Proceedings of the American Society for Engineering Management 2025 International Annual Conference
H. Zhang,G. Natarajan, and E.H. Ng eds

IMPROVING ELECTION SYSTEM SECURITY THROUGH SOFTWARE FAILURE MODES EFFECTS ANALYSIS

Vanessa Gregorio, B.S.
Hao Nguyen, M.S.
Skylar Gayhart, M.S.
Josh Dehlinger, Ph.D. *
Natalie M. Scala, Ph.D.
Towson University

***jdehlinger@towson.edu**

Abstract
The designation of election infrastructure as a critical infrastructure subsector by the U.S. Department of Homeland Security in 2017 highlights the ongoing need to safeguard these systems from emerging cyber, physical, and insider threats. As complex socio-technical systems, election infrastructure relies on the interaction between hardware, software, and human operators, making it vulnerable to a range of security risks. This study builds upon prior security assessments conducted by the U.S. Elections Assistance Commission of precinct count optical scanners (PCOS), the primary machines used for ballot scanning and tabulation. To do so, this work employs Software Failure Modes and Effects Analysis (SFMEA), a widely used method for identifying and mitigating software-related failures. Specifically, through an extensive literature review and structured application of SFMEA, 60 additional threats were identified and incorporated into an updated threat tree model. By integrating SFMEA, which takes a bottom-up approach to trace potential failure points, with threat tree analysis, a top-down method for identifying root causes, this research adapts a more comprehensive, bi-directional risk evaluation framework. The results enhance election system security by demonstrating how SFMEA can be systematically applied to strengthen threat assessments. Furthermore, the methodology demonstrates a systematic threat and mitigation analysis approach to address the cyber, physical, and insider risks, including those posed by adversaries and trusted insiders, that is also applicable to national critical infrastructure socio-technical systems and processes.

Keywords
Election security, critical infrastructure, software failure modes and effects analysis, attack trees

Introduction and Motivation
Over the past few decades, technology has become embedded in the fabric of our society, governance, and national critical infrastructure to the extent that it is now essential to conduct systematic, quantitative analyses to ensure resilience and security against evolving adversaries. The Department of Homeland Security defines 16 U.S. critical infrastructure sectors that include those systems and processes deemed important to the United States such that their failure or exploitation could gravely threaten national security and weaken the foundations of democracy (Cybersecurity and Infrastructure Security Agency, 2003). Increasingly, these critical infrastructure assets comprise of socio-technical systems (i.e., complex systems that involve the interaction of human, hardware, software, and other organizational components (Baxter & Sommerville, 2011)) and need to be resilient to the cyber, physical, and insider threats that could compromise their integrity (National Institute of Standards and Technology, 2018). Yet, many existing threat and mitigation analyses, approaches, and models do not holistically examine the cyber, physical *and* behaviors of human actors, such as trusted insiders, in the security of systems and instead simply rely on traditional cyber-physical systems threat analyses (Price, Scala & Goethals, 2019). This neglects the dual role of the trusted insider, which can be both a source of risk as well as a critical defense in recognizing and mitigating emerging risks (Kassel, Bloomquist, Scala & Dehlinger, 2024).

Critical infrastructure systems are also a key target for cyber attacks. For example, the 2021 DarkSide ransomware attack on the Colonial Pipeline forced a shutdown of the 5,500-mile fuel network, triggering gas shortages across the U.S. East Coast (Easterly & Fanning, 2023). While election systems (e.g., optical scanning and direct-recording

electronic voting machines), would not be designated as U.S. critical infrastructure under the Government Facilities sector until 2017 (Election Assistance Commission, 2017), they have been subjected to attacks by foreign adversaries. For example, the 2019 Senate Intelligence Committee concluded that the election systems in all 50 states had been targeted by the Russian Federation in 2016, and Special Counsel Robert Mueller testified before Congress that foreign interference in U.S. elections was ongoing and would continue to occur (Sanger & Edmonson, 2019). Thus, a deeper understanding of system architectures and potential failure modes across these critical sectors is essential for developing proactive security measures and ensuring the continued functionality and integrity of vital services in the face of persistent and evolving threats (Tsantikidou & Sklavos, 2024).

Despite the increasing attacks on election infrastructure, many existing threat and mitigation analyses frequently fall short in adequately addressing the complex interplay of cyber, physical, and insider threats within socio-technical systems and/or have not been updated to reflect the adaptive adversary (Scala, Goethals, Dehlinger, Mezgebe, Jilcha & Bloomquist, 2022). Specific to this work, in 2009 the Election Assistance Commission (EAC), in collaboration with the University of Southern Alabama, published a comprehensive study to identify and mitigate threats to U.S. elections across various voting technologies (United States Election Assistance Commission Advisory Board, 2009). This study involved an extensive literature review and multi-tiered verification process with input from election experts. However, since the study's publication, advancements in technology, adaptive adversaries, foreign interference, and the rise of voting misinformation/disinformation have introduced new complexities and highlights the critical need for updated risk assessments to address modern threats and ensure public trust in the electoral process, which is vital for maintaining democratic institutions.

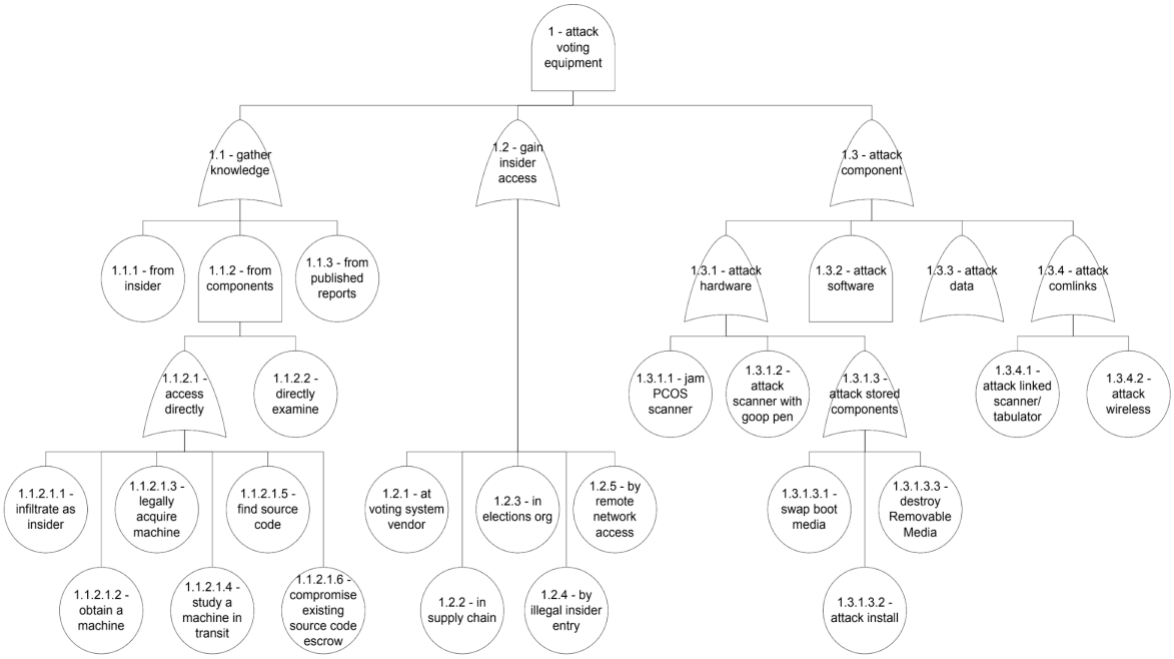
To build upon this prior risk analysis, the work presented in this paper specifically focused on and updated the precinct count optical scanner (PCOS) attack tree to include all currently known risks associated with these voting machines and will develop a comprehensive threat modeling and mitigation analysis. Attack trees provide a visual representation of potential threat scenarios, organizing risks hierarchically into branches and nodes that delineate generalized threats, specific events, and methods used to execute attacks (Schneier, 1999). PCOS voting machines scan and tabulate paper ballots and are the in-person voting equipment used in almost 70% of the country during the 2024 U.S. Presidential Election, as well as anticipated in the upcoming 2026 U.S. Elections (Verified Voting, n.d.). This work identified and analyzed more than 60 new and a rigorous, risk analysis process involving literature reviews, Software Failure Mode and Effects Analysis (SFMEA), and a Delphi Panel to evaluate the impact of threats. New risks were categorized by voting phases (i.e., pre-voting, voting, post-voting) and threat classifications (i.e., insider, physical, cyber). Specifically, the contributions of this work are:

1. An extensive review and adoption of SFMEA in a security context to identify new threats to PCOS election equipment to update the prior 2009 EAC PCOS attack tree.
2. Adoption of a complete bi-directional analysis approach of the risks and threats of the PCOS election equipment to produce a complete risk analysis and threat model.
3. A complete Delphi Panel analysis of all threats in an updated PCOS attack tree to enable the generation of minimal cut sets and quantitative scenario generation.

These findings form the foundation for a comprehensive and updated PCOS attack tree model and risk analysis, enhancing election security research and providing actionable insights to address evolving challenges in election infrastructure. The work here is part of a larger effort to understand and analyze the cyber, physical, and insider threats within election processes and to develop mitigations and actionable training to improve the integrity and security of our election infrastructure at the local level.

The remainder of the paper is organized as follows. The following section provides an overview of the background analysis approaches utilized in this work, including software threat/fault tree analysis, SFMEA, Bi-Directional Safety Analysis (BDSA), and software safety cases; background and related research in election security is also overviewed. Following that, the risk modeling and threat analysis approach used in this work to update the PCOS attack tree is detailed, including the application of SFMEA to identify and classify new cyber, physical, and insider threats to the PCOS attack tree. Next, a brief discussion of ongoing and future work stemming from the contributions of this paper is provided prior to offering some concluding remarks.

Exhibit 1. Partial Precinct Count Optical Scanner Attack Tree (United States Election Assistance Commission Advisory Board, 2009).



Background Work

The work presented here builds upon our prior work on risk analysis and threat modeling of the mail-voting election process (Scala, Goethals, Dehlinger, Mezgebe, Jilcha & Bloomquist, 2022) and leverages several analysis techniques from software safety analysis, including Software Fault Tree Analysis (SFTA), Software Failure Modes and Effects Analysis (SFMEA), Bi-Directional Safety Analysis (BDSA), and safety cases to analyze and model the cyber, physical, and insider threats against complex socio-technical systems and infrastructure, such as election infrastructure. The following subsections provide an overview of these analysis approaches as well as highlighting prior research efforts in election security.

Software Fault/Attack Tree Analysis

Software Fault Tree Analysis (SFTA) is an extension of classical hardware-centric fault tree methods that models software-specific fault scenarios in safety-critical systems that may propagate to a system-level failure and/or hazard/accident (Leveson, 1995). More specifically, SFTA is a top-down, deductive, backward analysis method that models the causal events contributing to an undesirable event (i.e., a hazard or accident) representing the root node. That is, SFTA initiates with a root node undesired event and analysis then determines the set of necessary pre-conditions to cause the root node event and are joined to the parent node by Boolean logic gates describing their contributing relation. This analysis process then continues for each child node subtree until basic, atomic events are reached. With tooling, this analysis allows for the generation of minimal cut sets and scenario generation to describe the conditions that could cause the root node, or undesirable event. SFTA has been applied to analyze critical infrastructure. For example, Feiler and Delange (2017) generated software fault trees from Architecture Analysis & Design Language (AADL) models of a nuclear-reactor protection system, allowing engineers to isolate minimal cut sets that could trigger hazardous shutdowns. Thumati and Kemp (2022) demonstrated that large-scale SFTA can be integrated into commercial reliability tool-suites to assess the safety of railway-signaling software and other infrastructure-centric control logic.

Similarly, attack tree analysis adopts the SFTA approach to be threat-centric and models the contributing threats that are necessary to cause the root node, security incident (Schneier, 1999). This analysis approach then graphically decomposes the complex combination of threats that can lead to the scenarios that can trigger the root node incident in a hierarchical, logic-gate representation that allows an analyst to develop mitigations in an attempt to prevent or lessen the occurrence of a security incident. Like SFTA, attack tree analysis has been used to analyze critical infrastructure. For example, Edge et al. (2006) pioneered their application to critical-infrastructure control systems,

enriching the notation with protection trees that map defenses to specific attack branches and support cost–benefit reasoning.

The work presented in this paper significantly extends the Election Assistance Commission's 2009 attack tree analysis (United States Election Assistance Commission Advisory Board, 2009). This prior attack tree model and risk analysis, partially shown in Exhibit 1, has three significant shortcomings preventing its useful application to the use of PCOS election equipment in today's adversarial environment. First, it has not been updated to reflect new cyber, physical, and insider threats. Second, SFTA and attack tree analysis examines an undesired event, iteratively and analytically tracing backwards to the causal events. Therefore, it is limited to the expertise of the analyst and may not be complete. Third, the existing PCOS threat tree model and risk analysis does not define each threat's attack cost, technical difficulty, discovery difficulty, nor its relative likelihood, disallowing a comprehensive mitigation/countermeasures analysis through the generation of minimal cut sets and quantitative scenario generation.

Software Failure Modes and Effects Analysis

Software Failure Modes and Effects Analysis (SFMEA), like SFTA, is an extension of a traditional hardware-focused reliability engineering approach to be able to predict hardware reliability with an objective to establish an overall probability that the product will operate without a failure for a certain period (Leveson, 1995). While SFTA is a top-down, backward search safety analysis approach, SFMEA is a table-driven, bottom-up, forward analysis approach that aims to identify potential failures and their resulting effects on the system. Specifically, the SFMEA process initially lists the components of a system and their associated failure modes; following this, the possible causes of the failure are listed and the effects on other components/subsystems are evaluated and listed along with the consequence on the overall system for each component's failure mode(s) (Reifer, 1979). This safety analysis approach is complementary to SFTA by starting with a failure and analyzing how the failure will impact the overall system.

SFMEA has been sparingly adapted as an approach to analyze the cybersecurity of critical infrastructure systems by treating malicious actions as failure modes for a hardware/software component. For example, Schmittner, Ma, Schoitsch & Gruber (2015) proposed the Failure-Mode, Vulnerabilities, and Effects Analysis (FMVEA) variant, which extends SFMEA columns with both attacker capabilities and exposure conditions and demonstrated its application to capture both safety faults and security risks for a cyber-physical automotive platform. More recently, Matsumoto, Iwasawa, Sakata & Kaneko (2023) utilized a security-SFMEA to derive requirements to keep autonomous mobile robots safe from denial-of-service and data-integrity attacks.

The work presented in this paper leverages SFMEA to update the EAC (2009) attack tree model and provide a more comprehensive risk analysis model by employing this bi-directional analysis approach, described next. Further, unlike prior efforts to include SFMEA as a cybersecurity analytical approach, this work includes the potential accidental and/or malicious actions of trusted insiders to the socio-technical systems comprising of critical infrastructure. This holistic, systems approach of explicitly including cyber, physical, and insider threats is an important contribution of the work since critical infrastructure systems should have an accompanying threat analysis case to systematically argue they have been thoroughly analyzed to be fit-for-purpose.

Bi-Directional Safety Analysis and Safety Cases

The results of a forward search analytical approach (e.g., SFMEA) and a backward search analytical approach (e.g., SFTA) will not yield the same results and, often, are both used in the safety analysis of safety-critical systems. Lutz and Woodhouse (1999) developed the Bi-Directional Safety Analysis (BDSA) approach to combine the advantages of these techniques, as the output of the forward search technique (i.e., the potential system-wide hazards) should match-up with the inputs of the backward search technique. Similarly, the output of the backward search technique (i.e., the low-level, local errors that cause a system-wide hazard) should match-up with the inputs of the forward search technique. That is, leveraging both complementary approaches allow for some verification of the completeness of an SFTA by ensuring that every major hazard listed in the SFMEA table is a subtree within the SFTA.

A complete and comprehensive safety analysis is necessary to make the argument that a system is acceptably safe for its intended purpose, captured in a safety case. For safety-critical systems, a *safety case* is a set of safety analysis artifacts that are developed through scientific, structured analyses to produce safety/reliability artifacts to demonstrate the "dangers associated with their use" and allowing the development of hardware, software, or processes to reduce the likelihood of a hazard or accident (Leveson, 2011). However, the socio-technical systems, including election systems, that constitute critical infrastructure may not have an accompanying *threat analysis case* to systematically argue they have been thoroughly analyzed for cyber, physical, and insider risks and to demonstrate their fitness for purpose. Further, many of the traditional cybersecurity analyses that have been applied to critical infrastructure systems (e.g., the EAC's (2009) attack trees for PCOS equipment) focus solely on physical and cyber threat scenarios

and do not take a holistic approach by including human behaviors and the actions of both adversaries and the trusted insiders responsible for administering these critical infrastructure systems (Price, Scala & Goethals, 2019).

The work presented here recognizes the need for a holistic, systematic, and quantitative approach to model and understand the risks of both the adversaries and trusted insiders who exploit threat scenarios to critical infrastructure systems and demonstrates an approach using the PCOS voting equipment as a case study.

Election Security

The current U.S. election equipment and processes, in particular the use of electronic voting systems and increased voter access processes, stem from the 2002 Help America Vote Act because of the *Bush v. Gore* U.S. Supreme Court case following the 2000 U.S. Presidential Election. This change from lever-based and/or punch card-based voting systems to, primarily, electronic-based voting systems (e.g., the PCOS voting machines examined in this work) prompted several research efforts in examining the cybersecurity of electronic voting systems. This includes, for example, Evans and Paul (2004) examined the reality and voter perceptions of the security and reliability of electronic voting systems. Yet, most election security research efforts have developed following the 2016 U.S. Presidential Election as election security and reliability became of interest within the national discourse, partly, as a result from concerns of foreign interference. Cahn (2017) documented vulnerabilities and issues in practice that have occurred with various types of equipment but did not provide a model for mitigations/countermeasures and did not specifically include vulnerabilities because of insider risk. Locraft, Gajendiran, Price, Scala & Goethals (2019) proposed a holistic approach that examines the cyber, physical, and insider risks to elections at the local level.

More recent election security research has focused on verification and cryptographic approaches to ensure the accuracy, confidentiality, integrity, and availability of ballots and vote counting. For example, Basin, Dreier, Giampietro, and Radomirović (2021) introduced a logic-based framework for verifying table-based elections and demonstrated how automated proof engines can confirm end-to-end integrity properties (e.g., individual verifiability and privacy) across thousands of symbolic execution paths. Bernhard and Wallach (2022) frames election security as an evidence driven discipline that must insist on leveraging verifiable technology and thorough statistical assurance and argues for the use of risk-limiting audits to verify election results and maintain the public trust in electronic ballot counting. Alsadi et al. (2023) proposed a protocol overlay that gives voters receipt-based proof that their encrypted ballots are included in the tally without altering the underlying service architecture. These representative efforts focus on the technical aspects of election security and developing formal proofs of protocol soundness, through statistically grounded post-election audits, to incremental deployment paths for end-to-end verifiable voting as an approach to strengthen election integrity but ignore the physical and insider threats to the process.

The work presented in this paper builds upon prior work of the U.S. Elections Assistance Commission (2009) that analyzed threats to various election equipment, including the PCOS voting machines examined in this work, and developed threat trees to catalog the threats and scenarios that could compromise the security and integrity of voting machines. Specifically, this work extends our prior efforts of examining the threats and a relative likelihood risk assessment of the mail voting process (Scala, Goethals, Dehlinger, Mezgebe, Jilcha & Bloomquist, 2022) applied to the PCOS voting machines, described next.

Risk Analysis and Threat Modeling Approach

To build upon and update the U.S. Elections Assistance Commission's (2009) threat tree model for the precinct count optical scan (PCOS) voting machine, a qualitative and quantitative risk analysis and threat modeling approach was developed that adapts the Bi-Directional Safety Analysis (BDSA) approach that leverages the Software Fault Tree Analysis (SFTA) and Software Failure Mode and Effects Analysis (SFMEA) complementary approaches to identify new threats and produce an updated, comprehensive threat tree. All newly identified threats to the PCOS voting machine and processes were analyzed and categorized, using a Delphi Panel, by type of threat (i.e., cyber, physical, or insider), timing in the voting process (i.e., prior to voting, on the day of an election, or following an election). Each threat is then quantified by its attack cost, technical difficulty, and discovery difficulty.

The EAC (2009) PCOS threat tree models just over 250 threats describing the cybersecurity scenarios that could impact the integrity of this voting machine but has not been updated to reflect the changing cybersecurity/technology landscape, adaptive adversaries, and increased foreign interference (United States Election Assistance Commission Advisory Board, 2009). Further, the EAC (2009) attack tree threats (i.e., leaf nodes) were not analyzed to further define each threat's attack cost, technical difficulty, discovery difficulty, nor its relative likelihood to occur. To identify gaps in the EAC (2009) attack tree model, this work conducted a comprehensive literature review of mainstream and non-partisan news articles, bipartisan or non-political think tanks' white papers, academic centers focusing on election security, voter instruction sheets, state-created election/voting documentation, election poll worker training manuals, etc. This led to the identification and analysis of more than 60 new threats that can impact

the integrity and operation of the PCOS voting machine. Each identified potential new threat to the PCOS voting equipment was then used as a failure mode seed to complete a SFMEA, partially shown in Exhibit 2, to understand how the exploitation of a threat.

Exhibit 2. Partial Precinct Count Optical Scanner Software Failure Modes and Effects Analysis (SFMEA).

Potential Failure Mode	Potential Effects of Failure	Potential Causes of Failure
Not signing out of poll books	Security and data privacy concerns (increased risk of unauthorized access to voter information or data breaches due to the failure to secure and sign out of poll books properly)	Lack of training or awareness
		Insufficient security protocols
		Human error or forgetfulness
Lack of tamper tape on equipment	Risk of unauthorized access	Inadequate equipment storage protocol
		Lack of personnel training on security measures
	Compromised equipment integrity	Failure in quality control procedures
		Insufficient physical security measures in election facilities
	Erosion of voter confidence (Lack of tamper tape may lead to doubts about legitimacy of the election)	Ineffective communication of security measures to the public
		Past incidents of tampering going unnoticed
Steal or destroy security key	Unauthorized Access to Sensitive Information	Physical security lapses
	Manipulation of election data	Insider collaboration
		Lack of encryption measures for data
Malicious emails	Phishing attacks (Users may fall victim to phishing attempts through deceptive emails)	Lack of user awareness and training
		Inadequate email filtering systems
		Use of email spoofing techniques
	Spread of malware to execute insider attack	Opening malicious email attachments
		Exploiting software vulnerabilities
		Lack of endpoint security measures

can impact the integrity and operation of the PCOS voting machine. For example, as shown in Exhibit 2, the "Lack of tamper tape on equipment" failure mode/threat, can lead to the unauthorized access to voting equipment.

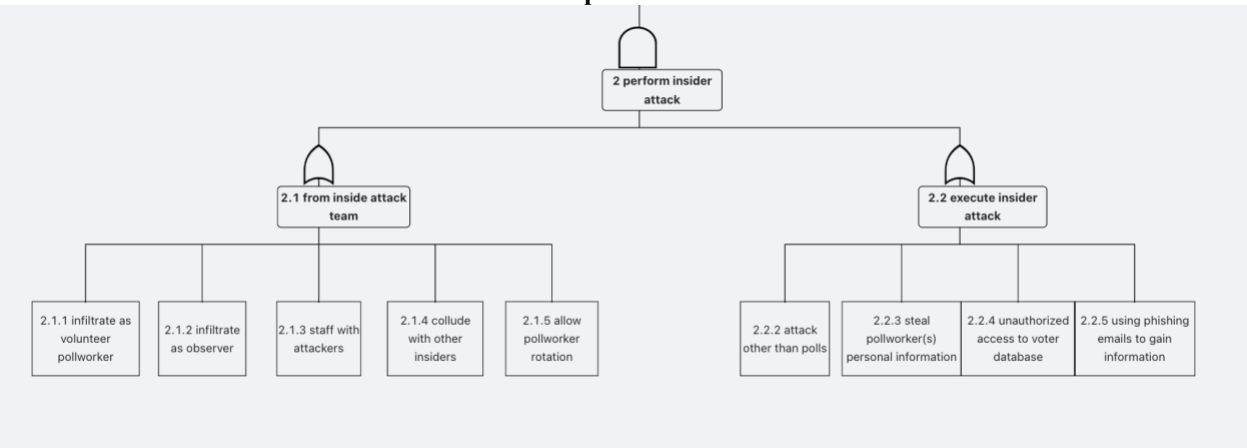
To enable rigorous risk analysis and the development of countermeasures/mitigations for the identified threats and the updated threat tree model, each newly identified threat and all previously identified threats from the EAC (2009) threat tree model were then categorized by two sets of criteria and evaluated to establish its relative likelihood of occurrence through a Delphi Panel. For each categorization, a Delphi Panel consisting of subject matter experts (SMEs) was utilized to independently record their entries and later met to discuss and arrive on an agreed, consensus category/value for each threat (Avella, 2016).

Specifically, we first follow the work of Price, Scala and Goethals (2019) to categorize each threat as a cyber, physical, or insider threat. Cyber threats include those that are related to computing and/or software attacks (e.g., the "malicious email" threat identified and shown in Exhibit 2); physical threats are those that are related to tampering with voting equipment or materials related to the voting process (e.g., the "steal or destroy security key" threat identified and shown in Exhibit 2); and, insider threats are those introduced, accidentally or maliciously, by trusted insiders to the voting process (e.g., "not signing out of poll books" threat identified and shown in Exhibit 2). This classification allows one to identify the *means* used to carry out a threat, better understand the nature of the threat, and how to develop mitigations/countermeasures. Among the 60 newly identified threats, this work classified them as 11 cyber threats, 27 physical threats, and 22 insider threats. Each threat was additionally categorized into the voting phases (e.g., pre-election, voting, or post-election) based on the EAC defined voting phases (United States Election Assistance Commission Advisory Board, 2021). This classification allows one to identify the *timing* by which a threat may occur when evaluating the PCOS voting machine vulnerabilities and further enables developing mitigations/countermeasures.

Finally, to allow for stronger threat scenario and mitigation/countermeasure development and analysis, each previous and newly identified threat was relatively quantified by its attack cost, technical difficulty, and discovery difficulty following the approach of Du and Zhu (2013). Briefly, attack cost and technical difficulty assessments are from the context of an adversary and are defined as the costs associated and skill needed, respectively, to perform an

attack on the system; similarly, discovery difficulty assess the ability necessary for the targeted organization/system to uncover an attack or system breach (Du & Zhu, 2013). These assessments are evaluated on a relative, defined scale

Exhibit 3. Partial Updated PCOS Threat Tree.



and, with the use of multi-attribute utility theory, can be used to determine the relative likelihood of the threat's occurrence as a proxy for an attacker's utility value and by leveraging a fully developed threat tree. This classification allows one to identify the relative *importance* of each threat through a calculation of its relative occurrence. Defining each threat with these characteristics allows for stronger risk analysis of the threat scenarios and prioritization of threats to address with developed mitigations/countermeasures.

Following the identification and analysis of new threats using SFMEA and the classification of each threat, as described previously, allows for the 2009 EAC PCOS threat tree model to be updated, reflecting new, emerging cyber, physical, and insider threats to election systems. The method for placing the new threats on the PCOS attack tree involved analyzing each threat along with its description and whether it was classified as insider, physical, or cyber, then placing it with similar threats under subtrees that made sense logically. This involved several discussions amongst the SMEs to arrive at a consensus to ensure threats were placed appropriately in the threat tree. These discussions also resulted in modifying the identified threats/failure modes in the SFMEA due to vagueness and a need for specificity in threat tree placement. For example, the "malicious emails" threat/failure mode, shown in Exhibit 2, when placed in the threat tree made it unclear as to what kind of malicious emails and how these would affect PCOS voting machines.

As a result, the SFMEA and updated PCOS threat tree for this threat was modified to "using phishing emails to gain information," specifying that phishing emails were the main threat that, when interacted with, could steal information like usernames or passwords from the target, allowing access to election infrastructure. This threat, detailed in the SFMEA shown in Exhibit 2, was placed in the PCOS threat tree, partially shown in Exhibit 3 as node 2.2.5, to contribute as a source to execute an insider attack. Furthermore, some nodes were modified and rearranged on the original attack tree to make a more cohesive and specific threat tree with better threat scenario logic, developing a better overall picture of the threat landscape for PCOS voting machines.

With each newly identified and analyzed cyber, physical, and insider threat from the SFMEA placed within the updated EAC PCOS threat tree model, this new model contains more than 310 threat terminal nodes that, in combination with other threats, can result in the root node security incident to occur. For example, the "execute insider attack" subtree shown in Exhibit 3 can be achieved if any of the four child threats (nodes 2.2.2 – 2.2.5) occur because of the logical OR node relationship. This type of analysis, *minimal attack cut sets*, analyzes the smallest collections of attacker actions (i.e., threats) to cause the root node to occur and represents the lowest-effort path to the objective; ranking them by effort, required capability, or exploit likelihood pinpoints the "weakest links" in the system's defensive posture (Schneier, 1999). Cut-set analysis from complete threat trees can inform mitigation/countermeasure planning through a mapping of each high-priority MACS to the defensive controls that would invalidate one or more of its constituent steps. Security engineers can then select countermeasures that dismantle whole classes of attacks rather than patching individual vulnerabilities ad hoc. The analysis derives all possible MACS. For example, threat scenarios allow for a deeper understanding of how cyber, physical, and/or insider threats can be exploited to cause a security incident and, when combined with the attack cost, technical difficulty, and discovery difficulty relative

assessments to indicate a threat scenario's relative likelihood of occurrence and enable prioritization of mitigation efforts.

The updated PCOS threat tree, with the large number of terminal node threats and more than 60,000 cutsets (i.e., threat scenarios), represents the multitude of ways that the PCOS voting machine's integrity can be compromised. This comprehensive and updated PCOS attack tree model and risk analysis, if paired with tooling to analyze threat tree models, can enhance election security by providing the approach and means to develop threat analysis cases to demonstrate that this particular voting machine type, and associated processes, has been thoroughly analyzed for cyber, physical, and insider risks and to demonstrate that it is fit for purpose in serving this critical national infrastructure role.

Concluding Remarks and Future Work

This research has demonstrated the effective integration of a Bi-Directional Safety Analysis (BDSA) approach that leverages a traditional software safety analysis technique, Software Failure Modes and Effects Analysis (SFMEA), with threat tree analysis to demonstrate how they can contribute to a comprehensive risk analysis and mitigation approach for analyzing the cyber, physical, and insider threats for socio-technical, critical infrastructure. Specifically, this work extended a prior approach that analyzed the threats towards the mail-voting process (Scala, Goethals, Dehlinger, Mezgebe, Jilcha & Bloomquist, 2022) using a BDSA approach employing SFMEA to update the U.S. Election Assistance Commission's (2009) precinct count optical scanner (PCOS) voting equipment, identifying and analyzing 60 additional threats. The enhanced threat tree model, incorporating these new threats, provides a more granular and realistic representation of potential vulnerabilities, which is crucial for developing targeted mitigation strategies. This approach not only strengthens the security posture of election systems but also offers a scalable approach applicable to other security-sensitive domains, including other critical infrastructure systems.

Planned future work is twofold. First, with an updated, complete attack tree for the PCOS voting machine, this work will leverage this threat model to complete a risk assessment of threat scenarios to identify the risks of most concern within the process across temporal phases plus an impact analysis of suggested policy implications and security mitigations and their ability to reduce cyber, physical, and insider risks. To do so, tool development is underway that can automatically generate the threat scenarios (i.e., cutsets) of a threat tree, enabling better analysis of the types of threats and threat scenarios (i.e., cyber, physical, or insider), timing of the threats (i.e., prior to voting, on the day of an election, or following an election), and calculating of the relative likelihood of occurrence. Second, leveraging the developed tool support to analyze the threat scenarios, mitigations/countermeasures will be developed and analyzed to demonstrate the impact they can have on the overall risk analysis for socio-technical critical infrastructure systems.

AI in Technical Writing

AI and AI-assisted technologies were not used in preparing this manuscript.

Acknowledgments

This work was partially supported by the Science of Security program at the United States Department of Defense.

References

Alsadi, M., Casey, M., Dragan, C. C., Dupressoir, F., Riley, L., Sallal, M., Schneider, S., Treharne, H., Wadsworth, J., & Wright, P. (2023). Towards end-to-end verifiable online voting: Adding verifiability to established voting systems. IEEE Transactions on Dependable and Secure Computing. Advance online publication. https://doi.org/10.1109/TDSC.2023.3327859

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, *11*, 305.

Basin, D., Dreier, J., Giampietro, S., & Radomirović, S. (2021, November). Verifying Table-Based Elections. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2632-2652).

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. *Interacting with computers*, *23*(1), 4-17.

Bernhard, M., & Wallach, D. S. (2022). *ACM TechBrief: Election security: Risk-limiting audits*. Association for Computing Machinery.

Cybersecurity and Infrastructure Security Agency (CISA). (2003, December 17). *Homeland Security Presidential Directive 7 | CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7

Du, S., & Zhu, H. (2013). *Security assessment in vehicular networks*. Springer Science & Business Media.

Easterly, J., & Fanning, T. (2023, May 7). *The attack on Colonial Pipeline: What we've learned & what we've done over the past two years.* Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

Edge, K. S., Dalton, G. C., Raines, R. A., & Mills, R. F. (2006, October). Using attack and protection trees to analyze threats and defenses to homeland security. In *MILCOM 2006-2006 IEEE Military Communications Conference* (pp. 1-7). IEEE.

Election Assistance Commission (EAC). (2017). *Elections - Critical Infrastructure*. https://www.eac.gov/election-officials/elections-critical-infrastructure

Evans, D., & Paul, N. (2004). Election security: Perception and reality. *IEEE Security & Privacy*, *2*(1), 24-31.

Feiler, P., & Delange, J. (2017). Automated fault tree analysis from aadl models. *ACM SIGAda Ada Letters*, *36*(2), 39-46.

Kassel, A., Bloomquist, I., Scala, N. M., & Dehlinger, J. (2024). Understanding the impact of poll worker cybersecurity behaviors on US election integrity. In *IISE Annual Conference. Proceedings* (pp. 1-6). Institute of Industrial and Systems Engineers (IISE).

Leveson, N. G. (1995). *Safeware: system safety and computers*. ACM.

Leveson, N. G. (2011). The use of safety cases in certification and regulation.

Lutz, R. R., & Woodhouse, R. (1999, February). Bi-directional analysis for certification of safety-critical software. In *1st International Software Assurance Certification Conference (ISACC'99)* (Vol. 2, p. 3).

Matsumoto, N., Iwasawa, H., Sakata, T., Endoh, H., Sawada, K., & Kaneko, O. (2023). Dependable connectivity for cyber–physical–human systems in open fields. *IEEE Transactions on Consumer Electronics*, *70*(1), 183-196.

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity. *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, *4162018*(7).

Price, M., Scala, N. M., & Goethals, P. L. (2019). Protecting Maryland's voting processes. *Baltimore Business Review: A Maryland Journal*.

Reifer, D. J. (1979). Software failure modes and effects analysis. *IEEE Transactions on reliability*, *28*(3), 247-249.

Sanger, D. & Edmonson, C. (2019, July 25). Russia targeted election systems in all 50 states, report finds. *The New York Times*, https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html

Scala, N. M., Goethals, P. L., Dehlinger, J., Mezgebe, Y., Jilcha, B., & Bloomquist, I. (2022). Evaluating mail-based security for electoral processes using attack trees. *Risk Analysis*, *42*(10), 2327-2343.

Schmittner, C., Ma, Z., Schoitsch, E., & Gruber, T. (2015, April). A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security* (pp. 69-80).

Schneier, B. (1999). *Attack trees*. In Proceedings of the 1999 Workshop on New Security Paradigms (NSPW '99) (pp. 90–97). Association for Computing Machinery. https://doi.org/10.1145/315125.315145

Thumati, B. T., & Kemp, J. (2022, January). Large-scale Fault Tree Implementation: A Software Tutorial. In *2022 Annual Reliability and Maintainability Symposium* (RAMS) (pp. 1-5). IEEE.

Tsantikidou, K., & Sklavos, N. (2024). Threats, Attacks, and Cryptography Frameworks of Cybersecurity in Critical Infrastructures. *Cryptography*, *8*(1), 7. https://doi.org/10.3390/cryptography8010007

United States Election Assistance Commission. (2021, February). *Requirements for the Voluntary Voting system Guidelines 2.0*.

United States Election Assistance Commission Advisory Board. (2009). *Election operations assessment: Threat trees and matrices and threat instance risk analyzer (TIRA)*. https://www.eac.gov/sites/default/files/eac_assets/1/28/Election_Operations_Assessment_Threat_Trees_and_Matrices_and_Threat_Instance_Risk_Analyzer_(TIRA).pdf

Verified Voting. (n.d.). *The Verifier — Voting Equipment — November 2024*. Verified Voting. https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2024

About the Authors

Vanessa Gregorio, B.S., is a Towson University spring 2024 graduate. She majored in Business Administration with a concentration in Legal Studies and was an Honor's College student during her tenure. She currently works for

the federal government as a Junior Program Analyst for Naval Air Systems Command's (NAVAIR) headquarters. Partaking in a trainee program where she rotates between the organization's various International Programs offices, she has supported the development of government-to-government agreements to provide USG military articles and services to dozens of foreign allies. She is pursuing a Paralegal Certification in the upcoming year to continue her legal education.

Hao Nguyen, M.S., graduated in 2024 from Towson University's Master of Science program in Supply Chain Management. During her studies, she served as a Research Assistant, specializing in data analysis and focusing on the information security behaviors of professionals across various industries. She also conducted research on poll worker education, analyzing the effects of insider and physical threats through threat tree analysis. Hao co-authored three articles during her studies. She has over six years of experience in the field and specializes in data analysis, with a focus on poll worker education and the information security behavior of professionals in various industries.

Skylar Gayhart, M.S., received her Master of Science, studying computer science with a focus in data science, from Towson University. She also has received her Bachelor of Science, studying Computer Science with a focus in cybersecurity, from Towson University. During her time at Towson, she was chosen as a Department of Defense (DoD) cyber scholar, now working at the DoD as a Cyber Analyst. Aside from this, she works at the Towson University Election Security lab, researching different election related topics on current procedures and infrastructure.

Josh Dehlinger, Ph.D., is a Professor in the Department of Computer and Information Sciences at Towson University. He received his Ph.D. in Computer Science from Iowa State University in 2007 and served as a Research Scientist in the Charles L. Brown Department of Electrical and Computer Engineering at the University of Virginia in 2008. His research expertise lies, broadly, in software safety/reliability, election security, machine learning for software engineering, and computer science education.

Natalie M. Scala, Ph.D., is a Professor in the College of Business and Economics, a Fellow of the Center for Interdisciplinary and Innovative Cybersecurity, and the Director of accelerated programs at Towson University. She is also a faculty affiliate of the Applied Research Lab for Intelligence and Security at the University of Maryland. She earned Ph.D. and M.S. degrees in industrial engineering from the University of Pittsburgh. Her primary research is in military and security decision analysis, including risk in voting systems, integrity of votes throughout the supply chain, poll worker education, and cybersecurity metrics and best practices.