7. An analysis of critical cybersecurity controls for industrial control systems

https://www.researchgate.net/publication/371703328_An_Analysis_of_Critical_Cybersecurity_Controls_for_Industrial_Control_Systems

Sekonya, N., & Sithungu, S. (2023). An analysis of critical cybersecurity controls for industrial control systems. *European Conference on Cyber Warfare and Security*, *22*(1), 410–419. https://doi.org/10.34190/eccws.22.1.1157

1. **Critical Role of ICS in Managing Industrial Processes**: Industrial Control Systems (ICS) are crucial in managing and operating complex industrial processes, particularly in critical infrastructure sectors like utilities, manufacturing, and water treatment facilities.
2. **Convergence of IT and OT in ICS**: Historically, ICS were isolated from IT networks, but the adoption of emerging technologies has led to a more connected ICS environment. This convergence of Information Technology (IT) and Operational Technology (OT) has introduced new cybersecurity challenges.
3. **Vulnerability to Cyberattacks**: The integration of IT and OT in ICS has made these systems more vulnerable to cyberattacks, which can disrupt industrial processes, cause physical equipment damage, and even lead to human casualties.
4. **Significant Cyberattacks on ICS**: There have been notable cyberattacks against ICS, such as the attacks on Ukraine's electricity infrastructure, demonstrating the potential for severe disruptions.
5. **SANS Institute’s Five ICS Cybersecurity Critical Controls**: In response to these threats, the SANS Institute published a whitepaper outlining five critical controls for ICS cybersecurity: ICS-specific incident response plans, defensible architecture, ICS network visibility and monitoring, secure remote access, and risk-based vulnerability management.
6. **Exploratory Examination of ICS Security Literature**: The paper conducts an exploratory examination of current ICS security literature to recommend security controls that align with the SANS Five ICS Cybersecurity Critical Controls.
7. **Mapping to NERC CIP Standards**: The paper maps the SANS Five ICS Cybersecurity Critical Controls to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards, which provide guidance on securing the Bulk Electric System (BES) and associated critical infrastructure.

These key points highlight the importance of adapting cybersecurity strategies in ICS environments to address the evolving landscape of cyber threats, especially with the increasing integration of IT and OT systems.