**Purdue Project and Weekly Assignment - Level 3**

Dante Worthington

For the third layer of our SCADA system, we focused on adding essential security and network management components to ensure both the reliability and security of the water filtration monitoring process. These additions enhance communication between critical parts of the system and provide necessary safeguards against potential threats or disruptions.

We started by incorporating a CISCO Switch to manage internal data routing between the PLC, RTU, SCADA monitoring system, and historian. The switch ensures that all devices remain interconnected, allowing seamless data flow while maintaining operational isolation from external networks.

Next, we added a Physical Firewall to protect the system from any external threats. Positioned between the SCADA monitoring station, historian, and other connected devices, the firewall filters traffic, preventing unauthorized access and mitigating the risk of cyberattacks or network intrusions.

Additionally, an Intrusion Prevention System (IPS) was implemented to monitor malicious activities and safeguard against any anomalies or attacks that could compromise the integrity of the system. The IPS works alongside the firewall, ensuring that any suspicious behavior is immediately flagged and mitigated before it causes harm.

The final network optimization step was the incorporation of UPS to provide emergency power in case of outages. The UPS ensures continuous operation and data preservation during power disruptions, safeguarding against data loss in the event of critical failures.

**COSTS:**

CISCO Router: $500 - $5,000

Alto Physical Firewall: $2,000 - $5,000

IPS-CISCO Firepower: $1,300 – $4,000

APC-Smart UPS: $400 - $700