Risk Management Decision Making for Security and Trust in Hardware Supply Chains

Zachary A. Collier
Collier Research Systems
Barboursville, VA, USA
zachary@collierresearchsystems.com

Thomas L. Polmateer
Dept. of Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
polmateer@virginia.edu

James H. Lambert
Dept. of Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
lambert@virginia.edu

Abstract—**Modern cyber-physical systems are enabled by electronic hardware and embedded systems. The security of these sub-components is a concern during the design and operational phases of cyber-physical system life cycles. Compromised electronics can result in mission critical failures, unauthorized access, and other severe consequences. As systems become more complex and feature greater connectivity, system owners must make decisions regarding how to mitigate risks and ensure resilience and trust. This paper provides an overview of research efforts related to assessing and managing the risks, resilience, and trust with an emphasis on electronic hardware and embedded systems. The research takes a decision-oriented perspective, from the perspective of scenario planning and portfolio analysis, and describes examples related to the risk-based prioritization of cyber assets in large-scale systems.**

Keywords— system security, hardware assurance, software assurance, firmware assurance, security, risk, vulnerability, threats, mission assurance, cyber, cybersecurity.

I. Introduction

The national and global infrastructure is increasingly dependent upon embedded electronic hardware components. Whereas we used to be able to think of physical and cyber systems as separate entities, we now must reframe our thinking in terms of cyber-physical systems. The U.S. National Institute of Standards and Technology [1] defines cyber-physical systems "smart systems that include engineered interacting networks of physical and computational components". Cyber-physical systems encompass a broad scope, sometimes conceptualized as having cyber, physical, and human dimensions [2]-[3].

As an example, modern vehicles contain hundreds of embedded sensors and control units, millions of lines of code, and Internet access [4]. While these hardware components and embedded systems add many useful functionalities, they also present vulnerabilities which can potentially allow malicious actors to steal and/or remotely access and control the vehicle [5]-[7]. Other applications related to healthcare, finance, defense, and critical infrastructure (e.g., the electric grid [8]-[9]) are similarly vulnerable, and necessitate the assessment of the security and trust of the embedded hardware which facilitate our daily lives [10].

The supply chains through which these components are procured and transported can be an entry point for untrusted and insecure electronics, making their way to the consumer. Counterfeit electronics, which may be relabeled, refurbished, or repackaged to misrepresent their authenticity, can make their way into the supply chain and can be created through a number of simple and advanced methods [11]-[13].

If counterfeit electronic components are integrated into products, a number of consequences can materialize, including reduced system functionality and unauthorized access to sensitive information. Companies face impacts in the form of lost profits, increased testing and repair costs, damaged reputation, products with decreased reliability, and legal liabilities [14]. Governments face even more serious issues, such as the possibility of reduced reliability and functionality of mission-critical defense systems [15]. One estimate of the impact of counterfeits on the semiconductor industry in the United States is as high as $200 billion [16].

Many factors contribute to the abundance of counterfeits within the supply chain, including the changing nature of the supply chain itself. Outsourcing of the fabrication of electronic components and the complex nature of the global electronics supply chain necessitates the authentication of components where the chain of custody may be unknown [17]-[19]. Obsolescence is another contributing factor, especially in sectors such as defense and aviation where systems are in service for longer life spans than the components from which they are comprised. The obsolescence caused through diminishing manufacturing sources and material shortages (DMSMS) means that components must sometimes be procured from untrusted sources, opening the door for counterfeits [20]-[25]. Finally, end-of-life considerations, including practices of disposing of electronic waste (e-waste), contribute to the prevalence of counterfeits [26].

While ideally all electronics would be purchased from trusted suppliers, the reality of the modern global supply chain is that this is not always possible. Components with unknown supply chain histories require testing and authentication techniques to ensure that the required levels of security and trust are met. How to make risk-informed decisions under this environment of uncertainty is a critical managerial task from a supply chain and risk management perspective.

In this paper, we describe research efforts at the system and application level. We describe cyber-physical systems research efforts in areas related to risk, resilience, and trust, as well as open challenges. A comprehensive cyber-physical systems security strategy is one which integrates analytics, modeling methods, business processes, and technological advances across all levels of the system hierarchy and across the entire system life cycle.

II. Example: Electronic Vehicle Charging Stations

Vehicle-to-grid (V2G) technology, including the charging stations, electric vehicles, power and transportation networks, and control systems represent complex cyber-physical systems [27]-[30]. Connected vehicle systems and associated V2G infrastructure elements are increasingly subject to security threats, including security of embedded hardware devices [27]. V2G technology enables fleet-vehicle batteries to provide frequency regulation (distributed shock absorption on the scale of milliseconds to seconds) to the power grid when they would otherwise be on stand-by for logistics operations. Several-minute intervals of battery availability at specified power throughputs are reserved and sold ahead in an e-commerce market. In addition to frequency regulation, V2G technology can also provide demand charge management, reducing a customer's monthly demand charge (which can make up a significant portion of a site's electricity bill) by discharging an EV to partially power a building during demand charge periods.

There is an opportunity for IoT systems integration (including manufacturing) of advanced chargers, network communications, fleet vehicles, batteries, and the associated e-commerce transactions among power utilities and their industrial customers. A software system that enables interoperability between EVs, chargers, the grid, and other energy assets (solar, wind, etc.) is a critical component of V2G technology. Once these components are installed on a customer's site, an operations management system can continuously analyze and execute optimal V2G monetization opportunities available given a fleet's logistic operating schedule.

The most important of these properties, and perhaps most worrying to industry, is the possibility of a cascading failure following an attack or failure of electronic hardware. Is has been shown for a simple coupled networks model that cascading failure effects lead to a drastic decrease in the number of links and nodes that need to be removed from the network to break it down into individual components [31]-[32]. Ganin et al. have illustrated a similar effect for the recovery after a failure [33].

III. Risk, Resilience, and Trust

Risk analysis has been historically focused on answering questions about what can go wrong, what is the likelihood of something going wrong, and what are the impacts in the case of the thing going wrong [34]. At the highest level of system abstraction, the systems and application level, risks can be associated with embedded hardware in terms of technical, operational, and programmatic perspectives. Technical risks are related to the intended functionality of the system, whereas operational risks and programmatic risks are related to the achievement of business and program objectives, such as meeting cost and schedule benchmarks [35].

DiMase et al. describe how supply chain risk management is only a slice of the larger and more complex issue of cyber-physical security [36]. They define ten areas of concern, from software assurance to life cycle management, each with its own regulatory governing bodies and guidance documents. They describe the need to take a systems view of the cyber physical security challenge, including a view of how security requirements flow down from operational, functional, and architectural system levels. In particular, perspectives from systems engineering and closely related disciplines such as risk analysis and decision analysis are needed to synthesize and integrate information across areas of concern and guide enterprise level decisions [36]. In addition, they mention multiple cross-cutting capabilities, such as decision analysis, risk analysis, education and outreach, and training, highlighting how security is a transdisciplinary problem, requiring expertise from an array of subject domains [36]-[37].

One of the major difficulties related to assessing the risks of counterfeit electronics in the global supply chain has been the lack of obtainable data regarding the prevalence of counterfeits. Moreover, situations where there are low-likelihood and high-consequence risks have been difficult for risk practitioners to contend with historically, given difficulties in determining how best to allocate resources for risk reduction activities [38]-[40]. Furthermore, not all security requirements can be tested for complicated systems, meaning that there will always be some undetected risk [41].

These concerns have led to some researchers to describe cyber resilience, where resilience is defined by The National Academy of Science as "the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events" [42]. The National Research Council describes a resilient system as "one whose performance degrades gradually rather than catastrophically when its other defensive mechanisms are insufficient to stem an attack. A resilient system will still continue to perform some of its intended functions, although perhaps more slowly or for fewer people or with fewer applications. Features of resilient systems include redundancies and the absence of single points of failure" [43]. With respect to cyber resilience, "cyber resilience (or resiliency) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. Cyber resiliency can be a capability of a system, a system-of-systems, a mission, a business function, an organization, or a cross-organizational mission; the term can also be applied to an individual, household, group, region, or nation" [44]. Sheffi [45] proposes supply chain resilience, which promotes the resilience paradigm in terms of building adaptability and the ability to bounce back from disruptions and stressors.

Several frameworks for cyber resilience have been proposed [46]-[49]. Bodeau and Graubert [49] describe the field of cyber resiliency engineering as an interdisciplinary exercise founded upon systems engineering, and drawing principles from allied topics including dependability, survivability, fault tolerance, contingency planning, and others. Linkov et al. [50] developed a matrix-based approach for the development of cyber resilience metrics, based on the stages of the event management cycle (Plan/Prepare, Absorb, Recover, Adapt) and operational domains (Physical, Information, Cognitive, Social). This resilience metrics development process was applied to industrial control systems [51].

A final related concept is trust. Trust in the context of cyber security has been defined in multiple ways, including the "qualified reliance on received information" [52]. In the context of supply chains, the concept of trust is similar. Trust is conceptualized as a belief held by an actor in the supply chain, that another actor will act consistently and do what they say that they will do [53]. Trust is related to reciprocity between parties, the alignment of purposes, consequences for breaking trust, and transparency of information shared between parties [54]. Mayer et al. [55] summarizes trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party."

IV. Risk-Based Decision Making in Cyber-Physical Supply Chains

Increasingly, hardware supply chains have been evolving toward supply webs, moving away from linear procurement and toward ecosystems that have been characterized as "dynamic, hyper-connected, and collaborative" [56]. Managing risks within these complex supply chains is a top industrial priority and focuses mainly on avoidance and mitigation of consequences associated with disruption events, as well as balancing expected losses with risk management costs [57]-[59]. Teng, Thekdi, and Lambert [60]-[61] describe program risk as the process of answering the questions:

- what are the scope of risks to be addressed;
- what are the allocations of resources across time, geography, topics;
- and what is the monitoring of the efficacy of risk management into the future.

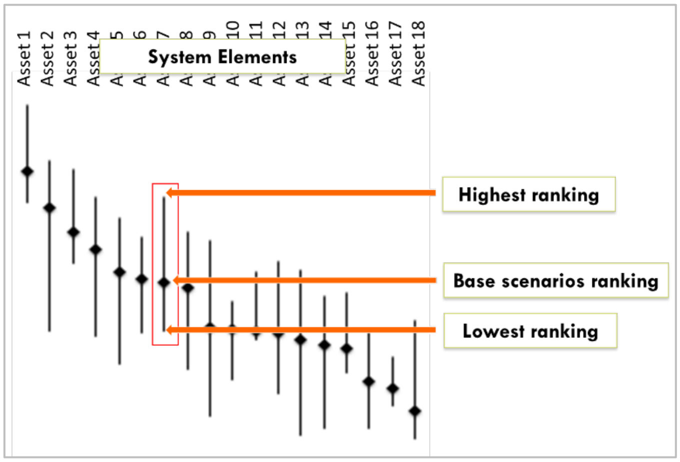

Fig. 1. Sample results showing prioritizatoin of cyber-physical assets across multiple disruptive scenarios.

Security and risk management need to go beyond the system boundary, looking toward the wider system of business processes and logistics networks, deriving relevant decision making parameters related to the broader hardware supply chain including specific resilience-enhancing initiatives and their relevant benefits, costs, and time constraints. Research is needed on methods, metrics, and testbeds for risk analysis of IOT devices and logistics systems, with the goal to develop risk analysis methods and decision making approaches along with relevant economic indicators for hardware networks and supply chains [51].

Principles and methods of scenario building can be brought to bear, considering emergent and future conditions involving environment, regulation, technology innovation, markets and economics, population and workforce behaviors, and other factors, both individually and in combination as scenarios, as demonstrated in [62]-[64]. For each of several risk scenarios of emergent conditions, a comprehensive risk analysis methodology would elicit from experts the increases or decreases in importance of criteria to rank IOT devices and systems of concern. With assessments of each device relative to threat, vulnerability, and consequence criteria, the system analyst or manager would be able to study the sensitivity of device criticality rankings to the scenarios, supportive of continuous adaptation and improvement toward industry aims.

The analysis would assist to determine what scenarios or combinations of risk scenarios are influential for critical embedded hardware components in a large-scale system. With this risk-based information, governments, scientific experts, policy-makers and various other stakeholders are able to make evidence-based strategic decisions leading to robust adaptive management of cyber security within complex interconnected systems and balance benefits, costs, and risks.

An open area of research related to decision making is that of metrics for security. Rostami et al. [65] proposed several technical metrics for security of hardware components against a variety of attacks. Hagen et al. [66] propose four metrics for assessing the performance of testing laboratories including effectiveness, efficiency, capacity, and capability. However, a unified framework for metric development across the various levels of system hierarchy has not been developed.

V. Resource Allocation to Portfolios of Security Measures

The risks posed by counterfeit electronics are numerous, and there exist a large number of potential risk mitigation measures which one can implement for a given system or across the enterprise. The task of identifying what specific countermeasures are used to reduce risk of counterfeit hardware is complicated by the many potential options available. While one can take a "defense in depth" approach and implement many safeguards, the question remains as to which ones in particular accrue the most security and trust benefits at the lowest cost. Each mitigation has associated with it a certain effectiveness in mitigating risks, but also comes at a cost. Moreover, mitigations can be implemented in combination with one another. These decisions must balance the inputs and concerns from upper management and organizational department such as supply chain management, finance, and IT.

The resulting question is that for a given level of risk reduction and a certain budget, what is the optimal investment strategy, in the form of combination of mitigations, to implement?

The risk reduction benefits of diversification are well known. In particular, risk can be decomposed into two components –

systematic and idiosyncratic (also called specific, or nonsystematic) risk. Through a well-diversified portfolio, much of the idiosyncratic risk can be reduced [67-68]. For example, Zhou et al. [69] applied a portfolio approach to flood risk management infrastructure. Instead of each asset being a stock, they modeled the returns from the implementation of various infrastructure assets such as retention areas, levees, etc. They found that diversification of flood risk management infrastructure in an area reduced the losses associated with floods.

In the same way, supply chain managers and risk managers require portfolio tools which can support cost-effective decision making through the development of a portfolio tool which aids the risk management investment decision process. Namely, methods and tools are needed which address the optimal "mix" of risk reduction countermeasures given several user-defined inputs related to cost and target risk. The goal is for users to investigate how to "buy down" the risk to acceptable levels.

VI. Conclusions and Future Work

As electronic hardware and embedded systems become more prevalent within the systems on which we depend in our daily lives, methodologies which provide risk-, resilience-, and trust-based insights into the system life cycle will become more important to the organizations tasked with maintaining a secure operating environment. While much research has been done on the chip, board, and assembly levels, research at the application and system level is required which integrates the technical risks with considerations related to business processes and human factors.

Another need faced by industry and government is the training of the current and future workforce to address these dynamic security issues. Training for the current enterprise workforce includes personnel beyond traditional IT professionals, and includes management and horizontally integrated personnel such as contractors. In terms of training the next generation workforce, institutions must provide educational curricula, hands-on experiential learning environments, and training opportunities that meet the needs of industry and government stakeholders [70].

References

[1] National Institute of Standards and Technology. (2017). Framework for cyber-physical systems: volume 1, overview. NIST Special Publication 1500-201.

[2] Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., Chen, S., Zhao, K. (2015). Cyber-physical-social system in intelligent transportation. *IEEE/CAA Journal of Automatica Sinica*, 2(3),320–333.

[3] Smirnov, A., Kashevnik, A., Shilov, N., Makklya, A., Gusikhin, O. (2013). Context-aware service composition in cyber physical human system for transportation safety. *13th international conference on ITS Telecommunications (ITST)*, pp 139–144.

[4] U.S. Government Accountability Office. (2016). Vehicle Cybersecurity. DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-World Attack. GAO-16-350, U.S. Government Accountability Office, Washington, DC.

[5] Burakova, Y., Hass, B., Millar, L., Weimerskirch, A. (2016). Truck Hacking: An Experimental Analysis of the SAE J1939 Standard. *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, Austin, TX.

[6] Greenberg, A. (2015). Hackers Remotely Kill a Jeep on the Highway - With Me in It. *Wired Magazine*. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

[7] Jafarnejad, S., Codeca, L., Bronzi, W., Frank, R. et al., (2015). A Car Hacking Experiment: When Connectivity Meets Vulnerability. *2015 IEEE Globecom Workshops (GC Workshops)*, San Diego, CA.

[8] He, H., Yan, J. (2016). Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory & Applications*, 1(1), 13–27.

[9] Sridhar, S., Hahn, A., Govindarasu, M. (2012). Cyber–physical system security for the electric power grid. *Proceedings of the IEEE,* 100(1), 210–224.

[10] Alguliyev, R., Imamverdiyev, Y., Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, 100, 212-223.

[11] Collier, Z.A., Hassler, M.L., Lambert, J.H., DiMase, D., Linkov, I. (2019). Supply chains. In: Kott, A., Linkov, I. (eds.), *Cyber Resilience of Systems and Networks*. Springer: Cham. pp. 447-462.

[12] Guin, U., Huang, K., DiMase, D., Carulli, J., Tehranipoor, M.;,Makris, Y. (2014). Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proceedings of the IEEE,* 102(8), 1207 – 1228.

[13] Sood, B., Das, D., Pecht, M. (2011). Screening for counterfeit electronic parts. *Journal of Materials Science: Materials in Electronics*, *22*(10), 1511-1522.

[14] Pecht, M., Tiku, S. (2006). Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. *IEEE Spectrum*, *43*(5), 37-46.

[15] US Government Accountability Office. (2010). Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods. GAO-10-423, U.S. Government Accountability Office, Washington, DC.

[16] Wood, G. (2016). Costly counterfeit electronic components in the supply chain can also be a safety concern. *IHS Markit*. http://blog.ihs.com/costly-counterfeit-electronic-components-in-the-supply-chain-can-also-be-a-safety-concern

[17] DiMase, D., Collier, Z.A., Carlson, J., Gray, 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.

[18] Villasenor, J. (2013). Compromised by Design?: Securing the Defense Electronics Supply Chain. Center for Technology Innovation at Brookings Institute.

[19] Mason, S.J., Cole, M.H., Ulrey, B.T., Yan, L. (2002). Improving electronics manufacturing supply chain agility through outsourcing. *International Journal of Physical Distribution & Logistics Management*, *32*(7), 610-620.

[20] Sandborn, P. (2013). Design for obsolescence risk management. *Procedia CIRP*, 11, 15 – 22.

[21] Rojo, F.J.R., Roy, R., Kelly, S. (2012). Obsolescence risk assessment process best practice. *Journal of Physics: Conference Series*, 364, 012095.

[22] Rojo, F.J.R., Roy, R., Shehab, E. (2009). Obsolescence management for long-life contracts: state of the art and future trends. *International Journal of Advanced Manufacturing Technology*, 49(9-12), 1235-1250.

[23] Sandborn, P., Prabhakar, V., Ahmad, O. (2011). Forecasting electronic part procurement lifetimes to enable the management of DMSMS obsolescence. *Microelectronics Reliability*, 51, 392-399.

[24] Singh, P., Sandborn, P. (2006). Obsolescence driven design refresh planning for sustainment-dominated systems. *The Engineering Economist,* 51(2), 115-139.

[25] Collier, Z.A., Lambert, J.H. (2019). Managing obsolescence of embedded hardware and software in secure and trusted systems. *Frontiers of Engineering Management,* doi: 10.1007/s42524-019-0032-5.

[26] Coalition for American Electronics Recycling. (2016). Unregulated E-Waste Exports Fuel Counterfeit Electronics that Undermine US National Security. http://americanerecycling.org/images/Counterfeiting_position_paper_3_1-16.pdf

[27] G. D'Anna (2019). *Cybersecurity for Commercial Vehicles*. Warrendale, PA: SAE International.

[28] Almutairi, A., Thorisson, H., Wheeler, J.P., Slutzky, D.L. and Lambert, J.H., 2018. Scenario-based preferences in development of advanced mobile grid services and a bidirectional charger network. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, *4*(2), 04018017.

[29] Almutairi, A., Wheeler, J.P, Slutzky, D.L., Lambert, J.H. (2019). Integrating Stakeholder Mapping and Risk Scenarios to Improve Resilience of Cyber-Physical-Social Networks. *Risk Analysis*, 39(9), 2093-2112.

[30] Thorisson, H., Almutairi, A., Wheeler, J.P., Slutzky, D.L. Lambert, J.H. (2017). Enterprise Management and Systems Engineering for a Mobile Power Grid. In *2017 25th International Conference on Systems Engineering (ICSEng),* pp. 99-105.

[31] Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature* 464, 1025–1028.

[32] Parshani, R., Buldyrev, S.V., Havlin, S. (2010). Interdependent Networks: Reducing the Coupling Strength Leads to a Change from a First to Second Order Percolation Transition. *Physical Review Letters*, 105(4), 048701.

[33] Ganin, A.A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J.M., Kott, A., Mangoubi, R., Linkov, I. (2016). Operational resilience: concepts, design and analysis. *Scientific Reports*, 6(1), 1-12.

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

[35] Horowitz, B.M., Lambert, J.H. (2006). Assembling off-the-shelf components: Learn as you go systems engineering. *Transactions on Systems, Man, and Cybernetics Part A,* 36(2), 286-297.

[36] D. DiMase, Collier, Z.A., Heffner, K., Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. Environment Systems and Decisions, 35(2), 291-300.

[37] Douba, N., Rütten, B., Scheidl, D., Soble, P., Walsh, D. (2014). Safety in the Online World of the Future. *Technology Innovation Management Review*, 4(11): 41–48.

[38] Fiksel, J., Polyviou, M., Croxton, K.L., Pettit, T.J. (2015). From Risk to Resilience: Learning to Deal with Disruption. *MIT Sloan Management Review,* 56(2), 1-8.

[39] Collier, Z.A., DiMase, D., Walters, S., Tehranipoor, M.M., Lambert, J.H., Linkov, I. (2014). Cybersecurity standards: managing risk and creating resilience. *IEEE Computer*, 47(9), 70-76.

[40] Park, J., Seager, T.P., Rao, P.S.C., Convertino, M., Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis,* 33, 356–367.

[41] Pfleeger, S.L., Cunningham, R.K. (2010). Why measuring security is hard. *IEEE Security & Privacy*, 8(4), 46-54.

[42] National Academy of Sciences. (2012). Disaster Resilience: a National Imperative. National Academic Press: Washington, DC. http://www.nap.edu/catalog.php?record_id=13457

[43] Clark D., Berson, T., Lin, H. (2014). At the nexus of cybersecurity and public policy, some basic concepts and issues. Washington, DC: National Research Council, The National Academies Press.

[44] Bodeau, D., Graubart, R. (2016). Cyber resilience metrics: Key observations. The MITRE Corporation.

[45] Sheffi, Y. (2005). Building a resilient supply chain. *Harvard Business Review,* 1(8), 1-4.

[46] U.S. Department of Homeland Security. (2016). Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide.

[47] Caralli, R.A., Allen, J.H., Curtis, P.D., White, D.W., Young, L.R. (2010). CERT® Resilience Management Model, Version 1.0, CMU/SEI-2010-TR-012; ESC-TR-2010-012.

[48] Smith, P., Hutchison, D., Sterbenz, J.P.G., Scholler, M., Fessi, A., Karaliopoulos, M., Lac, C., Plattner, B. (2011). Network Resilience: A Systematic Approach. *IEEE Communications Magazine*, 49(7), 88-97.

[49] Bodeau, D., Graubart, R. (2011). Cyber Resiliency Engineering Framework. 11-4436. The MITRE Corporation, Bedford, MA.

[50] Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, 33(4), 471–476.

[51] Collier, Z.A., Panwar, M., Ganin, A.A., Kott, A., Linkov, I. (2016). Security metrics in industrial control systems. In: Colbert, E.J.M., Kott, A. (eds.), *Cyber-security of SCADA and Other Industrial Control Systems,* Springer: Switzerland. pp. 167-185.

[52] E. Gerck. (2002). Trust as qualified reliance on informaiton. *The COOK Report on Internet*, Janauary 2002, pp. 19-24.

[53] Spekman, R.E., Kamauff Jr., J.W., Myhr, N. (1998). An empirical investigation into supply chain management: A perspective on partnerships. *International Journal of Physical Distribution & Logistics Management*, 28(8), 630-650.

[54] PwC. (2017). The principles of trust and evolution of trust. https://www.pwc.com/us/en/services/consulting/cybersecurity/navigating-trust/evolution-of-trust.html

[55] Mayer, R.C., Davis, J.H., Schoorman, F.D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, 20(3), 709-734.

[56] Kelly E, Marchese K. (2015). Supply Chains and Value Webs. Deloitte. https://www2.deloitte.com/us/en/insights/focus/business-trends/2015/supply-chains-to-value-webs-business-trends.html

[57] Vanany, I., Zailani, S., Pujawan, N. (2009). Supply Chain Risk Management: Literature Review and Future Research. *International Journal of Information Systems and Supply Chain Management,* 2(1), 16-33.

[58] Tang, C.S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, 103(2), 451-488.

[59] Kleindorfer, P.R., Saad, G.H. (2005). Managing Disruption Risks in Supply Chains. *Production and Operations Management,* 14(1), 53-68.

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

[61] Teng, K., 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*, 42(6), 1504-1513.

[62] Hamilton, M.C., Lambert, J.H., Connelly, E.B., Barker, K. (2016). Resilience analytics with disruption of preferences and lifecycle cost analysis for energy microgrids. *Reliability Engineering and System Safety*, 150, 11-21.

[63] Hamilton, M.C., Lambert, J.H., Valverde, J. (2015). Climate and related uncertainties influencing research and development priorities. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems. Part A: Civil Engineering,* 1(2), 04015005-1.

[64] Karvetski, C.W., Lambert, J.H. (2012). Evaluating deep uncertainties in strategic priority-setting with an application to facility energy investments. *Systems Engineering*, 15(4), 483-493.

[65] Rostami, M., Koushanfar, F., Karri, R. (2014). A Primer on Hardware Security: Models, Methods, and Metrics. *Proceedings of the IEEE*, 102(8), 1283-1295.

[66] Hagen, C., Hurt, S., Williams, A. (2014). Metrics That Matter in Software Integration Testing Labs. *Crosstalk,* 28(2), 24-28.

[67] Markowitz, H. (1952). Portfolio Selection. *The Journal of Finance*, 7(1), 77-91.

[68] Sharpe, W.F. (1964). Capital asset prices: A theory of market equilibrium under conditions of risk. *The Journal of Finance*, 19(3), 425-442.

[69] Zhou, Q., Lambert, J.H., Karvetski, C.W., Keisler, J.M., Linkov, I. (2012). Flood protection diversification to reduce probabilities of extreme losses. *Risk Analysis*, 32(11), 1873-1887.

[70] Hoffman, L.J. (2010). Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development. The George Washington University Cyber Security Policy and Research Institute.