Trust and Security of Embedded Smart Devices in Advanced Logistics Systems

Christopher M. VanYe
Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
cmv7ha@virginia.edu

Beatrice E. Li
Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
blx2wj@virginia.edu

Andrew T. Koch
Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
atk8jf@virginia.edu

Mai N. Luu
Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
ml9hq@virginia.edu

Rahman O. Adekunle
Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
aa3mf@virginia.edu

Negin Moghadasi
Engineering Systems and Environment
University of Virginia
Charlottesville, VA, USA
nm2fs@virginia.edu

Zachary A. Collier
Department of Management
Radford Univerisity
Radford, VA, USA
zcollier@radford.edu

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

David Barnes
Strategic Operations
and Surety Division
Systems Planning and Analysis Inc.
Alexandria, VA, USA
dbarnes@spa.com

David Slutzky
Fermata LLC
University of Virginia
Charlottesville, VA, USA
slutzky@virginia.edu

Mark C. Manasco
Commonwealth Center for
Advanced Logistics Systems
Richmond, VA, USA
mark.manasco@ccals.com

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

***Abstract*—This paper addresses security and risk management of hardware and embedded systems across several applications. There are three companies involved in the research. First is an energy technology company that aims to leverage electric-vehicle batteries through vehicle to grid (V2G) services in order to provide energy storage for electric grids. Second is a defense contracting company that provides acquisition support for the DOD's conventional prompt global strike program (CPGS). These systems need protections in their production and supply chains, as well as throughout their system life cycles. Third is a company that deals with trust and security in advanced logistics systems generally. The rise of interconnected devices has led to growth in systems security issues such as privacy, authentication, and secure storage of data. A risk analysis via scenario-based preferences is aided by a literature review and industry experts. The analysis is divided into various sections of Criteria, Initiatives, C-I Assessment, Emergent Conditions (EC), Criteria-Scenario (C-S) relevance and EC Grouping. System success criteria, research initiatives, and risks to the system are compiled. In the C-I Assessment, a rating is assigned to signify the degree to which criteria are addressed by initiatives, including research and development, government programs, industry resources, security countermeasures, education and training, etc. To understand risks of emergent conditions, a list of Potential Scenarios is developed across innovations, environments, missions, populations and workforce behaviors, obsolescence, adversaries, etc. The C-S Relevance rates how the scenarios affect the relevance of the success criteria, including cost, schedule, security, return on investment, and cascading effects. The Emergent Condition Grouping (ECG) collates the emergent conditions with the scenarios. The generated results focus on ranking Initiatives based on their ability to negate the effects of Emergent Conditions, as well as producing a disruption score to compare a Potential Scenario's impacts to the ranking of Initiatives. The results presented in this paper are applicable to the testing and evaluation of security and risk for a variety of embedded smart devices and should be of interest to developers, owners, and operators of critical infrastructure systems.**

***Index Terms*—Hypersonics; Bidirectional Charging; Trust and Security; Electric Vehicle Charging; Enterprise Resilience; Risk Register; Systems Integration**

I. Introduction

As today's world becomes increasingly centered around technology, there is an ever-increasing number of advanced logistical systems that use embedded smart devices [1] [2]. The rise of interconnected devices, called the Internet of Things (IoT), has led to a proportional growth in a systems' security

issues such as privacy, authentication, and secure storage of data [3] [4] [5]. As the IoT continues to expand in the future, everyday items could become key components of a personal security breach, leading to stolen identities, credit cards, and passwords [6] [7]. Escalating beyond just personal information security, these issues expand to systems such as large-scale power systems, whose failure could affect thousands of lives, to military weapons systems, whose security failure could leak information that threatens national security [8] [9]. Assessments of the defense supply chain have discovered an abundance of counterfeit electronic components, posing a critical threat to national security [10]. The supply chain for logistic systems must be secure, including the microelectronics embedded within the system, as the impacts of electronics from untrusted sources include confidentiality, integrity, and availability [11]. The urgent need for a robust supply chain is one that has been emphasized by members of the United States government at all levels, including President Biden.

In this model and analysis, three different testbeds are used: (1) a bidirectional electric vehicle charging system, (2) development and acquisition of hypersonics aviation technologies a Navy hypersonic glide body, and (3) logistics systems as a whole.The analysis will be used to recommend the most efficient ways to mitigate major risks to these systems. To do so, success criteria, initiatives, emergent conditions, and potential scenarios will be gathered. They will then be used to understand how specific risks to the system prevent system success and which initiatives have the potential to address those risks. The conclusion of the analysis will give recommendations to developers of the three systems of which initiatives should be invested in and which potential scenarios are the most disruptive.

II. Methods

This section describes a scenario-based preference model used to identify relevant initiatives, assess the influence of potential scenarios to prioritize investment in initiatives, and identify the most extreme disruptive scenarios, whether positive or negative [12] [13]. Success criteria are based on goals of the system set by the user of the system. Their relationships to the initiatives are developed to measure the potential impact of investing in specific initiatives.The set of criteria, $C = \{c_1, \ldots, c_i\}$,are derived from research of technological analyses, literature reviews, and expert opinions mainly describing the goals of the system. Initiatives development opportunities in the form of technologies, policies, assets, projects, or other such investments. The set of initiatives, $X = \{x_1, \ldots, x_i\}$ is developed through literature reviews and the review of third-party analyses. This list is not exhaustive and can be expanded according to stakeholder input or further research. As a part of the analysis, each success criterion is given a level of impact for each given initiative, indicating how well the initiative supports the criterion.

Emergent conditions are stakeholder beliefs or values, future events, or trends that could impact the system's ability to meet success criteria. These emergent and future conditions could potentially disrupt the prioritization of initiatives by posing danger to the system or exploiting vulnerabilities. The set of emergent conditions $E = \{e_1, \ldots, e_i\}$re drawn from stakeholder interviews and third-party literature. Scenarios, $S = \{s_1, \ldots, s_i\}$, are made up of one or more of the given emergent conditions and represent the most crucial challenges or risks that face the system on a larger scale, typically on the scale of international events or shifts.

After success criteria, initiatives, and potential scenarios have been established, the true analysis can begin. Three relevance options are assigned to criteria: High, Medium, and Low. These options are given based on how distinctly the impact to one success criteria would impact the others They correspond to weights decided upon by experts and stakeholders. These weights are created the criterion are again assessed for each scenario s_i. Through research based system context, each criterion is given one of five relevance measures based on how it changes under a given scenario. These measures are Decreases, Decreases Somewhat, No Change, Increases Somewhat, and Increases. Each measure is assigned a ratio for change. This re-weighting is done for each potential scenario. The scores are used to create the entries $(w_j)^p_k$in the $m_k \times n$ impact matrices W^p_k for scenario s_i.

Following the establishment of baseline criteria weights and re-weighting of criteria for each scenario, each criterion is then assessed on whether it is addressed by a given initiative. This is also performed through literature research and expert elicitation. The available levels of impact for initiatives assessments are strongly agree, agree, and somewhat agree. These assessments correspond to weights decided upon by stakeholders and experts. Thus, entries x_{ij}, the score initiative x_i receives for criterion c_j in an impact matrix X_i is created for each initiative. In summary, the criteria are first given a relevance measure in the baseline scenario, then each criterion is re-weighted based on the different scenarios. Criteria are then assessed on whether they are addressed by each initiative. A score for each initiative is then created under each scenario through a linear additive value function shown in (1).

$$V(x_i)_k = W_k X_i \tag{1}$$

Given a score for the initiatives, each can now be ranked and prioritized such that: if a given initiative's score under a given scenario is higher than that of another initiative under the same given scenario then the first initiative should be prioritized higher. Once arriving at a score for each initiative under each scenario the initiatives can be ranked where $R(x_i)^p_k$ represents the rank of initiative x under scenario s_i for the stakeholder perspective p. Thus, a disruptiveness measure for each scenario under each perspective, $D(s_k)$ can be obtained by using the sum of square ranking illustrated in (2).

$$D(s_k)^p = \sum_i = 1^n (R(x_i)^p_b - R(x_i)^p_k)^2 \tag{2}$$

Thus, it can be illustrated to stakeholders which scenarios are most and least disruptive to the system based on the outputs

of (2). The purpose of these scores is to determine a ranking of the most and least disruptive scenarios.

III. Demonstration

This section explores the application of this analysis on hypersonic glide bodies, bidirectional charging systems, and logistics devices as a whole. First, a set of criteria $C = \{c_1, \ldots, c_i\}$, taken from the analysis on hypersonic glide bodies, are listed in Table I and identified through discussion with industry experts and the review of third party literature. There are 20 total initiatives shown in Table II and were taken from the analysis done on bidirectional charging networks. The set of emergent conditions, $E = \{e_1, \ldots, e_i\}$, and potential scenarios are shown in Table III and are taken from the analysis on logistics devices. Both were sourced through literature research and analyses, as well as discussions stakeholders.

With the help of stakeholders and independent research, each of the initiatives were assessed qualitatively against all criteria. The initiatives were ranked based on how directly they influenced the success of the system through the determined criteria . These rankings were then converted to quantitative scores. The relative importance of the criteria was reevaluated at different scenarios and affects how important initiatives are and links with other assessments to help find the most important and potentially disruptive initiatives. The importance of the criteria and scenarios were then qualitatively assessed in light of each scenario to determine if they were to decrease, somewhat decrease, neutral, somewhat increase, or increase the system's ability to meet the criteria. The resulting method created a ranking of resilience of each initiative and the disruptiveness of each scenario.

TABLE I
Success Criteria Used for Hypersonic Glide Body Analysis

Index	*Criterion*
c.01	Cost Effectiveness
c.02	Tactical Surprise
c.03	Promptness
c.04	Defense Penetration/Resilience
c.05	Sufficient range to reach target
c.06	Lethality/Ability to destroy the target
c.07	Maneuverability: Flight Course Adaptability (ex: Mobile targets or Avoiding No-Fly zones)
c.08	Cyber Security (ex: Supply Chain threats)
c.09	Durability: Thermal Loadings across flight body
c.10	Accuracy/Increased destruction of Buried or Harden Targets without increased collateral damage
c.11	Cyber Resilience (ex: GPS Denial)
c.12	Deterrence without escalation
c.13	Maintain the National Hypersonic Technology Infrastructure: Assortment of critical wind tunnels and other ground testing facilities and Critical overland and overwater ranges

IV. Analysis of Select Scenarios

The following section describes three different potential scenarios, one from each of our specific test beds. The scenarios that will be covered are: Innovation in Detection, Electricity Market , and Proprietary Information Leak.

TABLE II
Initiatives Used for Bidirectional Charging Network Analysis

Index	*Initiative*
x.01	Simulation for market variability
x.02	Regional resource planning
x.03	Standards of encryption
x.04	Develop charge controllers
x.05	Understanding load cycles
x.06	Identify at-risk components
x.07	Test at-risk components
x.08	Develop tools for showing benefits of bidirectional charging
x.09	Analysis of time-of-use rates
x.10	Build out to rural networks
x.11	Analysis of long term wear on batteries
x.12	Understanding effects of battery use on the environment
x.13	Cost-effective resource allocation to portfolios of security measures for embedded devices in a large-scale system
x.14	Trusted Enterprise Communications and Cyber-Physical Integration of Advanced Fleet Electrical Vehicle Chargers in a Mobile Electric Grid
x.15	Secure Processor Design by RISC-V Framework
x.16	Current Sensing based On-chip Analog Trojan Detection Circuit Compatible with Chip Design and Validation Flow
x.17	Stochasticity, Polymorphism and Non-Volatility: Three Pillars of Security and Trust Intrinsic to Emerging Technologies
x.18	Design Obfuscation and Performance Locking Solutions for Analog/RF Ics
x.19	Connectionless RFID based Secure Supply Chain Management
x.20	Leveraging Hardware Isolation for Secure Execution of Safety-Critical Applications in Distributed Embedded Systems

A. Innovation in Detection

Hypersonic boost-glide weapons systems, such as the United States Navy's Conventional Prompt Strike (CPS), are designed around the application of their hypersonic speeds. One such application is the hypersonics glide body's core ability to have tactical surprise when being engaged [14]. Tactical surprise, in this context, is when the adversary only becomes aware that an attack is underway until it is too late to launch any type of countermeasure. For a system like Conventional Prompt Strike, which would be used in defense suppression or adversary weapon destruction in the opening of a conflict, the success of a deployment relies heavily on whether or not the adversary has warning of the incoming attack [15]. Due to this reliance on tactical surprise for the probable success of such hypersonic weapons systems, one of the most disruptive possibilities is adversarial innovation in detection.

Two core systems using the attack detection and warning systems are early-warning satellites and early-warning radars. Both of these systems, however, have drawbacks that prevent them from being well suited for the detection of hypersonic boost-glide systems. Currently, only the United States and Russia have full thermal array early-warning satellite systems in orbit around the planet that would be able to immediately detect that exact type of booster rocket used for hypersonic weapons [14]. With the technological hurdles and sheer cost of getting satellite technology setup in orbit, it is highly unlikely that any United States adversaries will invest in this technology bar one. China is innovating on its current capabilities and could in the future implement a similar capability as the United

TABLE III
EMERGENT CONDITIONS AND SCENARIOS USED FOR SCENARIOS ANALYSIS ON LOGISTICS DEVICES

Scenario	*Emergent Conditions*
s.01 Proprietary Information Leak	e.02 - Reverse Engineering By Opposition
	e.18 - Poorly Encrypted Data/No Data Encryption
	e.19 - Limiting Employee Access to Hardware
	e.20 - Pilot Testing of Services to Ensure Security Functionality
	e.21 - Auditability/Ease of Monitoring System Activity
	e.22 - Development of More Advanced Blockchain Storage/Distributed Data Storage
s.02 Cyber Attack on Active System	e.03 - Supply Chain Cyber Attacks - Trojans/Counterfeit hardware
	e.04 - Supply Chain Cyber Attacks - Faulty Publicly Sourced Parts
	e.05 - Denial of service
	e.06 - Distributed denial of service
	e.07 - Malware
	e.08 - Man-in-the middle
s.03 Supply Chain Threats	e.01 - Counterfeit product in supply chain
	e.03 - Supply Chain Cyber Attacks - Trojans/Counterfeit hardware
	e.04 - Supply Chain Cyber Attacks - Faulty Publicly Sourced Parts
	e.12 - Supply chain
s.04 Acquisition of System by Competitor	e.02 - Reverse Engineering By Opposition
	e.17 - User Authentication Issues
	e.19 - Limiting Employee Access to Hardware

States and Russia, especially with the current strides the world is making toward increased space travel. This adversarial innovation would change the battlespace across the world, as this lack of this form of detection capability, specifically in China, has been used in the interpretation of the application of hypersonic weapons [15]. The other major technology that could be adapted to detect hypersonic weapons is early-warning radars [16]. The major difference between these two technologies is that early-warning radars are extremely widespread, as the technology is much simpler and cheaper. In relation to hypersonic weapons specifically, the current standard early-warning radars would require modification to detect hypersonic weapons due to their higher-than-normal flight path [15]. These modified radars, along with more specialized radars used to detect ballistic missiles, could be employed directly in the detection of hypersonics [17] [18].

To counter this kind of disruptive innovation in adversarial detection, specific abilities and enhancements of hypersonic systems can be more thoroughly investigated and invested in for future hypersonic systems. Of course, a simple solution for these systems would be to push the speed boundary beyond current abilities. However, this would require further investment in the simulation of these systems to grow the understanding of the unique heat and air condition in the boundary layers around the glide body at faster than Mach 5 speeds [19]. Due to the novelty of these systems and their steep costs, simulation-based analyses are key in making progress towards the understanding of the environments surrounding the glide body in flight. Another way hypersonic systems could be further adapted to address the threat of innovation in adversarial detection, is the analysis of enhanced control and maneuverability abilities. Adaptive flight patterns due to the systems maneuverability in flight would allow the system to dynamically fly around areas with detect technologies, or at least avoid them for as long as possible during its flight to target. Controlling these systems during flight is a delicate and mostly automated task, in which there already are in-depth analyses into better algorithms for enhancing control [20] [21].

B. Electricity Market

The electricity market applies heavily to bidirectional charging since an unstable or unhealthy electric grid can knock out not only power to houses but also a person's accessibility to an electric car. Since the goal of bidirectional charging is to integrate electric cars more efficiently into the power grid, there need to be standards that are able to support both car charging and the current stress on the grid when followed correctly. Due to the closely-knit nature of both bidirectional charging and the resilience of an electric grid, the analysis has found that a change in the electricity market possesses the most potential in being one of the most detrimental scenarios.

One example of the issues with the current electricity grid is what happened in Texas recently. Due to a lack of preparation and no available help from outside power grids, the freezing weather that hit Texas knocked out electricity in almost every home in the state. Because Texas was not linked with any other grids from outside the state, it could not pull from neighbor's power grids to supplement their own supply [22]. Thankfully, with a new president comes new green energy incentives. President Biden is planning on pouring more money into the green market space in an attempt to move the United States away from fossil fuels [23]. This comes at a great time for bidirectional charging because as the country's electricity infrastructure further develops, so will the ability for external hardware like bidirectional charging ports to be added onto the grid.

Changes in the electricity market bring changes to key initiatives for bidirectional charging, like changes in battery costs, grid reliability, electricity prices, and generation of renewable energy. For example, a positive change in the electricity market might be because of reduced battery costs, increased reliability, lower electricity prices, increased generation of renewable energy, or a combination of all four. All of these things could help lower the cost of producing a bidirectional charger or increase the charger's reliability. While the exact effects of a down or upturn in the electricity market is unknown, it is almost certain that a negative change in the market will have large detrimental effects on bidirectional chargers while a positive change in the market will bring new opportunities to the space.

C. Proprietary Information Leak

Generally, proprietary information leak is when confidential information is released or obtained by unauthorized parties

[24]. For this scenario, the definition of a proprietary information leak will include an intent by the unauthorized party to use the leaked information to better their own device. Devices are often released into a competitive market, meaning even the slightest edge on a competitor can sway the annual revenue. Because of this, future innovations along with current technologies are often kept private from the public eye. A leak of these ideas could be catastrophic for a company and is therefore one of the most important scenarios to consider when looking at the overall security of connected devices.

Apple is one of the largest companies in the world and its iPhone is the best-selling phone of all time [25]. In 2007, right before Apple introduced the iPhone, the best-selling phone came from Blackberry. Since then, Blackberry no longer sells phones and focuses on industry software because of how quickly Apple took over the cell phone industry and how quickly other Blackberry competitors rushed to copy Apple. Back in 2007, if Blackberry stole the designs and ideas for the iPhone, the cell phone industry might look very different than what it does today. The iPhone would no longer be the leader of smartphones, but a close copy of what Blackberry could put out first since they had all the designs and security plans. Even today, if Samsung or Google were able to see the plans for the iPhone for the next 5 years, Apple would quickly go from the leader to a follower, lose out on millions in revenue, and lose market capitalization in the stock market [26].

The example above shows the importance of preventing an information leak. Leaks can come from anywhere from reverse engineering by a competitor to poorly encrypted data, all of which were covered in the research done in this paper. While the effects of these leaks can have different magnitudes depending on what actually gets released into a competitor's hands, all research points to seriously detrimental outcomes.

V. Results

TABLE IV
NORMALIZED DISRUPTIVE SCORES FOR BIDIRECTIONAL CHARGING

Rank	Scenario
1	s.09 - Change In Government Policy
2	s.03 - Electricity Market
3	s.06 - Funding Decreases
4	s.04 - Green Movement
5	s.02 - Public Support
6	s.08 - Obsolete Technology
7	s.05 - Technology Innovation
8	s.07 - Change of Vendor
9	s.01 - Private Support

TABLE V
RESILIENCE RANKING FOR INITIATIVES

Rank	Initiative
1	x.07 - Test at-risk Components
2	x.02 - Regional Resource Planning
3	x.06 - Identify at-risk Components
4	x.05 - Understand Load Cycles
5	x.11 - Analysis of Long Term Wear on Batteries

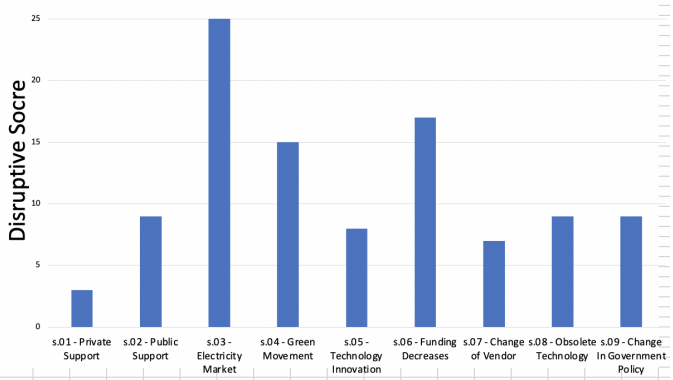

Fig. 1. Disruptive Scores for Each Scenarios Involved in Bidirectional Charging

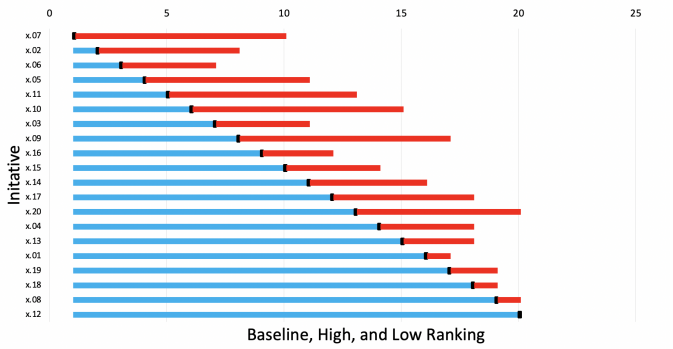

Fig. 2. Prioritization of Initiatives Related to Bidirectional Charging

There are two summary graphs. The summary graphs are used to visualize the raw input data from earlier tabs in the spreadsheet. As seen in Figure 1, each scenario is given a "Disruptive Score", meaning the higher the score, the more of an issue the scenario might be to the stakeholder. According to the summary graph, technology innovation and change of vendor have the lowest "Disruptive Score", which indicates that it would not have a significant effect on the changes of the system. So far, we have identified changes in the electricity market, funding decreases, and changes in public support of charging networks as the most disruptive scenarios. This means that an increase in one of these scenarios would lead to the greatest increase in system changes out of all the other scenarios and emergent conditions.

Figure 2 is an initiative ranking graph that aims to potentially aid in the prioritization of initiatives. The blue and red extensions highlight the possible range of each initiative from the baseline effect of such initiative, while the black bar shows the average ranking of each initiative. In this case, initiatives 7, 2, 6, 5, and 11 have the highest baseline rankings but as seen from the blue lines, all of them have the potential to be the most important initiative depending on how emergent conditions play out in the real world.

VI. Conclusion

Table VI provides a summary of several scenarios and the associated proposed actions that can support enterprise resilience of hypersonic glide bodies, bidirectional charging networks, and logistics devices. Ongoing and future work should address these several recommended actions [14] [27] [28].

TABLE VI
Key Findings For Enterprise Resilience of Advanced Logistics Systems to Emergent and Future Conditions

Selected Scenarios	Recommended Actions
s.03 - Innovation in Detection	Utilizing simulation-based analyses to advance understanding of the environmental conditions of the glide body in flight. Research into adaptive flight patterns will help evade detection technologies.
s.03 - Electricity Market	Increase in funding to ensure resilience and support in electric grids to mitigate the negative impacts of unforeseen circumstances such as extreme weather.
s.01 - Proprietary Information Leak	Establishing strategies to secure proprietary information and prevent information leaks such as data encryption or a movement towards blockchain for data storage.

Acknowledgment

This effort was supported in part by the National Science Foundation under Grant 1916760 "Phase I IUCRC University of Virginia: Center for Hardware and Embedded Systems Security and Trust (CHEST)", Systems Planning and Analysis Inc., Commonwealth Center for Advanced Logistics Systems, Fermata LLC, National Science Foundation Center for Hardware and Embedded Systems Security and Trust, Virginia Department of Transportation, and the United States Army Corps of Engineers.

References

[1] R. A. Martin, "Visibility control: Addressing supply chain challenges to trustworthy software-enabled things," *2020 IEEE Systems Security Symposium (SSS)*, 2020.

[2] Z. A. Collier, D. DiMase, K. Heffner, and I. Linkov, "Building a trusted and agile supply chain network for electronic hardware," in *Proceedings from the 20th international command and control research and technology symposium*, 2015.

[3] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, p. 544–546, 2018.

[4] V. G. Garagad, N. C. Iyer, and H. G. Wali, "Data integrity: A security threat for internet of things and cyber-physical systems," *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020.

[5] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures and design tools," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, p. 1–1, 2020.

[6] O. Ionescu, V. Dumitru, E. Pricop, O. Buiu, C. Cobianu, M. Raneti, S. Pircalabu, and C. Marica, "On the development of a robust cyber security system for internet of things devices," *2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 2019.

[7] S. Singh and D. Kumar, "Perceptions of security and privacy in internet of things," *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020.

[8] G. Tsochev, "Some security problems and aspects of the industrial internet of things," *2020 International Conference on Information Technologies (InfoTech)*, 2020.

[9] H. Chen, M. Hu, H. Yan, and P. Yu, "Research on industrial internet of things security architecture and protection strategy," *2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, 2019.

[10] U.S. Government Accountability Office, Feb 2016. [Online]. Available: https://www.gao.gov/products/GAO-16-236

[11] S. Ranger, "Huawei security: 'significant' engineering flaws are a risk to our telecoms networks, says uk," Mar 2019. [Online]. Available: https://www.zdnet.com/article/huawei-security-significant-engineering-flaws-pose-risk-to-networks-says-uk/

[12] M. L. Hassler, D. J. Andrews, B. C. Ezell, T. L. Polmateer, and J. H. Lambert, "Multi-perspective scenario-based preferences in enterprise risk analysis of public safety wireless broadband network," *Reliability Engineering System Safety*, vol. 197, p. 106775, 2020.

[13] R. C. Donnan, C. R. Edwards, A. R. Iyer, T. Karamete, P. F. Myers, S. E. Olson, R. S. Prater, D. J. Andrews, T. L. Polmateer, M. C. Manasco, and et al., "Enterprise resilience of maritime container ports to pandemic and other emergent conditions," *2020 Systems and Information Engineering Design Symposium (SIEDS)*, 2020.

[14] J. M. Acton, *Silver bullet?: asking the right questions about conventional prompt global strike*. Carnegie Endowment for International Peace, 2013.

[15] A. F. Woolf, *Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues*. Library of Congress, Congressional Research Service, 2014.

[16] H. Xie, S. Shi, F. Li, J. Su, D. An, G. Wang, X. Huang, L. Zhang, H. Xiao, Z. Zhou, and et al., "Evaluation and simulation of detection effectiveness of airborne early warning radar," *2017 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, 2017.

[17] J. Huang, H. Zhang, G. Tang, and W. Bao, "Radar tracking for hypersonic glide vehicle based on aerodynamic model," *2017 29th Chinese Control And Decision Conference (CCDC)*, 2017.

[18] Q. Yongjie, L. Jinrong, B. Liping, D. Hong, and L. Xiangru, "Detection probability of early warning radar against hypersonic cruise missile," *Proceedings of 2011 IEEE CIE International Conference on Radar*, 2011.

[19] J. B. Middlebrooks, E. Farnan, E. H. Matlis, T. C. Corke, C. D. Mullen, M. Mcmillan, and H. L. Reed, "Design of a hypersonic boundary layer transition control experiment utilizing a swept fin cone geometry in mach 6 flow," *AIAA Scitech 2021 Forum*, 2021.

[20] S. Jian-Bo, P. Xing-Hua, and Z. Yu-Shan, "Initial descent phase guidance for hypersonic glide vehicle," *2017 36th Chinese Control Conference (CCC)*, 2017.

[21] N. E. Gaiduchenko and P. A. Gritsyk, "Hypersonic vehicle trajectory classification using convolutional neural network," *2019 International Conference on Engineering and Telecommunication (EnT)*, 2019.

[22] E. Hirs, "Why the texas power market failed," Mar 2021. [Online]. Available: https://insights.som.yale.edu/insights/why-the-texas-power-market-failed

[23] M. Benintende, "Electricity market modernization and cost reductions powering the global grid battery energy storage market," Mar 2021. [Online]. Available: https://finance.yahoo.com/news/electricity-market-modernization-cost-reductions-155100206.htmlsoc_src=socialshsoc_trkm̃a

[24] E. Gessiou, Q. H. Vu, and S. Ioannidis, "Irild: An information retrieval based method for information leak detection," in *2011 Seventh European Conference on Computer Network Defense*, 2011, pp. 33–40.

[25] D. Pierce, "The complete history of the iphone-and what's coming next," Dec 2018. [Online]. Available: https://www.wired.com/story/guide-iphone/

[26] S. Du, J. Wang, and K. Gwebu, "Stock market reaction to data breaches: The moderating role of corporate social responsibility," in *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 2017, pp. 1–2.

[27] D. J. Andrews, T. L. Polmateer, J. P. Wheeler, D. L. Slutzky, and J. H. Lambert, "Enterprise risk and resilience of electric-vehicle charging infrastructure and the future mobile power grid," *Current Sustainable/Renewable Energy Reports*, vol. 7, no. 1, p. 9–15, 2020.

[28] H. Thorisson, F. Baiardi, D. Angeler, K. Taveter, A. Vasheasta, P. Rowe, W. Piotrowicz, T. Polmateer, J. H. Lambert, I. Linkov, and et al., "Resilience of critical infrastructure systems to hybrid threats with information disruption," *Resilience and Hybrid Threats: Security and Integrity for the Digital World*, vol. 55, 2020.