Business Process Modeling for Semiconductor Production Risk Analysis Using IDEF0

Zachary A. Collier[1], Andrew Gaskins[2], James H. Lambert[2]

[1] Radford University, USA

[2] University of Virginia, USA

Keywords: IDEF0, systems engineering, process reengineering, risk identification, product lifecycle

Abstract: Program managers must manage heterogeneous sources of risk across the semiconductor lifecycle, identifying vulnerabilities which, if exploited, have adverse consequences to mission and/or business objectives. Identification of sources of risk involves understanding the business processes involved in the production, use, and maintenance of components. Business process modeling is widely used to address technology research and development. A typical methodology for business process modeling is the IDEF family of modeling languages. The basic IDEF0 block represents a function, with associated inputs, outputs, controls, and mechanisms. This paper demonstrates risk identification and risk management through the use of an extended IDEF0 framework incorporating risk sources. The effort models the semiconductor lifecycle based on open source materials at multiple hierarchical levels, for example drilling down into fabrication and wafer manufacturing processes. Product lifecycle stages are associated to particular sources of risk. Several sources of risk are pervasive across stages, while others are particular to a stage. The results of this effort help program and product managers to know what risks should be managed, how risk countermeasures and resources should be coordinated, and how the performance of risk management activities should be monitored and evaluated.

Introduction

Semiconductors are an incredibly important global commodity. They enable smart devices across the vast economy and society. The enterprise of designing, manufacturing, testing, and packaging semiconductors is technologically complex and the global supply chain is similarly complex [1-2]. With the complexity of the lifecycle of semiconductors and their supporting supply chain, there are many sources of risk. For instance, a hardware-related attack was reported in which a tiny chip around the size of a grain of rice was covertly inserted into a circuit board providing a stealth doorway for remote network access [3]. Counterfeit electronic components can enter the supply chain, leading to degraded functionality and potential security concerns [4].

With routine and emerging sources of risk to firms engaged in the semiconductor lifecycle, a principled approach is needed to identify and manage the risks. The process of risk analysis can be defined as answering the following questions [5]: What can go wrong? How likely is it? What are the consequences? Similarly, three guiding questions that a risk program should answer are:

- What are the sources of risks to be managed, i.e., what is the scope of the program?
- How should multiple risk assessment, risk management, and risk communication activities be coordinated and what should be the basis for resource allocation?
- How will the performance of the risk program be monitored and evaluated? [6-7]

The first question refers to the sources of risk, and relates to the activity of risk identification. To aid in the risk identification process, we propose a business process modeling methodology. Business process modeling is used to understand the key processes of an existing business, serves as the basis for designing or outsourcing support systems (e.g., information technology systems), and can serve as the baseline for assessing and improving a system through a business process reengineering program [8].

At its core, a business process consists of its customers, a set of activities that are aimed at creating value for the customers, actors and resources that facilitate the processes such as people and machines, and one or more organizational units responsible for the process [9]. Graphical representations of business process are used to decompose the process and easily communicate a complex series of activities that are used for observing, integrating, optimizing, and changing process flows [10-11]. Business process mapping has been shown to improve transparency in systems, improving "recognition of status, problems, responsibilities, and interdependencies; facilitation of understanding, feedback, and communication; and enabling of decision making" [12].

In particular, business process modeling can be used to facilitate risk management. For example, business process models have been integrated with failure modes and effects analysis for healthcare organizations [13], and have been used to reduce disaster and accident risk for transportation infrastructure [14]. It has been applied to the enterprise function of risk management, modeling the functions that a risk program manager would undertake [6-7].

The methods described below add risk identification to the typical IDEF0 business process modeling language to model the semiconductor lifecycle at different levels of abstraction. Graphically representing the various lifecycle stages allows program and product managers to identify where sources of risk arise in the life cycle, and to devise targeted risk treatment strategies. The identification of lifecycle risks can facilitate the construction of a risk register to track and manage the various risks.

Methods

The IDEF0 modeling language addresses any system that is comprised of "things and happenings" [11]. Specifically, the basic units of the IDEF0 language are boxes and arrows. A box represents an activity, i.e., a thing that happens. Specifically, the activities represent functions that transform inputs into outputs by means of mechanisms and subject to controls [15]. Inputs describe what is consumed or transformed by an activity, outputs describe what results from an activity, mechanisms represent the "what" and "how" of an activity, and controls represent things that guide, determine, or constrain the activity [10-11, 15]. The basic graphical language is shown in Figure 1. Feldmann [11] provides a comprehensive overview of the technical details and practical elements associated with IDEF0 modeling.

To account for sources of risk in business processes, Lambert et al. [10] introduced a modified IDEF0 diagram (Figure 1). Whereas the traditional IDEF0 model captures the "as-planned" scenarios [16], the modified model captures deviations from the business process [10].

The stages of the semiconductor lifecycle are described differently and in varying levels of detail [17]. Given the hierarchical nature of IDEF0, one is able to decompose activities into multiple sub-activities until the needed granularity is reached [11]. We therefore began at a high level, and for certain stages, decomposed the stage into its constituent parts. For sources of risk, we used the classification described by Areno [18] across lifecycle stages (Table 1), except for high-granularity diagrams where specific risks are mentioned.

Results and Implications

Sample modified IDEF0 diagrams are shown in Figures 2-4. Figure 2 displays the several stages of the semiconductor lifecycle, beginning with design, followed by integration, which relates to the inclusion of third-party hardware or software intellectual property (IP) into the design. Next is the fabrication stage, followed by testing, provisioning, and finally deployment. Other authors separate the stages differently, for example packaging and testing are often combined into one phase while integration is subsumed under design [2]. For each of these stages, a number of risk sources are relevant. For example, for design, *R1 - Insider Threat*, *R2 - Design Tools*, *R3 - Third Party Plugins*, and *R4 - Attack on Design Networks* are identified as relevant for this lifecycle stage [18].

Figure 3 describes the various major phases of the Fabrication Stage. In this stage, the silicon wafer is prepared as well as the mask which serves as the "template" for the chip. Then processes of etching, electrode formation, and wafer inspection are subsequently performed. Each of these general steps can be decomposed into additional, lower-level steps.

Figure 4 illustrates how this further decomposition is possible - the process of *wafer manufacturing* (SP1-3-2 in Figure 3) can be further decomposed into steps such as *ingot pulling*, *ingot slicing*, *wafer polishing*, and *oxidation of the wafer surface*. Across the entire lifecycle, depending on how the steps are accounted, there are potentially over 700 separate steps in a semiconductor lifecycle [19], making the hierarchical nature of IDEF0 well-suited for the application.

In complex technological lifecycles, there are many sources of risk that can disrupt operations and negatively impact the organization. Different sources of risk may be relevant during different stages of the system or product lifecycle. Following the process of risk analysis outlined by Kaplan and Garrick [5], the first question to answer is "what can go wrong?", corresponding to the process of risk identification. By facilitating process visibility, business process mapping is a tool that managers can leverage to better understand their current systems and processes, and to facilitate the design of new systems and processes that mitigate identified risks.

For example, in Figure 2, one can see that the risk, *R1 - Insider Threat,* is relevant across all lifecycle stages. Given this pervasive threat, certain countermeasures like only using trusted suppliers, can have great benefit in reducing risk across the lifecycle.

Lessons Learned

The following are several practical lessons from the above use of business process mapping and risk identification.

First, when mapping out a business process, it is a best practice to integrate multiple perspectives. Complex systems and processes have many stakeholders who may hold different viewpoints about the process and how it can be improved. Model building should be an interactive and iterative process. Related to this is the option to model the same process using different modeling languages. For example, within the family of IDEF models, IDEF1 can be used to model information flows. Other methodologies falling under the umbrella of model-based systems engineering (MBSE), such as SysML, can also be used to graphically represent complex systems [20].

Second, it is important to keep a goal in mind when mapping out a complex process. According to Feldmann [11], "Never create a model for the purpose of creating a model." In the case of this paper, we built a model to help identify sources of risk associated with a complex product lifecycle. To this end, business process modeling can help management avoid surprises and changes related to products, processes, workforce, regulations, consumer demand, etc.

Third, the risk identification process is only an initial step of the overall risk management process. Specifically, while the graphical syntax of IDEF0 can help increase transparency and communication, managers still need to make decisions about risk mitigations, and so other risk management tools will need to be used. For example, the modified IDEF0 model described here could be linked with a risk register or FMEA tool to quantify and prioritize risks.

Finally, process or technology changes tend to have influences across a product lifecycle and supply chains. They almost always involve workers who must also change something about how their job is performed. For example, the change management literature describes that change involves five key steps – awareness of the need to change, desire to participate in the change, knowledge about how to change, ability to implement the change, and reinforcement to sustain the change [21]. An organization should have a process in place regarding the human dimensions of change management.

Conclusion

Today's supply chains are exposed to numerous sources of risk, from chip shortages to geopolitical tensions that can throw a company's production plan into disarray. The ability to effectively manage risks across the lifecycle of semiconductor components is important not only for the semiconductor industry itself, but for all of the many sectors that rely upon these chips for their own products and services, such as automotive, aerospace, healthcare, finance, defense, and many others.

Effective risk management starts with risk identification. A risk that cannot be identified cannot be managed. Understanding what risks occur in what areas of the product lifecycle can help managers to identify risk mitigations appropriate to that particular stage. Best practices that can also be applied across multiple stages, such as leveraging trusted suppliers for outsourced activities, to mitigate risk across the entire lifecycle. Integrating risk identification practices such as the business process modeling techniques described here within the larger systems engineering effort can facilitate the design of secure electronic components and secure systems that the components enable, meeting mission and business objectives and fulfilling user requirements.

Acknowledgements: This work was supported in part by the National Science Foundation under Grant 1916760 "Phase I IUCRC University of Virginia: Center for Hardware and Embedded System Security and Trust (CHEST)" and the Commonwealth Center for Advanced Logistics Systems (CCALS).

References

[1] Varas, A., Varadarajan, R., Goodrich, J., Yinug, F. (2021). Strengthening the global supply chain in an uncertain era. Boston Consulting Group and Semiconductor Industry Association.

[2] DiMase, D., Collier, Z.A., Muldavin, J., Chandy, J.A., Davidson, D., Doran, D., Guin, U., Hallman, J., Heebink, J., Hall, E., Shaffer, A.R. (2021). Zero trust for hardware supply chains: Challenges in application of zero trust principles to hardware. National Defense Industrial Association (NDIA) Electronics Division.

[3] Robertson, J., Riley, M. (2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek*, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[4] DiMase, D., Collier, Z.A., Carlson, J., Gray Jr., R.B., Linkov, I. (2016). Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex systems. *Risk Analysis,* 36(10), 1834-1843.

[5] Kaplan, S., Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis*, 1(1), 11-27.

[6] Teng, K.Y., Thekdi, S.A., Lambert, J.H. (2012). Risk and safety program performance evaluation and business process modeling. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans,* 42(6), 1504-1513.

[7] Teng, K.Y., Thekdi, S.A., Lambert, J.H. (2012). Identification and evaluation of priorities in the business process of a risk or safety organization. *Reliability Engineering & System Safety*, 99, 74-86.

[8] Eriksson, H.E., Penker, M. (2000). *Business Modeling with UML – Business Patterns at Work.* John Wiley & Sons: New York.

[9] Lin, F.R., Yang, M.C., Pai, Y.H. (2002). A generic structure for business process modeling. *Business Process Management Journal*, 8(1), 19-41.

[10] Lambert, J. H., Jennings, R. K., & Joshi, N. N. (2006). Integration of risk identification with business process models. *Systems Engineering*, 9(3), 187-198.

[11] Feldmann, C.G. (1998). *The Practical Guide to Business Process Reengineering Using IDEF0.* Dorset House Publishing: New York.

[12] Klotz, L., Horman, M., Bi, H.H., Bechtel, J. (2008). The impact of process mapping on transparency. *International Journal of Productivity and Performance Management*, 57(8), 623-636.

[13] Bevilacqua, M., Mazzuto, G., Paciarotti, C. (2015). A combined IDEF0 and FMEA approach to healthcare management reengineering. *International Journal of Procurement Management*, 8(1-2), 25-43.

[14] Tserng, H.P., Cho, I.C., Chen, C.H., Liu, Y.F. (2021). Developing a Risk Management Process for Infrastructure Projects Using IDEF0. *Sustainability*, 13(12), 6958.

[15] Menzel, C., Mayer, R. J. (1998). The IDEF family of languages. In: Bernus, P., Mertens, K., Schmidt, G. (eds.), *Handbook on Architectures of Information Systems* (pp. 209-241). Springer, Berlin, Heidelberg.

[16] Haimes, Y.Y., Horowitz, B.M. (2003). Risk-based methodology for scenario tracking, intelligence gathering, and analysis for countering terrorism. *Systems Engineering*, 6(3), 152–169.

[17] Samsung (2015). Eight major steps to semiconductor fabrication, part 1: Creating the wafer. https://news.samsung.com/global/eight-major-steps-to-semiconductor-fabrication-part-1-creating-the-wafer

[18] Areno, M. (2020). Supply chain threats against integrated circuits. Intel White Paper, https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/supply-chain-threats-v1.pdf

[19] Whalen, J. (2021). Three months, 700 steps: Why it takes so long to produce a computer chip. *The Seattle Times*, https://www.seattletimes.com/business/technology/three-months-700-steps-why-it-takes-so-long-to-produce-a-computer-chip/

[20] Zhang, L., F. Ye, K. Xie, P. Gu, X. Wang, Y. Laili, C. Zhao, X. Zhang, M. Chen, T. Lin, Z. Chen (2022). An Integrated Intelligent Modeling and Simulation Language for Model-based Systems Engineering. *Journal of Industrial Information Integration*, Volume 28, 100347.

[21] Hiatt, J.M., Creasey, T.J. (2012). *Change Management: The People Side of Change.* Prosci Inc.: Fort Collins, CO.

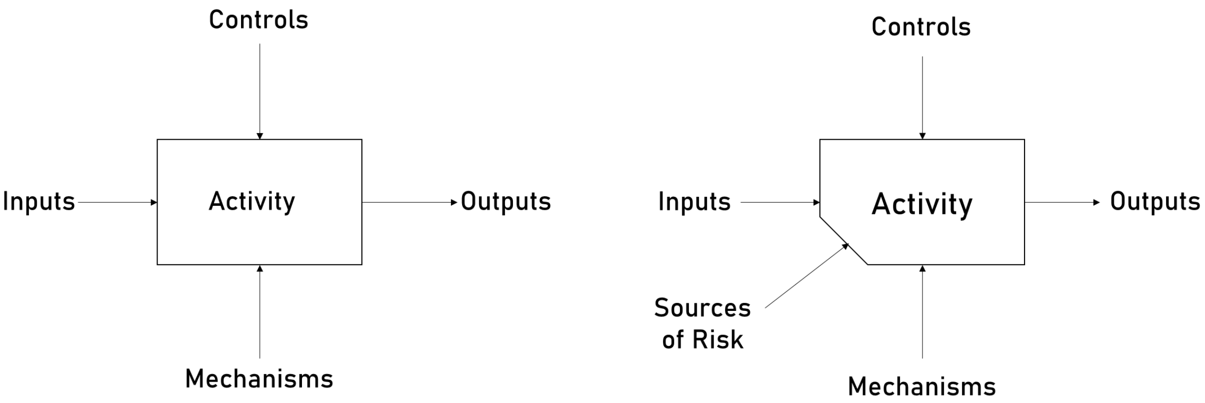

Figure 1: Traditional IDEF0 activity (left); Modified IDEF0 activity describing sources of risk (right)

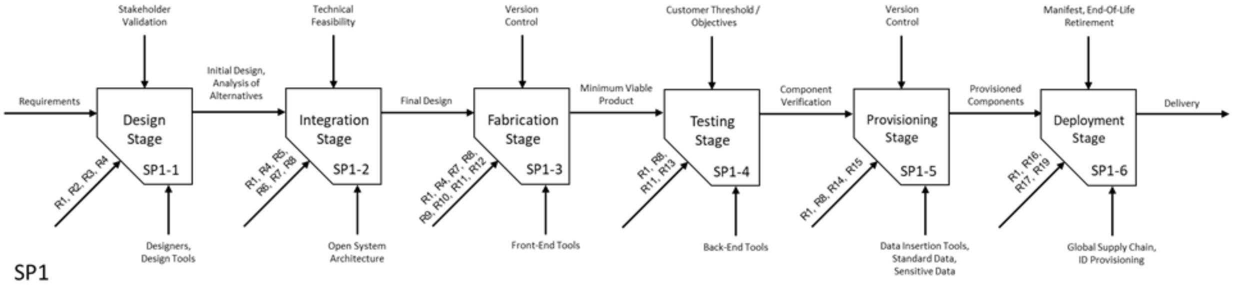

Figure 2: Overview of the Semiconductor Lifecycle with Risk Sources

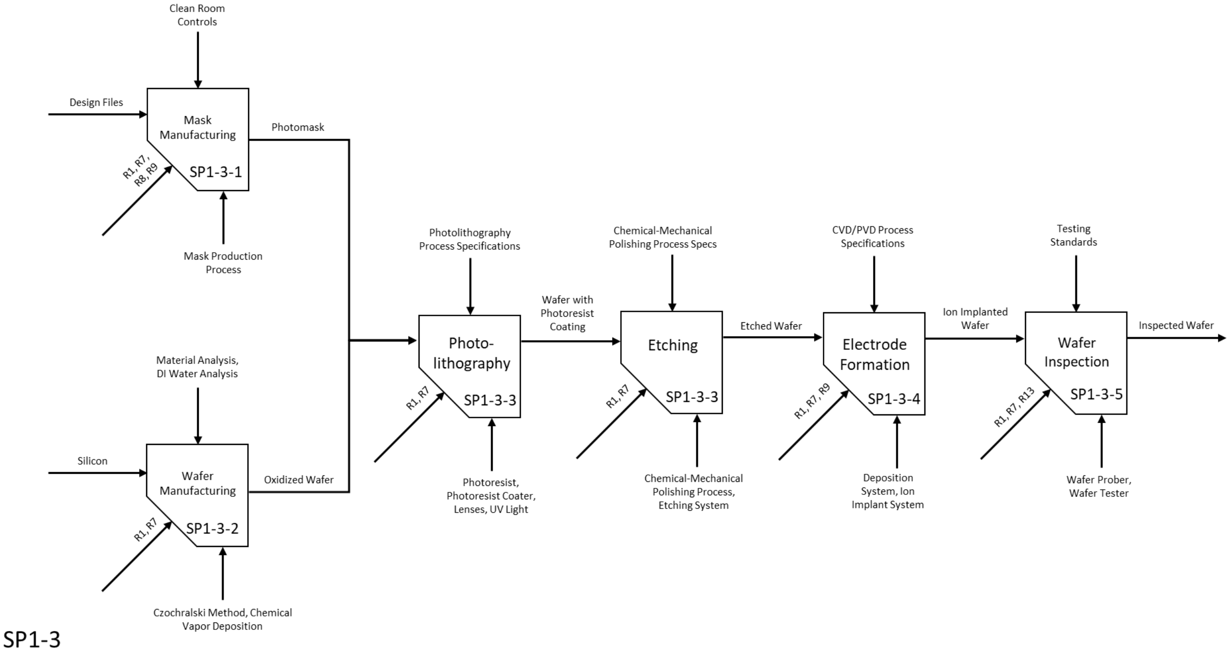
Clean Room Controls
Design Files
Mask Manufacturing
SP1-3-1
R1, R7, R8, R9
Mask Production Process
Photomask
Material Analysis, DI Water Analysis
Silicon
Wafer Manufacturing
SP1-3-2
R1, R7
Czochralski Method, Chemical Vapor Deposition
Oxidized Wafer
Photolithography Process Specifications
Photo-lithography
SP1-3-3
R1, R7
Photoresist, Photoresist Coater, Lenses, UV Light
Wafer with Photoresist Coating
Chemical-Mechanical Polishing Process Specs
Etching
SP1-3-3
R1, R7
Chemical-Mechanical Polishing Process, Etching System
Etched Wafer
CVD/PVD Process Specifications
Electrode Formation
SP1-3-4
R1, R7, R9
Deposition System, Ion Implant System
Ion Implanted Wafer
Testing Standards
Wafer Inspection
SP1-3-5
R1, R7, R13
Wafer Prober, Wafer Tester
Inspected Wafer
SP1-3

Figure 3: Fabrication Stage

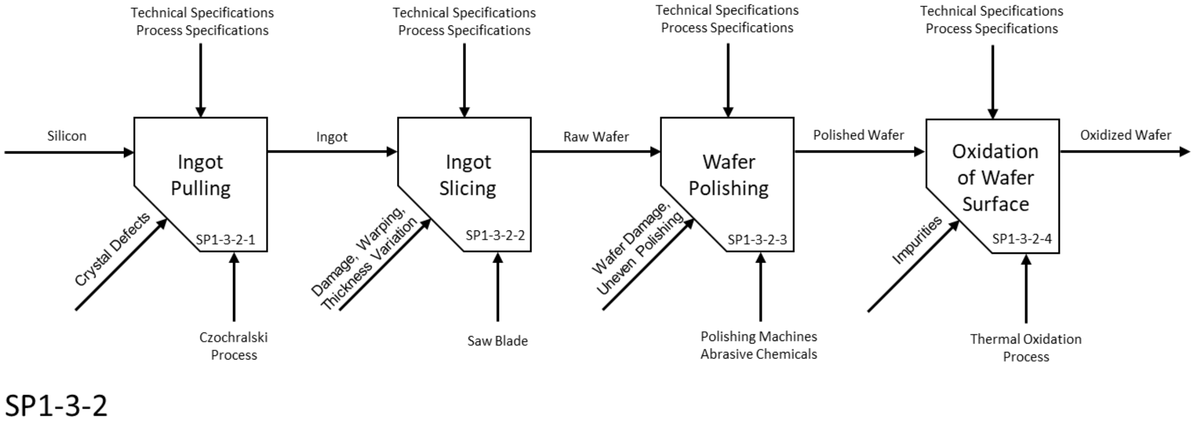

Figure 4: Wafer Manufacturing

Table 1: Lifecycle Risk Sources (adapted from [18])

Sources of Risk \ Lifecycle Stage	Conceptual/ Design	Integration	Manufacturing	Testing	Provisioning/ Configuring	Deployment
R1 - Insider Threat	+	+	+	+	+	+
R2 - Design Tools	+					
R3 - Third Party Plugins	+					
R4 - Attack on Design Networks	+	+	+			
R5 - Malicious Hardware		+				
R6 - Malicious Firmware		+				
R7 - Design Alterations		+	+			
R8 - Unauthorized Disclosure		+	+	+	+	
R9 - Insertion of Trojan Circuitry			+			
R10 - Insertion of Trojan Components			+			
R11 - Component Replacement			+	+		
R12 - Reverse Engineering			+			
R13 - Falsification of Test Results				+		
R14 - Insertion of Unsecure Values					+	
R15 - Improper Device Settings					+	
R16 - Physical Alteration in Transit						+
R17 - Replacement of Valid Firmware						+
R18 - Overproduction of Parts			+			
R19 - Fictitious Recycling						+

Biosketches

Zachary A. Collier is Assistant Professor in the Department of Management at Radford University. He is Co-Chair of the NDIA Electronics Division's Trust and Assurance Committee. Dr. Collier is a Fellow of the Center for Risk Management of Engineering Systems at University of Virginia, and a Visiting Scholar at the Center for Hardware and Embedded Systems Security and Trust (CHEST). His previous work experience includes the U.S. Army Engineer Research and Development Center, where he was a member of the Risk and Decision Science Team. He earned the Ph.D. in Systems Engineering from University of Virginia, a Master of Engineering Management from Duke University, and a Bachelor of Science in Mechanical Engineering from Florida State University.

Andrew W. Gaskins received a B.S. degree in aerospace engineering from The University of Texas at Austin, Austin, TX in 2019 and a M.E. in Systems Engineering from the University of Virginia, USA, in 2022. He is currently a Senior Consultant in Digital Engineering at Booz Allen Hamilton, Global Defense Sector. He was previously a Lead Systems Engineer at the Department of Defense, supporting the development of the United States Space Force. Mr. Gaskins is a member of the IEEE and the International Council on Systems Engineering.

James H. Lambert is a Professor of Engineering Systems and Environment, Director of the Center for Risk Management of Engineering Systems, and Site Director of the NSF Center for Hardware and Embedded Systems Security & Trust, each at the University of Virginia. Professor Lambert's interests are engineering systems and risk analysis. He is a Past President (2015–2016) of the Society for Risk Analysis (SRA). He is a Fellow of the AAAS, Fellow of the IEEE, Fellow of the ASCE, Fellow of the SRA, Diplomate of the American Academy of Water Resources Engineers (D.WRE), member of the International Council on Systems Engineering, and licensed Professional Engineer (P.E.). He is Editor-in-Chief of the Springer journal *Environment Systems & Decisions*. He is Area Editor of the Wiley journal *Risk Analysis*. He received a Ph.D. and M.S. in Civil Engineering at the University of Virginia, and a B.S.E. in Mechanical Engineering with a Certificate in Engineering Physics at Princeton University.