Adroit
Technologies

Service Level Agreement (SLA)

Detailed Document

Adroit
Health Services

COPYRIGHT

Advanced Worx 112 (Pty) Ltd
20 Waterford Office Park
189 Witkoppen Road (c/o Waterford Drive)
Fourways
South Africa

www.adroitscada.com

Version	Date	Author	Comment	Approval
1.0	14.05.2025	H. Pienaar	Original	
2.0	06.11.2025	J. Duncan	New Front Cover	
3.0	28.01.2026	J. Duncan	Update links	
4.0	17.06.2026	J. Duncan	New Front Cover	

Contents

1. Introduction

Our goal is to provide you with a reliable and high-quality software service that meets your needs in upholding a quality SCADA environment while managing system associated risk and vulnerabilities.

You get to be in front of the queue, whilst priority standby afford access to more resources, it further provides peace of mind, knowing a specialist support engineer is on standby 24/7.

Service Agreements are generally entered into for 12 / 24-month contracts with a 3-month cancelation notice period.

Risk management is the process of identifying, assessing, and mitigating risks that could potentially impact your organization. Our SLA facilitates and plays a key role in managing risk. The disaster recovery procedure is the first step to ensure all necessary safeguards are taken in case of a disruptive event, should the need arise to restore critical systems with minimum impact.

With the increasing sophistication of cyber threats, it is important for organizations to continuously evaluate and enhance their cybersecurity practices to stay ahead of potential threats and protect their digital assets, none less than your SCADA production environment.

2. Services

Services are grouped into primary action categories, which describe complementary services to affect a high available, secured, quality SCADA system.

2.1. Incident Management

Pertain to the management and resolution of any qualified enquire or reported issue related to the software product. Requests can be logged via multiple channels, which will raise an active case ("Incident"). The case will be assigned to a qualified support engineer and overseen by support manager. Escalation of critical cases is overseen by the support manager, which provides a detailed analysis of each case and monthly summary report.

The response times does not include a resolution but merely a response and being actioned accordingly. Business days is from 08h00 to 16h30 GMT+2, Monday to Friday and excludes public holidays.

2.2. Supporting Services

Describe ad-hoc or predefined maintenance service to address an unexpected event or to ensure an optimal and managed system. Priority support allows for managed support cases each receiving preferential treatment. Critical response provides a dedicated support engineer that will facilitate incident resolution faster, also extend to the readily availability of an engineer to be called to site on 24/7 standby.

2.3. Priority Support

Priority support refers to a specialised level of customer assistance and service provided to individuals or organisations who have a higher priority or urgency in receiving help and may involves prioritising their inquiries or problems over regular support requests. Here are some key features associated with priority support of which some may extend into other services:

- **Faster Response Times**: Priority support guarantees quicker response times compared to standard support. Customers can expect to receive a response within a shorter timeframe, usually within hours or even minutes, depending on the severity of the issue and the level of priority assigned.
- **Dedicated Support Channels**: Priority support often provides dedicated communication channels, such as dedicated phone lines, email addresses, remote access support, to ensure direct and immediate access to support agents or technicians. This option is expanded under the Critical response section that describe dedicated engineers.

- **Extended Support Hours:** Priority support may offer extended availability beyond regular business hours, including evenings, weekends, or even 24/7 coverage. This ensures that urgent issues can be addressed promptly regardless of the time of day. This option is expanded under the **Critical response section** that describe turn around options.
- **Expert Assistance**: Priority support typically involves access to a specialised team of knowledgeable and experienced support personnel who have expertise in handling complex or critical issues. These experts are equipped to provide advanced troubleshooting, in-depth guidance, and tailored solutions.
- **Escalation Procedures**: If an issue cannot be resolved by the initial support agent, priority support often includes streamlined escalation procedures. This means the case can be quickly passed to higher-level technicians or supervisors, ensuring efficient resolution, and minimising any potential delays.
- **Service Level Agreements (SLAs):** Priority support come with specific SLAs that outline the guaranteed response times, resolution times, and other performance metrics. These SLAs serve as a contractual commitment from the service provider to the customer, ensuring a certain level of **Quality Assurance**. The SLAs also cover maintenance, optimisation and performance measures that ensure further stability and quality service.
- **Proactive Monitoring And Maintenance:** Priority support offerings include proactive of systems or services to identify potential issues before they cause any disruption. This can help prevent problems and provide proactive support, ultimately enhancing the overall customer experience. This option is described in more detail under the **System Health Monitoring** which is a dedicated automated service offered as part of the SLAs.

2.4. Critical Response

Under SLAs, critical response and turnaround refer to the procedures and timeframes to address critical issues or system failures reported by users.

- **Issue Prioritisation:** When a critical issue is reported, it undergoes a prioritisation process to determine its severity and impact on users. Critical issues are typically classified as the highest priority and are given immediate attention due to their potential to cause significant disruptions or system failures.
- **Dedicated Resources and Availability:** SLA options issue dedicated resources on **standby 24/7** or restricted based on office hours. The dedicated support personnel will be led by customer focused support champion that would be familiar with the system. These resources are often allocated exclusively to focus on resolving the issue until it is resolved satisfactorily.
- **Response Time Commitment:** The support team commits to a specific response time for critical issues. This timeframe indicates how quickly the team will acknowledge the reported problem and initiate the resolution process. The response time does not describe the resolution time frame.
- **Engineer on Site:** Critical response afford an engineer on site in the pursuit of problem resolution. This covers the time allowed for, but restricted and not including travel and accommodation. This is a managed service at the discretion of the Service Provider.
- **Escalation and Collaboration:** If the initial team assigned to address the critical issue faces challenges or requires additional expertise, escalation procedures are followed. This may involve involving higher-level developers, architects, or specialists who can provide more advanced assistance and accelerate the resolution process. Collaboration among team members is encouraged to expedite problem-solving.
- **Communication and Updates:** Regular and transparent communication is maintained with the affected users or stakeholders throughout the critical response and resolution process. Updates regarding the progress, potential workarounds, or expected timeframes for resolution are provided to keep the users informed. Timely communication helps manage expectations and demonstrates a commitment to resolving the issue promptly.
- **Troubleshooting and Debugging:** The software maintenance team employs thorough troubleshooting and debugging techniques to identify the root cause of the critical issue. They analyse the software code, system configuration, and relevant logs to pinpoint the problem and develop an appropriate solution.
- **Turnaround Time:** The turnaround time refers to the period within which the critical issue is resolved, or a workaround is provided to restore normal system functionality. While the exact turnaround time can vary depending on the complexity of the issue, software vendors or development teams strive to resolve critical problems as quickly as possible. In some cases, a temporary fix or workaround may be implemented first, followed by a more comprehensive solution in subsequent software updates.

2.5. System Audit

The software system audit is a comprehensive examination and evaluation of the SCADA design, implementation, performance, security, and adherence to established standards and best practices. It involves reviewing various aspects of the project and system to assess its overall quality, reliability, and compliance with relevant requirements. The purpose of a software system audit is to identify strengths, weaknesses, and areas for improvement to enhance the system's efficiency, security, and maintainability. The audit extends as part of the **Quality assurance process** and preferred to be an on-site review, however, can be conducted remotely. Here are the key components typically involved in a SCADA system audit:

- **Documentation Review:** The audit begins with an analysis of the software system's documentation, including design specifications, architecture documents, user manuals, and operational procedures. This review ensures that the documentation accurately represents the system and its intended functionality.
- **Project Analysis:** The audit involves analysing the SCADA project design to evaluate its structure, readability, maintainability, and adherence to standards and best practices.
- **Functional Evaluation:** The audit assesses the software system's functional capabilities to determine if it meets the specified requirements and performs as expected. This includes the review of adequate use of all SCADA modules, components, and functionality to achieve optimal use and value.
- **Performance Assessment:** The performance of the SCADA system is evaluated to ensure it meets defined performance benchmarks and can handle expected user loads. This may involve load testing and measuring response times to identify performance bottlenecks or scalability issues.
- **Security Analysis:** The audit examines the system's security measures to identify vulnerabilities and potential risks. It includes assessing authentication mechanisms, authorisation controls, data encryption, input validation, and protection against common security threats.
- **Compliance Verification:** If the software system needs to adhere to specific industry standards, regulations, or compliance frameworks, the audit verifies compliance with those requirements.
- **System Maintenance and Support Evaluation:** The audit assesses the system's maintenance and support processes to determine if proper procedures are in place to handle updates, bug fixes, user support, and system monitoring. This evaluation includes reviewing change management practices, version control, incident response, and customer support procedures.
- **Reporting and Recommendations:** At the end of the audit, a detailed report is generated summarising the findings, including identified issues, weaknesses, and areas for improvement. The report may also provide recommendations for addressing the identified problems and enhancing the software system's overall quality, security, and performance.

2.6. Quality Assurance

Is a set of activities and processes that are designed to ensure that a product or service meets certain standards and expectations. Quality assurance oversee all other services rendered, ensuring each service is of the highest grade. This process ensures optimum use of the software, best in class support, training, and project engineering.

- **Service Level Management (SLM):** Is a practice or process within service department that focuses on establishing, monitoring, and managing service level agreements (SLAs) between service providers and customers. SLM aims to ensure that the agreed-upon services are delivered effectively and meet the customers' expectations and requirements. It involves defining, measuring, and improving service levels to maintain a high standard of service delivery.

2.7. Software Assessments

Is a process that evaluates the use and performance of software and services to ensure they meet agreed-upon standards. The assessment process involves analysing various aspects of the software, such as functionality, performance, security, and usability. The objective of the assessment is to identify areas where the software or project may not be meeting the agreed-upon standards, and to develop strategies for improving quality and performance. Assessments is conducted using standard utilities or standard operating procedure (SOP) guides under the heading of **System Health Monitoring**:

- **Server Activity Monitor** provides a host of performance measures and system configuration. The engineer will benchmark and review a set period and analyse overall performance.
- **Adroit Dump** is an agent server diagnostic utility that evaluate various internal components, file versions, configurations and object relationships which provides an in depth analysis reports with warnings.
- **Health Monitor Service** is a built-in real time performance tracker which raises critical performance event flags.
- **SLA Standard Operating Procedure** refer to a set of systems checks and evaluations through using various best practise guides or real-time action reviews.

2.8. Backup and Disaster Recovery

Backup and disaster recovery (BDR) is a crucial aspect of ensuring business continuity and safeguarding critical data and systems in the face of unexpected events or disruptions. BDR involves the implementation of strategies, processes, and technologies to create backups of data and systems, as well as to restore them in the event of a disaster or data loss incident. The following are a few critical processes covered under this service.

- **Data Backup:** Backup is the process of creating duplicate copies of configuration and project data and storing them in separate locations or mediums to guard against data loss. It involves regularly copying and preserving important files, databases, configurations, and other data assets. Backups can be performed at various intervals (e.g., daily, weekly, or in real-time) and can be stored on local devices, network storage, or off-site locations.
- **Backup Types and Methods:** Different backup methods and technologies can be employed based on the specific requirements of the system. Primary backups refer to the SCADA system\project while the secondary backup refer to system dependencies such as 3rd party databases.
- **Data Recovery:** Data recovery involves the process of restoring data from backups in the event of data loss or corruption. Depending on the backup strategy implemented, the recovery process can include restoring the most recent backup or point-in-time recovery mechanisms. The recovery process aims to minimise downtime and restore the data to its original state. The enterprise SLA affords and a standby engineer to assist with the recovery process.
- **Disaster Recovery Planning:** Disaster recovery planning encompasses the comprehensive strategies, policies, and procedures designed to ensure business continuity and minimise the impact of a major disruption or disaster. It involves identifying potential risks, assessing their potential impact, and developing recovery strategies. Under the SLAs we provide a comprehensive DRS document and procedure.
- **Disaster Recovery Testing**: Regular testing of the disaster recovery plan is essential to verify its effectiveness and identify any gaps or shortcomings. Testing can involve restoring backup files on a test environment to verify the process backup.
- **Off-site Storage and Redundancy**: To mitigate the risk of data loss due to physical disasters or localised incidents, backups are often stored in off-site locations. These locations can include remote data centres, cloud storage providers, or secure off-site facilities.
  The enterprise SLA offers secure cloud storage where at a minimum the latest month backup will be kept.

2.9. Software Vulnerability Management

- **Security and Threat Protection**: Risk identification involves identifying potential risks or threats to the software system, including risks related to data loss, data theft, unauthorised access, system failures, and other security-related issues. Vulnerability assessment involves identifying vulnerabilities or weaknesses in the software system that could be exploited by attackers. Actions refer to SCADA software patches and windows update management (windows security patches).

- **Software Security and Risk Audit:** A software security and risk audit is a systematic evaluation of SCADA application, system dependencies, and processes to identify potential security vulnerabilities, assess risks, and ensure compliance with security standards and best practices. The audit aims to identify weaknesses in software security measures, evaluate the potential impact of security breaches, and recommend appropriate mitigation strategies.

2.10. Documentation

Document everything: Documentation is essential to ensure that everyone involved in the service has a clear understanding of the system and its requirements. This includes documenting the engineering process, discovery analysis, test cases, and maintenance performed.

3. Service Description

	Service Item	Professional	Enterprise
Maintenance & Support	**Incident Management**	Incident tracking and ticketing system	Incident tracking and ticketing system
	Support Services	Office hours 08:00 to 16:30 (GMT +2)	Office hours 08:00 to 16:30 (GMT +2)
	Service Desk	Managed	Managed
	Telephonic Support	Managed	Managed
	E-mail Support	Managed	Managed
	Support Forum	Managed	Managed
	Knowledge Transfer	Full access (Wikki, Knowledgebase articles, Best Practice, Webinars)	Full access (Wikki, Knowledgebase articles, Best Practice, Webinars)
	Remote Support	Managed (4 hours fair use per case)	Managed
	Priority Support	Priority Support Channel	Dedicated Support Channel
	Faster Response Times	Guarantees quicker response times compared to standard support	Guarantees quicker response times compared to standard support
	Dedicated Support Channels	**Support Help Desk**, email addresses, remote access support	**Dedicated phone lines**, email addresses, remote access support
	Extended Support Hours	**Office hours** only with priority resolution	Priority resolution
	Expert Assistance	Access to a team of knowledgeable and experienced support personnel	Access to a **dedicated** specialised team of knowledgeable and experienced support personnel
	Escalation Procedures	Case is reviewed on an interval basis and only escalated after a determined period	Case is continuously monitored, escalated when required to achieve optimal resolution
	Proactive Monitoring and Maintenance	To identify potential issues before they cause any disruption	To identify potential issues before they cause any disruption
	Critical Response Time	**Excluded**	**24/7 Support**
	Issue Prioritisation		Priority depends on impact severity
	Dedicated Resource and Availability		Dedicated Team
	Response Time Commitment		4 hour response time
	Engineer on Site (Support cases)		2 Days p/m - Managed
	Communication and Updates		Continuous feedback
	Troubleshooting and Debugging		Dedicated Team
	System Audit	SCADA System Review	Comprehensive examination and evaluation of the SCADA System
	System Site Audit (Documentation, Project & Security Analysis, Function Evaluation)	**Annually**	**Biannual**
	Discovery, Analysis and Recommendations (Remote)	Monthly discovery report. Evaluating system performance, general configuration, and best practices	Monthly discovery report. Evaluate system performance, adoption of best practices, implement recommended optimisations.
	Software Maintenance	Version control and critical software updates	Version control and critical software updates
	Patches and minor feature releases	Managed	Managed
	Quality Assurance	Ensure the project & service meet certain standards and expectations	Ensure the project & service meet certain standards and expectations
	Service Level Management	Contract and Service Management, SOP and SLA feedback	Contract and Service Management, SOP and SLA feedback
	Service Management Reviews and System Feedback	**Limited** to standard document and report feedback	Document review and interactive feedback sessions
	Software Assessments	Evaluates the use and performance of software and services	Evaluates the use and performance of software and services
	System Health Monitoring	Automated System performance and vulnerability assessment	Automated System performance and vulnerability assessment
Risk Management	**Backup & Disaster Recovery (BDR)**	Provide a comprehensive BDR procedure	Provide a comprehensive BDR procedure
	Scheduled Backups	**Weekly** local backup scheduled, verified on monthly system review. No offsite storage	**Daily** local backup, weekly network storage, monthly offsite recovery backup, verified
	Recovery	Provide BDR procedure	Provide BDR procedure **with assisted recovery**
	Housekeeping	General file maintenance with cleanup and archiving	General file maintenance with cleanup and archiving
	Uptime Monitoring	System failure and event tracking	System failure and event tracking
	Remote Alerts	Email, Adroit Air notifications	Email, Adroit Air notifications
	Software Vulnerability Management	Deploy software patches or security enhancements	Deploy software patches or security enhancements
	Software Security and Risk Audit	**Annually**	**Biannual**
	Security and Threat Protection	**Annually**	**Biannual**

3.1. Clarifications

- **Limited** – Refers to defined process or task and a restriction of use for service, time based or number of occurrences
- **Managed** - Refers to restrictions within a **Fair Use Policy**.

3.2. Fair Use Policy

A software SLA (Service Level Agreement) Fair Use Policy is a set of guidelines that outlines the acceptable and reasonable use of software services provided under the SLA. It ensures that customers adhere to certain usage limits, prevent misuse, and maintain a fair and consistent experience for all users.

- **Usage thresholds**: Where an instance of a support case exceed any maximum threshold, whether time-based or resources based we reserve the right to charge for additional services. Recurring instances where it is deemed that a new instance has been raised on a concurrent or existing support case. Number of overall support cases or concurrent support cases where it is deemed to be unrealistic or will impede on the service quality.

- **Overuse consequences:** In the event where it is found that the fair use policy has be breached, we reserve the right to charge for all additional services at our standard or contracted rate, whichever is lower. The client will be informed of potential impact on service delivery, consequently we further reserve the right to cap services.

- **Differentiation between fair use and abuse:** Where the client has been advised against the use, implementation or known negative impact of software functionality, use or project design. Unauthorised or Non-certified user interaction with the system, reverse engineering, tampering with software components which led to the compromising system.

- **Dispute resolution:** Any potential breach would be internally escalated to the relevant service manager, who will communicate such to client representatives, which will require acknowledgment of potential cost or compromised service. Post service delivery resolution will be escalated to the service manager, account manager and client representative to concluded findings and recourse.

4. Terms and Conditions

Please note that the following Terms and Conditions apply:

- Terms and Conditions of Sale for any Hardware or Software purchases.

- Terms and Conditions for Service for any Service Level Agreements.

- Terms and Conditions for Hosted Solutions for any Hosted Solutions.