Core Automation

SCADA Alerting and Messaging RFI Functional and Non-Functional Requirements

Questions	Comments
Functional Requirements	
1. Real-Time Alarm Detection and Notification	
Real-time Detection: The system shall have the ability to continuously monitor SCADA systems and trigger corresponding notifications.	AlarmSuite for Aveva System Platform is service based, it continues to operate and send out alarms even when the local session is logged off. AlarmSuite for Intouch and Ifix runs as an application on the desktop and must remain in the same active desktop session as the running Intouch or Ifix SCADA.
Immediate Notification: The system shall deliver notifications to the designated personnel immediately upon alarm detection.	AlarmSuite plans are activated when an alarm condition becomes true, the plan is executed as it's designed and sends out alarm messages immediately, or delayed as per its plan. Alarm descriptions are retrieved from the SCADA. There is no need to recreate alarm descriptions
Acknowledgment Tracking: The system shall allow authorized personnel to acknowledge alarms in real-time, with the timestamp and user identification tracked. Acknowledgement shall be done via the same medium as the alarm notification. (SMS, email etc.)	AlarmSuite allows for remote acknowledgement of alarms. A user responds to the delivered messaged (SMS/email/App) with an acknowledgement ID. AlarmSuite records this action and updates the SCADA to show the alarm acknowledged and by whom. History of the alarm conversation is stored in AlarmSuite and can be searched.
Escalation Protocols: The system shall automatically escalate alarms to higher-level users or teams if not acknowledged or resolved within a software defined configurable time frame. A minimum of 3 levels of escalation shall be available.	Alarm annunciation to users is highly configurable, an alarm plan will escalate through a defined group of users. Each plan contains configurable wait times between each user, repeats, and escalation until the alarm is acknowledged or the plan finishes. A plan can be configured to repeat as many times as required, including pausing between repeat actions.
2. Notification Channels	
Primary Channel: The system shall support SMS communication for notifications	AlarmSuite Supports SMS bi -directional messaging, along with email and App for Android and Apple/IOS
Multiple Channels: The system shall support multiple communication channels for notifications, including email, mobile push notifications, voice calls, and desktop/web alerts.	AlarmSuite Supports SMS bi-directional messaging, along with email and App for Android and Apple/IOS. Extensibility can be provided by third party additions such as SMS/email to speech services.
Notification Customization: The system shall allow customization of the format and content of alarm notifications	AlarmSuite faithfully resends the alarm descriptions generated in SCADA, guaranteeing no miss-interpretation and requiring no repeat entry of alarm descriptions. Other detail such as Alarm Area can be prefixed into Alarm descriptions.

3. Alarm Filtering and Suppression	
Alarm Filtering and Grouping: The system shall allow operators to filter alarms based on pre-configured rules. The system shall categorize alarms into severity levels (e.g., critical, high, medium, low) and adjust notification behaviours accordingly. All filtering information should be based on metadata originating from the SCADA systems	AlarmSuite retrieves alarm priority information from the SCADA, each AlarmSuite plan can be configured to respond to a priority range, alarm only at defined times, on defined days. Alarm severity from System Platform is mapped to priority.
Alarm Suppression: The system shall provide mechanisms to suppress certain alarms during maintenance or other predefined conditions.	AlarmSuite enables suppression of individual alarms, or removal of entire areas of alarms as generated by SCADA.

4. Alarm History and Reporting	
Audit Trail: The system shall maintain an audit trail of all alarms, including trigger time, priority, acknowledgment, and resolution actions.	AlarmSuite history stores actions taken by AlarmSuite, including operator interactions.
Reporting: The system shall have the ability to generate reports on alarm frequency, response time, resolution time, and trends. These reports should be exportable in CSV or Excel format.	AlarmSuite history is stored in a SQL table and can be exported and queried as needed. AlarmSuite does not currently have native reporting capabilities.
Historical Alarm Management: The system shall have the ability to trim or purge historical alarms once they have been backed up.	AlarmSuite history can be stored for up to 1 year, default is 30 days. History is removed daily where it exceeds the threshold

5. User Roles and Permissions	
User Role-Based Access: The system shall support role-based access control (RBAC) to assign different access levels to users based on their roles (e.g., operators, engineers, managers etc.).	AlarmSuite UI (user interface) can be made available to user who require access. Control objects for AlarmSuite can be embedded directly into SCADA pages, SCADA security can be used to control access to those objects.
Multi-User Collaboration: The system shall support multi-user access, allowing real-time collaboration on critical alarms.	AlarmSuite is an extension of the SCADA alarming system. It faithfully repeats the SCADA alarms to users using defined plans for aggregation and activity. Multiple users can access the AlarmSuite interface simulataneously.

6. Mobile Access	
Mobile App Access: The system shall allow real-time alarms and notifications to be accessible via a mobile application for remote monitoring and acknowledgment.	AlarmSuite Mobile is an application for Android and IOS devices, allowing real time visualisation, acknowledgement , operator on/off call changes and history of alarms for AlarmSuite users.

7. Integration with SCADA and Other Systems	
SCADA Integration: The system shall integrate seamlessly with SCADA platforms to collect alarms. This includes communicating with the AVEVA System Platform, GE iFIX SCADA Systems and Emerson DCS.	AlarmSuite integrates with Aveva System Platform, Aveva Intouch and GE Vernova Ifix
Integration With Less Secure Environments: The system shall have a method of integrating to least secure environments like the internet via DMZ networks to transmit and receive data securely. This will easy the implementation of this system in the Purdue Model.	AlarmSuite Mobile app data uses MQTT to Core Automations secure broker service via non-standard ports. Only outgoing connections to our white-listed address are necessary for Mobile app communications. Some internal firewall modifications may be necessary in some circumstances.

8. Data Enrichment and Contextualization	
Contextual Information: The system shall be able to enrich alarm notifications with contextual information, including affected equipment, additional parameter values, fault description, suggested actions, and potential impacts.	AlarmSuite faithfully repeats the SCADA alarm descriptions to intended recipients. Contextual information can be added to the SCADA alarm descriptions, to be sent out by alarmSuite. Alarm Areas can be automatically prefixed to alarm messages

9. Acknowledgment and Response Logging	
Acknowledgment Logging: The system shall track which user acknowledged the alarm, when it was acknowledged, and what actions were taken.	AlarmSuite history tracks user acknowledgement, method and time.
Real-Time Status Updates: The system shall update the alarm status in real-time as it is acknowledged, resolved, or escalated.	AlarmSuite Mobile displays the current state and history of alarms. Alarms via SMS are sent on an entry to the alarm condition. Active alarm plans are cancelled when the alarm condition is cleared. Alarm state is not updated via SMS or email. AlarmSuite can be queried via SMS for quantities of active alarms.
SCADA Acknowledgement: Acknowledgements shall be forwarded to the SCADA system source so that all alarms acknowledged within the alarms notification software are also acknowledged in the SCADA system that originated them	AlarmSuite acknowledgements are tied to the SCADA system. Acknowledging them in AlarmSuite, acknowledges them in the SCADA. The operator name is appended to the alarm acknowledment in SCADA.

10. Calendar and Rostering	
Calendar Function: There shall be the ability to enter on-call staff in a calendar with the time when the staff are rostered to be on-call. Alarms are only send to staff which is on call when the alarm occurred.	Alarm plans within AlarmSuite allow the user to configure which hours, day of the week and group/order of operators will be notified of alarms. Monthly Calendar rostering is on the AlarmSuite Roadmap.
Calendar Function Data Entry: Data entry to the on alarm calander shall support both manual data entry and import from CSV, Excel or similar.	AlarmSuite does not currently offer this
Alarms Occurring Outside a Roster: If an alarm occurs at a time when nobody is on the roster, the alarm notification shall be held in a buffer and then sent to the next person who is rostered to be on call. This is only applicable if the alarm is still active at that time	AlarmSuite does not currently offer this

11. Configuration Access Control	
System Admin Access Restrictions: The system shall restrict access to configuration settings based on user roles and permissions. Only authorized personnel (e.g., system administrators) shall be able to modify configuration settings.	AlarmSuite requires local PC admin privileges in order to modify service-related changes. AlarmSuite operates as services on the machine which enables it to continue operating once a user session has been logged off that machine. Non local PC Admins are not able to modify configuration settings.
Role-Based Access: The system shall support role-based access control (RBAC) for configuration, ensuring that users only have access to the configuration settings relevant to their roles.	AlarmSuite SCADA objects allow for SCADA controlled access to operator changes. Access to the AlarmSuite UI can be controlled by others (Controlling who has access to the AlarmSuite Graphical User Interface for instance).

12. Audit Logging of Configuration Changes	
Change Tracking: The system shall maintain a detailed audit trail of all configuration changes, including the user ID, timestamp, and a description of the change made (e.g., altered alarm thresholds, changed notification channels).	AlarmSuite records basic changes in its local history i.e. alarm plan enable/disable, operator on/off call changes.
Log Access: The system shall provide access to logs and reports of configuration changes, enabling traceability and accountability for any modifications.	AlarmSuite stores logged changes to a SQL table which is accessible for further processing/monitoring

13. Multi-Factor Authentication (MFA) for Configuration Access	
MFA Enforcement: The system shall enforce multi-factor authentication (MFA) for any access to configuration settings, adding an extra layer of security for system administrators and other users who modify alarm configurations.	AlarmSuite user interfaces can be contained within an environment which uses MFA for access
MFA Methods: The system shall support various MFA methods	AlarmSuite user interfaces can be contained within an environment which uses MFA for access

14. Authentication	
Active Authentication: The system shall be able to authenticate against a Microsoft active directory	AlarmSuite user interfaces can be contained within an environment which uses MFA for access
Password Strength: If the system is not able to authenticate against Microsoft active directory it shall be able to enforce strong password policies for users accessing the configuration settings, including requirements for password length, complexity, and expiration.	AlarmSuite user interfaces can be contained within an environment which uses MFA for access
Periodic Updates: If the system is not able to authenticate against Microsoft active directory it shall require administrators to update passwords periodically to enhance security.	AlarmSuite user interfaces can be contained within an environment which uses MFA for access

15. Session Timeout and Auto-Logout for Configuration Interface	
Auto-Logout: The system shall automatically log out users from the configuration interface after a specified period of inactivity to prevent unauthorized access if a user leaves the session unattended.	AlarmSuite user interfaces can be contained within an environment to provide this
Failed Login Alert: The system shall provide an alert or notification if there are multiple failed login attempts to the configuration interface, indicating a potential security breach.	AlarmSuite user interfaces do not inherently contain their own security model, this is provided by wrap around systems like Windows logon credentials or SCADA access requirements

16. Encryption of Configuration Data	
Data Encryption: The system shall ensure that all configuration data (e.g., user permissions) is encrypted both at rest and in transit to prevent unauthorized access and tampering.	AlarmSuite stores configuration information in a SQL database.
Encryption Standards: The system shall use industry-standard encryption protocols, such as AES (Advanced Encryption Standard) for storing configuration data and TLS (Transport Layer Security) for transmitting it.	AlarmSuite Mobile app uses AES256 for data encryption of configuration data and is transmitted using TLS1.2

17. IP Whitelisting for Configuration Access	
Trusted IPs: The system shall support IP whitelisting, restricting configuration access to trusted IP addresses or address ranges. Only users within these designated networks shall be able to access the system's configuration settings.	AlarmSuite does not provide whitelisting facilities
Dynamic IP Updates: The system shall allow dynamic updating of whitelisted IPs, ensuring that remote administration or access from trusted networks is supported while preventing unauthorized external access.	AlarmSuite does not provide whitelisting facilities

18. Two-Step Verification for Critical Configuration Changes	
Change Confirmation: The system shall require two-step verification for critical configuration changes (e.g., altering notification channels, adding new users, changing alarm priorities).	AlarmSuite does not provide two step verification processes

19. Backup and Restore for Configuration	
Secure Backup: The system shall provide secure backup and restore functionality for configuration settings. Backup files shall be encrypted, and access to them shall be restricted to authorized personnel only.	AlarmSuite Graphical User Interface provides for export and import of Users, Groups and configured plans. These are exported in CSV or XML format and can be used to backup or upgrade/replace an AlarmSuite installation
Automated Backups: The system shall support automated backups of configuration settings at regular intervals to prevent data loss in case of system failure or unauthorized changes.	AlarmSuite uses a MSSQL server to store all configuration information. Standard SQL backup procedures can be used to prevent data loss or restore from unauthorised changes.

20. Secure API for Remote Configuration	
API Security: The system shall provide a secure API for remote configuration and allow access only with proper authentication mechanisms	AlarmSuite SCADA Objects allow for remote changes of some AlarmSuite features. Security and access to this is provided by the SCADA interface
API Rate-Limiting: The system shall rate-limit and monitor API usage for configuration access to detect and prevent potential misuse or brute-force attacks.	AlarmSuite does not monitor SCADA object usage, the SCADA interface may be used for monitoring access as can the MSSQL database containing the AlarmSuite installation

21. Configuration Change Approval Workflow	
Approval Workflow: The system shall implement an approval workflow for configuration changes, requiring that certain modifications be reviewed and approved by one or more designated users before being applied.	AlarmSuite does not currently support this
Change Notifications: The system shall send notification alerts to relevant stakeholders when a configuration change is initiated, providing an option to approve or deny changes before they are finalized.	AlarmSuite does not currently support this

22. Emergency Lockdown for Configuration	
Lockdown Mode: The system shall allow authorized personnel to initiate an emergency lockdown on the configuration settings in case of a security breach. During lockdown, configuration settings shall be read-only, preventing unauthorized changes until the security issue is resolved.	AlarmSuite relies on the SCADA and/or Windows environment to provide overarching security.

Non-Functional Requirements	
1. Performance	
Low Latency: The system shall deliver alarm notifications with minimal delay, ensuring near-instantaneous notification after detection (within seconds).	AlarmSuite works directly with the SCADA alarm bus, collection and initiation of Alarm plans is rapid, delivery of Alarms to users is at the discretion of the intermediate delivery system i.e. Telcos for SMS, Email system etc.
Scalability: The system shall be scalable to handle increasing numbers of alarms and users without performance degradation.	AlarmSuite is designed for up to 1000 concurrent alarms, plans are only limited by available storage, 1000 recipients per install. Alarms are requested hierarchy and only alarms within that hierarchy are interrogated.
2. Availability and Reliability	
High Availability: The system shall be available 24/7 with no downtime, ensuring continuous alarm distribution and notifications.	AlarmSuite operates as a suite of services on a PC. This provides excellent robustness and reliability.
Redundancy: The system shall provide redundancy mechanisms, such as backup servers and failover configurations, to ensure uninterrupted service during hardware or software failures.	Duplicate installations of AlarmSuite with offset delays provides a redundant alarm system with AlarmSuite
3. Usability	
Intuitive UI: The system shall provide an intuitive user interface (UI) for operators to view, acknowledge, and manage alarms, requiring minimal training.	AlarmSuite UI is intuitive and simple to use giving users a clear operational view of the alarm system. Built in help file includes excellant support along with screen shots and setup information.
Custom Dashboards: The system shall allow users to customize their dashboards to focus on the alarms or data most relevant to their role.	AlarmSuite SCADA objects provide a simple view of basic functions within the SCADA environment with which your operators are already familiar.
4. Fault Tolerance	
Error Recovery: The system shall recover gracefully from hardware, software, or network failures without losing critical alarm data or notifications.	AlarmSuite buffers alarm notifications in the event part of the alarm system becomes unstable and will transmit the notifications when it is able. Failed message retries is configurable.
Retry Mechanism: The system shall provide a retry mechanism for failed alarm notifications, with configurable retry intervals.	AlarmSuite plans offer many options for repeating and escalating alarm notifications if they remain unacknowledged
5. Maintainability	
Configuration Management: The system shall allow easy configuration of alarm rules, notification channels, escalation policies, and user roles.	Alarm plans are highly configurable and easy to manage from the AlarmSuite User Interface
Modular Design: The system shall be modular, allowing components (e.g., notification services, alarm filters, reporting) to be maintained or updated independently.	AlarmSuite operates as a group of services on the installation PC. They may be updated independently however we would recommend re-installtion should it be required. Configuration and setup is optionally brought through to later versions
Diagnostics: The system shall provide built-in diagnostic tools for troubleshooting and performance monitoring.	AlarmSuite utilizes Microsofts snap in for Event notification for troubleshooting and diagnostics.
6. Compliance	
Regulatory Compliance: The system shall support compliance with industry regulations and standards (e.g., IEC 62682 for alarm management).	AlarmSuite is designed and built by Core Automation, calling on many years of field experience to provide a product which works.
Data Retention: The system shall support data retention policies to store alarm logs for the required period for auditing and compliance purposes.	AlarmSuite history has a configurable storage retention time from 1 -365 days. Defaulted to 30 days.

7. Resource Efficiency	
Optimized Resource Usage: The system shall be optimized for efficient use of resources (e.g., CPU, memory, network bandwidth), minimizing overhead and ensuring the system runs efficiently.	AlarmSuite only requites 50MB of disk space to install and a negligible amount of RAM. It is efficient and is constantly tested for performance and reliability

8. Localization and Internationalization	
Multi-Language Support: The system shall support multiple languages to accommodate users in different geographic locations.	AlarmSuite supports the English language
Time zone Adjustments: The system shall adjust alarm notifications based on the user's time zone to ensure timely alerts.	AlarmSuite runs on the local PC time and will adjust according to the PC's clock.