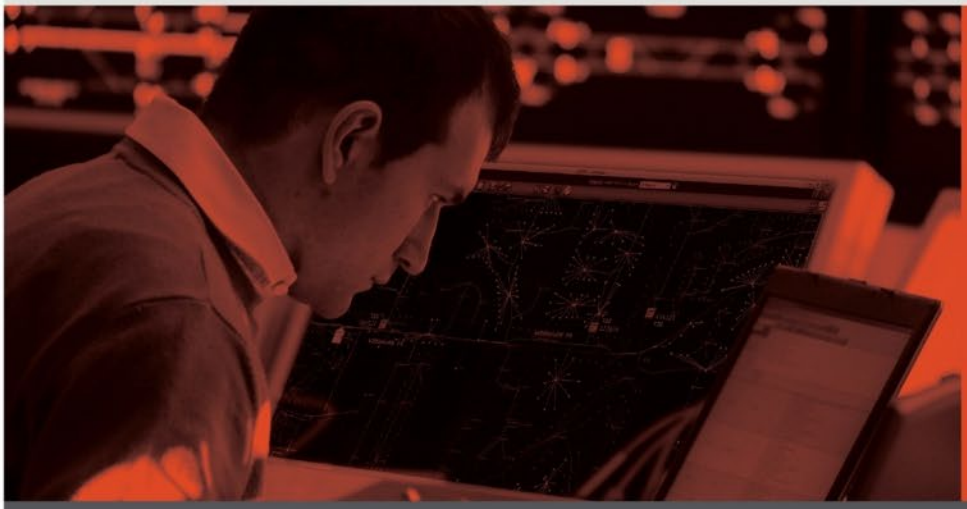
Survalent.



Volume 1
Technical and Commercial Proposal

SCADA SMTXU
City of San Marcos

Proposal No. A23-9-69421_Rev4

May 21, 2024

ORIGINAL

Survalent.

USA
1967 Wehrle Drive
Suite 1 PMB 122
Buffalo, New York
USA 14221

Phone: +1 (905) 826-5000
Fax: +1 (905) 826-7144
www.survalent.com

Document Control

Revision	Date of Issue	Author(s)	Brief Description of Change
4.0	May 21, 2024	Nivedita Pandit	Updated the reference information for Software License Agreement and Software Maintenance agreement.
3.0	May 8, 2024	Nivedita Pandit	PDS added to the base scope. Removed Phase 2 from the scope and document. Updated architecture and preliminary project schedule. Updated details of the Survalent Project Manager
2.0	April 11, 2024	Nivedita Pandit	Quote validity extended until September 1st, 2024
1.0	December 20, 2023	Nivedita Pandit	Quote validity extended until March 1st, 2024. Change in price.
0.0	October 17, 2023	Nivedita Pandit	Initial release for distribution.

Statement of Copyright, Confidentiality & Non-Disclosure

Table of Contents

List of Figures

List of Tables

Abbreviations and Acronyms

Abbreviation	Definition
ADMS	Advanced Distribution Management System
CIP	Critical Infrastructure Protection
DMZ	Demilitarized Zone
DNP3	Distributed Network Protocol
FAT	Factory Acceptance Test
FLISR	Fault Location, Isolation, and Service Restoration
GIS	Geographic Information System
ICCP	Inter Control Centre Protocol
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
NERC	North American Electric Reliability Corporation
ODBC	Open Database Connectivity
OMS	Outage Management System
OTS	Operations Training Simulator
RFP	Request for Proposal
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SQL	Structured Query Language
TASE.2	Telecontrol Application Service Element 2 (ICCP)
TCP/IP	Transmission Control Protocol/Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

1 Executive Summary

Survalent Technology Inc. ("Survalent") is pleased to submit this proposal for the supply and installation of a Supervisory Control and Data Acquisition System and Distributed Management System in response to the City of San Marcos ("San Marcos") request for proposal dated September 18, 2023.

This proposal is organized in three volumes, as follows:

1) Volume 1, Technical and Commercial Proposal
   - This document includes project specific details and all the Attachments requested by San Marcos
2) Volume 2, ADMS Standard Product Overview
   - Full software product catalog for reference only. No project specific information.
3) Software License Agreement Support Ts Cs - Final Rev4.
   - Software maintenance information and agreement. No project specific information
   - San Marcos is currently subscribed to Platinum support for Survalent SCADA system.

The Survalent ADMS is a tightly integrated SCADA, OMS, and DMS solution providing a common user interface for ease of operations, a unified real-time database for increased performance, and a single hardware platform to simplify IT maintenance and security. A fully integrated ADMS solution means that all stakeholders at San Marcos will have access to the same real-time information about outage conditions and field service operations allowing them to make better decisions, faster.

The Advanced Distribution Management System proposed by Survalent will allow San Marcos to successfully operate the distribution system in the presence of new technologies, while enabling the coordination of programs impacting the distribution system to be leveraged to optimize system economics, reliability, safety, and efficiency.

Take your ADMS to the next level with a solution that offers a low total cost of ownership

The challenges for utilities have never been greater. Grid modernization, the growth of embedded generation, rising customer expectations, the increasing intensity and frequency of storms, the threat of cyber-attacks, and additional regulatory oversight has put significant pressure on utility control systems to keep pace.

We understand your need to implement a system that gives the greatest flexibility in terms of network configuration, user functionality and future integration with new or upgraded systems.

The Survalent ADMS is a solution that can meet those challenges head on. Our proposal gives you the ability to go beyond your current system with a solution that offers enhanced functionality – now and into the future – in several critical areas as outlined below. And because our solution is easy to deploy, manage, scale, and use, it provides a low total cost of ownership. Customers that have switched from competitor products to Survalent have confirmed that it takes one third (1/3) the resources to operate and maintain the Survalent ADMS; this can add up to considerable savings over the lifetime of the system.

Protect and secure your network against cyber-attacks

The Survalent ADMS architecture is based on the specifications of the North American Electric Reliability Council's (NERC) Critical Infrastructure Protection standards, thereby reducing cyber security threats.

It's not just our technology that will drive project success

While our corporate roots trace back to technology that was used by NASA in the Apollo space missions, Survalent's 50+ year history has been dedicated to service in the utility industry. Our success has been fueled by meeting the growing expectations of the customers we serve: innovation, improvement, and commitment are at the heart of everything we do.

Trust is earned when actions meet words

We have an impressive list of highly satisfied customers ranging from small to large electric, gas, water/wastewater and transit utilities across the globe. This diversity gives us a broad perspective and a tremendous base of experience. Over 700 customers in 40 countries rely on us to provide solutions to control their critical network operations. Many of our customers have expanded beyond their initial Survalent SCADA investment to include our outage and distribution management solutions, resulting in over 800 successful implementations. And since 1983 – when we first began tracking this information – our customer retention rate has been 97.6%. I think you'll agree that this speaks to the success we've had in delighting our customers.

A culture of – and commitment to – innovation and continuous improvement

We have a very talented and experienced development team, and we're constantly reviewing and improving our processes to ensure that quality is built into every product we release, and actively managing every issue that our customers report. We provide many channels for customers to provide direct input into our product development efforts. Whether it's through our community forums, at our annual user conference, or through daily interactions, we have a culture of listening that allows us to focus on what our customers want to accomplish. It's a key starting point for product innovation, and it allows us to deliver the best possible user experience.

In addition, we've recently strengthened our senior management team, added additional resources to our software development and quality assurance groups, and improved processes across the board. We're investing heavily in these areas to be able to deliver on our customer commitments and drive the next phase of our growth.

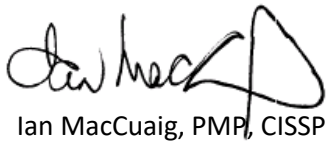
Our focus is on the long-term

Survalent is a privately-held company that is financially stable with zero-debt. Unlike many of our competitors – who operate as publicly-traded companies, who are hyper-focused on quarterly earnings, and who answer to shareholders – we're focused on the long-term and answer only to our customers. At 21%, we spend more of our top line revenues on research and development than Microsoft, Amazon and Google.

Price is what you pay; value and commitment is what you get

Thank you for the opportunity to participate in this RFP. We are eager to continue our partnership with the City of San Marcos and make your ADMS vision a resounding success. Additionally, we acknowledge Administrative Addendum No. 1 - Clarification of Proposal Due Date: "Thursday, October 19, 2023."

Survalent will also comply with all Federal, State and local laws and regulations. And confirm that a liability insurance policy will be provided within 10 days if awarded the Contract.



Ian MacCuaig, PMP, CISSP
Vice-President of Customer Success

"Electric utility people don't use the words 'good' and 'reliable' lightly. We just don't throw around words like that very often. But with Survalent, it's well-deserved."

- Central Georgia EMC

2 Relevant Experience Information

2.1 Our Company

Survalent has been in business for over 50 years, supplying, substation automation, and ADMS-SCADA systems to electric, water, and gas utilities since 1964.

Survalent Technology Corporation was formed by merging of three companies – Canada Systems Group, Dacasn and Quindar Products Canada on 1st January 1999.

Survalent office in USA, Survalent Technology Inc. was formed on 4th January 2016 in the State of Delaware.

Survalent has 50+ years history dedicated to service in the utility industry. Over 700 utilities in 40 countries rely on the SurvalentONE platform to effectively operate, monitor, analyze, restore, and optimize operations. By supporting critical utility operations with a fully integrated solution, our customers have significantly improved operational efficiencies, customer satisfaction, and network reliability.

Survalent's knowledge, experience and passion encompass every solution we provide to our customers, and we have many testimonials from our customers who have praised the ease of operation, low cost of ownership, and the high quality of our customer support service. Please refer to our web site www.survalent.com for further details.

Several major factors have contributed to our success:

- Our team has over 500 man-years of ADMS experience. We work closely with our clients to ensure our solutions meet their needs and work in their environment.
- Our system state-of-art architecture and our preparedness to embrace the latest technologies and incorporate them into our system design.
- Our commitment to quality assurance. Survalent has implemented an ISO 9001:2015 quality control system to ensure that projects meet or exceed the specifications.
- Our outstanding technical support, resulting in 97.6% customer retention.

Survalent is committed to the constant pursuit of customer satisfaction and to being the supplier of choice in the markets we serve by always meeting or exceeding customer requirements. Continuous improvement of quality, service and cost is the foundation of the company's success and is actively encouraged throughout the organization.

1. Location of headquarters and satellite offices that may be utilized during the project:

   USA Office

   Survalent Technology Inc.
   1967 Wehrle Drive
   Suite 1 PMB 122
   Buffalo, New York
   USA 14221

Headquarters
Survalent Technology Corporation
7965 Heritage Road
Brampton, Ontario
L6Y5X5

Other location (Satellite office)
Survalent Tehnolodzi Korporacija
Stiv Naumov 118a Skopje
Republic of Macedonia

2. Survalent Contact Information (and preferred method of communication)

   Stephen Ames, Regional Sales Manager
   M: +1(512) 413-5163
   Email: sames@survalent.com

2.2 Our Solution

Survalent makes real-time operational intelligence and control easy. We integrate data from across your network to ensure accurate information on current system conditions is continuously available in a form that allows users to quickly grasp and fully understand the actual operating conditions and take corrective action when necessary to maintain or restore reliable operations and business performance.

Following are some of the highlights of our proposed solution:

1) Our product platform is built upon scalable, secure, and open technologies that are proven to efficiently integrate, manage, and process data from a wide variety of sources. We have implemented open standards for real-time data access and data exchange including SQL, ICCP (TASE.2), OPC, MultiSpeak, SNMP, HTTP, XML, Web Services, SOAP, and FTP.
2) Our Windows-based platform is highly available, supporting a quad-redundant system architecture. Virtualization is fully supported.
3) Our product includes a robust SCADA system that includes data acquisition with a large library of communication protocols, data processing, high-performance graphics engine, historical data, switching orders, and more. Unlike many of our competitors, the Survalent platform supports on-line database edits with no downtime, no failovers, and no scanning delays when installing database and display updates.
4) Our product includes a complete suite of advanced Distribution Management System (DMS) applications that enable utilities to manage distributed energy resources, manage network loading at peak times, and to optimize the distribution network for improved asset utilization and overall network reliability. These applications include load forecasting, rotational load shedding, power factor control, dynamic voltage regulation, distribution network model, network topology processor, distribution power flow, distribution state estimator, cold load pickup, pre-switching validation, fault location, isolation, and service restoration (FLISR), and volt/var optimization (VVO).

5) The system supports many MultiSpeak interfaces including GIS, AMI, IVR, CIS, AVL, LM, WMS and more.

6) Our product is a fully integrated solution that provides a common user interface for all roles for ease of operations, a shared “as-operated” network model and real-time database for increased performance, and a single hardware platform to simplify IT maintenance and security.

7) Our product includes state-of-the-art tools for database and graphics generation that allow for rapid system installation and commissioning. Tools such as STC Explorer, IED Wizard, IED Control Panel, GIS Wizard, Express Database Builder, Analog Point Viewer, and Status Point Viewer provide user friendly, graphical user interfaces for common system administration tasks.

8) Survalent offers a very flexible licensing model, providing a system that is fully expandable. This allows the system to be incrementally expanded over time and as the network grows in order optimize the hardware and software investment.

2.3 Our Technical Support

Survalent provides outstanding technical support that is unparalleled in the industry:

a) Our 24/7 hotline technical support, as well as our professional and dedicated support team, has won praise from all of our customers and we have one of the highest levels of customer satisfaction in the industry. Technical support is provided from our headquarters in Brampton, Ontario, Canada as well as from our offices in South America, Europe, Mexico, and Asia.

b) Unlike many of our competitors, Survalent does not force customers to stay up-to-date with the latest version of our product in order to maintain their support contracts; as long as the support contract is current, our support team will provide technical support. However, Survalent strongly recommends that customers stay up-to-date with our product releases in order to take advantage of the latest functional and security updates, and to avoid difficulties implementing future product releases and patches.

c) Unlike many of our competitors, Survalent does not force customers to purchase upgrade services in order to upgrade their software. Our software has been designed to be easily upgraded, and the majority of our customers install the updates on their own. As long as your support contract is current, customers can download the latest software release from our web portal and implement it on their system. Our technical support team is available 24/7 to provide support if needed.

d) Having a large number of clients allows Survalent to keep our support costs low, leading to significantly lower cost of ownership for the ADMS platform over the lifetime of the system.

Figure 2-1: Global Support Structure

2.4 Project Team

To ensure successful project outcomes, Survalent has developed a project management methodology, based on the PMI Project Management Body of Knowledge (PMBOK), that focuses on providing quality products and services, frequent communication with the Client, and respecting our schedule commitments. We assign skilled resources that match project-specific needs, and our project managers meet weekly with management and technical staff to ensure our deliverables are on schedule, and to confirm that all teams and project resources are working together seamlessly. Our project budgets are managed weekly to ensure staffing and efforts are on track to meet our budget commitments.

Our team has grown into a firm of over 165 employees consisting of approximately 115 technical resources and project managers. Our experience in providing over 800 ADMS-SCADA, OMS, and DMS solutions to electric, water, and gas utilities world-wide has given us a good understanding of Client needs, and has allowed us to optimize our project delivery process. Exposure to projects, small and large, has proven that our product is scalable, flexible, robust, and highly performant.

Survalent will appoint a project team consisting of a Project Manager, a System Specialist, and other product specialists as needed to meet project-specific needs. For this project, Survalent has proposed the following team. Note: All team individuals are employees of Survalent.

1) **EVP Customer Success / Executive Sponsor**: Ian MacCuaig, PMP, CISSP. Ian is Executive Vice President of Customer Success at Survalent Technology and is responsible for proposals, project delivery, and customer services. Ian has over 30 years of experience in management consulting, project management, business analysis, engineering management, and software development within the energy sector. Ian has a succinct knowledge of grid operations, information technology, smart grid technologies, distributed energy resources, system integration and NERC CIP security standards. Ian will be the Survalent Executive Sponsor for this project.

2) **Operations Manager**: Joe De Filippis. Joe has been with Survalent for over 20 years and is responsible for insides sales and project delivery. Joe will work closely with the Project team to ensure the project runs on time and budget, allocating resources as needed to complete the project deployment.

~~3)~~ **Project Manager:** Carolina Faria. Carolina will manage all aspects of the project from award through commissioning of the system, to final handover to San Marcos. Carolina will serve as the main point of contact with San Marcos and will be accountable for the successful completion of the project, ensuring the final system adheres to the agreed timeline, budget, and specifications. Her responsibilities will include planning, implementing, monitoring, and controlling the progress of the project. Working closely with San Marcos, Carolina will develop the project plan and provide timely progress updates, clarifications, and project reports.

4) **GIS Specialist**: Jason Yang. Jason will be responsible for configuring the interface to the GIS, and performing the initial import of the GIS database and land base into SmartVU.

5) **System Specialist:** Kosta Ristovski. Kosta will be responsible for system installation, configuration, acceptance testing, technical training, and site commissioning.

6) **DMS Specialist:** Miguel Ceniceros. Miguel is the Development Leader for the Distribution Management System (DMS) team, and is responsible for the planning, design, development,

programming, and testing of the Power Flow, FLISR, Loss of Voltage (LOV), Volt Var Optimization (VVO), and Distribution Estate Estimator (DSE) applications.

7) **Interface Specialist:** Rick Hayden. Rick is responsible for the development of protocols, interfaces, and software applications for the Survalent SCADA and OMS products. He is the lead developer for MultiSpeak, a protocol that defines standardized interfaces among software applications commonly used by electric utilities.

8) **Test Coordinator**: Carolina Faria. In addition to her role as Project Manager, Carolina will also be the Test Coordinator responsible for ensuring that all tests are conducted in accordance with the requirements of this Technical Specification.

Please refer to Appendix E Resumes of this document for the above-mentioned team from Survalent

3 Reference List of Projects of Similar Scope, Size and Complexity

Jeremy Herring
Manager of Operations Systems
South Plains Electric Cooperative **(VMware enabled environment)**
110 N. Interstate 27
Lubbock, TX 79403
Office: (806) 775-7722
jherring@spec.coop

Tyler Hockenberry
Systems Engineer
Rayburn Electric Cooperative **(VMware enabled environment)**
950 Sids Road Rockwall, TX 75032
Office: 469-402-2099
thockenberry@rayburnelectric.com

Ro Smith
SCADA Manager
Weatherford Municipal Utility System **(VMware enabled environment)**
917 Eureka Street
Weatherford, TX 76086
Office: 817-598-4030
rsmith@weatherfordtx.gov

Justin Stroupe
Systems Control Manager
New Braunfels Utilities
355 FM 306
New Braunfels, TX 78130
Office: 830-608-8923
jstroupe@nbutexas.com

Ronnie Bludau
Operations Technology Superintendent
Bluebonnet Electric Cooperative
155 Electric Avenue
Bastrop, TX 78602
Office: 979-542-8669
ronnie.bludau@bluebonnet.coop

Allen Engelke
SCADA/Relay Control Engineer
Guadalupe Valley Electric
908 Curtiss St.
Schertz, TX 78154
Office: 512-677-0709
aengelke@gvec.org

4 Proposed Project Schedule, Strategy and Approach

The following section describes the technical solution proposed by Survalent.

4.1 System Goals and Objectives

The design of every Survalent system is based on the following goals and objectives:

1) **High Availability**. The Survalent system architecture supports dual-, tri-, and quad-redundant configurations that are fault tolerant so that any single hardware failure does not result in the loss of a critical function.
2) **System Responsiveness**. High performance user interface, data collection, and program execution times are provided, as well as the timeliness of making data available to the enterprise.
3) **Present Pertinent Information**. It is important that the system users have access to a full range of high quality real-time and historical data, as well as the tools to interpret the data to aid the staff in performing their jobs.
4) **Expandable/Scalable.** The Survalent system hardware and software is easily expandable and scalable and provides the capability to upgrade and/or add additional processors, memory, disk units, etc., and expand application programs or add new functions without major disruption to system operation.
5) **Security.** The Survalent system has appropriate security features that prevent unauthorized users from accessing the system and permits assigning various levels of access privilege to authorized users. The system also complies with NERC CIP standards and NISTIR 7628 guidelines.
6) **Advanced Applications.** As operational requirements and needs change, it becomes increasingly important to have good tools to ensure that the electric grid remains secure and is operated as efficiently as possible. The Survalent platform support several grid security and optimization algorithms, as well as advanced situational awareness features.
7) **Improved Operator Training**. Operator training simulation tools are fully integrated with the Survalent products, providing an offline environment for operator training.
8) **Maintainability**. State of the art auditing, editing, display building, and database generation tools are provided for system maintenance.
9) **Minimal Customization**. To the greatest extent possible, standard applications have been proposed to minimize customization to our standard product, thereby lowering the risk of implementation schedule delays and reducing the costs of system procurement and maintenance services.
10) **Compliance with Standards**. The Survalent platform complies with widely accepted standards for open systems, both from standards organizations as well as de facto standards. This enables utilities to select the best-of-breed hardware and software solutions to meet their future needs and greatly enhances the system's ability to communicate with enterprise systems and take advantage of web enabling technologies.

4.2 System Architecture

The Survalent ADMS system architecture has been designed to meet the functional, performance, availability, security and expandability requirements of critical systems and to allow the utility to grow and improve in areas such as customer service and response.

Industry-standard components are used throughout the ADMS system to ensure interoperability with systems from other vendors and to simplify future expansion. The system architecture is based on a distributed client/server architecture designed to internationally recognized standards in all areas of interconnectivity. The system architecture is based on the Open Systems Interconnection (OSI) seven-layer model, and the network equipment conforms to international standards.

The Survalent ADMS supports multiple environments as shown in Figure 4-1: System Architecture:

1) **SCADA/DMS Production System**: The SCADA/DMS System is the production environment used for the real-time monitoring and control of the power grid. It performs its function by using real-time data and produces information immediately applicable to real-time operations and represents a "best" estimate of the current "as-operated" real-time state of the power system.

2) **Corporate Access System**: The Corporate Access System is a collection of servers that collectively provide web-based access to ADMS functionality to Corporate users and external applications connected to the Corporate WAN. They also provide the long-term archive for historical data and reporting. The Corporate Access System is implemented as a demilitarized zone (DMZ); this architecture isolates Corporate users and external applications from the ADMS real-time database, thereby minimizing performance issues and data security concerns.

3) **Quality Assurance System (Sandbox - Existing license with current Platinum support)**: The Quality Assurance System is an offline environment used for testing hardware firmware updates, operating system patches, and software upgrades, updates, and hot fixes. The staging environment is a replication of the production environment, and full regression tests are performed in the staging environment prior to updating the production, development, and training environments to ensure all implementation steps and procedures are accurate

4) **Project Development System**: The Project Development System is an offline environment used for the generation, maintenance and testing of SCADA and DMS databases, network model, displays, and reports. Once tested and validated, the updated databases, displays, and reports are published to the production environment for use in real-time operations.

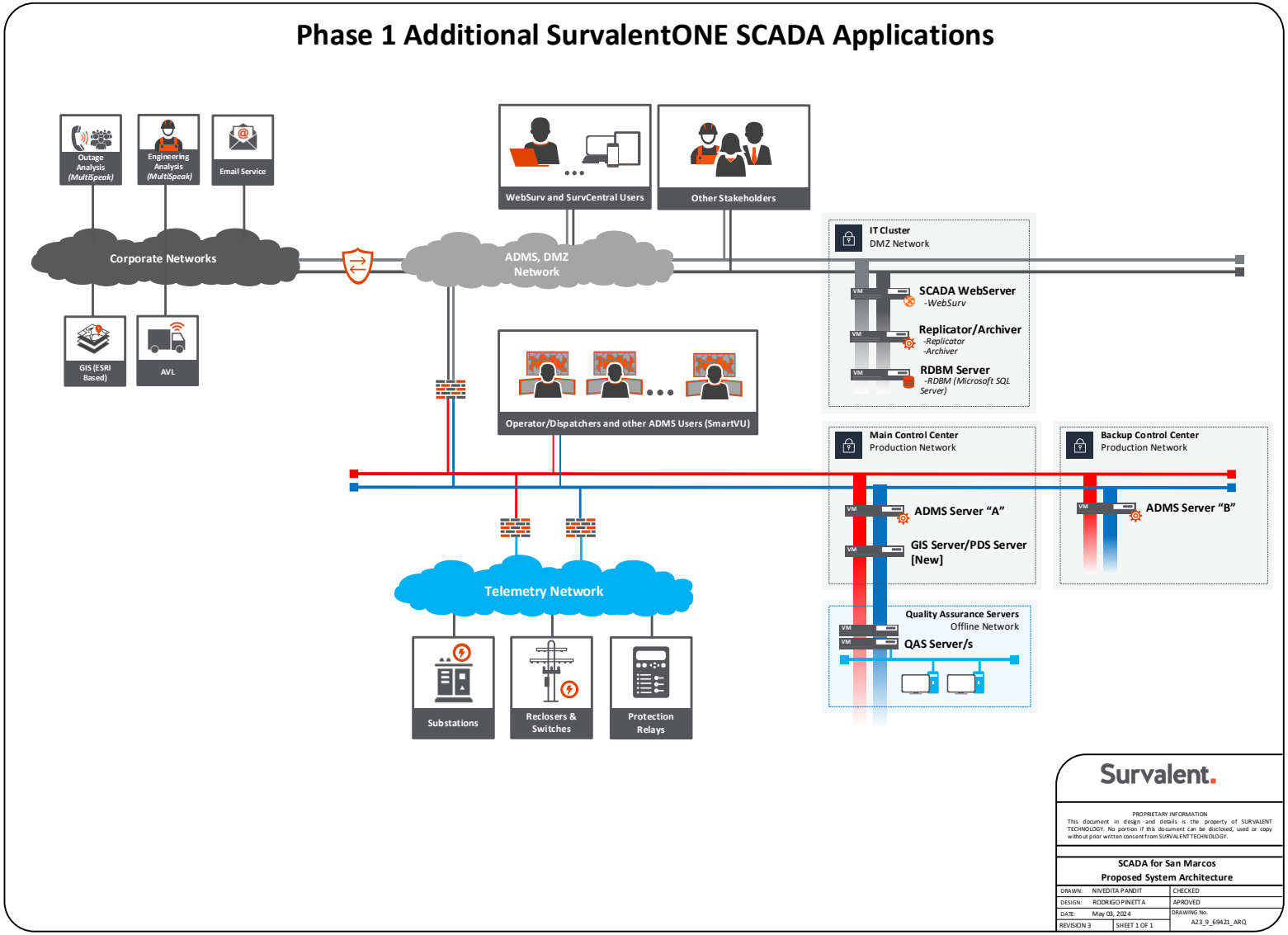


Figure 4-1: System Architecture

[THIS PAGE INTENTIONALLY LEFT BLANK]

4.3 System Components

4.3.1 Production System

4.3.1.1 ADMS Servers

The ADMS servers are responsible for processing all incoming information from the remote terminal units and external data links, and for executing the real-time supervisory control functions of the system. These servers incorporate a memory-resident real-time database to satisfy real-time data requirements, and perform functions associated with data acquisition such as limit checking, data conversion, alarm processing, calculated point processing, historical data collection, and supervisory control services. The ADMS servers are also responsible for executing the distribution management (DMS) applications such as network topology processing, distribution power flow, FLISR, and VVO, if these applications are selected.

Communication scanners running on the ADMS Servers collect the data from the RTUs and external data links. The raw data is then processed, written to the real-time database, and distributed to the other nodes of the system. Note that the communication scanners are not protocol translators; therefore, it is not necessary to maintain a separate database or define complicated point-mapping schemes; the data required by the communication scanners (such as channel configurations, baud rates, protocols, etc.) is configured in the ADMS database.

In order to achieve the high availabilities required for critical data and functions, the system architecture provides a simple but extremely powerful quad-redundancy scheme, as well as redundant local area networks. Fast, automatic failovers give rise to an enhanced availability of critical functions, an essential property of any mission-critical system.

4.3.1.2 Operator Workstations

Operator workstations are used for monitoring and controlling the distribution network. Each workstation is equipped with SmartVU, our next generation operator interface utilizing the power of modern graphics hardware and multi-CPU systems to accomplish high resolution graphics and speed.

SmartVU provides a tabbed interface which allows users to have quick access to a large number of views of their map, alarms, operation logs and graphs. SmartVU uses its own local copy of displays on which it overlays dynamic analog and status data retrieved from the database. Operator actions, such as control and alarm acknowledgement, are forwarded to the ADMS server for execution.

San Marcos owns unlimited user license for SmartVU.

4.3.2 Corporate Access System (DMZ)

The Corporate Access System is a collection of application servers and web servers that are configured in a demilitarized zone. The system has been designed with a three-tier architecture such that ADMS users and applications connected to the Corporate WAN will access the ADMS via the DMZ. All web interfaces have been built with .NET technology and run on the Microsoft Internet Information Services (IIS).

To support the web servers, the Corporate Access System maintains a near-real-time copy of the ADMS database in a relational database (RDBMS). This isolates Corporate users and external applications from

the real-time database thereby minimizing performance issues and data security concerns. The Corporate Access System also provides long-term storage of historical data by transferring the historical data into a parallel set of archive tables, and allowing the archive tables to grow to a much larger size.

To support the high availability requirements of distribution utilities, Survalent recommends that at least two load balanced web servers be provided for each function. Additional web servers can be provided depending on the number of concurrent users to be supported. The load balancing feature provided by Reverse Proxy Servers will distribute the users among the pool of servers available.

4.3.2.1 Replication Servers

The Replication Servers host the Survalent applications that are responsible for replicating near-real-time SCADA/ DMS data to a relational database in the Corporate Access System demilitarized zone. The relational database in the DMZ is comprised of the following tables:

1. SCADA data for the SCADA Web application.
2. Historical data for the long-term historical archive.

In keeping with security best practices, communication connection requests are always initiated from applications in high security zones to applications in lower security zones - never the reverse. This means that applications running on the Replication Servers only accept connection requests from applications running on the real-time SCADA/ DMS System (high security zone), they never initiate connections to the SCADA/DMS System.

4.3.2.2 RDBMS Servers

The RDBMS Servers are responsible for managing the relational database in the DMZ. The relational database in the DMZ is comprised of the following tables:

1) Near-real-time SCADA data for the SCADA Web application (WebSurv)
2) Historical data for the long-term historical archive; as a result, the RDMS Servers will require a large amount of disk space in order to store up to 7 years of historical outage data online.
3) User accounts, passwords, and user rights for all web applications. The STC Account Manager application is provided to manage user accounts and user rights.

4.3.2.3 SCADA Web Servers

The SCADA Web Servers host the web applications that provide real-time SCADA information to users via a web browser, without the need for custom installation or maintenance. The WebSurv (desktop) and SurvCentral (mobile) web applications allow Corporate users to call up and view any SmartVU graphical display, substation one-line, or tabular display. Refresh of dynamic data, alarms, and graphics can be user defined and achieved on a periodic basis every few seconds. Users can access reports, graphs, and point setting information in a Windows Explorer type interface. User logon is required so that only authorized users can access WebSurv and SurvCentral displays, and access is read-only (no controls). WebSurv and SurvCentral have been built with .NET technology and run on the Microsoft Internet Information Services (IIS). WebSurv and SurvCentral use HTML5, Silverlight or SVG (depending on browser capability) to render

dynamic SmartVU graphics in the user web browser, and support panning, zooming, dynamic line coloring and other dynamic features of the SmartVU interface.

4.3.3 Project Development System (PDS)

The Project Development System (PDS) provides an off-line environment for generating and testing display and database changes without affecting the on-line system. The PDS system is comprised of a PDS server and one or more PDS workstations equipped with up to eight monitors. The PDS provides tools to import distribution network data residing in a corporate GIS system or offline analysis tools into the ADMS.

The PDS is used to perform the following tasks:

a) Build the ADMS database and displays from multiple sources: existing corporate GIS information may be supplemented with data from offline analysis tools, Customer Information Systems, and other existing facilities management systems. GIS data is imported and validated for consistency, and invalid data can be returned to the corporate GIS for correction.

b) Control the transfer of modifications to the system databases and displays where the changes can be reviewed and approved before being transferred to the online system. A sophisticated reservation mechanism is used to collect database edits into “projects”, which are then published to the online system once the edits are tested and accepted on the Development System. This reservation system allows multiple users to edit the system databases and displays simultaneously without interfering with each other’s work.

The PDS provides a full set of ADMS functionality in an off-line environment. An off-line copy of the memory-resident databases is available on the ADMS Server for development and test purposes, so that database change orders can be applied and rolled-back as necessary to ascertain that the changes are correct. Display edits are stored on this server and may be validated with the off-line data so that they too can be verified before being distributed to the online system. Once the modifications have been tested and approved, they can be installed on the online system quickly and easily.

4.3.4 Quality Assurance System (QAS) – Sandbox (existing)

The QAS provides an environment to install, monitor, and evaluate software patches and updates including, but are not limited to, operating system patches, third party software patches, and Survalent software updates. Regression tests, including redundancy tests, can be performed and confirmed prior to installing the updates to the online system and hence minimizing considerably the risk to the online system. To support this functionality, the QAS can be configured to receive near-real-time data from the online system.

NOTE: This license is included as a free trial environment license as part of San Marcos’s current Platinum support plan.

4.3.5 Virtual Environment Platforms

Survalent uses the following criteria to determine the appropriate virtual environment:

- The Survalent ADMS will work within any virtual environment. Survalent performs factory testing using Microsoft Hyper-V, but many customers have successfully deployed our ADMS using VMWare and Nutanix.
- Survalent highly recommends using SSD Drives for optimal performance; storage type can be dynamic or fixed disk.
- When ADMS is intended to be dual redundancy or above, we recommend a comparable number of hosts to avoid a single point of failure.

The following table lists the recommended hardware components for system servers in virtualized environments for reference.

Table 4-1: Recommended VM Hardware components

Location:	VM:	V-Cores	RAM (GB)	Storage (GB)	Operating System (OS)	Third-Party Licenses
ADMS, Production System						
Primary Control Center	ADMS Server "A"	8	32	480	Microsoft Windows Server 2019 or later.	
Primary Control Center	GIS Server/PDS Server	8	16	480	Microsoft Windows Server 2019 or later.	Microsoft SQL Server 2019 or later Express Edition.
Backup Control Center	ADMS Server "B"	8	32	480	Microsoft Windows Server 2019 or later.	
Note 1: ADMS Server VMs are sized for up to 15 concurrent users and 25K points.						
ADMS, Corporate Access System (DMZ)						
Primary Control Center	Replicator/Archiver	4	8	480	Microsoft Windows Server 2019 or later.	
Primary Control Center	SCADA Web Server	8	16	480	Microsoft Windows Server 2019 or later.	
Primary Control Center	RDBMS (MS SQL) Server	8	16	480 GB minimum,	Microsoft Windows Server 2019 or later.	Microsoft SQL Server 2019 or 2022 Standard

Location:	VM:	V-Cores	RAM (GB)	Storage (GB)	Operating System (OS)	Third-Party Licenses
				+120GB per year for archiving		edition -15 CALs/16 Core License (for 15 concurrent Web users)
Physical ADMS Workstations						
Dell precision or similar		Intel Xeon W-2235 3.8GHz 6C/12T, 32GB RAM, 2 x 512GB Solid State Drive, NVIDIA Quadro P400, Windows 10 or 11 Professional Edition				Microsoft Office Pro is recommended, but not mandatory.

The proposed vCPU & RAM for the VMs is to handle the peak traffic/demand.

Within a virtual environment, VMs can be provisioned initially at 60% of the proposed compute (**except ADMS hosts, replicator & RDBMS**) and the organization can use its own hypervisor or 3rd party monitoring software, to monitor the VM resource utilization.

At any point in the future, if the VM utilization reaches 80%, IT can assign the vCPUs and RAM based on the proposal to avoid any performance-related issue.

Note: QAS license provides the capability for a copy of the system.

4.4 List of Deliverables

4.4.1 Phase 0: Existing SCADA software (Owned by San Marcos)

Item	Qty	Description	Price (USD)
		SurvalentONE SCADA Licenses	
1.	1	**SurvalentONE Base SCADA Software [Dual Server]** The base SCADA license includes data acquisition, data processing, alarm and event processing, and historical data management functions. It also includes the STC Explorer database editor which includes editing tools for database points, access control, control zones, system parameters, station cloning, point modelling, and setup of advanced applications. Other features include command sequencing, alarm suppression, event data recording and archiving, IED control panels, mapboard driver, and remote alarm annunciation. SurvalentONE SCADA software licenses are valid for unlimited points.	EXISTING
2.	1	**SurvalentONE SmartVU (Unlimited Concurrent Users)** SmartVU provides a modern, intuitive, user friendly user interface for managing the distribution network using high quality graphics driven by a powerful graphics engine. The SmartVU environment includes a tabbed interface that provides quick access to a large number of graphic displays including single-line diagrams, geographical maps, trend graphs, summary displays, operations log, and tabular views of the distribution network. The graphic displays support layers, panning, zooming, decluttering, dynamic line coloring, hyperlinks, and other dynamic display features as well as standard graphics formats such as JPG, BMP, PDF, etc. One license is required for each concurrent user.	EXISTING
3.	1	**SurvalentONE Standard DNP3 Protocol** The DNP3 scan task is designed to communicate with one or more devices that use the DNP3 protocol over serial asynchronous or TCP/IP communication lines. The scan task conforms to Level 2 of the DNP3 Application Layer protocol as specified in the Subset Definitions published by the DNP3 User's Group. This license is for the standard DNP3 protocol implementation, Secure DNP3 Protocol is also available under a separate license.	EXISTING
4.	1	**SurvalentONE Modbus RTU Protocol** The MODBUS RTU scan task is designed to communicate with one or more devices that use the MODBUS RTU protocol over serial asynchronous or TCP/IP communication lines.	EXISTING
5.	1	**SurvalentONE Alarm Suppression** Alarms Suppression allows a defined hierarchy of primary/secondary alarm	EXISTING

Item	Qty	Description	Price (USD)
		point relationships. These relationships may be used for either alarm suppression or group acknowledgement, or both.	
6.	1	**SurvalentONE Command Sequencing** Command Sequencing is an easy-to-use high-level scripting language used to define and execute scripts that use database points as variables. Command sequence scripts can be used to perform calculations, switching sequences, distribution automation, open-loop control, or closed-loop control.	EXISTING
7.	1	**SurvalentONE Disturbance Capture** The Disturbance Capture application monitors changes to all analog and status points periodically, defines events that trigger disturbance data captures, monitors disturbance triggers and generates disturbance data capture files.	EXISTING
8.	1	**SurvalentONE Event Data Recording** Event Data Recording records all status changes, operator controls and Sequence of Events (SOE) data. Non-SOE events are time-stamped to the nearest second, and SOE events are stamped to the nearest 1 millisecond subject to the capabilities of the RTU.	EXISTING
9.	1	**SurvalentONE IED Control Panel** IED Control Panel is a rapid graphical user interface development tool for SmartVU. The IED Control Panel application is a companion product to the IED Wizard, but can be used as a stand-alone product. It allows users to interact with a graphic representation of an intelligent electronic device (IED), just like they were standing in front of it. The IED Control Panel application contains an extensive library of the most common IEDs available on the market, including SEL, Cooper, ABB, Beckwith, and PML.	EXISTING
10.	1	**SurvalentONE IED Wizard** IED Wizard is a tool that automates the creation of the database for an intelligent electronic device (IED). In just a few simple steps, the wizard creates the required points in the SCADA system database. All of the telemetry and control addresses are generated automatically. The IED Wizard completely eliminates the tedious error-prone data entry of telemetry addresses and mapping tables. The IED Wizard contains an extensive library of the most common IEDs available on the market, including SEL, Cooper, ABB, Beckwith, and PML.	EXISTING

Item	Qty	Description	Price (USD)
11.	1	**SurvalentONE Operations and Outage Accounting** The Operations and Outage Accounting application is based on the Event Data Recording facility that records all status changes and control operations in an event data file. Every night at midnight, the Operations and Outage Accounting application scans the previous day's event data to generate that day's accounting information. Special-purpose report programs produce operations and outage reports. An equipment editor allows you to define the devices for which you want operation and/or outage accounting.	EXISTING
12.	1	**SurvalentONE Remote Alarm Annunciation** The Remote Alarm Annunciation application provides the ability to send an e-mail/paging/SMS message for certain alarms. The user can define which points are annunciated in this fashion, and for each point, which alarms (e.g., which states for a status point and which limits for analog point). Note: SMS supported via email to local cellular provider or using modem approved by local cellular provider; client is responsible for implementing interface with local cellular provider.	EXISTING
13.	2	**SurvalentONE Replicator & Archiver Single Server** Replicator provides near-real-time replication of the ADMS-SCADA database to a SQL Server database in the DMZ, providing access to ADMS-SCADA data by external systems. Archiver provides long-term storage of historical data in the DMZ by transferring the historical data into a parallel set of archive tables, and allowing the archive tables to grow to a much larger size, or even indefinitely. Note: Microsoft SQL Server License is not included.	EXISTING
14.	1	**SurvalentONE WebSurv Portal Single Server** The WebSurv portal provides the ability to display near-real-time ADMS information to corporate users via web browser and without the need for custom installation or maintenance. WebSurv allows the user to call up and view any SmartVu graphical display, substation one-line, or tabular display. Refresh of dynamic data, alarms, and graphics can be user defined and achieved on a periodic basis every few seconds. WebSurv supports panning, zooming, dynamic line coloring and other dynamic features of the SmartVu interface. Each concurrent WebSurv user requires a SQL Server user license. Note: Compatible web browsers: Google Chrome, Microsoft Edge, Safari	EXISTING
15.	1	**SurvalentONE QA / Test Environment (Sand box environment)** The Quality Assurance / Test environment license provides a sandbox environment for testing software and hardware updates, including operating system patches, prior to installing the updates on the online systems. The Quality Assurance / Test environment is configured as closely	EXISTING

Item	Qty	Description	Price (USD)
		as possible to the Main Control System in order to be able to test all system functionality, including failover. Note: This license is included as a free trial environment license as part of San Marcos's current Platinum support plan.	
16.	1	**SurvalentONE MultiSpeak EA Interface** This MultiSpeak interface is used to publish analog and status point data to an external Engineering Analysis (EA) system. Note: Refer to the product overview document for details of messages supported; any custom interface will be quoted and priced separately.	EXISTING
17.	1	**SurvalentONE SCADA Add-in** A Microsoft Excel add-in that allows the user to export real-time and historical data from the SCADA system into Microsoft Excel. All point data fields (not just values) are available to export. The menu commands are available from the standard menu bar within Microsoft Excel. Note: Microsoft office software and license is not included.	EXISTING

Note: It is assumed that existing Survalent licenses have been installed, implemented, configured, and are running.

4.4.2 Phase 1: SCADA (additional SurvalentONE SCADA software and services)

Item	Qty	Description	Price (USD)
		SurvalentONE SCADA Licenses	
18.	1	**SurvalentONE OPC UA Client** OPC Unified Architecture (OPC UA) is a cross-platform, open-source, IEC62541 standard for data exchange. The OPC UA Client supports the Data Access information model. It provides the ability to exchange data with OPC UA- compatible end devices, independently of their software platform, machines, industrial processes, or architecture. Compared to the legacy OPC DA protocol, OPC UA provides added security with payload encryption, peer authentication and connection auditing by the means of certificates. Other OPC interfaces such as Historical Data Access (OPC HDA) and Alarms and Events (OPC AE) are not currently supported Note: OPC UA Client is available in V22.2 or later.	INCLUDED
19.	1	**SurvalentONE SNMP Protocol** The SNMP scan task is designed to communicate with one or more devices using the Simple Network Management Protocol, a protocol typically used to manage devices connected to a TCP/IP network.	INCLUDED

Item	Qty	Description	Price (USD)
20.	1	**SurvalentONE OPC UA Server** OPC Unified Architecture (OPC UA) is a cross-platform, open-source, IEC62541 standard for data exchange. The OPC UA Server supports the Data Access information model only. It supports both subscription and publish-subscribe modes and offers relevant quality codes for supervisory control. Compared to the legacy OPC DA protocol, OPC UA provides added security with payload encryption, peer authentication and connection auditing by the means of certificates. Other OPC interfaces such as Historical Data Access (OPC HDA) and Alarms and Events (OPC AE) are not currently supported. Note: OPC UA Server is available in V22.0 or later.	INCLUDED
21.	1	**SurvalentONE Switching Orders with Guarantees** A switch order is a sequence of steps involving both switching operations and tags that produce conditions for which a guarantee may be issued. Each switch order can contain up to 200 steps. Guarantees, also known as clearances or work permits, are database forms that allow you to issue and track permits for engineering and operations staff working on the electricity system. The application produces a unique permit number and tracks to whom and when the permit was issued. Each permit can have up to 50 tags associated with it.	INCLUDED
22.	1	**SurvalentONE Network Topology Processor** The Network Topology Processor application calculates the energized/de-energized status of electric, gas and water line sections, and displays them on world maps. The calculation is based on the topology of the system and the current status of breakers and valves. For an electrical line section, the system supports 3-phase distribution, and computes the status of each phase independently, such that line sections that are downstream of non-ganged switching devices may contain a mix of energized and de-energized phases. The user can specify colors for “partially energized” or “partially looped” etc. The topology processor includes a feeder trace function that allows the user to select a trace color and have the extent of a feeder highlighted in the selected trace color. Multiple simultaneous traces in different colors are supported.	INCLUDED
23.	1	**SurvalentONE GIS Wizard** The GIS Wizard is used to import the distribution network model and geographic displays into the ADMS. The GIS Wizard checks for the absence of essential electrical information such as phase, KVA and section names and provides an additional level of electrical connectivity check to ensure the data that is imported is complete and correct. It also checks the spatial relationship for your field devices such as transformers and service locations, ensuring the secondary network is accurate. The graphical user interface allows the GIS Specialist to quickly locate database objects with data issues, enabling them to quickly fix them in the GIS	INCLUDED

Item	Qty	Description	Price (USD)
		Note: Requires an ESRI ArcGIS for Desktop Basic license (not included). Note: Hardware is not included. This application normally runs on the PDS Server. Note: Requires a GIS Wizard adapter specific to the customer GIS.	
24.	1	**SurvalentONE GIS Wizard - ESRI GNM Adapter** GIS Wizard adapter that provides an interface to import ESRI GIS data stored in Geometric Network Model (GNM) format into the SurvalentONE ADMS. Customer is responsible for providing and configuring the tools to export the connectivity model, distribution transformers, service locations, generators, primary meters, and DMS network model information to a geodatabase (.gdb) file or SQL tables according to Survalent specifications. The interface supports both full import and incremental import.	INCLUDED
25.	1	**SurvalentONE MultiSpeak OA Interface** This MultiSpeak interface is used to publish SCADA analog and status point data to an external Outage Analysis (OA) system. Note: Refer to the product overview document for details of messages supported; any custom interface will be quoted and priced separately.	INCLUDED
26.	1	**SurvalentONE MultiSpeak AVL Interface** This MultiSpeak interface is used to exchange vehicle location data with an external Automatic Vehicle Location (AVL) system. The vehicle positioning information is stored in analog and status points in the SCADA database, where it can be viewed and manipulated like any other SCADA data. In addition, special features are provided in SmartVU to allow this data to be used to position mobile icons in displays. Note: Refer to the product overview document for details of messages supported; any custom interface will be quoted and priced separately.	INCLUDED
27.	5	**SurvalentONE SurvCentral (Per Concurrent User)** A companion product to WebSurv, SurvCentral provides display access using HTML5 protocol for mobile devices such as mobile phones and tablets. Each concurrent SurvCentral user requires a SQL Server user license. Note: Compatible web browsers: Google Chrome, Microsoft Edge, Safari	INCLUDED
28.	1	**SurvalentONE Base DMS Software [Dual Server]** The base Distribution Management System (DMS) software provides support for a distribution network model. This license is a pre-requisite for the advanced DMS applications such as FLISR, Distribution Power Flow, Distribution State Estimator, Cold Load Pickup, Pre-Switching Validation, Distribution Contingency Analysis and Volt/Var Optimization (VVO)	INCLUDED
29.	1	**SurvalentONE Protection Settings Manager**	INCLUDED

Item	Qty	Description	Price (USD)
		The Protection Settings Manager (PSM) application is used to manage protection settings at locations where you want to have the settings groups maintained by the Master station. The program operates by executing user-defined rules at each location. You can define as many rules as you need for each device. Inputs to rules consist of both SCADA points and line section energized/de-energized states	
30.	1	**SurvalentONE FLISR/LOV [25 feeders][Level 1]** The FLISR/LOV application helps minimize the downtime caused by outages that trip and lock out breakers in a distribution substation. The FLISR/LOV application works in conjunction with hardware, software, telecommunications and grid engineering to decrease the number of customers affected by a power outage by automatically opening and closing switches to isolate compromised sections of line and to re-energize healthy sections of the system to restore energy distribution Note: Site license is based on fair use limit of up to 25 feeders.	INCLUDED
		Survalent Professional Services	
31.	1	**Project Management _Phase 1** Survalent will assign a Project Manager to coordinate the activities of the project including kickoff meeting, project schedule, project status report, managing resources, coordinating remote services, and coordinating on-site activities.	INCLUDED
32.	1	**Remote workshops** This includes: 1) GIS workshop 2) FLISR workshop 3) Protection Setting Manager workshop	INCLUDED
33.	1	**Remote services for Network topology implementation for 2 substations** This includes: a) Preparation of resources for network topology implementation (colors, color tables, fonts and pmacros) b) Applying network topology on substation level for 2 substations c) Linking the connectivity import with 6 outgoing feeder mains from 2 substations.	INCLUDED
34.	1	**Remote services for GIS import** This includes: a) Conversion of GIS data with the use of GIS Wizard and GIS Import Configuration Editor application and preparation for importing the connectivity model from the owner's system with ~27 feeders.	INCLUDED

Item	Qty	Description	Price (USD)
		b) Customer guidance and check of the GIS file during the clean-up process (customer's responsibility); c) Import of service territory dwg d) Preparation of the graphics for the connectivity import: creating SCS color tables, GIS pmacros and GIS Symbols e) Import of the connectivity model from the GIS database into the SCADA system with the use of Survalent Connectivity Import facility f) Generating database points for manual switches g) DB import of transformers and customer service locations. h) Transformers and meters import in SmartVU. ***Please refer to section Pre-requisites.**	
35.	1	**Remote services for MultiSpeak AVL interface** This includes: a) Remote AVL interface setup: • configuring AVL service • setting up to 10 vehicle types b) Configuring max. 20 vehicles c) Creating mobile icons for each vehicle type Note: Customer is responsible for configuring the MultiSpeak interface on the external system.	INCLUDED
36.	1	**Remote services for MultiSpeak Outage Analysis (OA) Installation** This includes: Remote system administration services for installation and configuration of the MultiSpeak Outage Analysis (OA) interface on the Survalent platform. Services must be completed within 3 months unless mutually agreed by both parties. Note: Customer is responsible for configuring the MultiSpeak interface on the external system.	INCLUDED
37.	1	**Protection Settings implementation for 6 feeders** This includes: Defining protection for up to 18 devices in Protection Devices Editor • Defining Rules for the protection devices • Setting up a group value for each rule per device • Defining statements for each rule per device	INCLUDED
38.	1	**Remote services for Setup and configuration of 3 switch orders**	INCLUDED
39.	1	**Remote services for FLISR Implementation for 6 feeders**	INCLUDED

Item	Qty	Description	Price (USD)
		This includes: a) Database preparation: • Creation of 3 points for each feeder that triggers FLISR (FLISR mode, FLISR enable and FLISR lockout) • Assigning lockout points to the 6 corresponding feeders • Creation of alarm format, command state strings and 3 global FLISR points b) Graphics preparation: • Generating colors color tables, fonts and pmacros. • adding pMacros to the SLDs for FLISR status • adding pMacros to the connectivity for the fault targets at the downline reclosers c) FLISR implementation: • Assigning global FLISR points • Creating default records for DMS tables • Enable FLISR for up to 6 feeders (linking the points to the DMS records) • Add fault targets at the downline devices • Global FLISR settings: selecting the 3 FLISR points • KVA aggregation via STC Explorer (reading KVA from transformers in GIS and assignment to conductors) • Creating summary views for FLISR d) FLISR simulation testing for 6 feeders	
40.	1	**On-Site System Engineering Services (5 Days)** Five consecutive days of on-site system engineering services for system installation, commissioning, testing and operator training.	INCLUDED
41.	1	**On-Site Training - System Administration – Level 1 (5 Days)** This 5- consecutive day on-site course is designed for individuals who will be responsible for installation, configuration, and maintenance of the SCADA System.	INCLUDED
42.	1	**Remote services for performance tuning (3 days)**	INCLUDED
Item	**Qty**	**Description**	**Price (USD)**
		SurvalentONE PDS License and services	
43.	1	**SurvalentONE PDS Single Server** The Project Development Server (PDS) is an offline system where a user can create a project to track all database and graphic edits without affecting the production system. Once a user has completed all their edits in the PDS and are satisfied with the changes made, they can then publish their changes to the production system. The PDS supports multi-user editing for both the graphics and database editing.	INCLUDED

Item	Qty	Description	Price (USD)
44.	1	**Remote services to setup PDS Single server application**	INCLUDED

4.4.3 Platinum Support Plan

Since San Marcos has an active existing Platinum support plan for Survalent SCADA system, we have included calculations for Platinum support plan in Attachment C – Cost Proposal.

Item	Qty	Description	Price (USD)
		Support Plan	
45.	1	**Platinum SCADA/DMS Support Plan** The Platinum SCADA/DMS Support Plan provides the following: a) Access to the latest software releases of the delivered SurvalentONE software components, effectively providing an extended warranty on all software components and providing access to the latest product features. b) Access to the Survalent Support Portal which includes the ability to create and track support cases, and provides access to software downloads, product documentation, knowledge base articles, live chat, and support forums. c) 24x7 access to priority, telephone emergency support from the Survalent Support Team. Cases will be treated on a first - come, first serve basis. d) 3 Global User Conference training passes and conference passes per year. e) 25 hours (not more than 8 hours per day) per year of Remote Services. All services will be performed by Survalent staff from Survalent offices. Any hours not used during the support period will expire. f) Access to a Survalent System Engineer on - site for 2 days to provide technical assistance with software updates, assess system health and performance, perform system tuning, and any other technical assistance desired. Site visit is once per year and must be used during the support period.	Please refer Attachment C for Pricing

4.5 Scope of Work

4.5.1 Survalent Responsibilities

Survalent will have overall design responsibility for the project including but not limited to the design, development, assembly, implementation, testing, delivery, installation, commissioning, and warranty of the system. Specifically, Survalent responsibilities will include, but not be limited to, the following items and services related to the system:

Project Management:

1) Supply of the ADMS software as per the List of Deliverables in Section 0.
2) Project management, coordination with San Marcos, smooth communication flow, manage the work plan, schedule, and scope of services as per San Marcos's expectations and Survalent's procedures for on-time completion of the project. Establish the baseline schedule, monitor progress against the baseline, reviews as needed for schedule recovery and delivery of project status reports.
3) Provide administration and clerical support to organize, track and archive project documents. Supply of project documentation including design documents, user manuals, configuration and security settings, drawings, etc.
4) Providing software support, provided that San Marcos establishes and maintains an annual Software Support Agreement.
5) Supplying project documentation including design documents, user manuals, configuration and security settings, drawings, etc.

Phase 1: SCADA (Additional SurvalentONE SCADA Licenses and Services)

6) Supply of the ADMS-SCADA software as per the List of Deliverables in section 4.4.2 of this document.
7) Remote workshops for:
    - GIS workshop
    - Protection Setting Manager
    - FLISR
8) Implementing network topology on 2 substations and training the customer so that they can implement it on the rest.
9) Setup the SurvalentONE PDS.
10) Importing the connectivity model, distribution transformers, and service locations from the GIS. This service will be implemented in two phases:
    a) Phase 1: Data import analysis services to evaluate the GIS feeder connectivity model, distribution transformers, and service locations to validate the quality of the GIS data for use in the Survalent ADMS. Services include:
        i) Configuration of the Survalent GIS Wizard in preparation for importing the feeder connectivity model, distribution transformers, service locations.

ii) Import GIS data into Survalent GIS Wizard. The GIS Wizard performs a number of data validation checks to ensure the consistency and accuracy of the data, and provides a detailed list of informational, warning, and error messages. The graphical user interface provides an easy way to navigate to each object that has issues.

iii) Provide guidance to the City of San Marcos on how to remedy any issues that were found during the analysis of the GIS data in GIS Wizard.

iv) Provide training to utility staff on how to re-import the GIS data into the GIS Wizard for on-going updates.

Survalent services are done remotely from their offices and all file exchanges are done through a secure server. City of San Marcos must provide a properly formatted geodatabase (.gdb) file or shape files containing the feeder connectivity model, distribution transformers, and service locations. Details of the data requirements will be provided by Survalent.

City of San Marcos is responsible for correcting the GIS data to address any issues identified, and for re-importing the data into the GIS Wizard following the evaluation services provided by Survalent. Additional services can be quoted by Survalent to assist with this activity, if needed.

b) Phase 2: Services to import the GIS feeder connectivity model, distribution transformers, and service locations from the GIS Wizard into the Survalent ADMS. These services are performed after the GIS Evaluation Services have been completed and City of San Marcos has resolved any data quality issues identified. Services include:

i) Import of service territory map into the Survalent ADMS based on DWG, OpenStreetMap, or Google map files provided by City of San Marcos

ii) Configuration of the Survalent ADMS graphics (color tables, pmacros and symbols) based on consultation with City of San Marcos

iii) Import of the connectivity model, distribution transformers, and service locations into the Survalent ADMS, including generation of the SCADA database points for the manual switches.

iv) Provide guidance to City of San Marcos on how to remedy any issues found during the analysis of the GIS data in SmartVU.

v) Provide training to City of San Marcos staff on how to re-import the GIS data into the Survalent ADMS following changes to the GIS data.

Survalent services are done remotely from their offices and all file exchanges are done through a secure server. Configuration of the connectivity model within the substations is included in the database and graphics conversion.

City of San Marcos is responsible for re-importing the GIS data into the Survalent ADMS following the initial import services are completed by Survalent. Additional services can be quoted to assist with this activity, if needed."

11) Setup and configure the MultiSpeak OA and AVL interfaces on the Survalent system. This proposal assumes that San Marcos's corporate systems are compatible with the MultiSpeak messages outlined in Volume 2, Appendix B Supported MultiSpeak Interfaces.

12) Remotely setup and configure SurvalentONE FLISR application on 6 feeders (from the 2 substations) and train the customer so that they can implement FLISR on remaining feeders. Please refer to Vol.2 ADMS Standard Product Overview, Section 6.5 FLISR for additional details.

13) 5 consecutive days of onsite installation and commissioning and operator training.

14) 5 consecutive days of onsite training to system administrators so that they will be self-sufficient and able to operate, maintain, and upgrade the system as per the list of deliverables in Section 4.4.

15) Remote tuning all software parameters to meet the system availability and performance requirements.

4.5.2 San Marcos Responsibilities

San Marcos will be responsible for providing the proper environment and facility for the system, and for performing the support work associated with the project specifically as follows:

Infrastructure, facilities, and System software preparation

1) Providing proper building and facilities including environmental control on-site and for all equipment and security initiatives within the control center (i.e.: sensor card access), such that only authorized users can gain access to ADMS-SCADA equipment.

2) Providing all hardware, including servers, workstations, enclosure, telecommunication equipment, peripherals, cabling, and related support material.

3) Provision and deployment of all the hardware, backup tools, virtual-replicas, and the configuration of the disaster recovery environment.

4) Providing any third-party software like Microsoft SQL licenses, Microsoft office, third-party security software such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS), or anti-virus software that may be required for the system.

5) Reviewing and approving project deliverables such as the software documentation, user manuals, display and report formats, drawings, progress reports, training program, quality assurance program, acceptance tests and related documentation, support service procedures (among other examples, training and maintenance), and documentation of the as-built system.

6) Coordinating work to be completed at San Marcos facilities, such as external equipment connection, Field Testing, etc.

7) Configuring the WAN equipment and maintaining the firewall rules based on inputs from Survalent.

8) Provide the backup software and backup server hardware, configuration, and integration of the software with the corporate backup hardware (i.e.: backup server, tape library or drives).

9) Preparing deficiency reports and retesting to confirm their resolution by Survalent.

10) Installation of all equipment at San Marcos facilities.

11) Providing facilities for on-site training.

12) Conducting the Field Tests.

13) Disconnection and removal of the systems being replaced, if any.

14) Installation and implementation of the existing SurvalentONE SCADA licenses listed in List of Deliverables section 4.4.1.

Phase 1: Additional SurvalentONE SCADA

15) Participate in all remote workshops conducted by Survalent.
16) Provide existing database and single line diagrams of substations in AutoCAD.
17) Implementing Network Topology on remaining substations.
18) San Marcos is responsible for correcting the GIS data to address any issues identified, and for re-importing the data into the GIS Wizard following the evaluation services provided by Survalent.
19) Provide the GIS files and other information related to system interfaces.
20) Configure AVL and OMS interface on third party systems.
21) Implementing and installing FLISR on remaining feeders.
22) Participate in the training.
23) Ensure compliance and fulfill the requirements specified in Appendix F Pre-requisites of this document for the listed applications.

[THIS PAGE INTENTIONALLY LEFT BLANK]

4.6 Preliminary Project Schedule

Please refer to Figure 4-2: Preliminary Project Schedule for an overview of the proposed implementation schedule.

Survalent.

Project Schedule

ID	Task Name	Duration	Predecessc	Resource Names
1	**City of San Marcos SCADA & DMS**	**140 days**		
2	**Project Initiation Phase**	**11 days**		
3	Receipt of Contract	0 days		STC - Project Delivery Manager
4	Internal project review and project setup	5 days	3	STC - Project Manager;STC - Project De
5	**Project Plan (All Phases)**	**5 days**		
6	Prepare the Integrated project plan with all vendor tasks, and dependencies	5 days	4	STC - Project Manager;STC - Project De
7	Delivery	0 days	6	STC - Project Manager
8	Project launch/kickoff meeting	1 day	7	STC - Project Manager;STC - System Sp
9	*Project Initiation complete*	*0 days*	*8*	
10	**Phase 1 - SCADA (Additional software and sevices)**	**124 days**		
11	**Phase 1 - Implementation Phase**	**43 days**		
12	**Workshops**	**1 day**		
13	PSM - Protection Setting Manager - Workshop	0.5 days	8FS+5 day	Customer;STC - System Specialist
14	FLISR - Workshop	0.5 days	13	Customer;STC - System Specialist
15	**SCADA**	**7 days**		
16	Network Topology Implementation (2 Substations)	2 days	14	STC - System Specialist
17	Switch Orders and Guarantees (3 Orders)	1 day	16	STC - System Specialist
18	PSM - Protection Setting Manager (6 Feeders)	3 days	17	STC - System Specialist
19	PDS - Project Development System - Installation, Commissioning, and Training	1 day	18	STC - System Specialist
20	**Interfaces**	**9 days**		
21	OA Interface (MultiSpeak)	3 days	15	STC - System Specialist
22	AVL Setup (MuliSpeak)	6 days	21	STC - System Specialist
23	**GIS Import Services**	**33 days**		
24	**GIS Data Workshops**	**12 days**		
25	GIS Data Workshop - Session 1	1 day	14	Customer;STC - System Specialist GIS
26	GIS Data Workshop - Session 2	1 day	29	Customer;STC - System Specialist GIS
27	**GIS Data**	**32 days**		
28	[Customer] GIS - Data Adjustments and Clean-up	10 days	25	Customer
29	*[Customer] GIS - Data Submission*	*0 days*	*28*	*Customer*
30	Connectivity Import and Validation	22 days	29	STC - System Specialist GIS
31	[Customer] GIS - Data Adjustments and Clean-up 2	5 days	30SS+5 da	Customer
32	*GIS Services Phase Complete*	*0 days*	*30*	
33	FLISR (6 Feeders)	9 days	32	STC - System Specialist
34	**Phase 1 - Deployment Phase**	**21 days**		
35	Phase 1 - On-Site Installation and Commissioning	5 days	11	STC - System Specialist;Customer
36	Phase 1 - On-Site Training	3 days	35	STC - System Specialist;Customer
37	Phase 1 - Remote Perfromance Tuning (Optimization)	3 days	36FS+10 c	STC - System Specialist;Customer
38	*Phase 1 Complete*	*0 days*	*11;34*	
39	**Customer Activities**	**60 days**		
40	[Customer] SCADA - Remaining Substations (6 Substations)	20 days	38	Customer
41	[Customer] FLISR - Remaining Feeders (19 Feeders)	40 days	40	Customer
42	**Payment Milestones**	**80 days**		
43	*Contract Award*	*0 days*	*3*	*Customer;STC - Project Manager*
44	*Completion of Kickoff Meeting*	*0 days*	*9*	*Customer;STC - Project Manager*
45	*Completion of SCADA and Interfaces Implementation*	*0 days*	*22*	*Customer;STC - Project Manager*
46	*Completion of GIS Services*	*0 days*	*32*	*Customer;STC - Project Manager*
47	*Completion of FLISR Implementation*	*0 days*	*33*	*Customer;STC - Project Manager*
48	*Final System Acceptance*	*0 days*	*38*	*Customer;STC - Project Manager*

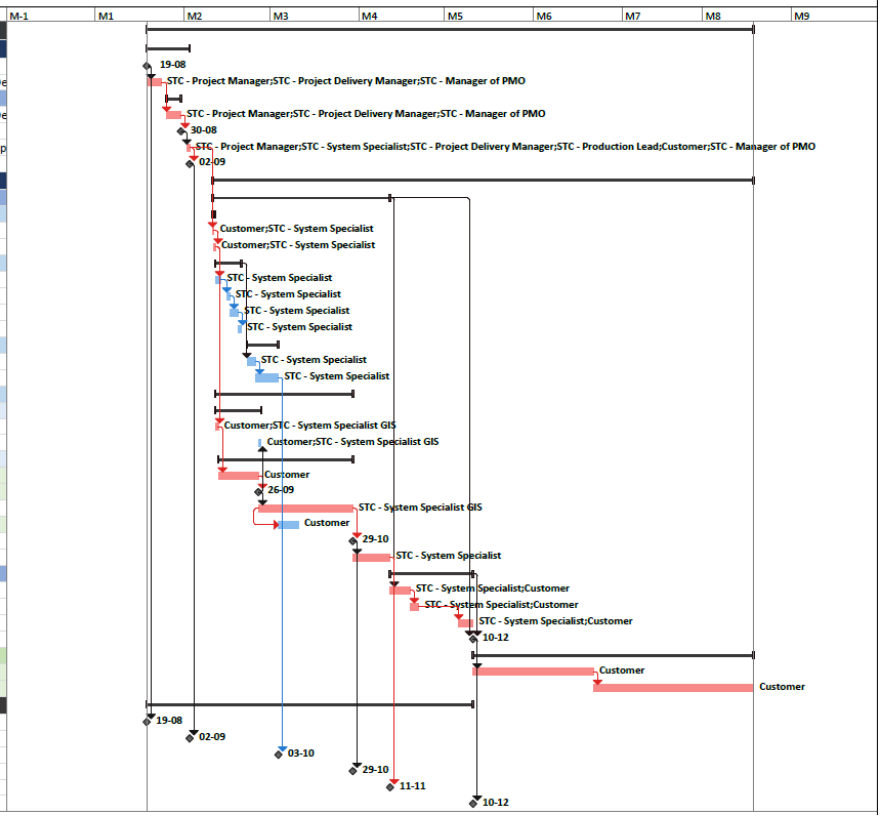


Figure 4-2: Preliminary Project Schedule

4.7 Warranty

This proposal includes a 12-month warranty for SurvalentONE DMS from date of site acceptance. Survalent warrants that our products will be free from defects in materials and workmanship under normal use during the warranty period. Nonetheless, Survalent strongly recommends that clients register for a Software Support Plan at the beginning of the warranty period in order to receive the many benefits of the Support Plans. Support Plans are normally effective for a period of one year, but multi-year Support Plans are also available.

"I have no doubt about Survalent's commitment to our success, and I appreciate your personal interest and commitment to ensure that success."

- Clallum PUD

5 Information Questionnaire and Assurances

Please refer to Appendix B – Attachment B Vendor Information Questionnaire and Assurances of this document for details.

[THIS PAGE INTENTIONALLY LEFT BLANK]

6 Price Proposal

Please refer to Appendix A – Attachment C – SCADA RFP Cost proposal form for details

[THIS PAGE INTENTIONALLY LEFT BLANK]

7 Local Business Presence

Survalent lists its headquarters and satellite office that may be utilized during the project in section 2.1 Company information of this document. While Survalent does not have a physical local presence in San Marcos, Survalent assures that our team has a strong track record of successfully executing similar projects from headquarters and Macedonia office.

Survalent has successfully implemented San Marcos's SCADA system in past from these locations and is confident that it can successfully implement this project to your satisfaction. We look forward to discussing how we can tailor our approach to meet your specific requirements.

[THIS PAGE INTENTIONALLY LEFT BLANK]

8 House Bill 89 Verification Affidavit

Please refer to Appendix C – Attachment D House Bill 89 verification affidavit for details.

[THIS PAGE INTENTIONALLY LEFT BLANK]

9 Conflict of Interest Questionnaire (CIQ)

Survalent has reviewed the Attachment E Conflict of Interest questionnaire and confirms that there is no conflict of interest in this situation. Survalent takes ethical considerations very seriously and have implemented stringent measures to ensure transparency and fairness in all our dealings with City of San Marcos.

[THIS PAGE INTENTIONALLY LEFT BLANK]

10 Commercial

10.1 System Prices

Please refer to Attachment C - SCADA RFP Cost Proposal in Appendix A_Rev 3.

Unless otherwise noted, all prices are in cleared funds and do not include any taxes, levies, imports, duties, charges, fees and withholdings of any nature. If San Marcos is compelled to make any such deduction, it will pay to Survalent such additional amounts as are necessary to ensure receipt by Survalent of the full amount which Survalent would have received but for the deduction.

End User: City of San Marcos

Shipping Terms: EXW Ontario, Canada

Please send purchase order to stcorder@survalent.com

This quote is valid until September 1st, 2024 and is based on Contract and Terms and Conditions found at sanmarcostx.gov/StandardTermsandConditions, (b) Software License Agreement, and (c) Support and Maintenance Terms and Conditions, as applicable.

Note 1: SurvalentONE DMS software licenses are valid for up to 25 feeders and includes 12 months warranty from date of operational use.

Note 2: Software licenses are non-refundable and cannot be exchanged.

Note 3: Survalent reserves the right to issue temporary licenses until payment has been received in full.

Note 4: Survalent reserves the right to periodically audit the end user system configuration to ensure the software has been deployed in accordance with the Survalent Software License Agreement.

Note 5: Please ensure the end user client name is identified on the purchase order; purchase orders may be rejected if this information is missing.

Note 6: Services will be scheduled at a mutually agreeable time. Customer changes to the agreed schedule may result in an additional charge.

10.2 Payment Milestones

Milestone	Payment (%)
Receipt of order	25%
Completion of project kickoff	10%
Completion of SCADA and Interfaces Implementation	25%
Completion of GIS Services	25%
Completion of FLISR Implementation	10%
Final Acceptance	5%
Total	100.00%

10.3 Terms and Conditions

Survalent confirms that it has read Appendix F: Contract and Terms and Conditions found at sanmarcostx.gov/StandardTermsandConditions and agrees to it with no redline comments.

10.4 Software License Agreement

Please refer to the document “COSM Software License Agreement Support Ts Cs – final Rev4”.

10.5 Software Maintenance Agreement

Please refer to the document “COSM Software License Agreement Support Ts Cs – final Rev4”.

10.6 Authorized Signature

The undersigned hereby:

1) Declares that the Proposal herein, including the statements made and the information provided in the Proposal are complete, accurate and true in every detail.

Signature: 

Print Name: Rodrigo Pinetta

Title: Director, Proposals and Solutions Engineering

Date: May 21, 2024

[THIS PAGE INTENTIONALLY LEFT BLANK]

Appendix A Attachment C - SCADA RFP Cost Proposal

[THIS PAGE INTENTIONALLY LEFT BLANK]

ATTACHMENT C - SCADA RFP Cost Proposal

This cost sheet should be completed fully by the Supplier. The prices include both base requirements and optional requirements. When Suppliers can provide a more detailed cost breakdown of component elements, they are encouraged to do so. However, component pricing should be functionally placed under the appropriate software, hardware, or services pricing element and clearly labeled by name, function, and capability.

#	Item Description	Supplier Description	Quantity	Unit Price	Total Price
A. Phase 0 SCADA System - Existing Survalent SCADA					
1. Software & Licensing Costs (List basic SCADA software license costs under this section. Do not include special applications here.)					
1.1	Phase 1.1: Dual Redundant SCADA Software License - Existing Licenses	Existing Survalent SCADA. Please refer Volume 1 Section 4.4.1 List of Deliverables Item 1 - Item 17 It is assumed that the existing Survalent licenses have been installed, implemented, configured, and are operational.	1	0.00	0.00
				Phase 0 - Software Costs	0.00

#	Item Description	Supplier Description	Quantity	Unit Price	Total Price
B. Phase 1 SCADA System - Additional SCADA Licenses					
2. Software & Licensing Costs - Phase 1: Additional SCADA licenses					
2.1	Phase 1.2: Additional SCADA sofware Licenses	Please refer Volume 1 Section 4.4.2 List of Deliverables Item 18 - Item 30	1	$ 156,866	$ 156,865.50
				Phase 1 - Software Costs	$ 156,865.50
3. Hardware Costs					
3.1	Two Synchronized Host Computers			$ -	N/A
3.2	Host Servers			$ -	N/A
3.3	Operator Work Station (Local/Remote)			$ -	N/A
				Phase 1 - Hardware Costs	N/A
4. System Engineering Services for Phase 1 SCADA Additional Licenses					
4.1	Phase 1: System Engineering and Configuration	Please refer Volume 1 Section 4.4.2 List of Deliverables Item 32 - Item 39	1	$ 107,000	$ 107,000.00
4.2	Phase 1: Project Management	Please refer Volume 1 Section 4.4.2 List of Deliverables Item 31	1	$ 14,000	$ 14,000.00
				Phase 1 - Engineering Services Costs (In-house)	$ 121,000.00
5. On-site Support Services for Phase 1 SCADA Additional Licenses					
5.1	Phase 1: System Installation and Commissioning	Please refer Volume 1 Section 4.4.2 List of Deliverables Item 40 (5 consecutive days of onsite services: 4 days for Installation and Commissioning of Survalent software and 1 day Operator training)	1	$ 18,375	$ 18,375.00
5.2	~~Phase 1: Operator Training - 2 weeks - See Section VII.C.2. of Specification~~	Included in section 5.1 above. Given that San Marcos has existing Survalent SCADA system installed and operational, Survalent believes this duration of training is not necessary.	1	$ -	$ -
5.3	~~Phase 1: On-site Small Instruction and troubleshooting - 2 weeks - See Section VII.C.3. of Specification~~	Given that San Marcos has existing Survalent SCADA system installed and operational, Survalent believes these services are not necessary. Survalent has included all the required services including a 3 days remote services for performance tuning for successful implementation of the Phase 1.	1	$ -	$ -
				Phase 1 - Engineering Services Costs (On-Site)	$ 18,375.00
6. Additional Services or Costs - *Clearly identify and present unit costing*					
6.1	Administrator Training	Survalent has included 5 consecutive days of onsite training in the scope for Phase 1 Please refer Volume 1 Section 4.4.2 List of Deliverables Item 41	1	$ 18,375	$ 18,375.00
				Phase 1 - Additional Onsite Services Costs	$ 18,375.00

ATTACHMENT C - SCADA RFP Cost Proposal

This cost sheet should be completed fully by the Supplier. The prices include both base requirements and optional requirements. When Suppliers can provide a more detailed cost breakdown of component elements, they are encouraged to do so. However, component pricing should be functionally placed under the appropriate software, hardware, or services pricing element and clearly labeled by name, function, and capability.

#	Item Description	Supplier Description	Quantity	Unit Price	Total Price
A. Phase 0 SCADA System - Existing Survalent SCADA					
1. Software & Licensing Costs (List basic SCADA software license costs under this section. Do not include special applications here.)					
1.1	Phase 1.1: Dual Redundant SCADA Software License - Existing Licenses	Existing Survalent SCADA. Please refer Volume 1 Section 4.4.1 List of Deliverables Item 1 - Item 17 It is assumed that the existing Survalent licenses have been installed, implemented, configured, and are operational.	1	0.00	0.00
				Phase 0 - Software Costs	0.00

#	Item Description	Supplier Description	Quantity	Unit Price	Total Price

#	Item Description	Supplier Description	Quantity	Unit Price	Total Price
D. Master Summary					
Phase 0: Existing SurvalentONESCADA software licenses					
Software & Licensing Costs		Vol 1 : List of Deliverables Section 4.4.1			$ -
				Total Phase 0 Price	$ -
Phase 1: Additional SurvalentONE SCADA software licenses and services		Vol 1 : List of Deliverables Section 4.4.2			
Software & Licensing Costs for Phase 1 SCADA Additional Licenses					$ 156,866
Hardware Costs					$ -
System Engineering Services for Phase 1 SCADA Additional Licenses					$ 121,000
On-site Support Services for Phase 1					$ 18,375
Additional Onsite Services or Costs for Phase 1					$ 18,375
				Sub-total Phase 1 Cost	$ 314,615.50
				Phase 1 Discount	$ (96,030.00)
				Total Phase 1 Discounted Price (as per Rev 2)	**$ 218,585.50**
SurvalentONE PDS Single Server Software License		Added to the base offer as requested by San Marcos. Please refer to Vol 1 : List of Deliverables Section 4.4.2 (item 43)			$ 41,179
SurvalentONE PDS Single Server Software setup services		Added to the base offer as requested by San Marcos. Please refer to Vol 1 : List of Deliverables Section 4.4.2 (item 44)			$ 2,750
				Total SCADA without Tax	**$ 262,514.00**

ATTACHMENT C - SCADA RFP Cost Proposal

This cost sheet should be completed fully by the Supplier. The prices include both base requirements and optional requirements. When Suppliers can provide a more detailed cost breakdown of component elements, they are encouraged to do so. However, component pricing should be functionally placed under the appropriate software, hardware, or services pricing element and clearly labeled by name, function, and capability.

#	Item Description	Supplier Description	Quantity	Unit Price	Total Price
A. Phase 0 SCADA System - Existing Survalent SCADA					
1. Software & Licensing Costs (List basic SCADA software license costs under this section. Do not include special applications here.)					
1.1	Phase 1.1: Dual Redundant SCADA Software License - Existing Licenses	Existing Survalent SCADA. Please refer Volume 1 Section 4.4.1 List of Deliverables Item 1 - Item 17 It is assumed that the existing Survalent licenses have been installed, implemented, configured, and are operational.	1	0.00	0.00
				Phase 0 - Software Costs	0.00

#	Item Description	Supplier Description	Quantity	Unit Price	Total Price
D. Post Installation SCADA Service Contracts			**Phase 0**	**Phase 1**	**Total**
D.1	Technical Support and Software Upgrade Year 1* - Platinum	*Please refer Volume 1 Section 4.4.3 List of Deliverables Item 45 for description.* *Survalent offered our highest level of support for estimation since San Marcos is currently using Survalent Platinum support for their SCADA system. Survalent has other support plans available (Silver and Gold) which are lower in price than the platinum support plan. Please refer to Volum 3 Survalent ADMS Software Maintenance for details.* *All software upgrades can be self performed and as stated in the Volume 3, Survalent does not charge for software upgrades as log as the customer has an active support plan..* *For the 5 year Post Installation Service contracts estimation purposes, Survalent has included annual increase of 6%. Survalent Support Plan fees are subjection to change in the future based on inflationary or CPI Index.* *Multiple year contracts could offer advantageous program subscription pricing.* ***Note: Added PDS support price ($4,117- support for Year 1) to the Phase 1 support prices***	$ 29,639.00	$ 16,523.00	$ 46,162.00
D.2	Technical Support and Software Upgrade Year 2 - Platinum		$ 31,417.34	$ 17,514.38	$ 48,931.72
D.3	Technical Support and Software Upgrade Year 3 - Platinum		$ 33,302.38	$ 18,565.24	$ 51,867.62
D.4	Technical Support and Software Upgrade Year 4 - Platinum		$ 35,300.52	$ 19,679.16	$ 54,979.68
D.5	Technical Support and Software Upgrade Year 5 - Platinum		$ 37,418.55	$ 20,859.91	$ 58,278.46
				Post Installation Service SCADA Contract Costs	**$ 260,219.49**

Note 1: The Post Installation Service Contracts includes support for existing and base licenses only and does not include support on optional licenses.

Note 2: The onsite/remote services price is for the services performed in 2024. Rates may increase based on the Consumer Price Index (CPI) for services performed in 2025 onwards.

Appendix B Attachment B Vendor Information Questionnaire and Assurances

[THIS PAGE INTENTIONALLY LEFT BLANK]

ATTACHMENT B

VENDOR INFORMATION QUESTIONNAIRE AND ASSURANCES

Name of Company:	SURVALENT TECHNOLOGY Inc.
Primary Office Address (City/State/Zip):	7965 HERITAGE ROAD, BRAMPTON, ONTARIO, L6Y5X5
Telephone Number:	905-826-5000
Email Address:	sames@survalent.com
DUNS Number (if applicable):	
Company has been in business since:	1999

Form of Ownership (check one):

☒ State Incorporated/Registered Delaware / Date Incorporated/Registered Jan 04, 2016

☐ LLC

☐ Joint Venture

☐ Partnership: If Partnership, select one: ☐ Limited or ☐ General

☐ Individual

List of Partners, Principals, Corporate Officers or Owners:

Name	Title
Steve Mueller	President/Director

List of Corporate Directors:

Name	Title
Steve Mueller	President/Director

1. Have you had any contracts terminated for default or other performance reasons? ☐ Yes ☒ No If yes, explain:

2. Has your company been convicted of a criminal offense involving fraud, theft, bribery, kickbacks, or unlawful gifts to a public official? ☐ Yes ☒ No If yes, has the conviction occurred within three (3) years immediately preceding either the date of submission of a bid/proposal, or the date of award of the contract?
If yes, explain:

3. Is your company involved in pending investigation or criminal prosecution of a criminal offense involving fraud, theft, bribery, kickbacks, or unlawful gifts to a public official?
   ☐ Yes ☒ No If yes, explain:

4. Does your company have pending claims, investigations, or civil litigation involving allegations of fraud, misrepresentation, or conversion?
   ☐ Yes ☒ No If yes, explain:

5. Does your company have previous final judgments against the City for breach of contract, fraud misrepresentation or conversion?
   ☐ Yes ☒ No If yes, explain:

6. Has your company failed to timely pay/remit sales tax, property tax, or utility payments to the City of San Marcos?
   ☐ Yes ☒ No If yes, explain:

7. Has your company refused to execute a contract following an award by the San Marcos City Council?
   ☐ Yes ☒ No If yes, explain:

8. Has your company violated the anti-lobbying provisions in a current or previous City of San Marcos procurement process by contacting a member of the San Marcos City Council prior to the award of a contract?
   ☐ Yes ☒ No If yes, explain:

9. Has your company furnished unauthorized substitutions of materials not meeting contract specifications in a current or previous contract with the City of San Marcos?
   ☐ Yes ☒ No If yes, explain:

10. Non-Collusion Certification: By signing below as an authorized signer, the Bidder certifies that ALL items below are true and correct concerning its bid.

    1) You are fully informed of the contents of the bid and the circumstances of its preparation.
    2) Your bid is genuine and is not a collusive or sham bid.
    3) Neither you nor anyone else acting on behalf of your company has agreed, colluded, or conspired in any manner with any other bidder, firm, or person to submit a collusive or sham bid, or to refrain from bidding, or sought by communication or conference with any other bidder, firm, or person to fix the prices, overhead, profit, or any cost element in your bid or in any other bid, or to secure through any collusion, conspiracy, or agreement any advantage against the City of San Marcos or any other bidder.
    4) The prices quoted in your bid are fair and proper and are not affected by any collusion, conspiracy, connivance, or unlawful agreement on the part of your company or anyone acting on its behalf.

11. Prohibition on contracts with companies that boycott Israel. Chapter 2271 and 808, Texas Government Code restricts the City from contracting with companies that boycott Israel. By signing below and submission of the HB89 Verification form, the Bidder certifies that it is does not boycott Israel and will not during the term of this contract. Failure to maintain the requirements under this provision will be considered a material breach. *(HB89 Verification form required if contract value is greater than $100,000.)*

12. Prohibition on contracts with companies that do business with Iran, Sudan, or a foreign terrorist organization. Section 2252 of the Texas Government Code restricts the City from contracting with companies that do business with Iran, Sudan, or a foreign terrorist organization. By signing below as an authorized signer, the Bidder certifies that it does not do business with Iran, Sudan, or a foreign terrorist organization. Failure to maintain the requirements under this provision will be considered a material breach.

13. Prohibition on contracts with certain foreign-owned companies. Section 2274 of the Texas Government Code (SB2116) restricts the City from contracting with companies that do business with certain foreign-owned companies in connection with critical infrastructure if the company is granted direct or remote access; and if the company is owned by citizens of or is directly controlled by the government of China, Iran, North Korea, Russia, or a "designated country", or headquartered in China, Iran, North Korea, Russia, or a designated country. Designated country is Governor-designated country as a threat to critical infrastructure. By signing below as an authorized signer, the Bidder hereby certifies that it does not do business with certain foreign-owned companies in connection with critical infrastructure as described herein. Failure to maintain the requirements under this provision will be considered a material breach.

14. Prohibition on contracts with companies that discriminate against firearm and ammunition industries. Section 2274 of the Texas Government Code (SB19) restricts the City from contracting with companies that discriminate against firearm and ammunition industries. By signing below as an authorized signer, the Bidder certifies that it does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association; and will not discriminate against the same during the term of this contract. *(Only applies to companies with 10 or more full-time employees and for a contract value greater than $100,000.)* Failure to maintain the requirements under this provision will be considered a material breach.

15. Prohibition on contracts with companies boycotting Certain Energy Companies. Section 2274 of the Texas Government Code (SB13) restricts the City from contracting with companies that boycott energy companies. By signing below as an authorized signer, the Bidder certifies that it does not have a practice, policy, guidance, or directive boycotting energy companies, and will not discriminate against the same during the term of this contract. *(Only applies to companies with 10 or more full-time employees and for a contract value greater than $100,000.)* Failure to maintain the requirements under this provision will be considered a material breach.

16. I hereby certify that our business is an Equal Employment Opportunity (EEO) employer and does not and will not discriminate in employment and in subcontracts based on race, color, sexual orientation, gender identity, national origin, sex, age, disability or economic condition. I further attest that this policy is documented in our Employee Handbook. As an EEO employer, we prohibit retaliation, discharge, or discrimination against any employee or applicant for employment or against any subcontractor or supplier.

I, Rup Dhami, as Chief Operating Officer

Name of Individual — Title & Authority

of Survalent Technology Inc., declare under oath

Company Name

that the above Statements, including any supplemental responses attached hereto, are true and correct, and that the representations made herein are accurate to the best of my knowledge and are based upon a diligent search of records. I further acknowledge that any failure to conduct a diligent search or to make a full and complete disclosure may result in cancellation of my contract by the City of San Marcos, and possibly debarment.

Signature

SURVALENT TECHNOLOGY CORPORATION

[THIS PAGE INTENTIONALLY LEFT BLANK]

Appendix C Attachment D – House Bill 89 Verification

[THIS PAGE INTENTIONALLY LEFT BLANK]

ATTACHMENT "D"
HOUSE BILL 89 VERIFICATION
(This affidavit must be completed and submitted with bid/proposal.)

Pursuant to Sections 2271.001, 2271.002, 808.001, Texas Government Code:

1. *"Boycott Israel" means refusing to deal with, terminating business activities with, or otherwise taking any action that is intended to penalize, inflict economic harm on, or limit commercial relations specifically with Israel, or with a person or entity doing business in Israel or in an Israeli-controlled territory, but does not include an action made for ordinary business purposes; and*

2. *"Company" has the meaning assigned by Section 808.001, except that the term does not include a sole proprietorship.*

3. *Section only applies to a contract that is between a governmental entity and a company with 10 or more full-time employees; and has a value of $100,000 or more that is to be paid wholly or partly from public funds of the governmental entity.*

As the undersigned legal representative of Sunvalent technology, (Business Name)
after being duly sworn by the undersigned notary, do hereby depose and verify under oath that the company named-above, under the provisions of Subtitle F, Title 10, Government Code Chapter 2271:

a. **Does not boycott Israel currently; and**
b. **Will not boycott Israel during the term of the contract City of San Marcos, Texas.**

(Business Representative Signature)

October 10, 2023
(Date)

Chief Operating Officer
(Title)

STATE OF Ontario §
COUNTY OF Peel. §

On this day, BEFORE ME, Rajendei Dhami personally appeared and personally-known to me or proved to me on the basis of satisfactory evidence to be the individual whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her capacity, and that by his/her signature on the instrument, the individual executed the instrument for purposes and consideration therein expressed.

GIVEN UNDER MY HAND AND SEAL OF OFFICE this 10 day of October, 2023

AJAY PAL SINGH DUGGAL NOTARY PUBLIC ONTARIO

.2022

Ajay Duggal
Barrister and Solicitor
AD Lawyers
201 County Court Blvd., Suite ~~300~~ 304
Brampton, ON L6W 4L2
P: 905.451.0099 F: 905.451.5526

NOTARY PUBLIC in and for the State of Ontario, Canada.

Attestation/Witness Only
No Legal Advice Sought or Provided

[THIS PAGE INTENTIONALLY LEFT BLANK]

Appendix D Customer Testimonials

[THIS PAGE INTENTIONALLY LEFT BLANK]

February 3rd, 2023

To: Ayat Rezaeifar, PMP
Survalent Technologies
7965 Heritage Road
Brampton, ON
Canada, L6Y 5X5

Mr. Rezaeifar,

This letter serves as a formal notice for the successful completion of the SCADA Replacement Project between The City of Fountain and Survalent Technologies as of February 2nd, 2023. All work has been satisfactorily completed on time, on budget, and in accordance with the agreed upon terms. All invoices have been submitted and paid in full.

As the project manager and a representative for The City of Fountain Utilities Department, I would like to extend my sincere thanks to Survalent Technologies for your exemplary work. Your commitment to the success of this project is greatly appreciated. I look forward to working with you on any related projects that may present themselves in the future.

Best Regards,

Eric Reinhardt
SCADA Project Manager
Journeyman Lineman/Foreman
City of Fountain
Office (719)393-4947
Cell (719) 440-9519

City Treasurer, City of Weimar: "Gail did an excellent job of training us. There were several IT issues on our side. Gail was very patient and worked with us. She is very knowledgeable and can teach the SCADA system in a way that is easy for us to understand. Gail would have loved to show us a million other things, but she showed us everything we need to operate the system and get the data we need. Thank you very much."

Manager of Power Generation, Kodiak Electric: "We couldn't be happier with the onsite training provided by Gail with Survalent. The session went so we'll we're planning to add the onsite check-up/training session to our annual budget."

Substation Technician, Washington State Power: "We really love Survalent. We're looking forward to using some of your innovative technology to improve our system."

Director of Engineering and Operations, Sussex Rural Electric Cooperative: "We are pleased with the project and the product you delivered. I was especially impressed with Zoran's work. His commitment, patience, and thoroughness was exceptional."

Chief Operating Officer, Peninsula Light Co.: "We had literally our entire distribution system de-energized due to a storm this weekend for over 2.5 hours. Transmission took it out. The Survalent never missed a beat. It has been awesome throughout what is turning out to be the largest storm in recent memory!! Dispatch cannot wait to try out the OMS after the differences we saw in performance between Survalent and the current OMS."

Distribution Engineer, Umatilla Electric Cooperative: "I would like to add that Kosta has done a great job so far. Everyone here at UEC has been very impressed with his hard work ethic, calm demeanour, and willingness to help whenever a question arises. During his two week tenure at UEC for system commission/optimization he was never late and showed up eager to work on the project. We could not be more pleased to have him on this project. That also goes for everyone at Survalent, including yourself. Every time we have had any questions or concerns there has been a timely response. Thank you and everyone at Survalent for everything thus far."

Appendix E Resumes

[THIS PAGE INTENTIONALLY LEFT BLANK]

Ian MacCuaig, PMP, CISSP

Tel: 905.285.9497

Fax:905.826.7144

imaccuaig@survalent.com

RESPONSIBILITIES AT SURVALENT:

Ian is Executive Vice President of Customer Success and Solutions at Survalent Technology and is responsible for proposal management, inside sales, project management, system engineering, and customer services. With over 30 years of experience with real-time control systems, Ian has a broad range of experience in management consulting, project management, business analysis, engineering management, and software development within the energy sector. Ian has a succinct knowledge of grid operations, information technology, smart grid technologies, distributed energy resources, system integration and NERC CIP security standards.

WORK EXPERIENCE:

During his career, Ian has held key leadership roles in proposals, project delivery, product management, and customer services for energy control systems including SCADA, Generation Management Systems (GMS), Energy Management Systems (EMS), Distribution Management (DMS), and Outage Management Systems (OMS). His career progressed within the Energy Control Systems division of GE Digital Energy where he acquired broad knowledge of operational technologies and information technologies. Ian has a successful track record managing large, complex projects and has worked with some of the largest electric utilities in North America and internationally including Hydro-Quebec, ENERGEX, Powerlink Queensland, AVANGRID, National Grid, Pacific Gas and Electric, and Taiwan Power to name a few.

EDUCATION:

Bachelor of Computer Science, Honors Program
Concordia University, Montreal, Quebec, Canada

Comprehensive Project Management
McGill University, Montreal, Quebec, Canada

REGISTRATION/LICENSES:

PMP Certification
CISSP Certification

Gustavo Maragno , PMP

Tel:905.285.2258

Mobile: 437-929-8974

gmaragno@survalent.com

EDUCATION:

MBA Executive International in Project Management

B.SC in Mechatronic, Robotics and Automation Engineering

RESPONSIBILITIES AT SURVALENT:

Gustavo joined Survalent Technology in 2018 as a Senior Project Manager in the Project Delivery department. As a Senior Project Manager, he was responsible for managing all aspects of Advanced Distributed Management System (ADMS) projects, from the contract award to the final handover to the customer.

In 2021, he was promoted to Manager, Project Manager Office (PMO). As a Manager of the PMO, he was responsible for establishing and managing the Project Management Office, which is responsible for standardizing project management practices, ensuring alignment with organizational goals, and improving overall project performance and efficiency.

In 2023, he was promoted to Director of Projects. As a Director of Project, he is responsible for overseeing and directing the execution of various projects to achieve strategic objectives. Also, responsible for high-level management role that focuses on the planning, execution, and successful completion of projects within the organization, directing and managing not only the Project Delivery Department but also the Project Management Office (PMO).

WORK EXPERIENCE:

He has over 25 years of experience directing, managing, coordinating, and executing automation engineer projects in the public and private sectors of the energy industry such as Utilities, Power Plants, Substations, Transformers, Co-Generation, and so on. He also has good experience in the industrial automation industry sector (Chemical, Automotive, and Pharmacy).

He has a solid background in developing and managing control and supervisor systems such as ADMS, SCADA, OMS, DMS, PLC, HMI, SDCD, and so on.

REGISTRATION/LICENSES/CERTIFICATIONS:

Project Management Professional (PMP), #1988832

Joe De Filippis

Tel: 905.285.2235

Fax: 905.826.7144

joed@survalent.com

EDUCATION

Diploma, Electronics Technologist

Humber College, Toronto, Ontario, Canada

RESPONSIBILITIES AT SURVALENT

Joe is the Manager of the Project Delivery and Inside Sales team which includes the project leaders, engineers, and system specialists who are responsible for the design and implementation of SCADA Master Stations, RTUs, and controllers for projects globally. He also oversees the implementation of advanced applications such as the outage management system (OMS) and distribution management system (DMS).

Joe is involved from the project proposal stage to implementation. Once the project is awarded, he works closely with his team to ensure the project runs on time and on budget, and that our customers' expectations and contractual obligations are met. He coordinates with Survalent's development, finance, and product teams, and with the customer for system deployments, ensuring the customer is satisfied with the process and setup.

WORK EXPERIENCE

Joe joined Survalent over 20 years ago and has successfully deployed over 600 SCADA systems worldwide. He has considerable knowledge of all Survalent customers, their systems and Survalent software and applications.

Joe's career began in the telecommunications industry as a Test Technician at TAI. He then moved to the energy industry as an Engineering Technologist at Endacom 2000, where he design and tested power meters from prototype to production.

Carolina Faria, PMP

Tel: 289.401.4002

Fax: 905.826.7144

cfaria@survalent.com

RESPONSIBILITIES AT SURVALENT:

Carolina joined Survalent Technology in 2021 as a Project Manager in the Project Delivery team. Along with her engineering degree, she is also a Project Management Professional certified (PMP). Carolina is responsible for managing all aspects of Advanced Distributed Management System (ADMS) projects from contract award through commissioning of the system to its final handover to the client. As the main point of contact for customers, she is ultimately accountable for the successful completion of projects, ensuring that the final system is developed in accordance with the agreed upon timeline, budget, and specifications. She is responsible for planning, implementing, monitoring, and controlling the project's progress. In close collaboration with customers, she develops the necessary project plans and provides timely progress updates, clarifications, and various project reports, such as schedule updates, financial updates, change orders, risk analysis, lessons learned, and punch list tracking logs.

WORK EXPERIENCE:

Carolina has 15 years of experience in the technology solutions and automation industries. As an Engineer, she managed electrical field monitoring equipment, developed business requirements, and performed functionality testing. Additionally, she has experience as a Project Manager, managing a software system for tracking activities for switches, transformers, RTUs, and substations.

REGISTRATION/LICENSES:

Project Management Professional (PMP), #1985747

MBA Business Management with emphasis on Projects

Bachelor’s degree in engineering major in Electronic and Telecommunication

Daniel Nechay, M.Eng.

T: 905.285.2266

F: 905.826.7144

dnechay@survalent.com

EDUCATION

Master of Engineering, Computer Engineering
McGill University, Montreal, Quebec, Canada

Bachelor of Engineering, Computer Engineering
McGill University, Montreal, Quebec, Canada

RESPONSIBILITIES AT SURVALENT

Daniel is a Product Manager at Survalent and is responsible for the OMS and DMS portfolios, and the cyber-security approach for Survalent's advanced distribution management system (ADMS). His work with customers include conducting product demonstrations and training sessions, hosting workshops to demonstrate new features, and requirements gathering from customers for future product enhancements.

Based on market research and customer feedback, Daniel provides recommendations to the development team for new products, and enhancements to existing products that would benefit customers. He collaborates with partner companies to determine how their solutions can be integrated into Survalent's ADMS to provide more value to utilities.

WORK EXPERIENCE

Prior to joining Survalent, Daniel was a Field Application Engineering Manager at Corinex Communications responsible for the support of broadband over powerline projects for AMI and medium voltage communications. In this role, he was involved in all aspects of the project from the pre-sales, deployment and the post-deployment support stages. At OmniGlobe Networks, Daniel was a System/Network Engineer and aided in the development, deployment and maintenance of satellite and broadband internet and cellular networks to provide access to remote and rural areas across Canada.

Jason Yang

Tel: 905.285.9480

Fax: 905.826.7144

jyang@survalent.com

EDUCATION

Master, China University of Geosciences

Master, McMaster University

RESPONSIBILITIES AT SURVALENT

Jason is the team lead managing design and development of GIS/CIS integration software, which is capable of modelling and QA\QC utility data for SCADA, OMS and DMS projects. He has an excellent understanding of GIS principles and hands-on experience of ArcGIS for Desktop, ArcGIS for Server, ArcSDE, Portal for ArcGIS and ArcGIS Online. He also has web development experience in ASP.net (MVC), JavaScript, HTML, XML, IIS, restful web service and ArcGIS for Server.

Jason also provides online or site training and troubleshooting services. He also provides support for user documentation.

WORK EXPERIENCE

Jason joined Survalent in 2013. Before Survalent he was working as software developer at Region of Peel, Ontario and worked on Multiple project development and maintenance.

TOOLS AND TECHNOLOGIES

Visual Studio, C#, C++, VB, Python, JavaScript, TypeScript

REGISTRATION/CERTIFICATIONS/LICENSES

Certified ScrumMaster

Miguel Ceniceros

Tel: 905.285.2241

Fax: 905.826.7144

miguelc@survalent.com

EDUCATION

Industrial Electronics Engineering Degre, Laguna Institute of Technology, Torreon, Mexico

RESPONSIBILITIES AT SURVALENT

Miguel is the Development Leader for the Distribution Management System (DMS) team, and is responsible for the planning, design, development, programming, and testing of the Power Flow, FLISR, Loss of Voltage (LOV), Volt Var Optimization (VVO), and Distribution Estate Estimator (DSE) applications.

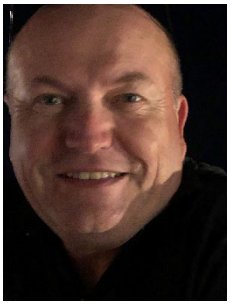
WORK EXPERIENCE

Miguel joined Survalent in 1999, as a senior developer in the software development group. Over his tenure, Miguel assumed positions of progressive responsibility. He is the primary designer and developer at Survalent for software that falls under the DMS scope. This line of software is considered advanced in the utility industry – its function is to analyze and optimize the network. His projects and scope of work include:

- DXF Converter for WorldView
- Adapted the System Configuration Station software to handle gas and water networks.
- Developed and programmed the Power Flow analysis solution.
- Multispeak interfaces for OMS and EA packages with Survalent's systems
- Developed the Fault Location, Isolation and Service Restoration (FLISR) and Loss of Voltage (LOV) applications.
- Designed the Volt-Var Optimization (VVO) and Distribution State Estimator for Survalent's Power Flow (DSE)
- Managed the DMS team to develop the following applications.
    - Restoration Study
    - Contingency Analysis
    - DMS Dashboard
    - Fault Location
    - Automatic Generation Control
    - Short-Term Load Forecast

Prior to joining Survalent, Miguel worked at SENSA where was responsible for the development of one of the first large scale FLISR systems for Comisión Federal de Electricidad (CFE) in Mexico. At CFE, he created the first HMI for CFE's distribution substations in Mexico City and developed an HMI for CFE's transmission substations.

From 1997 to 1998, he worked at Sistemas Electronicos de Potencia Automatización y Control (SEPAC) where he was in charge of R&D, successfully integrating SEPAC's SCADA with a third-party engineering analysis application. He also created several applications for interfacing and exploiting data from protection devices, as well as a predictive maintenance package for transmission transformers.



Rick Hayden

Tel: 905.285.2235

Fax: 905.826.7144

rickhayden@survalent.com

EDUCATION

Bachelor of Computer Science (Honors) 1984

University of Manitoba, Winnipeg, Manitoba, Canada

RESPONSIBILITIES AT SURVALENT

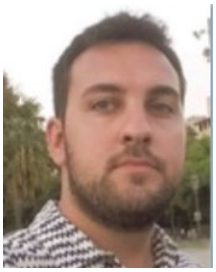
Rick is the Team Lead for the protocol and interfaces development team. He is responsible for the planning, design, development and testing of protocols to field equipment and interfaces to other systems.

WORK EXPERIENCE

Rick has over 39 years of experience in SCADA and the automation control industry. He has been involved in all areas of SCADA. He has developed drivers to PLC's, IED's and RTU's using industry standard protocols, including OPC, Modbus, DNP, ICCP/TASE.2, IEC61850, GOOSE, IEC60870-101 and IEC60870-104. He has also been involved with interfacing AMI, CIS, GIS and data historians.

TOOLS AND TECHNOLOGIES

Visual Studio, C++, C#



Kosta Ristovski

T: +389 2 3228 849

kosta@survalent.com

EDUCATION

Bachelor of Science, Electrical Engineering

Electro-technical Faculty, Ss. Cyril and Methodius University in Skopje, Macedonia

RESPONSIBILITIES AT SURVALENT

Kosta is a Senior System Engineer at Survalent and is responsible for the delivery of Advanced Distribution Management Systems (ADMS) projects, system testing and commissioning, user training, projects related documentation and remote assistance of different nature: customer preparation for commissioning, troubleshooting, assistance upon request.

Kosta specializes in database and GUI development, implementation and testing of communication protocols (DNP, Modbus, ICCP, OPC, IEC-61850, SNMP), GIS, FLISR integration, as well as WebSurv integration. Since joining Survalent, Kosta has been directly involved in more than 50 SCADA deployments globally.

WORK EXPERIENCE

Kosta joined Survalent in 2012 as System specialist and has experience with ADMS integration including the Database and graphics generation, system installation and commissioning, system administrator and operators training delivery.

TRAINING CERTIFICATES

Project Management (SEMOS Education, 2014); Administering a SQL Database Infrastructure (SEMOS Education, 2017); Administering the Web Server (IIS) Role of Windows (SEMOS Education, 2017); ICND1 and ICND2 (SEMOS Education, 2018)

Appendix F Pre-requisites for a Successful Service Implementation

1) Pre-requisites for GIS import

The customer is responsible for providing error free GIS file. Survalent will assist in the file cleanup and data conversion check (lack of information and ambiguous connections) followed by a report on detected errors. The customer is obliged to correct the GIS errors before an import can be conducted. The process can take multiple GIS file exchange iterations until completed.

2) Pre-requisites for FLISR implementation

Listed below is the mandatory data per equipment type that the customer needs to provide for successful implementation of FLISR:

a) Feeder main
- Rated phase amps (the maximum amount of current that the feeder can supply before triggering its protection).
- Recloser status
- Voltage, current and power factor (if connected KVA scaled by feeder injection load transfer option is used)

b) Telemetered devices (switches, breakers, tie switches)
- Current (A) and Voltage (kV) ratings of the device
- Status of the fault target indicators for the device used to determine the fault location
- Lockout point (pseudo or telemetered) for the devices that can trigger FLISR event.
- Lockout timer for the devices that can trigger FLISR event but don't have telemetered lockout point.
- Voltage, current (A) and power factor for the devices that can trigger FLISR event and the connected KVA scaled by feeder injection load transfer option is used.

c) Conductor
- Transformer KVA (the sum of all connected KVA transformer ratings connected to the conductor). For connectivity import, the transformers KVAs are read from the GIS and assigned to the conductor with Survalent KVA aggregation utility. For manually drawn schematics, the KVAs must be manually assigned to each conductor as part of the FLISR implementation service.

d) Substation transformer
- Nominal voltage of the low and high side of the substation transformer

There may be additional data that will be required which would be discussed during the project integration.

[THIS PAGE INTENTIONALLY LEFT BLANK]

Appendix G Response to Addendum VIII

SCADA Doc Section No.	Description Section Number	Meets Guidelines	Don't Meet Guidelines	Complete Explanation if Response does not meet Guidelines and Alternate Solution
II.	System Architecture	✓		
III.A & B	SCADA Server Functional Req.	✓		N/A Survalent is current SCADA vendor. It is assumed that existing SurvalentONE SCADA licenses are installed, implemented and running.
III.C	Configuration	✓		
III.D	Communications	✓		Survalent SCADA supports all protocols listed except: Allen Bradley, ASW
III.E	Security	✓		The system has been strategically designed to offer a robust level of cybersecurity, taking into account an evaluation of the typical types and levels of cyber risks that the system is likely to encounter. Our secure environment for the Survalent ADMS system aligns with the relevant requirements outlined in the NERC Cyber Security standard and adheres to the guidelines in NISTIR 7628. Most of the cybersecurity requirements from NERC CIP version 5 are already integrated into our standard Support Plant Tiers. However, certain requirements specific to NERC CIP-13 may incur an additional premium cost. It's important to note that NERC CIP-13 services are typically of interest only to Transmission Utilities that must fully comply with NERC regulations. For more detailed information, please refer to Appendix H of this document, which provides a summary of NERC CIP requirements. If San Marcos requires compliance with these additional services

SCADA Doc Section No.	Description Section Number	Meets Guidelines	Don't Meet Guidelines	Complete Explanation if Response does not meet Guidelines and Alternate Solution
				related to NERC CIP-13, we can provide details on the associated premium pricing upon request.
III.F	System Sizing	✓		Included as part of existing SurvalentONE SCADA software
III.G	Hardware Platform	✓		Noted. It is understood all the hardware will be provided and installed by San Marcos.
III.H	Host Server	✓		Please refer to Section 4.3.7 for VM environment details
III.I	Workstation Consoles	✓		Please refer to Section 4.3.7 for recommended specifications.
IV.A	Data Acquisition	✓		Included as part of existing SurvalentONE SCADA software
IV.B	Supervisor Control	✓		Included as part of existing SurvalentONE SCADA software
IV.C	Communications	✓		Included as part of existing SurvalentONE SCADA software
IV.D	Data Processing	✓		Included as part of existing SurvalentONE SCADA software
IV.E	Authentication & Access Control	✓		Included as part of existing SurvalentONE SCADA software
IV.F	User Rights	✓		Included as part of existing SurvalentONE SCADA software
IV.G	Area of Responsibility	✓		Included as part of existing SurvalentONE SCADA software
IV.H	Tag Management	✓		Included as part of existing SurvalentONE SCADA software
IV.I	Database Editor	✓		Included as part of existing SurvalentONE SCADA software
IV.J	Alarms	✓		Included as part of existing SurvalentONE SCADA software
IV.K	Reports	✓		Included as part of existing SurvalentONE SCADA software
IV.L	Data Collection & Storage	✓		Included as part of existing SurvalentONE SCADA software
IV.M	Data Testing	✓		Included as part of existing SurvalentONE SCADA software
V.A	Graphical User Functional Req.	✓		Included as part of existing SurvalentONE SCADA software

SCADA Doc Section No.	Description Section Number	Meets Guidelines	Don't Meet Guidelines	Complete Explanation if Response does not meet Guidelines and Alternate Solution
V.B	Drawing Tools	✓		Included as part of existing SCADA software
VI.A	SCADA System Application	✓		Included as part of Phase 1: Additional SCADA applications
VI.B	Command Sequence	✓		Included as part of existing SurvalentONE SCADA software
VI.C	Control Panel Templates	✓		Included as part of existing SurvalentONE SCADA software
VI.D	Disturbance Capture	✓		Included as part of existing SurvalentONE SCADA software
VI.E	Event Data Recording	✓		Included as part of existing SurvalentONE SCADA software
VI.F	External Alarm Bell	✓		SurvalentONE SCADA supports this functionality. However, the license is not included in the price. Survalent will provide the license price of this function upon request.
VI.G	External Clock Interface	✓		SurvalentONE SCADA supports this functionality. However, the license is not included in the price. Survalent will provide the license price of this function upon request.
VI.H	Fault Data Recorder	✓		SurvalentONE SCADA supports this functionality. However, the license is not included in the price. Survalent will provide the license price of this function upon request.
VI.I	IED Wizard Templates	✓		Included as part of existing SurvalentONE SCADA software
VI.J	Inter Control Center Protocol	✓		SurvalentONE SCADA supports this functionality. However, the license is not included in the price. Survalent will provide the license price of this protocol upon request.
VI.K	Virtual RTU	✓		Survalent supports all the listed Virtual RTU applications and will provide the price for particular function upon request.
VI.L	Interface To Microsoft Excel & Access	✓		SurvalentONE SCADA Add-in is part of existing SurvalentONE SCADA software

SCADA Doc Section No.	Description Section Number	Meets Guidelines	Don't Meet Guidelines	Complete Explanation if Response does not meet Guidelines and Alternate Solution
VI.M	Primary/Secondary Alarm Suppression	✓		Included as part of existing SurvalentONE SCADA software
VI. N	MultiSpeak	✓		Please refer to Volume 2 Standard Product Overview Appendix B Supported MultiSpeak Interfaces
VI.O	MultiSpeak Network Model Import	✓		
VI.P	MultiSpeak Dynamic GIS Viewer	✓		SurvalentONE SCADA supports this interface. However, the license is not included in the price. Survalent will provide the license price of this interface upon request.
VI.Q	MultiSpeak Engineering Analysis	✓		Included as part of existing SurvalentONE SCADA software
VI.R	MultiSpeak Load Management	✓		SurvalentONE SCADA supports this interface. However, the license is not included in the price. Survalent will provide the license price of this interface upon request.
VI.S	MultiSpeak Outage Analysis	✓		Included in Phase 1
VI.T	Network Database Access API	✓		SurvalentONE SCADA supports this interface. However, the license is not included in the price. Survalent will provide the license price of this interface upon request.
VI.U	Network Topology Processor	✓		Included in Phase 1
VI.V	OPC Client/Server	✓		Included in Phase 1
VI.W	Operations and Outage Accounting	✓		Included as part of existing SurvalentONE SCADA software
VI.X	Remote Alarm Annunciation	✓		Included as part of existing SurvalentONE SCADA software
VI.Y	SCADA Replicator	✓		Included as part of existing SurvalentONE SCADA software
VI.Z	Simple Network Management Protocol	✓		Included in Phase 1

SCADA Doc Section No.	Description Section Number	Meets Guidelines	Don't Meet Guidelines	Complete Explanation if Response does not meet Guidelines and Alternate Solution
VI.AA	Switch Order Preparation	✓		Included in Phase 1
VI.BB	Browser	✓		
VI.CC	Support Servers	✓		QAS: This license is included as a free trial environment license as part of San Marcos's current Platinum support plan. OTS and Data Forwarding: SurvalentONE SCADA supports all these licenses server applications and can be purchased at additional costs if the application is required by San Marcos in future.
VI.DD	Project Development Sys	✓		SurvalenONE SCADA supports this licenses server application and is included in base offer. Please refer to Appendix A - Attachment C SCADA RFP Cost Proposal for details
VI.EE	Distributes Energy Resources	✓		Survalent understands that DERMS is part of future requirement. Although Survalent complies to most of the points as current functionality or part of future DERMS roadmap, further discussion with San Marcos is required understand the essential requirements. The DERs/DERMS solution is not included in the price.
VII.A	GUI Interface Design	✓		Survalent SmartVU application does not support the real-time weather radar with a 50-mile radius view. However, SurvalentONE Short Term Load Forecasting produces either 24-hour or 7-day load forecasts based on forecasted weather and historical load and weather data or a 24-hour forecast based on the weighted average of the load from the past several weeks. Short Term Load Forecasting license can be purchased at additional cost if the application is required by San Marcos in future.

SCADA Doc Section No.	Description Section Number	Meets Guidelines	Don't Meet Guidelines	Complete Explanation if Response does not meet Guidelines and Alternate Solution
VII.B	Sand Box Tracking Period	✓		San Marcos owns the SurvalentONE QA/Test environment Licenses as a free trial environment license as part of San Marcos's current Platinum support plan.
VII.C	Onsite Services	✓		Alternate: Since the San Marcos has SurvalentONE SCADA system successfully installed and operational, Survalent has made recommendations and incorporated the necessary onsite services for additional SCADA applications and DMS applications.
VII.D	Payment Schedule		✓	Alternate: Since the given payment schedule is tailored towards new SCADA system, it is not applicable to Survalent since San Marcos has existing SurvalentONE SCADA. Survalent has suggested the payment schedule in Section 10.2 of this volume.

Appendix H Summary of NERC CIP requirements

NERC CIP-002 BES Cyber Security Identification and Categorization

To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to mis-operation or instability in the BES.

How Survalent Can Help

1) [NERC CIP-002] [*Optional*] During the deployment phase, Survalent can provide a document that identifies the ADMS physical assets including servers, workstations, and networking equipment provided by Survalent as well as a system architecture diagram. The document will also list the relevant information for each physical asset including hostname, network interfaces, IP addresses, operating system version, Survalent software version, etc. We can also provide services to help classify each asset as high, medium, or low impact depending on the system architecture.

NERC CIP-004 Personnel & Training

To minimize the risk against compromise that could lead to mis-operation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.

How Survalent Can Help

1) [NERC CIP-004] [*Base*] Survalent maintains a rigorous process to evaluate the trustworthiness and suitability of all personnel within the company and those providing services to utilities. This process includes thorough background checks to ensure that employees who have access to sensitive information are trustworthy and do not pose a security risk. Background checks may include criminal history checks, credit checks, and verification of previous employment and education. In addition, all our personnel undergo regular cybersecurity awareness training to proactively mitigate the risks of malicious activities and threats.
2) [NERC CIP-004] [*Optional*] During the deployment phase, Survalent can provide training with an emphasis on cybersecurity concepts, potential threats, cybersecurity awareness, SurvalentONE authentication, integration with Active Directory and LDAP, user rights and privileges, granting or revoking permissions, password configuration and enforcements, file-sharing and permissions, remote access, DMZ applications, security event logging and Windows event logging. By conducting this training, utilities can effectively underscore the importance of fostering a culture of cybersecurity awareness throughout the organization and the significance of maintaining a secure environment within the electric power industry.
3) [NERC CIP-004] [*Optional*] Survalent can provide user training specifically designed to enable utility personnel to effectively carry out their roles and responsibilities using the SurvalentONE ADMS product. These courses are meticulously designed to ensure that individuals involved in ADMS activities possess the essential knowledge and skills needed to successfully use the SurvalentONE ADMS.

NERC CIP-005 Electronic Security Perimeter

To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

How Survalent Can Help

1) [NERC CIP-005] The Survalent ADMS product has been designed with a strong focus on cybersecurity, incorporating industry-standard practices to ensure compliance with NERC CIP requirements. The software architecture aligns with the principles of the Purdue model, which provides a framework for segmenting industrial control system networks from corporate enterprise networks and the internet. The model is used as a baseline architecture for all industrial control system frameworks such as API 1164 and NIST 800. When designing the ADMS system architecture, it is important to evaluate the links external users, devices, or control systems to ensure communications are secure.
2) [NERC CIP-005] Survalent supports secure-by-design telemetry protocols such as Secure DNP3 and Secure ICCP, as well as secure connections to our web applications in the DMZ. By utilizing secure communications to external devices and users, customers can demonstrate compliance with NERC CIP-005 standards and enhance the overall electronic security of their ADMS. Implementing secure communications aligns with the NERC CIP requirements by providing the necessary measures to secure telemetry data, maintain data integrity, enforce authentication, and control access within the electronic security perimeter.
    a) **Data Confidentiality and Integrity:** Secure telemetry protocols offer protection against various network-based attacks, such as eavesdropping and man-in-the-middle attacks. By employing encryption, these protocols ensure that telemetry data and control commands are transmitted securely and cannot be intercepted or altered by unauthorized entities. This helps safeguard the integrity and confidentiality of data as it traverses the network infrastructure.
    b) **Authentication and Access Control:** Secure communications facilitate strong authentication mechanisms to verify the identities of remote users, devices and external control centers. This helps prevent unauthorized entities from accessing or manipulating critical infrastructure systems. By implementing robust access controls, only authorized devices and entities with proper authentication credentials can establish connections and exchange data, reducing the risk of unauthorized access or malicious activity.
3) [NERC CIP-005] [*Base*] All SurvalentONE Web Applications have SSL/TLS capability, enabling the establishment of a secure communication channel. By utilizing SSL/TLS, sensitive data is encrypted during transit, user credentials are protected through encryption, and defenses against man-in-the-middle (MITM) attacks are enhanced. This commitment to industry standards aligns with the principles of NERC CIP-005, bolstering the overall security posture of your organization. Implementing TLS helps safeguard against unauthorized access, data breaches, and network-based attacks, ensuring the protection of valuable information.
4) [NERC CIP-005] [*Base*] The SurvalentONE system architecture uses fewer servers than other vendor solutions, which reduces the overall attack surface area. With fewer individual software components and interfaces, there are fewer potential entry points for malicious actors to exploit and makes it easier to upgrade and patch. This consolidation minimizes the number of potential vulnerabilities, making it easier for utilities to secure and monitor effectively.
5) [NERC CIP-005] [*Base]* As part of the deployment, Survalent provides the list of firewall ports used by every SurvalentONE application.

6) [NERC CIP-005] [*Optional]* As part of the deployment, Survalent can provide a system architecture design document describing the data flows between the environments (Production, DMZ, etc.)
7) [NERC CIP-005] [*Base*] Survalent maintains a Windows Hardening Manual that outlines the steps to improve the security posture of the servers and workstations by applying security configurations, such as applying latest operating system patches, disabling unnecessary services, enforcing strong password policies, enabling firewalls, and implementing secure remote access methods. When the hardware is provided by Survalent, our team will harden the equipment before we ship it to the utility, otherwise it can be performed by utility personnel or included in the Survalent scope of work (*optional*). Windows hardening can play a vital role in achieving compliance with NERC CIP-005.
8) [NERC CIP-005] [*Optional*] Windows hardening also involves installing and configuring anti-malware software. This helps protect against malware threats and aligns with the requirements of NERC CIP-005 R3 regarding malware protection. Our ADMS solution has been deployed with multiple antivirus and malware products including Microsoft Defender, Norton 360, Malwarebytes, and McAfee Total, among others and Survalent can provide the services to install and configure the anti-virus solution on the ADMS equipment.
9) [NERC CIP-005] [*Optional*] Windows hardening emphasizes the importance of regular patching and updates to address known vulnerabilities. Keeping Windows systems up-to-date with the latest security patches from Microsoft and Survalent helps meet the requirements of NERC CIP-005, which includes timely patch management as part of an overall security program. Survalent offers the flexibility to assist customers with installing patches and updates either remotely or on-site. Customers have the option to conduct the installation themselves while receiving support from Survalent, or they can choose to opt for turnkey patch management services provided by Survalent. The frequency of these patch management services can be tailored to the utility's preference, whether it's on a monthly, quarterly, or yearly basis, aligning with their existing practices. The services can be encompassed within the Support hours offered in the Gold and Platinum support tiers, or they can be provided through an augmentation services contract or quoted based on specific requirements as per the customer's request.
10) [NERC CIP-005] [*Optional*] Keeping the Survalent product software up-to-date with the latest major version helps meet the requirements of NERC CIP-005, which includes timely patch management as part of an overall security program. Survalent provides new software releases and patch releases to customers that purchase and maintain a Software Maintenance Plan. This service provides a valuable means of protecting the investment in SurvalentONE products. The releases are available for customers to download, test, and install at their convenience. Major advantages of this service include:
    a) Survalent strongly recommends that customers stay up-to-date with our product releases to take advantage of the latest functional and security updates, and to avoid difficulties implementing future product releases and patches. Additional support fees may be levied for products that Customers continue to use after the product end-of-life date.
    b) Our software has been designed to be easily upgraded, and most of our customers install the updates on their own. Our technical support team can be scheduled to provide remote assistance if needed, or the update can be coordinated with an annual on-site visit by one of our System Specialists.

    Please note the following:

- We test new versions of the product on the latest stable version of third-party software (i.e. the version must have been commercially available for at least 6 months), plus one version back. This includes Windows operating system, SQL Server database, etc.
- The versions we used for our product tests are identified in the release notes. Customers should carefully review this information before attempting to install and use a new version of the product.
- We will provide support for systems running older versions of third-party software provided the software is still supported by the original equipment manufacturer (OEM). If the OEM is no longer providing security patches for their software, we will not support it.
- Installing software upgrades in conjunction with major system upgrades involving replacement or upgrade of hardware, operating systems, or relational databases should not be attempted without Survalent on-site assistance. A separate quotation should be requested for assistance with major system upgrades by sending an email to sales@survalent.com.

11) [NERC CIP-005] [*Optional*] Survalent can provide remote or on-site assistance for ADMS penetration tests conducted by the customer or conduct an ADMS penetration test for the customer. Penetration test helps ensures that organizations regularly evaluate their ADMS architecture for potential vulnerabilities and take appropriate measures to address them. By conducting vulnerability tests at regular intervals, organizations can identify weaknesses, misconfigurations, or software vulnerabilities that could be exploited by unauthorized individuals. The services can be encompassed within the remote support hours offered in the Gold and Platinum support tiers, or they can be provided through an augmentation services contract or quoted based on specific requirements as per the customer's request.
12) [NERC CIP-005] [*Optional*] The SurvalentONE ADMS supports several offline environments that assist utilities in designing their deployment strategies. These environments, namely the Project Development Environment (PDS), Quality Assurance System (QAS), and Operator Training Environment (OTS), play a crucial role in facilitating comprehensive testing, validation, and training activities within controlled and segregated settings. By conducting these activities offline, we mitigate the potential risks associated with modifications, updates, or training exercises in the live production environment, thereby enhancing the dependability, security, and compliance of the operational systems.
    a) Project Development Environment (PDS): The PDS is a dedicated environment used for developing and testing database and graphic changes before deploying them in the production environment. By having a separate offline environment, utilities can perform thorough testing, validation, and quality assurance activities without impacting the live operational systems. This helps ensure that any changes or updates introduced to the production environment are stable, reliable, and aligned with the security requirements specified in NERC CIP-005.
    b) Quality Assurance System (QAS): The QAS serves as a controlled environment for conducting extensive testing and quality assurance processes on system updates, patches, and new software releases. It allows utilities to assess the functionality, performance, and security aspects of these updates before they are deployed in the live production environment. By thoroughly testing changes in the QAS, utilities can identify and address any vulnerabilities, compatibility issues, or unintended consequences that may impact the reliability or security of the operational systems. This ensures that only validated and secure updates are implemented, reducing the risk of disruptions or security incidents that could potentially violate NERC CIP-005 requirements.
    c) Operator Training Environment (OTS): The OTS is specifically designed to simulate real-world operating scenarios for training purposes. It provides utility operators with a safe and controlled

environment to practice their skills, learn new procedures, and familiarize themselves with the operational systems. By having an offline training environment, utilities can enhance their operators' capabilities without compromising the security or integrity of the live production systems. This ensures that operators are well-prepared, competent, and capable of responding effectively to various situations while adhering to the security practices mandated by NERC CIP-005.

NERC CIP-007 System Security Management

The main objective of NERC CIP-007 is to manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against any compromise that could lead to mis-operation or instability in the Bulk Electric System.

How Survalent Can Help

1) [NERC CIP-007] [*Base*] The SurvalentONE ADMS product offers strong user authentication capabilities through its system management tools. Users can authenticate using their ADMS user account and password, or they can leverage a corporate directory service like Microsoft Active Directory accessed via the LDAP protocol. Additionally, SurvalentONE supports a two-factor authentication scheme for an added layer of security. Every log-on and log-off activity is recorded as an event and securely stored in an audit trail, ensuring accountability and traceability to help comply with the NERC CIP-007.
   a) Integrating with Active Directory and LDAP allows utilities to enforce access controls based on user roles, groups, or organizational units defined in the directory services. This enables proper segregation of duties and restricts access to authorized individuals only. Additionally, implementing 2FA/MFA as part of the access control process enhances security by mitigating the risks associated with compromised passwords or credentials.
   b) Survalent software maintains detailed audit logs and ensures accountability for user access and actions. Integration with directory services and 2FA/MFA mechanisms can help capture and record user authentication events, access requests, and other relevant activities. These audit logs can be utilized to monitor access, detect suspicious behavior, investigate security incidents, and demonstrate compliance during audits. These align with the NERC CIP-007 compliance.
   c) The SurvalentONE ADMS incorporates robust user account password management tools, allowing for customizable configurations. Administrators can define various password policies, including password length, frequency of change, required complexity, number of login attempts, and automatic logout for inactive sessions. Additionally, we have implemented a secondary password feature that can be enabled as a prerequisite before sending controls to the field. Passwords are securely encrypted with 128-bit encryption and are neither stored nor transmitted in plaintext. The system allows for password length greater than twelve (12) characters and includes options for password complexity, such as the inclusion of alphanumeric and mixed-case characters. Administrators can set the frequency of password changes to 1, 30, 90, 180, or 365 days, enhancing security practices. Furthermore, the system enforces various security measures, such as preventing the username from being part of the password, requiring a specified number of upper and lower case characters, special characters, and disallowing the reuse of previous passwords. It also ensures that the password field does not contain repeated strings of identical characters.

d) The SurvalentONE ADMS product provides configurable settings for the number of allowed failed login attempts per account, as well as a blocked timeout period that prevents further login attempts after the threshold is exceeded. Additionally, the system supports an inactivity timeout feature, automatically logging out the user after a specified period of inactivity. Account activity logging can be customized to capture login successes and failures. The logging mechanisms are flexible and can be configured to use the remote Syslog protocol for seamless integration with existing logging infrastructure. Furthermore, the system generates and presents a comprehensive log list report, containing details such as the application used and the access time.

2) [NERC CIP-007] [*Base*] During the delivery of the services Survalent will disable or remove all default and guest accounts. Survalent will never store passwords electronically or in vendor-supplied hardcopy documentation in clear text unless the media is physically protected.
3) [NERC CIP-007] [*Optional*] During the deployment phase, Survalent can provide a document that identifies the users that have been configured on the ADMS, their user rights and privileges, which data zones/regions they have access to (areas of responsibility), and authentication policies.
4) [NERC CIP-007] [*Base*] The Survalent ADMS provides detailed logs of all log on/log off events and alerts when unauthorized access is detected. Additionally, the Survalent ADMS provides easy access to reports including all the events logged. These logs can be used to monitor access, detect suspicious behavior, investigate security incidents, and demonstrate compliance during audits.
5) [NERC CIP-007] [*Base*] The Survalent ADMS supports secure connections using SSL/TLS certificates for applications running in the DMZ including WebSurv, SurvCentral, ARA, OMS Web Dashboard, OMS Web Call Handler, and OMS Mobile Crew.
6) [NERC CIP-007] [*Base*] For remote access to SmartVU, the Survalent ADMS can be configured to use a secure jump server using Microsoft Web RDP that provides end-to-end encryption. Our architecture design emphasizes appropriate user access controls, including authentication mechanisms, authorization processes, and password management to prevent unauthorized access to critical systems and data.
7) [NERC CIP-007] [*Base*] Survalent personnel will strictly comply with the utility's procedures for accessing any cyber security assets, whether it involves remote connections or on-site visits. When visiting utility premises, Survalent will adhere to established protocols, which include presenting appropriate personal and company identification, stating the purpose of the visit, following safety procedures, prominently displaying visitor badges, and adhering to any instructions provided by the assigned local escort, among other requirements.
8) [NERC CIP-007] [*Base*] If the need to establish a remote connection arises, Survalent will adhere to the customer's remote access policies. If the customer has their own secure remote access methods in place to protect their cyber assets or specific resources from unauthorized access, Survalent will utilize those methods. In cases where the customer does not have a secure remote access solution, Survalent will use a secure application called GoToAssist. This application ensures the protection of session data through end-to-end encryption. All remote connections are encrypted and can only be accessed by authorized Survalent personnel. Screen-sharing data, keyboard/mouse control data, transferred files, remote diagnostic data, and text chat information are all encrypted. No unencrypted information is ever stored on the system.

NERC CIP-008 Incident Reporting and Response Plan

To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.

How Survalent Can Help

1) [NERC CIP-008] [*Optional*] Survalent can host a cyber security workshop to assist utility personnel in creating a Cyber Security Incident Reporting and Response Planning for the ADMS system. This involves identifying risks associated with the ADMS system architecture, providing recommendations to mitigate those risks, addressing any remaining risks, and offering additional guidance for a complete incident response plan. The incident response plan encompasses procedures, periodic tasks, documentation, and coordination plans to ensure an effective response to incidents.
2) [NERC CIP-008] [*Optional*] Survalent can provide assistance and guidance to utilities in the recovery phase after an incident affecting the SurvalentONE ADMS. This could involve offering recommendations on system restoration, data recovery, and implementing additional security measures to prevent future incidents.

NERC CIP-009 Recovery Plans for BES Cyber Systems

To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.

How Survalent Can Help

1) [NERC CIP-009] [*Base*] The Survalent ADMS provides software-based redundancy and disaster recovery solutions. Additionally, the Survalent ADMS can be integrated with many commercial data backup solutions.
2) [NERC CIP-009] [*Optional*] Survalent can assist the utility to design a comprehensive Recovery and Restoration Plan for the ADMS system that encompasses various strategies, including data backups, virtual machine snapshots, software-based redundancy, replication, and disaster recovery, or hypervisor-based high availability. This Recovery and Restoration Plan outlines the steps and procedures necessary for restoring ADMS functionality in case of an incident.
3) [NERC CIP-009] [*Base*] The SurvalentONE product incorporates robust logging capabilities that enable the identification of triggers or events that initiate the switchover between redundant applications or activate the disaster recovery assets. These logs serve as a valuable resource for understanding the cause and sequence of actions during the recovery process.
4) [NERC CIP-009] [*Base*] Survalent ensures compliance with NERC CIP-009-5 through the provision of an online data backup tool that offers flexible execution options. This tool allows users to initiate backups either on-demand or based on predefined schedules. It enables the dumping of online event data into offline files, which can then be securely stored on tape for backup purposes. In the event of a need for recovery, these offline files can be accessed and restored, allowing for seamless retrieval and reporting of the event data.
5) [NERC CIP-009] [*Base*] Survalent offers options up to quad (4) software-based redundancy for the ADMS servers in a hot-standby fashion; this redundancy can also be used to address disaster recovery strategies with seamless switching between the production system to the disaster recovery system. By implementing software-based redundancy, organizations can create redundant copies of data and systems, enabling swift recovery in the event of an incident or failure. These redundant backups act as a safeguard, allowing for the seamless restoration of data and ensuring minimal downtime.

Software-based redundancy also facilitates the creation of replicas, which are exact copies of the primary systems or data. These replicas can be utilized for testing, development, or disaster recovery purposes. By maintaining up-to-date replicas, organizations can quickly switch to these redundant systems in case of emergencies, preserving data integrity and availability.

6) [NERC CIP-009] [*Base*] In addition, software-based redundancy offers disaster recovery alternatives. These alternatives provide contingency plans that can be activated when primary systems or data become unavailable or compromised. By having predefined disaster recovery procedures in place, organizations can swiftly recover their operations and maintain the functionality of the ADMS, thus meeting the requirements of NERC CIP-009. Hypervisor-based disaster recovery further enhances the overall resilience of the system. It involves the replication of virtual machines and their associated data to a separate offsite location. In the event of a major incident or disaster at the primary site, these replicated resources can be quickly activated to restore services and ensure business continuity.
7) [NERC CIP-009] [*Optional*] When making a NERC CIP-009 backup and recovery strategy, customers need to test the process and procedures often without compromising the production system. Survalent offers the option to add a Quality Assurance System (QAS). With an offline QAS system, organizations can simulate various scenarios, such as system failures or data corruption, and execute backup and recovery procedures in a controlled manner. This enables comprehensive testing and validation of the effectiveness and reliability of the backup and recovery mechanisms.

   Furthermore, the offline QAS system provides an ideal environment for training personnel involved in backup and recovery activities. It allows them to familiarize themselves with the procedures, practice recovery operations, and refine their skills without any impact on the live production systems. This training and preparation contribute to better preparedness and efficiency in real-world backup and recovery scenarios.

   Additionally, the offline QAS system enables organizations to assess the integrity and completeness of backups, ensuring that all critical data and configurations are properly captured and stored. It allows for the verification of backup consistency and the ability to restore systems and data to their desired state in a controlled testing environment.

NERC CIP-010 Configuration, Change Management, and Vulnerability Assessment

To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to mis-operation or instability in the Bulk Electric System (BES).

How Survalent Can Help

1) [NERC CIP-010] Our approach includes the provision of several offline environments that assist utilities in designing their deployment strategies and meeting the requirements of NERC CIP-010. The Project Development Environment (PDS) and Quality Assurance System (QAS) play pivotal roles in ensuring compliance with NERC CIP-010 requirements for configuration, change management, and vulnerability assessment, for example:
   a) The PDS serves as a crucial tool for managing and documenting changes made to the database, graphics, and configurations of the ADMS server. It facilitates logging and auditing of these changes, providing a comprehensive record of modifications for accountability and traceability

purposes. By maintaining a clear audit trail, the PDS enables organizations to demonstrate compliance with configuration and change management requirements.

b) Moreover, the PDS offers the capability to test these changes in an offline environment before implementing them in the production system. This pre-production testing ensures that any potential issues or conflicts are identified and resolved before deploying changes to the live environment. It enables organizations to assess the impact of configuration and change modifications, validate their functionality, and mitigate risks associated with improper configurations or changes.

c) On the other hand, the QAS provides an entire offline environment dedicated to vulnerability assessments of both the operating system (OS) and the ADMS software. It allows organizations to conduct thorough testing and analysis of vulnerabilities without affecting the production environment. By simulating real-world attack scenarios, the QAS enables the identification and remediation of vulnerabilities before they can be exploited in the live system.

d) Additionally, the QAS facilitates the implementation of security patches, updates, and upgrades in a controlled and isolated environment. It allows organizations to test the compatibility and functionality of these changes before applying them to the production system. This helps ensure that the necessary security measures are implemented effectively while minimizing the risk of unintended consequences or disruptions to critical operations.

By leveraging the capabilities of the PDS and QAS, organizations can achieve a robust and compliant approach to configuration, change management, and vulnerability assessment as required by NERC CIP-010. These systems provide the necessary tools and environments for comprehensive testing, validation, and documentation, thereby enhancing the overall security and reliability of the ADMS infrastructure.

2) [NERC CIP-010] As stated in NERC CIP-007, as part of our release process all software distributed externally goes through a centralized and secure build environment owned and maintained by dedicated build staff. During the build process, all compiled files (DLLs, EXEs) and installation kits are automatically digitally signed. This ensures the integrity of the deployed software and guards against tampering. We use a code-signing certificate authority and renew certificates every three years.

NERC CIP-011 Information Protection

To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to mis-operation or instability in the Bulk Electric System (BES).

NERC CIP-012 Cyber Security Communications Between Control Centers

Ensure secure and reliable communication between control centers within the Bulk Electric System (BES). This standard focuses on establishing requirements for the protection of communication channels and protocols used for control system data exchange between control centers.

NERC CIP-012 aims to address the cyber security risks associated with communication networks and systems that support the operation and control of the electric grid. By implementing robust security measures, the objective is to prevent unauthorized access, data tampering, and disruption of control center communications.

How Survalent Can Help

1) [NERC CIP-012] [*Optional*] As outlined in NERC CIP-005, the SurvalentONE ADMS product supports secure-by-design telemetry protocols such as Secure DNP3 and Secure ICCP for secure and reliable communication between control centers. Implementing secure communications aligns with the NERC CIP requirements by providing the necessary measures to secure telemetry data, maintain data integrity, enforce authentication, and control access within the electronic security perimeter.
2) [NERC CIP-012] If Secure DNP3 or Secure ICCP are not supported by the remote control center, Survalent recommends configuring a virtual private network (VPN) between sites. Implementing a VPN establishes a secure tunnel that enables direct routing, authentication, and end-to-end encryption during the transmission of data between control centers. This ensures the confidentiality and integrity of the data. The VPN solution provides an additional layer of security, addressing the requirements of NERC CIP-012 and helping utilities maintain a compliant cyber security communication framework between control centers.

NERC CIP-013 Supply Chain Risk Management

The main purpose is to mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.

NERC CIP-013 establishes requirements for managing supply chain risks associated with the acquisition and use of BES Cyber Systems and components within the Bulk Electric System (BES). This standard focuses on ensuring the security and integrity of the supply chain for critical assets that are essential for the reliable operation of the electric grid.

NERC CIP-013 aims to address the risks posed by compromised or malicious components or software that may be introduced through the supply chain. It emphasizes the need for entities to establish a comprehensive Supply Chain Risk Management (SCRM) program to identify, assess, and mitigate potential risks.

1) [NERC CIP-013] [*Base*] As outlined in NERC CIP-004, Survalent maintains a rigorous process to evaluate the trustworthiness and suitability of all personnel within the company and those providing services to utilities. This process includes thorough background checks to ensure that employees who have access to sensitive information are trustworthy and do not pose a security risk. Background checks may include criminal history checks, credit checks, and verification of previous employment and education. In addition, all our personnel undergo regular cybersecurity awareness training to proactively mitigate the risks of malicious activities and threats.
2) [NERC CIP-013] [*Base*] As part of our standard cybersecurity practices, Survalent regularly applies software patches on our network equipment, servers, workstations, and laptops. Survalent also monitors the National Vulnerability Database (NVD), security bulletins, and vendor upgrade emails to stay up to date with any known vulnerabilities related to third-party and open-source libraries that Survalent uses and distributes. Survalent also conducts regular vulnerability scans and penetration tests to identify and evaluate potential risks associated with our products and our environments. When vulnerabilities are identified, Survalent manages the vulnerabilities and provides critical updates and patches to mitigate and correct the vulnerabilities as soon as possible.
3) [NERC CIP-013] [*Base*] As part of our dedication to meeting NERC CIP compliance requirements, we have implemented robust security measures to ensure the integrity and confidentiality of all customer data stored on our equipment. These measures include utilizing secure transfer methods that encrypt

data end-to-end during transmission and using disk-level encryption on all mobile devices. When the customer data we receive includes a copy of the ADMS database, we sanitize the database to remove sensitive information such as IP addresses, customer names, phone numbers, etc. prior to using it for our tests. We also keep a log of all customer databases stored on our equipment identifying when the data was received, where it is stored, and who is responsible for each copy of the data. Access to customer data is strictly controlled and granted only for authorized personnel. Survalent personnel are periodically reminded to delete customer data from their equipment when no longer needed.

4) [NERC CIP-013] [*Base*] As outlined in the NERC CIP-007, Survalent personnel will strictly comply with the utility's procedures for accessing any cyber security assets, whether it involves remote connections or on-site visits.
5) [NERC CIP-013] [*Base*] We prioritize the implementation of industry best practices, robust security measures, and continuous improvement in our development processes to significantly minimize the risk of including malicious code in our software. At Survalent, we have established comprehensive measures to ensure the security and integrity of our software in compliance with NERC CIP-007. Here's an overview of our practices:
   a) Vulnerability Monitoring: We regularly monitor the National Vulnerability Database (NVD), security bulletins, and vendor upgrade emails to stay updated on any known vulnerabilities related to third-party and open-source libraries we utilize and distribute. This allows us to promptly address any identified vulnerabilities.
   b) Secure Development Tools and Frameworks: We employ secure development tools and frameworks that are recognized for their robust security features. This helps us build software with built-in security measures from the ground up.
   c) Security Testing: We utilize automated security testing tools (within Nuget packages, for example) to scan our code for potential vulnerabilities, including common security issues like injection attacks and insecure authentication. This automated scanning is integrated with our build system and triggered on each nightly build.
   d) Third-Party Component Monitoring: We diligently monitor third-party components and dependencies to ensure their security. This helps us identify and address any vulnerabilities in the software components we use.
   e) Product Vulnerability Management: We maintain a list of all third-party and open-source libraries we distribute and regularly update them to the latest versions. This is done at release intervals, prioritized based on security risk. Each update is tracked through separate Jira tickets for progress tracking and revision history.
   f) Escalation and Prioritization: We escalate and prioritize security-related issues identified through internal validation or customer engagements. These issues are tracked within our issue management system and integrated into our development process for timely resolution.
   g) Penetration Testing: We conduct penetration tests on our web applications as part of the release process. This is carried out by external consultants, and we address any issues identified and share learnings with the entire team to enhance our security practices. Retesting is often performed to validate the resolution of security vulnerabilities.
   h) Supported Platforms: We maintain and publish a Supported Platforms list, which tracks the end-of-life for supported operating systems and browsers. This ensures that our software remains compatible with secure and up-to-date platforms.
   i) Software Development Process: Our software development process adheres to ISO 9001 standards for quality assurance. We undergo an annual ISO audit to ensure compliance. The

process includes stages and quality controls for design, development, planning, change management, and validation.

j) Source Code Control and Access Control: Access to our source code control repositories is restricted to developers only and audited. Permissions are set for both projects and repositories independently. Developers must raise a Pull Request and undergo a code review for code to be committed. Our code/build infrastructure is on-premise and accessible only via a VPN.

k) Code Reviews: Code reviews are performed on all code commits by qualified Team Leaders. These reviews ensure adherence to good coding practices, such as avoiding unsafe functions and calls, handling errors gracefully, ensuring appropriate user rights, and incorporating logging and tracing capabilities.

l) Infrastructure and Tool Updates: We update compilers within a two-year timeframe, while other development infrastructure and tools are updated more frequently to incorporate the latest security features and fixes.

m) Secure Build Environment and Digital Signing: All software distributed externally goes through a centralized and secure build environment owned and maintained by dedicated Build staff. During the build process, all compiled files (DLLs, EXEs) and installation kits are automatically digitally signed. This ensures the integrity of the deployed software and guards against tampering. We use a code-signing certificate authority and renew certificates every three years.

6) [NERC CIP-013] [*Base*] Survalent actively engages in improving our software's security and incident response capabilities. This includes identifying vulnerabilities that affect our product, addressing the vulnerabilities, releasing patches and updates in a timely manner, and staying informed about emerging threats and best practices in incident response.

7) [NERC CIP-013] [*Optional*] Through enrollment in the NERC CIP-013 extended Support Plan, Survalent will collaborate with utilities and other stakeholders during incident response activities. This could involve sharing information about vulnerabilities or threats, assisting in the investigation and analysis of incidents, and offering technical support to help mitigate the impact of the incident.

8) [NERC CIP-013] [*Optional*] Through enrollment in the NERC CIP-013 extended Support Plan, Survalent will collaborate with utilities and other stakeholders with any cyber-related documentation associated with the SurvalentONE ADMS provided by Survalent.

9) [NERC CIP-013] [*Optional*] Through enrollment in the NERC CIP-013 extended Support Plan, Survalent will collaborate with utilities and other stakeholders during incident response activities. This could involve sharing information about vulnerabilities or threats, assisting in the investigation and analysis during audits, and offering technical support to help mitigate the impact of any incident.

10) [NERC CIP-013] [*Optional*] Through enrollment in the NERC CIP-013 extended Support Plan, Survalent will provide proactive notification of security incidents related to Survalent products or services. Survalent will notify the utility within three business days by telephone or email using the CIP Contact Information of any security incident to the products or services as per NERC CIP-013.

11) [NERC CIP-013] [*Optional*] Through enrollment in the NERC CIP-013 extended Support Plan, Survalent will provide a Software Bill of Materials (SBOM); the SBOM serves as a detailed inventory of all the components and dependencies within the ADMS application. It provides visibility into the software supply chain, enabling utilities to identify and assess potential vulnerabilities and risks associated with each component. By having access to the SBOM, utilities can conduct a thorough analysis of the software's security posture and determine if any components pose a potential threat to the BES Cyber System.

12) [NERC CIP-013] [*Optional*] As part of the NERC CIP-013 extended Support Plan, Survalent will assist the utility by providing evidence that demonstrates performance and adherence to the NERC CIP-013 requirements.

[THIS PAGE INTENTIONALLY LEFT BLANK]

Appendix I ISO 9001 Certificate

[THIS PAGE INTENTIONALLY LEFT BLANK]

CERTIFICATE OF REGISTRATION

This is to certify that

Survalent Technology Corp.

7965 Heritage Road, Brampton, Ontario L6Y 5X5 Canada

operates a

Quality Management System

which complies with the requirements of

ISO 9001:2015

for the following scope of certification

The Registration covers the Quality Management Systems as it applies to sales, design, software production, commisioning, training and support for automation solution software systems Survalent ONE (SCADA) for utility and industrial applications.

Certificate No.:	CERT-0118393	Original Certification Date:	June 13, 2002
File No.:	003903	Certification Effective Date:	May 1, 2021
Issue Date:	April 26, 2021	Certificate Expiry Date:	April 30, 2024

Frank Camasta
Global Head of Technical Services
SAI Global Assurance

Certified System ISO 9001

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT IAF

Registered by:
QMI-SAI Canada Limited (SAI Global), 20 Carlson Court, Suite 200, Toronto, Ontario M9W 7K6 Canada. This registration is subject to the SAI Global Terms and Conditions for Certification. While all due care and skill was exercised in carrying out this assessment, SAI Global accepts responsibility only for proven negligence. This certificate remains the property of SAI Global and must be returned to them upon request.
To verify that this certificate is current, please refer to the SAI Global On-Line Certification Register:
https://www.saiglobal.com/en-us/assurance/auditing_and_certification/certification_registry/

SAI GLOBAL INFORM. INSPIRE. IMPROVE.

Control your critical network operations with confidence

With Survalent, you can control your critical network operations with confidence. We're the most trusted provider of advanced distribution management systems (ADMS) for electric, water/wastewater, gas, and transit utilities across the globe.

Over 500 utilities in 30 countries rely on the SurvalentONE platform to effectively operate, monitor, analyze, restore, and optimize operations. By supporting critical utility operations with a fully integrated solution, our customers have significantly improved operational efficiencies, customer satisfaction and network reliability.

Our unwavering commitment to excellence and to our customers has been the key to our success for over 50 years.

> "Thanks again for all the work, explanation, advice and assistance. The expertise and advice on our configuration is much appreciated.
> Your willingness to anticipate our needs and help us avoid traps we wouldn't otherwise be aware of is invaluable to us"
>
> - Hydro One Brampton

Survalent.

info@survalent.com ▪ survalent.com ▪ 905-826-5000