Q-Net Security Industrial Control System Use Case
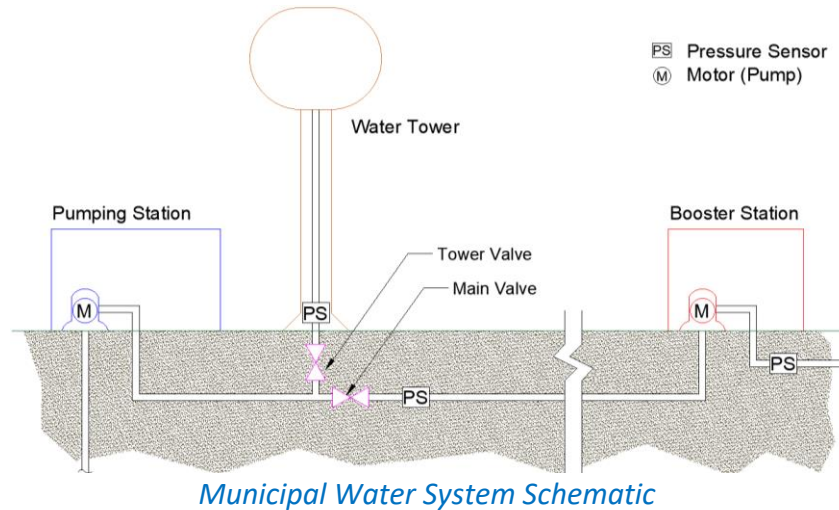
An independent test conducted by Red Berry Innovations demonstrated the effectiveness of Q-Net Security's quantum compute-resistant cybersecurity solution in an Industrial Control System (ICS) environment. Focus was placed on an ICS platform due to the recent escalation of cyber-attacks on critical infrastructure and the often poorly implemented and aged security configurations of typical ICS environments.

Municipal Water System Schematic

This effort emulated a municipal water system, shown in the schematic, consisting of a main pumping station, water tower, and booster station. Although not included in the figure, the test bed also featured a Security Operations Center (SOC) that served a supervisory role, remotely monitoring all systems via a public network.

The SOC was the focus of the cyberattack, where a Red Team attacker gained physical access to the facility. With this access, the attacker successfully performed two attacks: 1. implanting a backdoor on an engineering workstation, and 2. capturing unencrypted network traffic. The backdoor attack allowed the attacker to connect to the workstation from a device outside the SOC's network. In the second attack, the attacker accessed the unencrypted traffic enabling changes to the data to cause malicious effects. Both attacks allowed remote control and manipulation of the water system controls to cause a system shutdown that would result in a devasting outcome for the households relying on the water.

To mitigate both attacks, a Q-Net Security solution was installed in the ICS environment. Installing the equipment was a straightforward and effortless process. The previous attacks were re-tried but the Q-Net technology rendered both attacks ineffectual. This provided compelling evidence that Q-Net solution delivers an easily implemented and effective means of mitigating potential and existing cyber threats in an ICS environment.

As exemplified in this independent test, a municipal water delivery system was exploited as the network and systems were fully compromised and controlled. However, once secured with a drop-in secure Q-Net overlay, the ICS environment was impregnable and invisible to the nefarious actors. Q-Net Security provides a "plug-and-play" solution for the most important cybersecurity problems in any industry!