ABSTRACT

Control systems are used in a number of different industrial sectors and critical infrastructures, including manufacturing, distribution, and transportation. Failure of these control systems because of malware or other faults would be catastrophic for critical infrastructure and would result in significant losses. Adverse operating conditions, such as those found in networked control systems, exacerbate the likelihood of vulnerability to malware attacks. The prospect of severe adversarial assaults such as buffer overflow, conventional faults, and especially stealthy Ladder Logic Bombs is a serious cause of concern in Industrial Control Systems (ICS) with novel attacks such as Struxnet. Decoupled at-distance Electromagnetic spectrum-based monitoring of faults and malware is more robust and can likely be integrated into Industrial Control System frameworks. Our failure analysis and Machine Learning (ML) modeling approach is fundamentally different from traditional methods in that we propose a Hybrid Quantum Artificial Intelligence-based Electromagnetic (EM) Spectral domain-based analysis approach that is completely decoupled from the controller processor and can predict PLC fault/malware conditions, including stealth Ladder Logic Bombs and buffer overflow attacks. Further, robust Supervisory Control Systems (SCSs) that interface with programmable logic controllers (PLCs) are essential components of Industrial Control Systems (ICSs) that handle critical infrastructure. Modern industrial control systems, on the other hand, are made up of densely linked Internet of Things (IoT) nodes. Because of their networked nature, supervisory control systems are also susceptible to widespread cyberattacks. As a result, in the case of a coordinated attack on IoT control systems, the dependability of Supervisory control decision-making procedures is jeopardized and need to be decoupled from the attacks. This work also develops a Fuzzy inference Engine-based supervisory monitoring technology based on the characteristics of the Hybrid Quantum AI-based analysis of the EM spectrum to reduce industrial plant downtime and false alarms by localizing adversarial attacks/faults, risk severity levels, and impacted nodes, as well as having dependability and malware immunity in networked Industrial control systems. The Hybrid QAI technique improved prediction accuracy by up to 88 percent when identifying different control system viruses and defects in 6-stage pipelined processors. The Fuzzy inference engine in the Mamdani Inference System architecture has been found to reduce the risk of false alarms and downtime.