ALLIANT TECHNOLOGIES

Transforming Operational Efficiency

THE SUCCESS STORY OF ALLIANT CUSTOM SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AT A MAJOR FREIGHT AND PARCEL COMPANY

Problem

Off the shelf SCADA systems used by our customers were restrictive to modifications, had limitations, and came with license fees. We started with a simple two-part question, what elements do you need and what is important to you? Some of our customers' requirements were:

- Security of the software
- Scalability
- Reliability
- Extendable
- Web based
- Zero license fees
- Simple update roll out of new versions to all applicable facilities
- Templatization of screens and data
- High quality visuals using Vector Graphics
- Ease of use by all levels of users
- Less than one year turnaround for software, testing, documentation and training.

Solution

Our SCADA software solution is designed using a microservice architecture using containerization for scalability and resiliency. The application provides the following functionality:

- Visualization through either Windows-based client or a new web-based client (includes mobile accessibility). This includes per-user favorites.
- Connectivity to industrial devices, including PLCs and other systems for monitoring.
- Connectivity to databases and other standard web-based APIs.
- Logging and data collection functionality to both retrieve and store data to external systems.
- Alarming including current alarms, historical alarms, and custom alarm filtering per-user.
- Integrated Microsoft Entra ID logins leverage existing customer infrastructure for users, passwords, and role-based access.

Using this microservice design allows for components to be added and removed without interfering with other services, as well as scaling by adding additional microservices to handle additional load. The solution also supports running multiple redundant instances, and allows for both horizontal and vertical scaling.

A communications module for OPC/UA is included. This allows for the SCADA system to communicate to any modules that require OPC/UA protocol.

CIP Security is part of the solution for a secure method of communication with Ethernet/IP devices. This allows for encrypted communication to any device that supports the CIP Security protocol. Non-encrypted communication is still supported.

The web-based client requires the use of a Microsoft Entra ID login by interfacing with the customers controlled Entra ID infrastructure. It uses role-based management to assign permissions to the users, preventing access to restricted functionality.

Drilling down into screens is intuitive and clear due to the use of Vector Graphics. The template enforces consistency throughout the facilities.

Conclusion

All elements within the Problem Statement section above were incorporated in the solution plus others. The timeline was achieved, including successful on-site testing at two facilities. Roll out has started to multiple facilities within the network. Our customer has a very powerful and flexible tool with no license fees. Problem solved!