5. Vulnerability-Based Impact Criticality Estimation for ICS

Vulnerability-Based Impact criticality Estimation for industrial control systems. (2020, June 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9138886

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9138886

1. **Impact of Cyber Threats on Industry Control Systems (ICS)**: The paper addresses how cyber threats critically affect the reliability and availability of modern ICS, emphasizing the need for effective cybersecurity risk evaluation and control.
2. **Necessity of Quantitative Evaluation**: It highlights the importance of quantitatively evaluating cybersecurity risks in ICS, given the variety of vulnerabilities and cyber threats that exist.
3. **Introduction of MAVCA Model**: The paper presents a probabilistic Multi-Attribute Vulnerability Criticality Analysis (MAVCA) model. This model aims to estimate impact and prioritize remediation efforts in ICS networks, focusing on three major attributes: vulnerability severities, attack probabilities, and functional dependencies of vulnerability host components.
4. **Integration of CVSS Concepts**: The MAVCA model abstracts from the Common Vulnerability Scoring System (CVSS) concepts, integrating various sub-metrics to quantify the impact severity and prioritize mitigation efforts.
5. **Focus on Identifying the Weakest Link**: The paper emphasizes the importance of identifying and securing the weakest link in an ICS network, as adversaries often target the most vulnerable functional entity in an operational chain.
6. **Case Study Validation**: The proposed MAVCA model is validated through a case study on a miniature ICS testbed, demonstrating its effectiveness in identifying critical vulnerabilities and setting security priorities.
7. **Contribution to Larger Security Frameworks**: The metrics derived in this work can serve as sub-metrics inputs to a broader quantitative security metrics taxonomy and can be integrated into the security risk assessment scheme of larger distributed systems. This approach facilitates a more speedy and proactive security response in ICS environments.