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 Statement

The off-the-shelf SCADA systems used by our customers were restrictive in terms of modifications, presented limitations, and had licensing fees. We started with a simple, two-part question: What elements do you need, and what is important to you? Our customers outlined several key requirements, including:

- Software security
- Scalability
- Reliability
- Extendability
- Web-based
- Zero licensing fees
- Simple rollout of software updates across all applicable facilities
- Templatization of screens and data
- High-quality, vector-based graphics
- User-friendly interface
- Turnaround time of less than one year for software development, testing, documentation, and training

## The Solution

Our SCADA software solution is built on a microservice architecture, using containerization for scalability and resiliency. The application provides the following functionalities:

- Visualization through either a Windows-based client or a new web-based client (with mobile accessibility), including 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 which leverage existing customer infrastructure for users, passwords, and role-based access.

- The microservice-based 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 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 also still supported when required.
-
- The web-based client requires the use of a Microsoft Entra ID login by interfacing with the customers controlled Entra ID infrastructure. Role-based management is used 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 standardized screen template enforces consistency throughout the facilities.

## Conclusion

All elements within the Problem Statement section above were incorporated in the solution—along with others. The timeline was achieved, including successful on-site testing at two facilities. Roll out has started across multiple facilities within the network. Our customer now benefits from a powerful, flexible SCADA solution with zero licensing fees. Problem solved!