 2016*, pp. 1-6, doi: 10.1049/cp.2016.0857.

Sadhasivan, S. (2023). Quantification of FPGA Threats, Countermeasures and Residual Risk Computation. *Information Systems and Cyber Division,* 21 Feb. 2023.

Salmani, M., Tehranipoor, & Plusquellic J. (2012). A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time. In *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, 20*, Jan. 2012, doi: 10.1109/TVLSI.2010.2093547.