Final Year Project

Software Requirements Specification

For

Survaillant

Version: 1.0

Team Members: Maaz Ahmad
Marryam Azhar
Uswa Fatima
Advisor: Dr. Fahad Ahmad Satti

Date of Preparation: 22nd ctober 2023

Table of Contents

Table of Figures

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

The purpose of this document is to define the software requirements for "Survaillant," a cybersecurity approach through proactive monitoring, audit and control. This software, at its core, improves the security of Supervisory Control and Data Acquisition (SCADA) systems by providing comprehensive real-time monitoring, anomaly detection, and security threat identification. Survaillant aims to safeguard critical infrastructures and industrial operations by mitigating potential cyber threats that could compromise the integrity and stability of these vital systems. By offering AI based logic and notification mechanisms, it contributes to the overall protection of SCADA networks and critical operations.

1.2 Document Conventions

This document follows the project documentation conventions outlined by the IEEE SRS template and aligns with the standards practiced by SEECS, NUST. It includes the detailed description of functional and nonfunctional requirements, system features, external interfaces, and all the prominent aspects of the software. Each requirement statement is assigned its own priority and headings are organized hierarchically in accordance with standard formatting practices.

1.3 Intended Audience and Reading Suggestions

This document is primarily intended for developers, testers and advisors of the project team as well as the SCADA administrators within the industrial sector who are potential users of Survaillant. The content of this SRS can be approached sequentially, following the numbering of headings, for a complete understanding of the software and its specifications. It is recommended to refer to the use cases and, if necessary, the interface prototypes to gain a practical understanding of the software's expected behavior.

1.4 Product Scope

Survaillant is an intelligent solution that addresses the unique security challenges of SCADA environments. This software is for the use of SCADA system managers and administrators to protect their critical SCADA system against unauthorized access, cyber threats, and potential vulnerabilities. The system will identify any anomalies and potential threats by analyzing the SCADA network traffic. The system will generate alerts on potential anomalous behavior and the users can respond to these

alerts, enabling proactive approach. Survaillant is trained on intelligent machine learning algorithms enabling efficient anomaly detection and identification of potential threats.
Survaillant supports compliance with industry-specific and regulatory security standards and frameworks and is built according to NIST's "Guide to Industrial Control Systems (ICS) Security."
It directly supports the broader corporate goals of safeguarding critical infrastructure like smart grids, ensuring operational excellence, and maintaining regulatory compliance.

2. Overall Description

2.1 Product Perspective

Survaillant is an autonomous and specialized tool for improving the security of industrial infrastructure. It is designed to address the existing gap in the security applications specifically tailored for Scada systems and their unique communication protocols. Although it draws inspiration from contemporary network-based intrusion detection systems, Survaillant uses advanced machine learning algorithms for incorporating anomaly detection and security threat detection in a single platform, preempting harm to the SCADA system. Its user interface offers network traffic statistics and allows the users to promptly respond to system-generated security alerts.

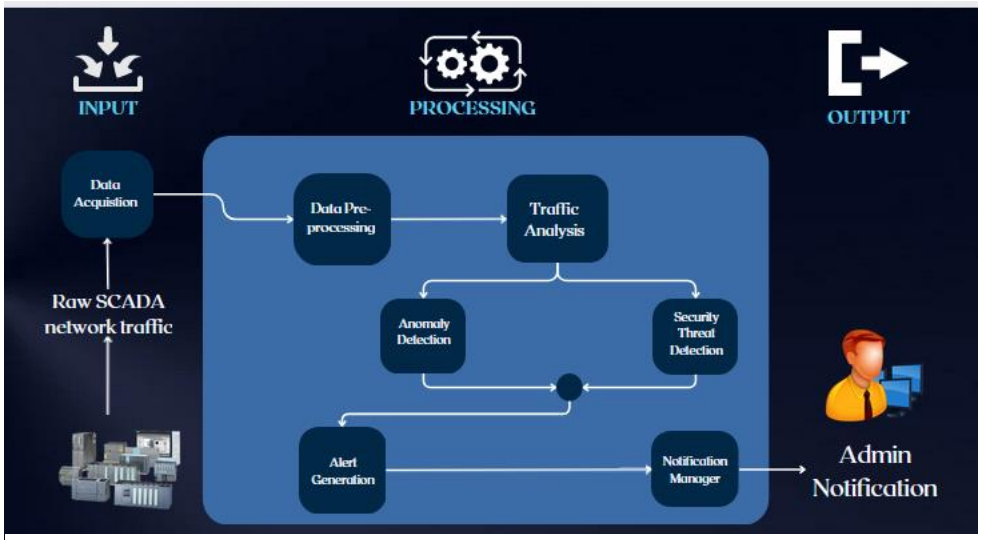

Figure 1: Survaillant phases and Components

2.2 Product Functions

- Monitoring of network traffic within SCADA systems.
- Application of advanced machine learning algorithms for anomaly detection.

- Identification and analysis of potential security threats within SCADA networks.
- Implementation of user authentication and access control mechanisms to ensure secure access.
- Provision of a user-friendly interface for viewing network traffic statistics
- Development of a notification system
- Generation of prompt security alerts to notify system administrators.
- Management of system-generated alerts and responses to potential security threats

2.3 User Classes and Characteristics

The software will be used specifically in the SCADA environment. Since Survaillant is a security-based solution, only the following user classes will have access to the system after proper authentication.

2.3.1 Scada Administrators

SCADA administrators will have administrative access to Survaillant for monitoring and for oversight of security measures. They possess moderate technical knowledge and use Survaillant to ensure the overall security and compliance of the SCADA environment.

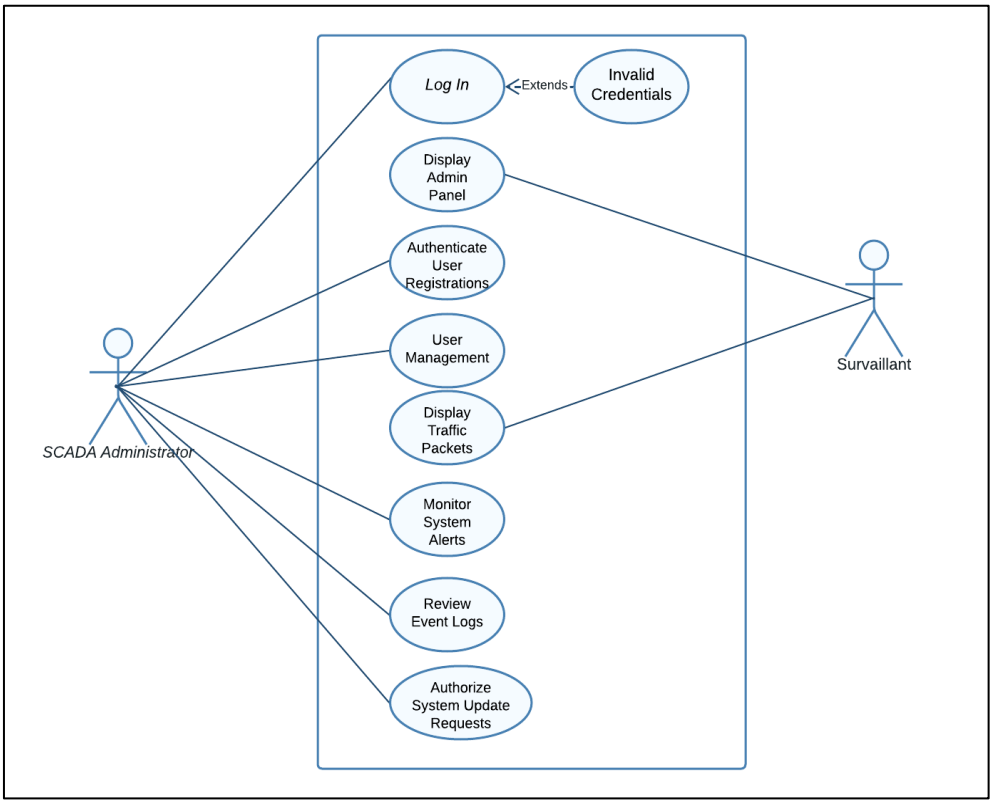

Figure 2: Use Case Diagram - Administrator

2.3.2 Scada Security Team

This user class includes security professionals and cybersecurity professionals working 24/7 to monitor the SCADA systems. They are granted full access to Survaillant to monitor and respond to security alerts generated within the environment. Members of the security team possess advanced technical knowledge and have the authority to manage and configure this software.

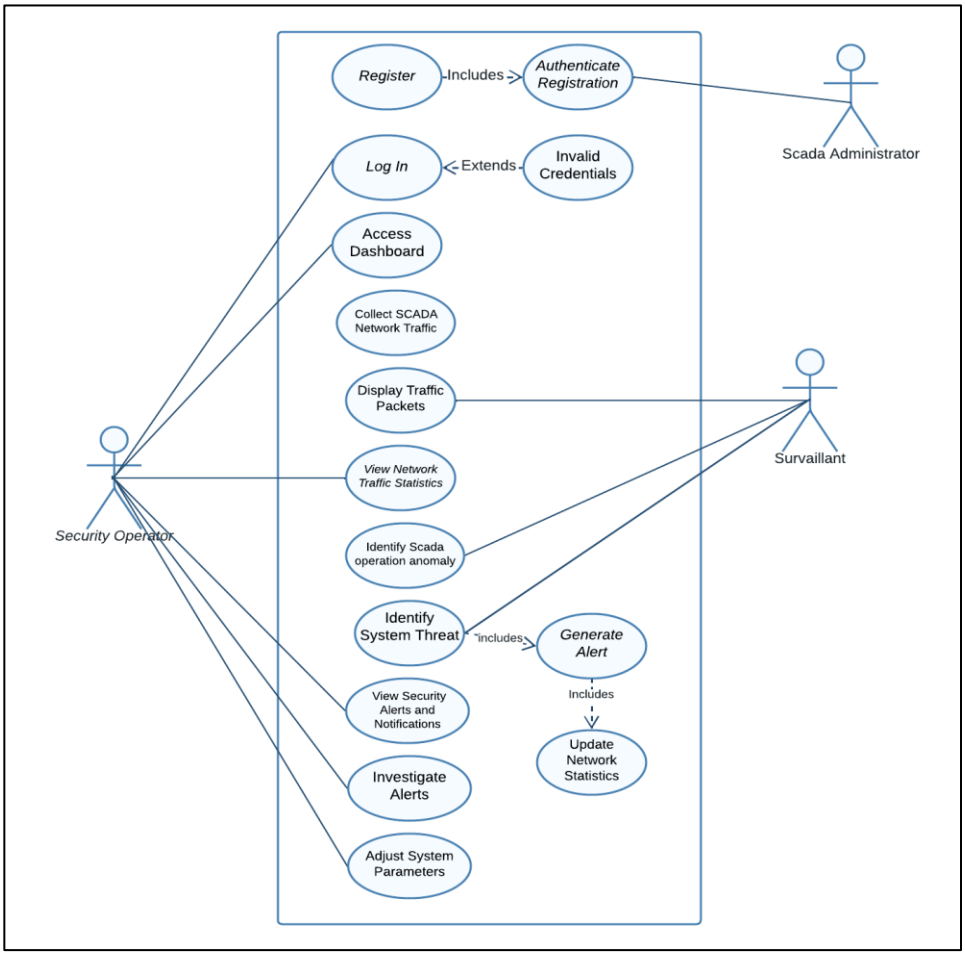

Figure 3: Use Case Diagram - Security Operator

2.3.3 Auditors

Auditors specializing in SCADA, whether internal or external, have limited access to Survaillant for evaluating the security and compliance of Survaillant.

2.4 Operating Environment

The App shall be compatible with the following operating environments:

- Platform: React
- Machine learning platforms: TensorFlow and scikit-learn
- Programming language: python

2.5 Design and Implementation Constraints

- The application must adhere to NIST guidelines and industry approved safety standards such as IEC 61508 and IEC 62443.
- Traffic monitoring should include the communication protocols unique to the SCADA network including modbus and dnp3 in addition to TCP/IP protocols.
- It must operate at the network layer of the TCP/IP stack.
- It must be resource-conscious to prevent any performance degradation in the SCADA systems it monitors.
- The GUI must be user-friendly to be easily understood by the SCADA administrators and display network traffic statistics in the form of charts and graphics.
- The customer's organization will be responsible for maintaining the delivered software. Therefore, the software should be designed with a focus on ease of maintenance, updates, and troubleshooting.
- The software may require additional computational resources for the training of machine learning models, potentially requiring dedicated graphics processing units (GPUs) or server-grade hardware to meet the processing demands.
- The system will use python libraries for its backend development. The web-based frontend will be developed using React.

2.6 User Documentation

As the user interface is extremely easy to understand, user documentation is deemed not necessary, but it shall be prepared if needed be based on the feedback from the users. Complete Software Requirements Specification will be provided.

2.7 Assumptions and Dependencies

- Historical network traffic data required for machine learning model training is of sufficient quality and quantity. The accuracy and volume of this data will significantly impact the effectiveness of Survaillant.

- The first version of Survaillant can be easily integrated with the SCADA systems used in the electrical grids.
- Survaillant's design and operation complies with the current industry-specific regulations and standards in 2023-2024. Any changes in regulatory requirements may necessitate software modifications.
- Survaillant's design and operation complies with the current NIST security guidelines in 2023-2024. Any changes in these security guidelines may necessitate software modifications.
- Python libraries will be used for machine learning and model training.
- The user will know how to respond to a particular alert generated by the system.
- Survaillant can scale to accommodate larger SCADA networks and increasing data volumes by training the software on the particular larger dataset. Scalability challenges may arise if the software is deployed in significantly larger environments.

3. External Interface Requirements

3.1 User Interfaces

3.1.1 Landing Page (Common to All users)

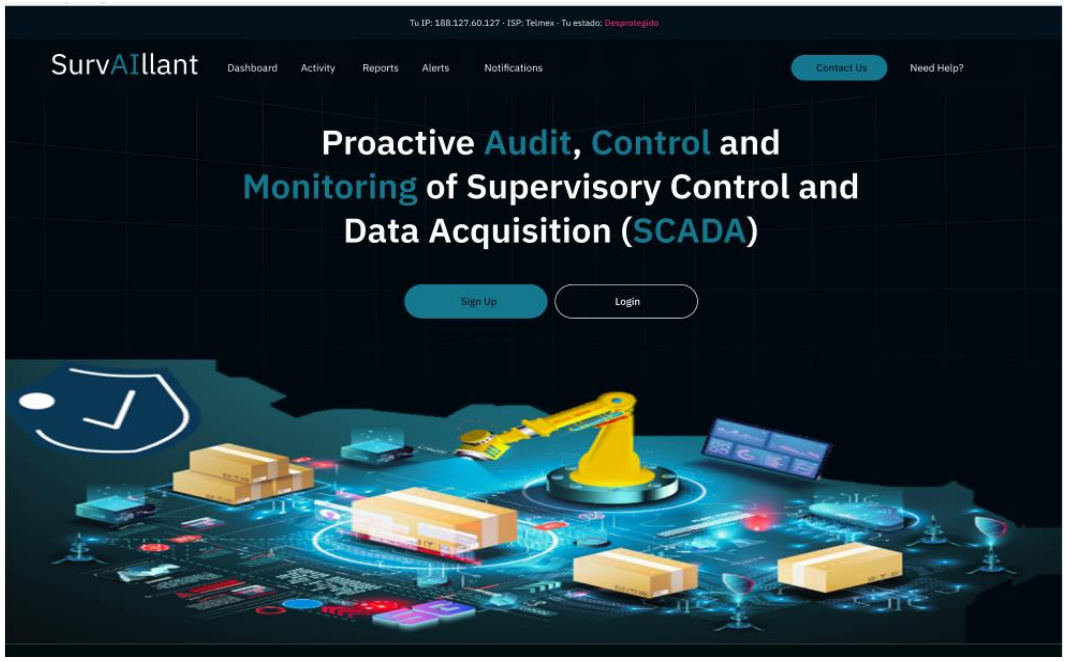

Figure 4: Survaillant Landing Page

3.1.2 User Registration

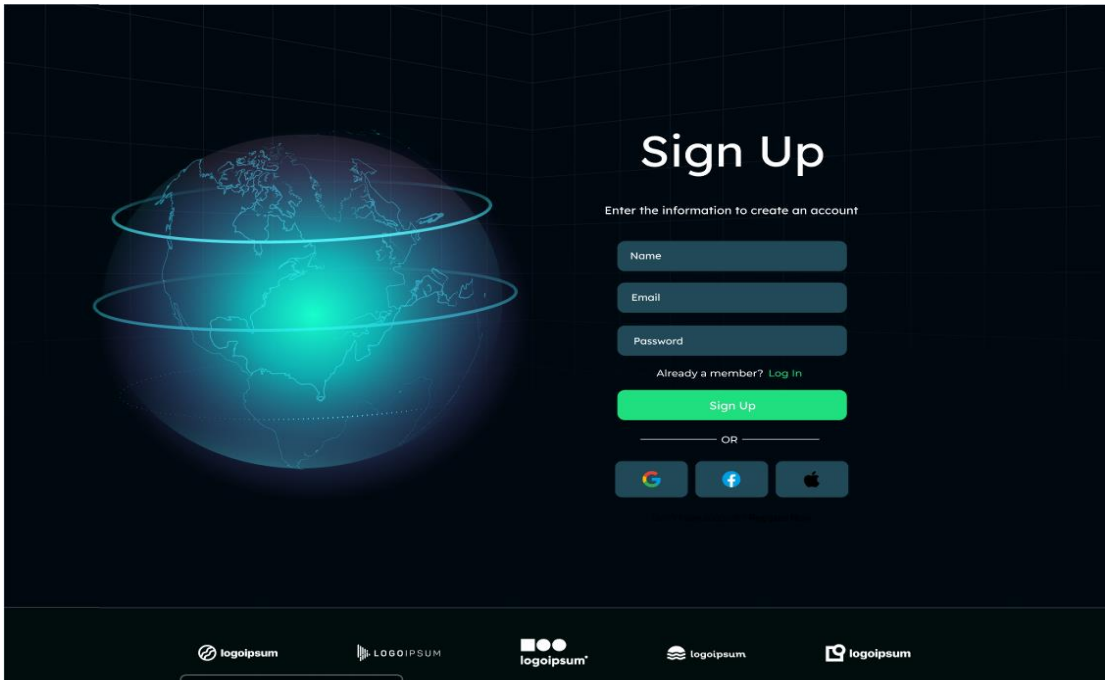

Figure 5: Survaillant Sign up

3.1.3: Logging in

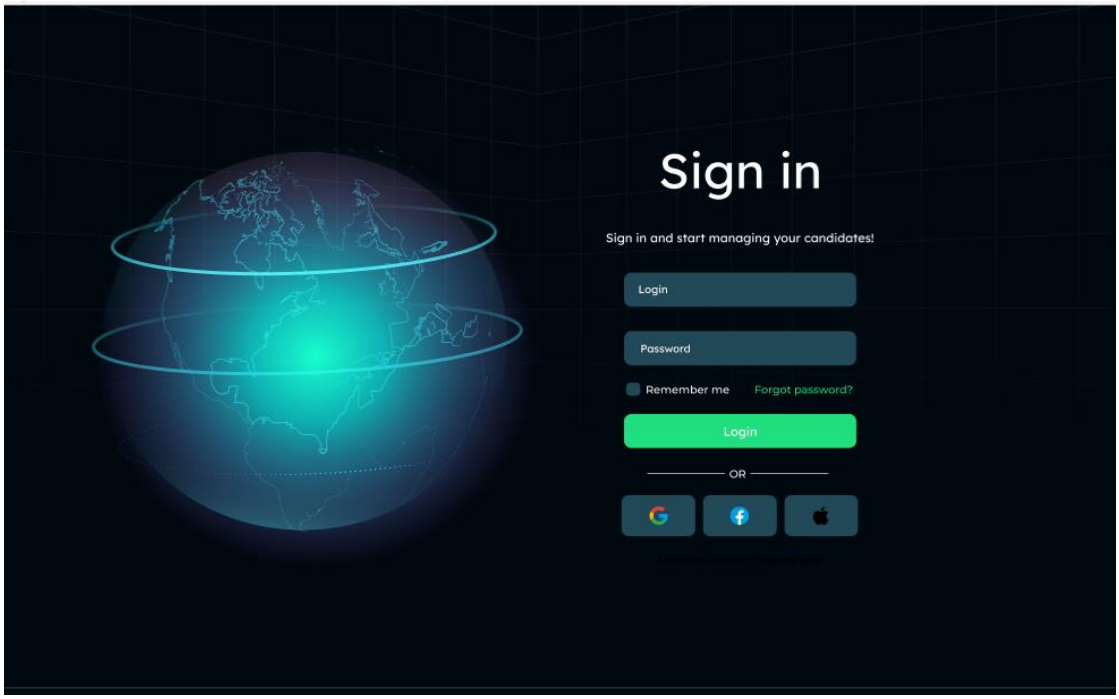

Figure 6: Survaillant Login

3.1.4: Dashboard

Figure 7: Survaillant user Dashboard

3.1.5: Network Traffic Activity

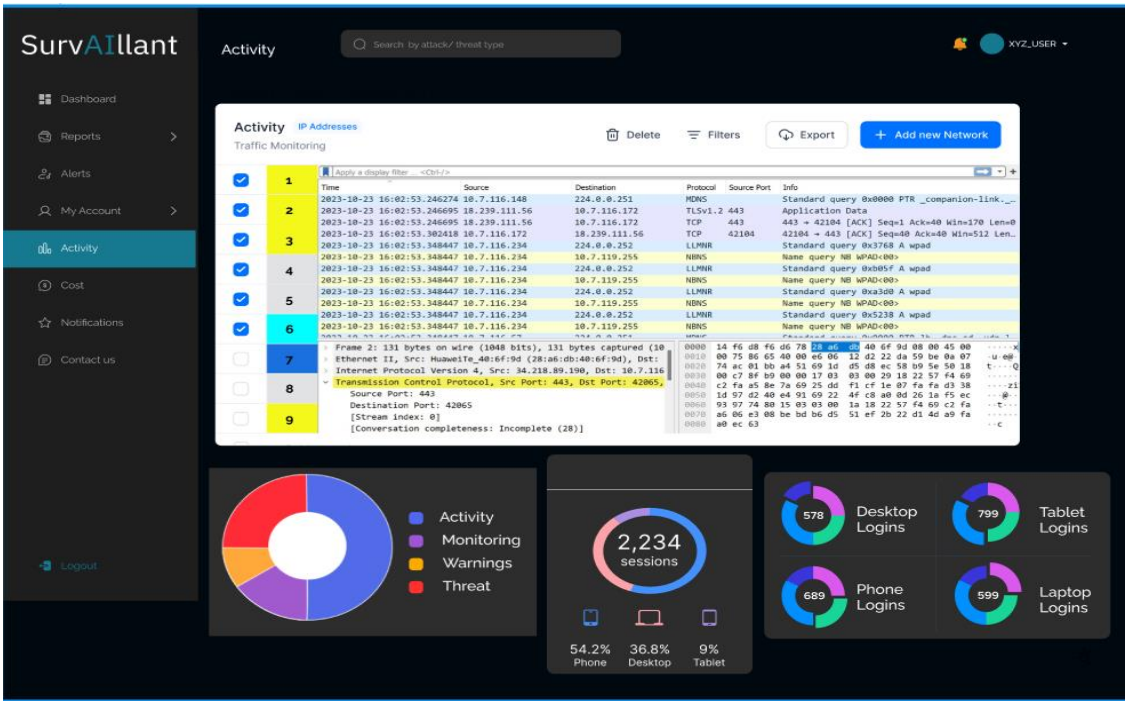

Figure 8: Survaillant Network Traffic Activity

3.2 Hardware Interfaces

Survaillant is hosted on the web server and is accessed over https. The interface from web-based Survaillant is directly to the SCADA server located in the operating control room and is implemented via a REST API. Using the Rest API will allow for the bi-directional flow of alerts from Survaillant to SCADA and the network traffic from SCADA to Survaillant. Survaillant may utilize data storage devices such as hard drives, SSDs, or cloud-based storage solutions for storing the network traffic data and historical event logs.

3.3 Software Interfaces

Survaillant is a web-based security application and is supported on standard web browsers including Google Chrome, Mozilla Firefox and Microsoft Edge. Only computers in the SCADA Security Operations Center can access the web-based software; mobile access is restricted due to security permissions. It uses MySQL as its database to store event log data and uses python's machine learning libraries TensorFlow, scikit-learn and PyTorch to implement machine learning algorithms. The user interfacing of Survaillant is done through Node.js.

3.4 Communications Interfaces

Data transfer over the internet will primarily utilize standard communication protocols HTTPS over the TCP/IP stack. The communication amongst the SCADA devices will be through the modbus/tcp protocol.

4. System Features

4.1 User Authentication and Access Control

4.1.1 Description and Priority

This feature ensures that only the authorized and registered users have access to the Survaillant system. User authentication adds a layer of security and control to the application. This is a high priority task because only the higher managers and security operators should be allowed to manage the security alerts.

4.1.2 Stimulus/Response Sequences

1. Stimulus: A user attempts to register to gain access the Survaillant system. Response: The system prompts the user to enter valid credentials, including username and password. This information is sent to the admin panel for approval.

2. Stimulus: An administrator attempts to grant, revoke aur update user access. Response: The system allows the admin to manage user access privileges.

3. Stimulus: After successful registration, the user attempts to access Survaillant. Response: The system prompts the user to enter valid credentials, including username and password. On providing correct credentials stored in the database, the user gains access to the system.

4.1.3 Functional Requirements

REQ-1: The app will prompt user to choose between “Register” and “Login”.
REQ-2: The system must implement a secure user authentication mechanism, including username and password validation.
REQ-3: Password policies, such as complexity requirements and expiration, should be enforced.
REQ-4: When logging in, the app will verify entered credentials against database and display error message if invalid; otherwise, will navigate to the dashboard.
REQ-5: Failed login attempts should be logged, and account lockout mechanisms should be in place to prevent brute force attacks.
REQ-6: Maximum of three login attempts should be allowed after which the account should be locked.
REQ-7: Users must have the ability to reset their passwords through a secure process in case they forget their credentials.

REQ-8: Administrators should be able to manage user roles and permissions, including creating, updating, and deleting user accounts.

REQ-9: Any user (other than admin) is only granted access to Survaillant dashboard once the access is granted by the administrator and user is registered.

REQ-10: The system should restrict access to sensitive functions, data, and settings based on user roles and permissions.

4.2 Network Traffic Monitoring

4.2.1 Description and Priority

Feature Priority: High

This feature continuously monitors and analyzes the SCADA network traffic data to identify abnormal patterns or behaviours. This is a high priority feature since each and every packet has to pass through this procedure to ensure it does not harm SCADA procedures.

4.2.2 Stimulus/Response Sequences

Stimulus: The system captures traffic data from the SCADA system and processes it. Response: The pre-trained models of Survaillant analyze each packet and the traffic statistics are displayed on the dashboard.

4.2.3 Functional Requirements

REQ-1: The system must capture network traffic data from SCADA devices and network communication.

REQ-2: The system must support the capture of network traffic from a variety of SCADA communication protocols, including Modbus TCP, DNP3, and IEC 60870-5-104.

REQ-3: Network traffic data must be stored securely for analysis and classification.

REQ-4: Advanced algorithms must be used to detect suspicious or anomalous network patterns, including potential cyberattacks.

REQ-5: Users must be able to access historical network traffic data for analysis purposes.

4.3 Anomaly Detection and Alerting

4.3.1 Description and Priority

Feature Priority: High

Anomaly detection enables Survaillant to detect anomalies in the normal operation in SCADA and promptly alert relevant personnel to potential security threats. These anomalies are usually produced due to unintentional threats including human error, environmental hazards, and hardware/software failures. This is a high priority task to ensure a proactive approach to security by identifying potential threats before they cause significant harm to key infrastructures.

4.3.2 Stimulus/Response Sequences

1. Stimulus: The system continuously monitors SCADA network traffic and uses machine learning algorithms to classify traffic as normal or abnormal. Response: If any deviation is detected from the pre-defined sensor values and system behavior, it is regarded as anomalous behavior and an alert is generated.

2. Stimulus: A user reviews the generated alerts in the Survaillant interface. Response: The system displays detailed information about the alert so user can take the appropriate action.

4.3.3 Functional Requirements

REQ-1: The system must learn the ‘normal’ traffic characteristics using the elegant machine learning algorithms.

REQ-2: If an anomaly is detected, the system must promptly generate an alert, specifying the nature and severity of the anomaly.

REQ-3: The system should log all anomaly alert-related activities, including user actions, comments, and status changes.

REQ-4: The system should be able to accurately catch anomalous behaviour keeping false positives to a minimum.

REQ-5: The system should be able to learn and adapt to new types of anomalies as they emerge, continuously improving its detection capabilities.

REQ-6: The system should be able to update charts and graphs summarizing the overall security posture, including the number of detected anomalies, their distribution by severity, and the response times to alerts.

4.4 Security Threat Detection

4.4.1 Description and Priority

Feature Priority: High

This feature enables Survaillant to identify and respond to security threats in SCADA systems to protect critical infrastructure from potential outsider attacks. This is a high priority feature because the system must be able to identify intentional attacks.

4.4.2 Stimulus/Response Sequences

1. Stimulus: The system continuously monitors SCADA network traffic and tries to identify the traffic as normal or malicious. Response: if the system identifies a particular packet as malicious or if a particular traffic stream signifies a security attack, the system generates alerts and blocks the affected packets.

2. Stimulus: A user reviews the generated alerts in the Survaillant interface. Response: The system displays detailed information about the alert so user can take the appropriate action.

4.4.3 Functional Requirements

REQ-1: The system must employ advanced security threat detection mechanisms based on machine learning algorithms.

REQ-2: If a threat is detected, the system must promptly generate an alert, specifying the nature and severity of the threat.

REQ-3: Security threat detection should cover various types of attacks, including unauthorized access, DOS, malware, and data breaches.

REQ-4: Detected security threats must be categorized by severity, enabling users to prioritize incident response.

REQ-5: Users with appropriate privileges must have the ability to access detailed threat information, including affected devices and potential vulnerabilities.

REQ-6: The system should be able to distinguish between legitimate network traffic and potential threats, minimizing false positives in alert generation.

4.5 Notification System

4.5.1 Description and Priority

Feature Priority: Medium

Survaillant notifies relevant personnel and stakeholders about critical events and alerts in real-time.

4.5.2 Stimulus/Response Sequences

1. Stimulus: A critical security alert is generated by the system. Response: The software sends notifications to authorized users and security personnel.

2. Stimulus: Aadministrator configures the notification preferences in the Survaillant interface. Response: The system acknowledges the user's preferences and delivers notifications accordingly.

4.5.3 Functional Requirements

REQ-1: The system must generate notifications according to the severity of the generated alerts.

REQ-2: Survaillant must offer a user-friendly dashboard for different user roles, including security operators, administrators, and managers.

REQ-3: Users should be able to specify their preferred notification channels and settings, including time windows for alerts and escalation paths for unacknowledged alerts.

REQ-4: The system must ensure the secure and reliable delivery of notifications to the intended recipients.

REQ-5: It should offer the capability to group users into roles, allowing notifications to be sent to specific groups based on the nature and severity of alerts.

REQ-6: The system must provide alert acknowledgment mechanisms, allowing users to confirm their awareness of critical alerts.

REQ-7: In cases of unacknowledged alerts, the system should escalate notifications to higher levels of authority or additional personnel.

REQ-8: The system must maintain a trail of all notifications sent, received, acknowledged, and escalated for auditing purposes.

REQ-9: Notifications should include detailed information about the alert, including the source, nature, and severity of the detected threat.

REQ-10: The system should categorize the alerts based on their severity level. Alerts can be categorized as "critical," "major," "minor," or other predefined severity levels.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

5.1.1: The system should be able to analyze SCADA traffic and detect anomalies just-in-time, ensuring a prompt response to potential security incidents.

5.1.2: It should handle an increasing number of connected devices and data points without a significant degradation in performance. It must support at least 30 devices simultaneously.

5.1.3: It should generate alerts and notifications within 1 second of detecting a security incident.

5.1.4: It should exhibit a high level of accuracy in identifying security threats and anomalies within the SCADA network to minimize false positives and negatives

5.1.5: Survaillant should allow the administrator to easily customize of security rules and policies, to meet the specific security needs of different SCADA environments.

5.2 Safety Requirements

5.2.1: The system must ensure the integrity of critical SCADA data, preventing unauthorized access, tampering or manipulation of data.

5.2.2: Survaillant must adhere to industry approved safety standards such as IEC 61508 and IEC 62443 to mitigate risks and protect against potential harm.

5.2.3: Its operation does not compromise sensitive information within the SCADA systems it monitors.

5.2.4: It must be efficient enough to keep false positives at a minimum, reducing the likelihood of unnecessary system disruptions due to incorrect anomaly detection.

5.2.5: Prior to using it, the users must understand how to operate the software effectively, reducing the risk of misconfiguration or misuse that could compromise SCADA safety.

5.3 Security Requirements

5.3.1: The system should implement strong user identity authentication, allowing only the registered users to access the system.

5.3.2: Survaillant must comply with relevant regulations and industry standards such as NIST SP 800-82, IEC 62443, and ISA/IEC 62443 to ensure data security.

5.3.3: The administrators will be required to change passwords every month to ensure compliance to the CIA triad**.**

5.3.4: Survaillant should provide role-based access control to limit access to authorized personnel and features.

5.4 Software Quality Attributes

5.4.1: The system should have an uptime of at least 98% and should be able to recover from failures automatically.

5.4.2: The codebase should follow best practices for coding and documentation, making it easy for future developers to maintain and update the system.

5.4.3: The user interface should be intuitive, with a low learning curve for administrators and operators.

5.4.4: The system should be available 24/7 to guarantee uninterrupted protection with minimal downtime.

5.5 Business Rules

5.5.1: the software must undergo regular updates and patches to address security vulnerabilities and maintain its effectiveness against evolving threats.

5.5.2: Changes to the system, including configurations and rule updates, should follow a documented change management process and require approvals from designated personnel.

5.5.3: Users should adhere to security protocols and report any suspicious activity promptly to maintain system integrity

6. Other Requirements

TBD

Appendix A: Glossary

SCADA: Supervisory Control and Data Acquisition
AI: Artificial Intelligence
IEEE: Institute of Electric and Electronic Engineers
SRS: Software Requirements Document
NIST: National Institute of Standards and Technology
ICS: Industrial Control System
RTU: Remote Terminal Unit
HMI: Human Machine Interface

GUI: Graphical User Interface
GPU: Graphics Processing Unit
API: Application Programming Interface
SSD: Solid State Drive