Technology Trends

SCADA Systems

Enterprise Architecture, Chief Technology Branch

Version 0.1
Date 2019-07-10

Shared Services Canada
Services partagés Canada

Canada

Table of Contents

Business Brief

Supervisory Control and Data Acquisition (SCADA) is a computer system comprised of hardware and software used for gathering, analyzing, and reporting real-time data on various aspects of industrial utilities and equipment in industries such as telecommunications, water, waste control, and oil and gas.[1]

SCADA can control industrial processes locally or at remote locations, monitor, gather, and process real-time data, directly interact with devices such as sensors, valves, pumps, and motors through Human-Machine Interface (HMI) software, and can record events into a log file for hard drives.[2] Additionally, SCADA can provide the user with warnings by sounding alarms if situations develop into hazardous scenarios in industrial plants.

SCADA systems are used to control and maintain efficiency, distribute data for smarter decisions, and communicate system issues to help mitigate downtime. SCADA systems are the backbone of many modern industries.[3]

Although industries began using computers in the 1950s. SCADA systems were not used until the 1960s.[4] By this time, automated communications were able to transmit pertinent data from remote sites to monitoring equipment through the use of telemetry.[5] Telemetry allows for automated communications to transmit measurements and other data from remotes sites to monitoring equipment.

The term SCADA first came into prominence in the early 1970s, with a rise of microprocessors and PLCs (programmable logic controllers) that paved the way to control and monitor automated processes.[6] SCADA and advanced metering infrastructure (AMI), were precursors to general-purpose Internet of Things (IoT) technology and devices.

Before the introduction of SCADA, industrial organizations relied on manpower to manually control and monitor equipment by using relays, timers, analog meters, dials, and push buttons. As industrial floors expanded, there developed a need to control equipment over long distances without having to send someone to the remote location to interact with each device.[7]

Technical Brief

A SCADA system is comprised of a software and hardware architecture. Several hardware components interface with one another to process data and perform the execution of control operations. The system is centralized allowing it to communicate with wired and wireless technologies on client devices.

Components of a SCADA system include, supervisory computers, remote terminal units (RTU), programmable logic controllers (PLU), a communication infrastructure, and a human machine interface. Installed on a supervisory computer is the necessary software responsible, for communication with field connectors and actuators. These include the RTU, PLCs, and the HMI software running on the operator workstation. An RTU or PLC can be used to connect the sensors to the actuators, they are networked to receive commands and transfer data from the supervisory computer. To execute commands are RTU is embedded with control logic like "ladder logic". PLCs operate in a similar fashion but are capable of executing more sophisticated control commands and are often used in place of RTUs. A PLC is a fast controller capable of near real-time response time. However, when scaling up to a larger solution a distributed control system (DCS) is more suitable in this role as a larger number of I/O points can be handled. A communication infrastructure or network is used is used to connect the RTUs or PLCs to the supervisory computers. The network can be a LAN or WAN depending on whether the SCADA system's data processing is web-based in house, or cloud-based via a third party provider. The network makes use of industry standard protocols or manufacturing protocols. Both the RTUs and PLCs will operate autonomously with near real-time latency [2]. In the event of a network failure they will continue to execute that last command issued by the supervisory computer. The human machine interface is an operator's window into the supervisory system. Plant information is presented to the operating personnel graphically in the form of mimic diagrams.

Industry Use

The global SCADA market is expected to reach approximately USD 21.57 billion by 2023, registering a CAGR (compound annual growth rate) of 9.80% during the forecast period…the solutions and services segment is expected to grow with the fastest CAGR of 11.37% during the forecast period, due to the need for industrial process management and obtaining operational insights by processing huge data volumes.

SCADA systems have been leveraged in industries like power generation and oil and gas refinement for nearly a decade. AES is an international power company that invests in multiple sources of renewable energy such as hydro, wind, solar, and biomass generation. In 2010, the North Palm Springs Corporation decided to implement a SCADA system as part of their AES IV Wind Energy project. The plan was to initialize 49 wind turbines as part of a SCADA and

alarming system. The goal for the system was to monitor the status of the wind turbines while providing an availability measurement. In addition the system is supposed to validate the amount of energy produced versus the amount of energy predicted by the manufacturer's power curve. AES used an OPC server, and did not want any software to be installed on the turbine protocol. They wanted the turbine data process, and the monitoring process to be able to change out independently. In addition to this they wanted the HMI not to be installed on client computers. This avoided control users outside of the domain from experiencing authorization issues, while still providing them with the ability to perform SCADA functions. The company has reported a drastic decrease in development costs, and improved efficiency [12].

Pemex is an oil and gas company that has been leveraging a SCADA system for quite some time but recently wanted to update their solution. The goal of the project was a measurable and efficient natural gas measurement site. They wanted to deliver complex flow calculations to the gas measurements control site.

Canadian Government Use

The Government of Canada (GC) relies heavily on Information Technology (IT) to conduct its operations and daily business activities. IT is plays an integral role in government operations while also being a key enabler in transforming the business of the GC. IT is an essential component of the GC's strategy to address digital transformation challenges and enhancing services to the public for the benefit of citizens, businesses, taxpayers, and employees.[8]

However, since SCADA systems are predominantly applied to industrial utilities and equipment, the Canadian provincial and municipal governments are the primary public organizations that utilize and interact with SCADA technology. This is because these levels of government tend to be responsible for governing industries within their provincial jurisdiction and often own and directly manage industrial utilities.

For example, the Ontario Provincial Government uses SCADA systems within the Ontario Clean Water Agency, an Agency to the Ministry of the Environment, which provides Ontario clients with total solutions in water and wastewater management.[9]

Additionally, the Alberta Provincial Government is using water management SCADA systems in multiple provincially-owned water projects. The Alberta Government's SCADA Data Management System (SDMS) is installed in 30 different workstations and contains four servers [13].

The GC, may not utilize SCADA systems as much as provincial and municipal organizations, however Public Safety Canada (PS) in its mandate to protect National Critical Infrastructure is involved with educating critical infrastructure owners on SCADA cyber issues and best practices. PS holds Industrial Control Systems (ICS) Security Events that aims to assist Canada's infrastructure owners to better secure their most critical industrial control systems such as SCADA and IT assets.[10]

Implications for Shared Services Canada (SSC)

Value Proposition

Although SCADA systems are generally meant for monitoring and controlling industrial and manufacturing processes, for an organization like Shared Services Canada (SSC) there are potential beneficial use cases available.

Data centers require strict cooling and power management systems. SCADA systems are applicable for these purposes and improves efficiency and operational reliability in these areas. Equipment status can be monitored, delivering information to mobile devices connected to the network [7]. Alarm notification and handling are made easier by this which improves the overall response time to maintenance issues. Issues can be actively identified before they escalate into problems.

SCADA systems can provide large amounts of data on utility plants and equipment and provides a graphic interface to connect thousands of sensors across a wide region for various monitoring and controlling operations. This display can be represented to operators in various formats depending on the industry. The most advantageous aspect is that through advanced protocols and application software, data can be monitored from anywhere in the world and all events are logged backed-up in case of system failures.[11] A SCADA system can increase the life of equipment by allowing users to make predictive judgments about equipment lifecycle. In the same manner labour cost is reduced with efficient resource allocation for troubleshooting. The system gives flexibility to choose equipment and systems based on performance rather than compatibility with an installed base.

While SCADA can be used as a building management tool, data logging and reporting as an automated process means there is no longer a need to staff a position for someone to do this work and reduces salary costs and shifts analysts to high priority tasks.

An additional benefit here is the fact a plant's processes can be scaled up since there all the data is dropped into a single repository. SCADA systems generally make use of a database for all the data entries. This is also means the data can be processed from this point and report are formulated automatically. A user is able to highlight parameters of interest when monitoring. Threshold limits and severity warnings can be assigned to these parameters where alarms can be generated when they are reached [1].

Challenges

The significance of the specific challenges regarding SCADA systems depends on whether the system is inside-the-fence, or outside-the-fence. This means that either the system is restricted to single building or plant, or is distributed at various locations.

In this regard, outside-the-fence applications present greater risk. Power and communications are two of the biggest limitations on these types of applications. Outside-the-fence requires greater network coverage, since the SCADA network cannot be limited to a building wide LAN. This also leaves a system more prone to cyber security threats as outside-the fence networks require IP addresses, and this is a major challenge for operators when discussing the accuracy and efficiency of SCADA systems.

Additionally, there are generally two types of threats to SCADA systems. The first is the threat of unauthorized access to the control software. This can be changes made deliberately by human access or, those made due to virus infection and other software threats on the control host machine. The second threat is packet access or network segments that host SCADA devices. These threats are especially present on a distributed implementation of a SCADA system. The severity of these threats is dependent on the design and deployment of the network. The problem can be made worse when a SCADA system is adopted into an existing corporate network already with its own security and authentication protocols [11].

Two issues arise with its potential for a data centre. In the event that a cascade of alarms are triggered, this can hide the underlying cause of the issue. In addition, since SCADA networks use standard internet protocols this makes them susceptible to attack and outages. Specifically for a data centers, data center infrastructure management (DCIM) tools are better suited. It is technically still a form of SCADA since it does involve data monitoring and the execution of control functions, however it is specifically focused on the data center.

Another challenge for SCADA is related to its increasing obsolescence. SCADA is being overtaken and absorbed by Internet of Things (IoT) technology and devices. Over time, there will be more and more functional overlap between SCADA requirements and capabilities and that of IoT systems in industrial and operational intelligence systems.

Other challenges to SCADA is the complexity of PLC based SCADA systems in terms of their hardware unites and dependent components. Complex systems require skilled operators, analysts, and programmers to maintain and properly extract value from a SCADA system. Additionally, integrating remote assets with SCADA systems are not as straightforward as perceived.

Connectivity is another challenge. Telecommunications operators may have strong coverage in some areas, but limited signal in others. Obtaining SIM cards and data plans from multiple carriers to ensure reliable connectivity and verifying which carriers offer reliable network strength at each remote installation location is a difficult and costly undertaking.

In addition, network strength can vary considerably based on unpredictable conditions such as weather.[12] Although Low-power Wide Area Networks (LPWAN) show promise, however, network coverage is still limited, and tight bandwidth limitations dictate the type, amount, and transmission frequency of data. Along the same issues is that many LTE cellular and satellite networks are too power intensive to enable fully-autonomous operations for long durations with frequent data transmission.[13]

Considerations

The GC invests a significant portion of its annual budget on IT equipment and supporting infrastructure. Without adequate monitoring and visibility, approaches to managing IT investments can be difficult and can undermine the effective and efficient delivery of GC programs and services.

For SSC, using a SCADA system to support the management of the Enterprise Data Centers may be beneficial for monitoring cooling needs and sensitive IT equipment. However, SSC should consider the infrastructure, networking, and storage requirements partner departments may request in order to run SCADA systems for their own operations.

Most enterprises will need skills both in building and managing their own SCADA capabilities, and skills in leveraging third-party capabilities. SSC should consider the talent it requires to for the custom work required to implement SCADA

systems, as well as aligning SCADA service offerings with current legacy equipment and corporate strategies.

SSC should also ensure that future infrastructure strategies include policy instruction or direction on SCADA. Different operational requirements from partner departments will drive different SCADA and storage requirements. SSC will need to have a plan in place to manage the future infrastructure and network needs if partner departments pursue greater SCADA operations.

SSC will need to consider how it will handle the implementation of SCADA for itself and partner departments while balancing the understanding that SCADA is reaching a point of increasing obsolescence. SCADA is being overtaken and absorbed by Internet of Things (IoT) technology and devices. SCADA is a vertical solution, meaning it is isolated to specific industry types such as utilities. Today, SCADA has moved from a proprietary software to what is known as Open-SCADA, which increasingly depends on commonly available hardware and Operating Systems. However, many remote monitoring and control needs can now be met through IoT platforms that include open-source frameworks. Additionally, since the IoT market is much larger and serves more customers due to cross-functionality it will likely be the future of remote monitoring and controlling. Many small utility companies may utilize Open-SCADA models, however bigger companies will continue adopting IoT platforms. It will be necessary for SSC to understand this shift in technology and plan accordingly.

In terms of securing SCADA systems, SSC can take several steps to mitigate the risk of security threats. Strict limitations on access and authority control need to be placed on external connections. This is especially true for distributed SCADA networks (i.e. outside-the-fence).

Enhancing security can also be done using virtual private networks (VPN). Access to paths to the internal network should be minimized. This includes encryption of files, directories, and emails, as well as developing control and monitoring methods to cope with any contingencies in the SCADA equipment. With SCADA systems it is important to scan for vulnerabilities. Patching deficiencies in security remains the most effective solution. As a preventative measure SCADA control software should use per user authentication, authorization and logging controls.

SSC should consider evaluating the current Service Catalogue in order to determine where SCADA can be leveraged first to improve efficiencies, reduce costs, and reduce manual administrative burdens of existing services. Additionally, determining how SCADA will integrate into existing services on a

consistent basis. Any new procurements of devices or platforms should have high market value and can be on-boarded easily onto the GC network such as Terraform or AWS. SSC should avoid applying SCADA for production mission-critical apps at the onset. SSC should pilot and establish SCADA test clusters and scale the success. With all new cloud-based technologies, piloting is preferred. Focus should first be on a narrow set of objectives and a single application scenario to stand up a test SCADA.

References

1. https://www.quora.com/What-are-the-benefits-of-a-SCADA-System
2. https://www.elprocus.com/scada-systems-work/
3. https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf
4. https://www.dpstele.com/scada/tutorial-white-paper.php
5. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf
6. https://www.manufacturing.net/article/2017/04/scada-data-center
7. https://www.datacenterknowledge.com/archives/2014/04/16/optimizing-power-system-monitoring-control
8. https://www.csemag.com/articles/selecting-a-critical-power-monitoring-and-control-technology/
9. https://iiot-world.com/smart-manufacturing/values-challenges-scada-systems-outside-fence-applications/
10. https://www.parasyn.com.au/article/the-top-5-problems-with-scada-systems/
11. https://journals.sagepub.com/doi/pdf/10.1155/2012/268478
12. https://iconics.com/Production/media/Literature/SuccessStories/ss-AES.pdf
13. https://ca.linkedin.com/jobs/view/scada-systems-support-specialist-at-government-of-alberta-1068747485
14. https://www.marketwatch.com/press-release/scada-market-2019-global-industry-share-size-future-demand-global-research-top-leading-players-emerging-trends-region-by-forecast-to-2023-2019-05-09

[1] https://www.webopedia.com/TERM/S/SCADA.html
[2] https://inductiveautomation.com/resources/article/what-is-scada
[3] https://inductiveautomation.com/resources/article/what-is-scada
[4] https://www.webopedia.com/TERM/S/SCADA.html
[5] https://www.theearthawards.org/a-brief-history-of-the-scada-system/
[6] https://www.theearthawards.org/a-brief-history-of-the-scada-system/

[7] https://www.theearthawards.org/a-brief-history-of-the-scada-system/
[8] https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755
[9] http://www.ocwa.com/who-we-are
[10] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/vnts-en.aspx
[11] https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-SCADA.html
[12] https://iiot-world.com/smart-manufacturing/values-challenges-scada-systems-outside-fence-applications/
[13] https://iiot-world.com/smart-manufacturing/values-challenges-scada-systems-outside-fence-applications/