4. Zero Trust Approach for the cybersecurity of ICS

A Zero Trust approach for the cybersecurity of Industrial Control Systems. (2022, December 14). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10013559

1. **IT/OT Convergence in Industrial Plants**: Industrial plants are increasingly adopting digital and interconnected technologies, integrating software applications into their operational technology (OT) systems. This convergence offers efficiency and flexibility benefits but also introduces cyber vulnerabilities, as these systems were not originally designed for open internet access.
2. **Inadequacy of Traditional Security Solutions**: The frequency of successful cyber attacks in these environments indicates that typical multi-layer network security solutions, designed for rigid and stable infrastructures, are inadequate for the new complexities in industrial contexts.
3. **Applicability of Zero Trust Architecture (ZTA)**: The paper explores the implementation of ZTA principles in industrial settings. This involves designing, implementing, and testing an integrated defensive solution that moves away from implicit trust within a network.
4. **Identity-Centric Approach in ZTA**: The proposed ZTA model in an industrial context focuses on an identity-centric approach, increasing system security and flexibility while providing complete network visibility. This approach is particularly relevant for strengthening legacy systems and adopting new technologies with minimized cyber risks.
5. **Challenges of Perimeter-Based Defense Strategies**: The rapid adoption of advanced control systems and the need for remote access, including smart working and BYOD models, are exposing the limitations of traditional perimeter-based defense strategies in industrial environments.
6. **Innovative ZTA Solution for Industrial Sector**: The paper introduces an innovative ZTA solution for the industrial sector, emphasizing continuous authentication and authorization, device segmentation, and a trust algorithm that considers user and device information. This solution is adaptable to both on-premise and cloud-based architectures.
7. **Prototype Implementation and Evaluation**: The implementation of the proposed ZTA solution is evaluated through a working prototype. This evaluation demonstrates that a modern cybersecurity architecture can enhance the defense capabilities of IT-oriented industrial systems, providing a dynamic and flexible security model that can adapt to various architectural needs and security postures.