National Conference on Advanced Research in Science, Engineering, Management and Humanities
(NCARSEMH – 2025)
27th July, 2025, Jharkhand, India.

CERTIFICATE NO : NCARSEMH /2025/ C0725722

A Study of Cyber Security Vulnerabilities and Threats Limited to Tier-1 of Enterprise Wise Scada System

Dandu Ramesh
Research Scholar, Ph.D. in Computer Science Engineering, P.K University, Shivpuri, M.P., India.

ABSTRACT

In modern industrial environments, SCADA (Supervisory Control and Data Acquisition) systems are the backbone of operational technology, but they are increasingly exposed to cybersecurity vulnerabilities and threats, particularly at Tier-1, which typically comprises the core control layer including human-machine interfaces (HMIs), programmable logic controllers (PLCs), and essential communication networks. Tier-1 is crucial because it directly interacts with critical operational components, and any compromise can have cascading effects on the entire enterprise. Vulnerabilities at this level often stem from outdated software, unpatched firmware, weak authentication mechanisms, and insecure network configurations. Attack vectors include malware injections, phishing attacks targeting operators, man-in-the-middle (MITM) attacks on communication protocols, and insider threats exploiting privileged access. Threats such as ransomware or targeted Advanced Persistent Threats (APTs) can disrupt real-time operations, leading to potential production downtime, equipment damage, and even safety hazards. Additionally, Tier-1 systems often lack strong encryption or anomaly detection capabilities, making them susceptible to reconnaissance and lateral movement by attackers. Effective mitigation requires a combination of strategies including network segmentation, strict access control, regular security audits, intrusion detection systems, and operator training. Addressing cybersecurity at Tier-1 is critical for safeguarding enterprise-wide SCADA operations, ensuring system integrity, operational continuity, and resilience against both internal and external cyber threats.