Temasek Defence Systems Institute

Applicability Analysis Of The Zero Trust Paradigm For Operational Technology

Author: Song Meng Wee (ST Engineering)
Thesis advisor: Prof. Thuy D. Nguyen (Naval Postgraduate School)
Co-advisors: Dr. Cynthia E. Irvine (Naval Postgraduate School)

Motivation

The 2023 Singapore cybersecurity strategy and the U.S. federal government have both emphasized the adoption of the Zero Trust paradigm for safeguarding critical infrastructures. Yet, the practicality and advantages of implementing Zero Trust in Operational Technology (OT) systems still remain largely unknown. Organizations such as the National Institute of Standards and Technology and the Cybersecurity agency of Singapore have provided guidelines for applying Zero Trust to OT systems, however, these guidelines are not sufficiently detailed.

Research Questions

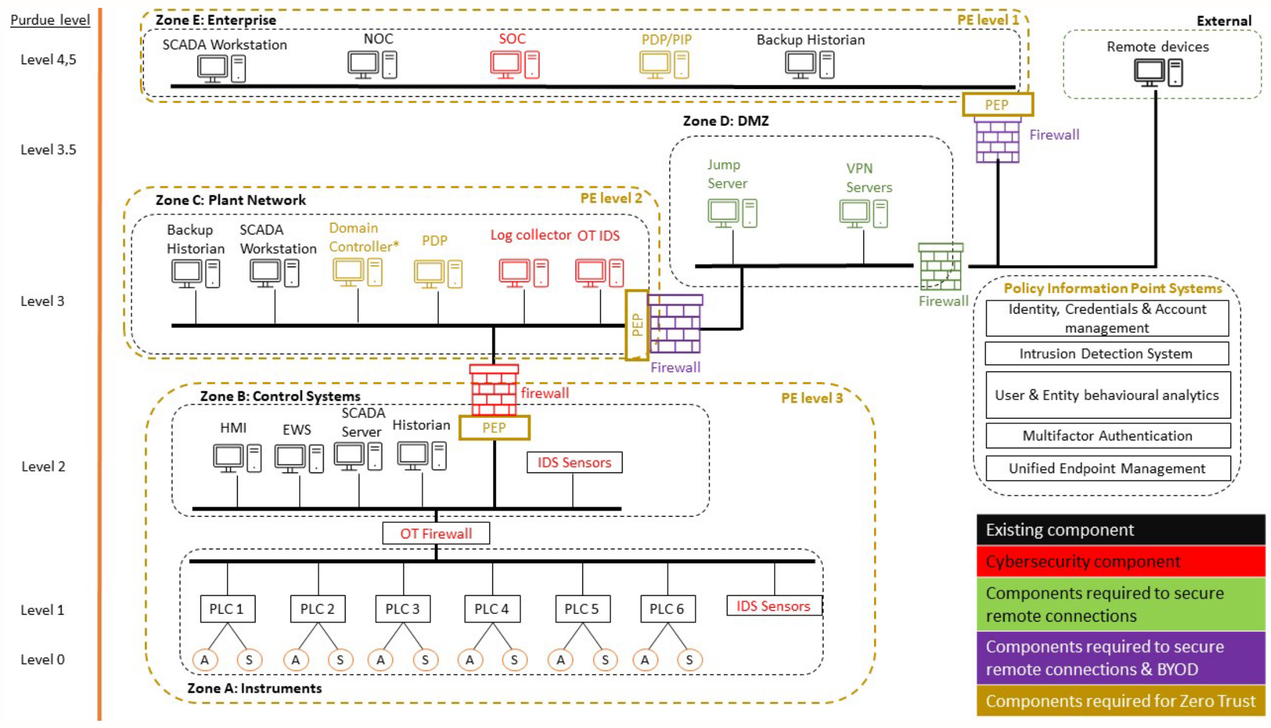
- Can ZT modernize and secure legacy OT systems?
- Can ZT enable secure remote connection?
- Can ZT allow personal devices to be used securely?

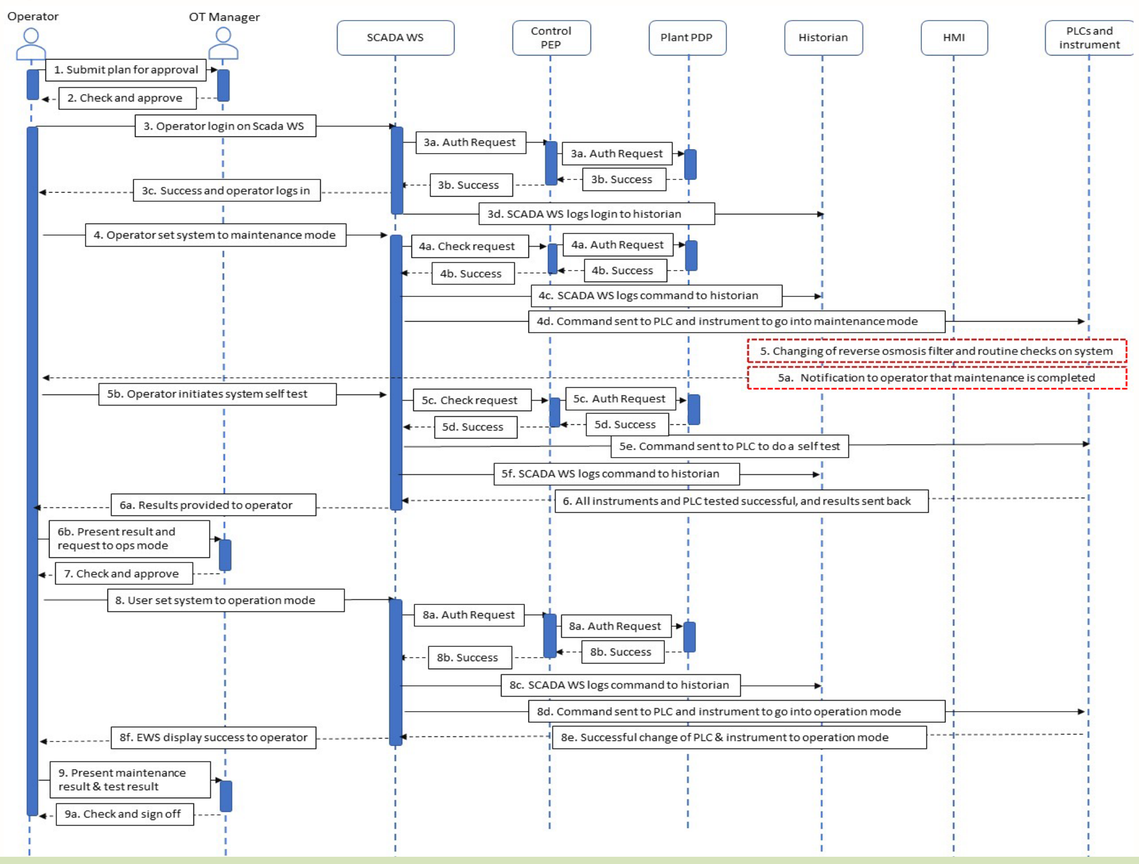
Key Issues Legacy OT Networks

- Limited computing resources and network bandwidth
- Lack of audit functionality
- Lack of cybersecurity awareness

Research Methodology

1. Develop a water treatment concept of operation using SUTD's Secure Water Testbed.
2. Conduct threat modelling on project requirements to identify potential threats and corresponding mitigation methods.
3. Implement mitigation measures to enhance security based on identified threats.
4. Apply the Zero Trust paradigm to the mitigated OT architecture.
5. Analyse the feasibility and practicality of Zero Trust in day-to-day water treatment operations.





Results

Benefits

Research findings demonstrate the feasibility of implementing Zero Trust in legacy OT systems, highlighting its proactive capabilities in securing OT networks against external remote connections and personal devices.

Drawback

Zero Trust relies heavily on software agents, which can lead to potential issues such as denial of service to critical processes or the compromise of these agents. Moreover, the validation points within the Zero Trust framework carry the risk of becoming single points of failure.

NUS National University of Singapore