RBAT

شراكة بين شركة برزان القابضة وشركة راينميتال

A BARZAN HOLDINGS AND RHEINMETALL JOINT VENTURE

# BARZAN C2 (A Barzan Holdings Product)

## V2.12.1

### Security Target V.2.5

**Document History**

| Version | Description | Date | Author |
|---|---|---|---|
| 0.1 | First Draft | 14/07/2025 | Ramzan Zafar |
| 0.2 | ST document update | 27/07/2025 | Ramzan Zafar |
| 0.3 | ST document update | 03/08/2025 | Ramzan Zafar |
| 0.4 | ST document update | 12/08/2025 | Ramzan Zafar |
| 0.5 | ST document update | 18/08/2025 | Ramzan Zafar |
| 0.6 | ST updated based on evaluator feedback | 20/08/2025 | Ramzan Zafar |
| 0.7 | ST updated based on evaluator feedback | 21/08/2025 | Ramzan Zafar |
| 0.8 | ST updated based on evaluator feedback | 24/08/2025 | Ramzan Zafar |
| 0.9 | ST updated based on evaluator feedback | 10/09/2025 | Ramzan Zafar |
| 1.0 | ST updated based on evaluator feedback | 22/09/2025 | Ramzan Zafar |
| 1.1 | ST updated based on evaluator feedback | 25/09/2025 | Ramzan Zafar |
| 1.2 | ST updated based on evaluator feedback | 30/09/2025 | Ramzan Zafar |
| 1.3 | ST updated based on evaluator feedback | 06/10/2025 | Ramzan Zafar |
| 1.4 | Updates related to External communication | 13/10/2025 | Ramzan Zafar |
| 1.5 | Updated as per the feedback. | 16/10/2025 | Ramzan Zafar |
| 1.6 | Added communication protection in backend | 20/10/2025 | Ramzan Zafar |
| 1.7 | Updated audit log from FDP_ACF1 | 30/10/2025 | Ramzan Zafar |
| 1.8 | NCSA feedback | 09/11/2025 | Ramzan Zafar |
| 1.9 | NCSA and Beem feedback | 27/11/2025 | Ramzan Zafar |
| 2.0 | Certification body feedback fixes | 01/12/2025 | Ramzan Zafar |
| 2.1 | ASE-GR08 | 02/12/2025 | Ramzan Zafar |
| 2.2 | GR09 | 03/12/2025 | Ramzan Zafar |
| 2.3 | ASE-GR08 updates | 11/12/2025 | Ramzan Zafar |
| 2.4 | GR11 Updates for TLS | 24/12/2025 | Ramzan Zafar |
| 2.5 | GR15 Updates | 29/12/2025 | Ramzan Zafar |

# Table of Contents

# 1 INTRODUCTION

## 1.1 REFERENCES

| | |
|---|---|
| **ST Title** | Barzan C2 (A Barzan Holdings Product) Security Target |
| **ST Version** | V.2.5 |
| **TOE Title** | Barzan C2 (A Barzan Holdings Product**)** |
| **TOE Version** | V2.12.1 |
| **Assurance Level** | EAL2 |
| **CC Identification** | • Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2022<br>• Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 2022<br>• Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 2022<br>• Common Methodology for Information Technology Security Evaluation (CEM), Version 2022 |

*Table 1: ST and TOE References*

## 1.2 TOE OVERVIEW

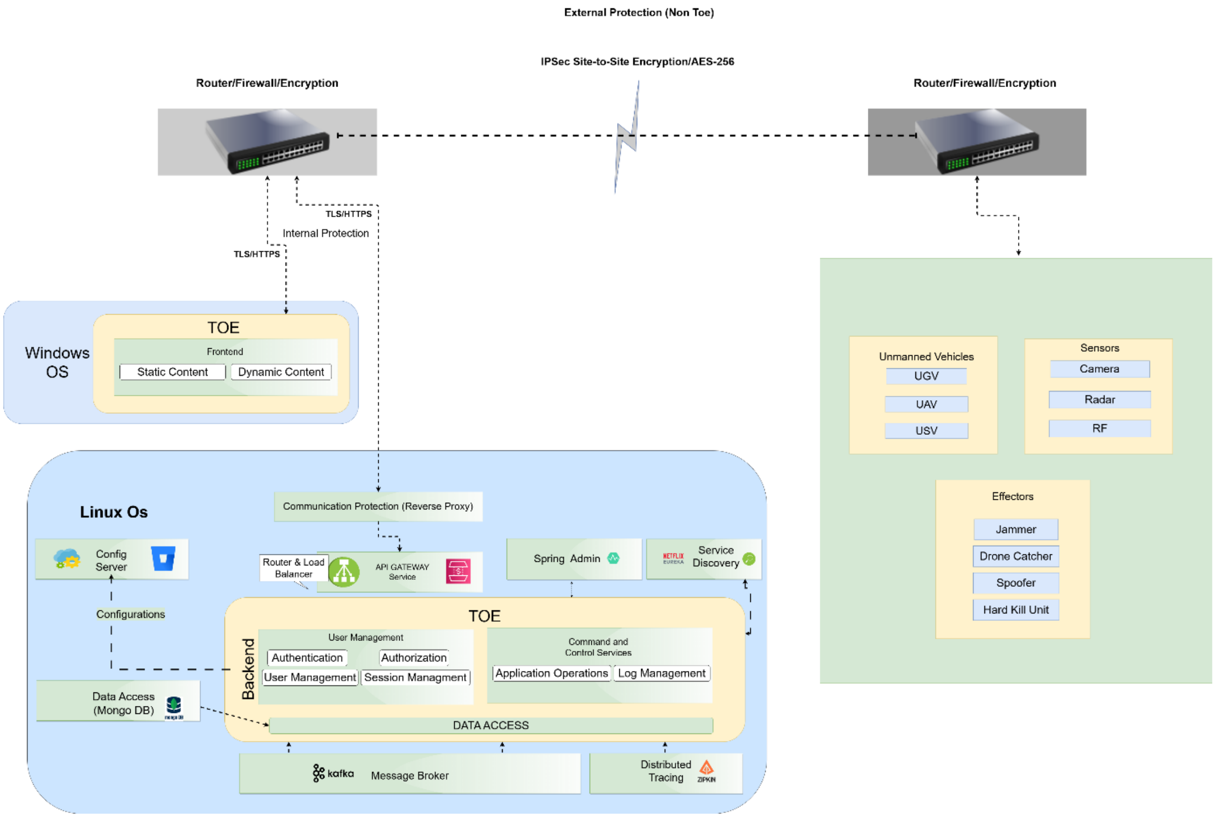
### 1.2.1 TOE USAGE AND SECURITY FEATURE

Barzan-C2 is Command and Control (C2) software designed to empower users with intuitive and secure tools to plan, execute and monitor operations. It comprises two core components:

- **User Workstations**: Running on Windows, these provide the C2 Front-End application, offering GUIs and video streaming clients. Operators can easily interact with the system to monitor real-time data, view video feeds, and manage operations efficiently.

**Back-End Server:** Hosted on Linux with Docker and Spring Cloud containerization, this component supports critical services, including User Management, which handles authentication, authorization, and session management to enforce secure access control, Log services, which generate and store logs of operational commands, security events, and system configuration changes, ensuring accountability and traceability of all system activities, and Command and Control services, which manage the orchestration of sensors and effectors to enable coordinated and reliable system operations. Together, these services ensure scalable performance and secure, mission-critical functionality.

Barzan-C2 equips users with essential C2 capabilities, such as real-time situational awareness, sensors and effectors management, decision support, track management, GIS capabilities, Surveillance management, zone and alarm management, video recording/replay, post-incident analysis, device/unit management, and user management, enabling effective and secure operations.



Major security features of the TOE are listed below:

## Security Audit

The TSF maintains comprehensive security audit logs in accordance with FAU_GEN.1 and FAU_GEN.2. Audit data cover security-relevant events (authentication attempts, access control decisions, management actions) as well as critical operational events.

The audit log records date/time, event type, subject identity, source IP address, object involved, and the outcome of each auditable event. This ensures complete traceability of both application-level and security-relevant activities.

### Protection of Security Functionality

The TSF ensures the confidentiality, integrity, and availability of critical Command and Control functions. It protects against unauthorized access, disclosure, or modification of mission-critical operations, operational commands, and security parameters. TSF enforces strict access control mechanisms to ensure that only authorized administrators and operators can interact with sensitive functions, thereby preventing compromise of confidential data or unauthorized execution of security-relevant actions. In addition, the TOE safeguards these functions from tampering or disruption, ensuring continuous and reliable system operations.

### User Data Protection

TSF safeguards sensitive data, operational parameters, and classified information through robust access control mechanisms. Access to data and functions is permitted only to users with an **authorized role** (Administrator, Operator, or custom-defined roles). This ensures that each user can access only the data and operations explicitly permitted under their assigned role, preventing unauthorized disclosure or misuse of operational information.

### Identification and Authentication

The system requires authentications for all users accessing Command and Control functions. Authentication includes username/password verification and role-based access tokens. Only **authenticated users with the appropriate authorized role** can issue commands and access mission-critical data. This ensures that commands and sensitive data access are restricted to users explicitly granted the necessary operational or administrative roles.

### Security Management

Authorized administrators can manage **user accounts and roles**, assign and revoke operational roles, configure system parameters, and maintain security policies. This includes creating, modifying, or deleting user accounts, adjusting roles (Administrator, Operator, or custom-defined roles), and enforcing security policies across the TOE. These capabilities ensure that access to security-relevant functions is restricted to authorized users only, in accordance with organizational policy.

### TOE Access

TSF enforces strict controls on user access to the TOE by implementing robust session management functions.

- **Session Termination:** The TOE automatically terminates inactive user sessions after a configurable period of inactivity, with 15 minutes set as the default value. Administrators may adjust this timeout parameter through the management interface

according to organizational security requirements.
Users may also manually terminate their own sessions at any time.

- **Disabled Accounts:** Session establishment is denied for accounts that have been disabled by an administrator. Once disabled, a user cannot authenticate or access the system until explicitly re-enabled.
- **Concurrent Session Limit:** Each user is limited to a maximum of one concurrent session. This ensures that users cannot bypass security restrictions by opening multiple sessions simultaneously.
- **Administrator Control:** In cases where an account is locked due to repeated authentication failures, only an authorized administrator can re-enable access.

**Trusted Path / Trusted Channel:**
The TOE establishes trusted communication channels between its internal components (Frontend ↔ Backend) using TLS 1.3 to ensure the confidentiality and integrity of TSF data. Communication between the Backend and the Database (MongoDB) is also secured through TLS 1.2 connections configured and managed by the TOE itself, providing authenticated and encrypted communication between these trusted IT products.

Consequently, **the TOE is responsible for securing internal communications (covered by FPT_ITT.1)**, while **the trusted channel between the TOE and the database is covered by FTP_ITC.1**.
Protection of external communications with components such as sensors and effectors is ensured by the **operational environment**.

These combined protections ensure that all TSF data exchanged within the TOE and with trusted internal IT products remain confidential, integral, and protected from unauthorized disclosure or modification during transmission.

### 1.2.2 TOE TYPE

Barzan-C2 is Command and Control (C2) software designed to provide robust and secure operations against threats. The system is structured into two primary components: User Workstations and Back-End Server, each tailored to deliver specific functionalities for user.

The User Workstations component is hosted on the Windows operating system. It delivers C2 Front-End (FE) application, which is equipped with user-friendly graphical user interfaces (GUIs) and video streaming clients. This setup ensures seamless interaction for operators, enabling efficient access to critical system features and real-time video feeds.

The Back-End Server component operates on the Linux operating system and leverages Docker and Spring Cloud containerization technologies. This component hosts a suite of services, including Business modules, SEMS modules, Communication Gateway, Map Engine, Database, and Video Streaming module. The containerized architecture facilitates efficient distribution and management of these services across multiple containers, ensuring scalability and reliability.

Barzan-C2 supports a comprehensive set of secure Command and Control capabilities tailored for users. These include situational awareness, decision-making support and tracks management. The system also enables identification of friendly or foe entities, camera-based identification with visual auto-tracking, control, and display.

Further enhancing its functionality, Barzan-C2 provides zone and alarm management, video recording and replay, post-incident management, device and unit management, and user management. These features collectively ensure a robust and secure operational environment for countering threats and surveillance.

### 1.2.3 FIRMWARE/HARDWARE/SOFTWARE REQUIRED BY TOE

The TOE requires distributed architecture with backend server, user workstations, and communication infrastructure. The system operates through secure communication channels to send commands to backend and requires specialized hardware for operations.

**Barzan C2 Backend Requirements:**

| **Type** | **Details** |
|---|---|
| OS | Ubuntu Server 22.04 LTS or latest |
| Web Server | Embedded Jetty Server 12.0 |
| Database | Mongo DB 8.0 |
| Processor | INTEL CORE I9-13900K |
| RAM | 256 GB (DDR5 5GHz) or more |
| Hard Drive | 12TB or more |
| Graphics | Nvidia Quadro RTX4000 8GB |
| SSD | 1TB NVMe or more |
| Container Runtime | Docker Engine 26 |
| Spring Cloud | 2024.0.0 |

**TOE User Workstation Requirements:**

| **Type** | **Details** |
|---|---|
| OS | Windows 10 Pro |
| Environment | Electron 27.3.11<br>Node JS 18.17.1 |
| Processor | INTEL CORE I7 -12700KF |
| RAM | 32GB or more |
| Hard Drive | 2TB or more |
| Graphics | RTX 4070 |
| SSD | 1TB SSD or more |

*Table 2: TOE Operational Environment*

## 1.3 TOE DESCRIPTION

### 1.3.1 PHYSICAL SCOPE OF TOE

Barzan C2 operates as a distributed command and control system consisting of multiple interconnected components. The TOE is delivered in person on a secure storage device by RBAT trusted personnel. A tamper-evident label is affixed to the package to prevent manual intervention and indicates that the product has not been tampered with.

#### *1.3.1.1 Software Components:*

- **Barzan C2 Backend v1.0**
- **Barzan C2 Frontend v1.0**

#### *1.3.1.2 Guidance Documents:*

- **Barzan C2 User Manual v.1.1**

#### *1.3.1.3 NON-TOE Components:*

- Integrated 3rd Party Hardware and Software (Sensor & Effectors) and related communication infrastructure
- Data storage hardware systems
- Network/firewall infrastructure provided by the operational environment.

### 1.3.2 LOGICAL SCOPE OF TOE

The logical scope of the TOE encompasses the following security functionality:

**Security Audit:** The TSF generates comprehensive audit logs for all Command and Control operations, including operational commands, operator actions, and security events. Audit data include timestamps, operator identification, command details, and execution results as specified in **FAU_GEN.1**.

**Protection of Security Functionality:** The TOE ensures the integrity and protection of Command and Control functions through secure internal data transfer mechanisms in accordance with **FPT_ITT.1** and **FTP_ITC.1**.
**FPT_ITT.1** protects TSF data from disclosure and modification when transmitted between separate parts of the TOE (for example, Frontend ↔ Backend).
**FTP_ITC.1** applies to the trusted channel established between the TOE and another trusted IT product—specifically, the connection between the Backend and the Database (MongoDB)—which is protected through TLS 1.2 to ensure confidentiality, integrity, and endpoint authentication.

Protection of communication with **external systems** (such as sensors and effectors) is provided by the **operational environment**, which establishes site-to-site IPsec tunnels or equivalent mechanisms.
This layered approach ensures that both internal and trusted inter-component communications are protected by the TOE, while external links remain securely managed by the operational environment.

**User Data Protection:** TSF implements a role-based access control (RBAC) model. System Administrator and Operator are default roles, but administrators may define additional roles. Access is granted based on operator levels and operational roles as defined in FDP_ACC.1 and FDP_ACF.1.

**Identification and Authentication:** The system requires authentications for all the users to access the system. TSF maintains comprehensive user attributes including operational roles (FIA_ATD.1). Authentication failures are handled according to FIA_AFL.1, with automatic account lockout after multiple failed attempts Additionally, the TSF enforces password complexity requirements through FIA_SOS.1, ensuring that secrets conform to defined organizational policies for length and character composition.

**Security Management:** Authorized administrators can manage operator privileges, assign roles, configure parameters, and maintain security policies through the management interface (FMT_MSA.1, FMT_SMF.1). The TSF enforces role-based access control through hierarchical roles, including System Administrator and Operator, in accordance with FMT_SMR.1. Additionally, FMT_MSA.3 ensures that default values for security attributes are restrictive by design, reducing the attack surface during object creation. Administrators may override these defaults as required for operational needs.

**TOE Access:** The TOE enforces secure session management through both TSF-initiated and user-initiated termination mechanisms. In accordance with **FTA_SSL.3**, the TOE automatically terminates inactive user sessions after a configurable timeout period (default 15 minutes) to prevent unauthorized access from unattended terminals. Consistent with **FTA_SSL.4**, users may also manually terminate their own sessions. When the period of inactivity exceeds 15 minutes, the TOE automatically logs out the user and redirects them to the login page.
In addition, the TOE enforces session control by denying session establishment for disabled user accounts and limiting each user to a single concurrent session. This ensures that user sessions are actively managed and prevents users from bypassing access restrictions by maintaining multiple simultaneous sessions. Re-authentication requires administrator intervention, ensuring controlled restoration of access.

**Trusted Path / Communication Protection:** The TOE protects internal communications between its distributed components (Frontend ↔ Backend) through **TLS 1.3**, satisfying **FPT_ITT.1**, which ensures confidentiality and integrity of TSF data exchanged within the TOE.
Communication between the Backend and the Database (MongoDB) is secured by the TOE using **TLS 1.2**, fulfilling **FTP_ITC.1** requirements for a trusted channel with another trusted IT product.

Protection of communication with **external entities—**including sensors, effectors, and third-party subsystems—is outside the TOE boundary and is ensured by the **operational environment** through IPsec tunnels or equivalent network security mechanisms.

These combined measures guarantee secure transmission of TSF data within the TOE boundary and over trusted channels, while external link protection is maintained by the operational environment.

# 2 CONFORMANCE CLAIM

The TOE does not claim conformance to any predefined functional packages.

## 2.1 CC CONFORMANCE CLAIM

This ST claims conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 2022, *Conformant*
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 2022, *Conformant*
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 2022, *Conformant*

The Common Methodology for Information Technology Security Evaluation, Version 2022 must be considered.

## 2.2 PP CLAIM

This ST does not claim conformance to any protection profile.

## 2.3 PACKAGE CLAIM

Evaluation Assurance Level is EAL2.

# 3 SECURITY PROBLEM DEFINITION

## 3.1 ASSUMPTIONS

The assumptions are described below.

**A.PROTECT** It is assumed that all hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secure data. Each of these appliance configurations is securely managed by administrators to provide protection of secure data in terms of its confidentiality and integrity.

**A.PHYSICAL** It is assumed that the TOE's hosting environment is physically protected against unauthorized access.

**A.TIME** It is assumed that the TOE can access a reliable time source for accurate timestamping of events.

**A.ADMIN_TRUST**

The Linux system administrator responsible for managing the underlying server infrastructure on which the TOE is deployed is assumed to be trustworthy and properly trained. The administrator will not attempt to compromise the security of the TOE and will follow all documented operational procedures.

**A.CERT_TRUST**

The TOE uses a self-signed TLS certificate for securing communications between the Frontend and Backend components. It is assumed that the self-signed certificate used by the Backend server is installed in the trusted certificate store of all client workstations on which the Frontend application will run. This ensures that clients can validate the authenticity of the Backend server and prevent man-in-the-middle (MITM) attacks during TLS connection establishment.

## 3.2 THREATS

The threat agents are described below.

- Attackers who have knowledge of how the TOE operates and are assumed to possess a basic skill level and intend to alter TOE configuration settings/parameters and no physical access to the TOE.
- TOE users who have extensive knowledge about the TOE operations and are assumed to have a high skill level, moderate resources to alter TOE configuration settings/parameters and physical access to the TOE.

The TOE address the following threats are applicable listed in table below.

**T.UNAUTH (Attacker):** An unauthorized user may attempt to gain access to the TOE to view sensitive information, execute commands, or disrupt C2 operations.

- **Assets:** TOE resources, mission-critical data, operational commands.
- **Adverse Action:** Unauthorized access, disclosure, modification, or disruption.

**T.DoS (Attacker): An** attacker may attempt to disrupt system availability through network attacks, resource exhaustion, or system overload.

- **Assets:** TOE availability and system resources.
- **Adverse Action:** Service disruption and denial of legitimate access.

**T.PRIVIL_ESC (TOE user):** An authorized user may attempt to exceed their authorized privileges or misuse legitimate access to compromise system security.

- **Assets:** User roles, access control mechanisms, system configuration.
- **Adverse Action:** Privilege escalation, unauthorized system changes.

**T.CHANNEL (Attacker):** An attacker may attempt to intercept, sniff, or tamper with communications between frontend and backend components.

- **Assets:** Data in transit between TOE components
- **Adverse Action:** Interception, modification, or replay of communications.

**T.BRUTE (Attacker):** An Attacker may repeatedly try to guess authentication data to use this information to launch attacks on the TOE

- **Assets:** User credentials.
- **Adverse Action:** Credential compromise through brute force.

**T.MISCONFIG (TOE User)**: An unauthorized or inadequately authorized user may change security configurations, disable protections, or introduce insecure settings, weakening the TOE's security posture.

- **Assets:** Security configuration and protection mechanisms
- **Adverse Action:** Misconfiguration, disabling security controls.

**T.SESSION_HIJACK (Attacker)**: An attacker may take over an active session by stealing session identifiers or exploiting inadequate session management, thereby impersonating a legitimate user without needing to re-authenticate.

- **Assets:** Active user sessions, session tokens.
- **Adverse Action:** Session takeover and impersonation.

**T.DATA_EXPOSE (Attacker):** An attacker may attempt to intercept or modify sensitive data exchanged between system components.

In the current setup, communication between the backend and database occurs over a secure Docker network on the same host, minimizing the risk of eavesdropping. However, the system is also designed for deployments where these components may run on separate machines or network segments. To ensure consistent protection in all cases, communication between the backend and database is secured using TLS 1.2 with certificate-based authentication, preventing unauthorized access or tampering with data in transit.

- **Assets: Operational and security data exchanged with external systems.**
- **Adverse Action:** Unauthorized disclosure or manipulation of data.

## 3.3 ORGANIZATIONAL SECURITY POLICY

**P.NETWORK**: There should be appropriate network layer protection, with a firewall in place that only permits access through the required ports. Access by remote authorized users (administrators or operators connecting via a secure VPN) must be explicitly defined, documented, and restricted to the necessary roles and functions. All other external connections are denied.

**P.AUDIT_BACKUP**
The operational environment shall ensure that audit logs generated by the TOE are backed up regularly and retained securely. Backups shall be performed either at predefined intervals (daily, weekly) or when log files reach a specified quota threshold. This policy ensures that audit logs remain available for accountability and forensic purposes and prevent storage exhaustion on the host machine caused by unbounded log growth.

# 4 SECURITY OBJECTIVES

## 4.1 SECURITY OBJECTIVES FOR TOE

**O.AUTH:** The TOE must require all users to be uniquely identified and successfully authenticated before accessing TOE resources or functions. Authentication mechanisms must enforce robust password complexity requirements and account lockout after repeated failed attempts and to resist brute force and credential-guessing attacks, ensuring only legitimate users gain access and all actions are attributable to specific users.

**O.AUDIT:** TOE must generate comprehensive audit data for all security-relevant and operational events, including commands, operator actions, identification, authentication, access control decisions, and security management actions. Audit data must include reliable timestamps, event details, subject identity, and outcomes. The TOE must protect these audit logs from unauthorized access, modification, or deletion, ensuring accountability and forensic capability.
The storage, long-term maintenance, and retention of these audit data are performed by the Operational Environment (**OE.AUDIT_BACKUP**), which ensures secure backup and preservation of audit data for accountability and forensic purposes.

**O.MNGMNT:** The TOE must restrict access to management functions to authorized administrators only, ensuring they can securely create, modify, and delete user accounts, assign roles, configure system parameters, and manage security policies.

**O.ACCESS_CONTROL:** TOE must enforce a **role-based access control policy** to ensure that only authorized users can perform specific operations on defined objects. Access roles are based on predefined roles (Administrator, Operator) as well as administrator-defined roles. This ensures fine-grained control of operational and security functions.

**O.SESSION_CONTROL:** The TOE must enforce secure session handling, including automatic termination after a defined period of inactivity, user-initiated session termination, and denial of session establishment for disabled accounts or when the concurrent session limit is reached.

**O.DATA_PROTECT:** The TOE must protect the confidentiality and integrity of TSF data transmitted between its components using secure communication mechanisms to prevent unauthorized disclosure or modification during transmission.

## 4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

**OE.NETWORK** The operational environment ensures that appropriate network-layer protection mechanisms are in place to maintain confidentiality and integrity of data exchanged between TOE and external systems.
This includes the establishment of secure communication channels (e.g., IPsec or equivalent mechanisms) for all network traffic between TOE and external entities, as well as firewall configurations that restrict access to only the required ports and protocols. These measures prevent unauthorized interception, modification, or access by attackers and ensure that TOE users can communicate securely with the TOE components.

**OE.SEC_ENV** The operational environment ensures physical and environmental security of the TOE. Unauthorized access shall be restricted and all components in the operational environment shall be secured. Only specifically authorized people shall be allowed to access critical components.

**OE.CREDEN** The operational environment ensures that all access credentials, such as passwords or other authentication information, are protected by the users (by complying with organizational policies and procedures disallowing disclosure of user credential information) in a manner which maintains organizational IT security objectives.

**OE.RELIABLE_TIME_SOURCE** The operational environment ensures that TOE has access to a reliable and accurate time source, such as an internal NTP (Network Time Protocol) server, to support trustworthy timestamps in audit data and time-dependent functions.

**OE.AUDIT_BACKUP** The operational environment ensures that audit logs generated by the TOE are backed up regularly and retained securely. Backups shall be performed either at predefined intervals (daily, weekly) or when log files reach a specified quota threshold. This prevents storage exhaustion on the host machine and ensures audit data remains available for accountability and forensic purposes.

**OE.ADMIN_TRUST**

The IT environment shall ensure that only trustworthy and competent personnel are assigned as Linux system administrators responsible for managing the server infrastructure on which the TOE is deployed. These administrators shall be properly trained, vetted, and follow all documented security procedures to maintain the integrity of the underlying platform.

**OE.CERT_TRUST**

The operational environment shall ensure that the self-signed TLS certificate used by the Barzan C2 Backend server is installed in the trusted certificate store (Root or Trusted Root Certification Authorities) of all Windows client workstations on which the Frontend application is deployed... System administrators are responsible for distributing the certificate and verifying its installation...

## SECURITY OBJECTIVE RATIONALE

The following table demonstrates that all security objectives trace back to the threats, OSPs and assumptions in the security problem definition.

| | THREATS | OSPs | ASSUMPTIONS |
|---|---|---|---|

|  |  | T. UNAUTH | T. PRIVIL_ESC | T. DoS | T. CHANNEL | T. MISCONFIG | T. | T.DATA_EXPOSE | T. BRUTE | P. NETWORK | P. AUDIT_BACKUP | A. PHYSICAL | A. TIME | A. PROTECT | A.CERT_TRUST | A. ADMIN_TRUST |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **SECURITY OBJECTIVES FOR TOE** | O. AUTH | X |  |  |  |  |  |  | X |  |  |  |  |  |  |  |
|  | O. AUDIT | X | X |  |  | X |  |  | X |  |  |  |  |  |  |  |
|  | O.ACCESS_CONTROL |  | X |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | O.DATA_PROTECT |  |  |  | X |  |  | X |  |  |  |  |  |  |  |  |
|  | O.SESSION_CONTROL |  |  |  |  |  | X |  |  |  |  |  |  |  |  |  |
|  | O. MNGMNT |  | X |  |  | X |  |  |  |  |  |  |  |  |  |  |
| **SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT** | OE. CREDEN | X |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | OE. SECURE_ENV |  |  | X |  |  |  | X |  |  |  | X |  | X |  |  |
|  | OE.RELIABLE_TIME_SOURCE |  |  |  |  |  |  |  |  |  |  |  | X |  |  |  |
|  | OE. NETWORK |  |  | X |  |  |  | X |  | X |  |  |  |  |  |  |
|  | OE.AUDIT_BACKUP |  |  |  |  |  |  |  |  |  | X |  |  |  |  |  |
|  | OE.CERT_TRUST |  |  |  |  |  |  |  |  |  |  |  |  |  | X |  |
|  | OE.ADMIN_TRUST |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X |

Table 3 Security Objective Rationale

**T.UNAUTH**

***O.AUDIT*** ensures that all access attempts and security-relevant actions are logged, enabling traceability of user and administrator activities. **O.AUTH** ensures that each user must be uniquely identified and authenticated before accessing TOE resources_and_enforces strong authentication mechanisms, such as password complexity requirements and account lockout after repeated failed attempts, thereby mitigating brute-force and guessing attacks that could lead to unauthorized access**. OE.CREDEN** ensures that users protect their own access credentials in line with organizational policies. Together, these objectives ensure that unauthorized access attempts are prevented, detected, and appropriately mitigated.

**T.PRIVIL_ESC**

***O.ACCESS_CONTROL*** ensures that users are limited to the actions allowed by their assigned roles, while ***O.MNGMNT*** provides administrators with secure management capabilities to control sensitive attributes and configurations, including those related to authentication, authorization, and data disclosure. Additionally, ***O.AUDIT*** guarantees that all privilege-related events are logged, enabling detection and investigation of misuse. Thus, these objectives collectively address the risk of privilege escalation or bypassing access controls.

**T.DoS**

***O.MNGMNT*** defines an Access Control Policy to take needed measures against denial of service attacks. Since this threat needs additional measures which need to be taken by the operational environment of the TOE, it is addressed by ***OE.SEC_ENV***. ***OE.NETWORK*** ensures that those responsible for the TOE ensure that appropriate network layer protection, that there is a firewall in place that only permits access through required ports for external users to access the server.

**T.CHANNEL**

***O.DATA_PROTECT*** ensures that the TOE uses secure communication mechanisms to protect the confidentiality and integrity of TSF data transmitted between TOE components and trusted external IT products. This prevents attackers from intercepting, modifying, or replaying communication and ensures that sensitive operational information remains protected during transmission.

**T.BRUTE**

This threat is addressed by **O.AUTH**, which enforces account lockout after repeated failed authentication attempts and requires strong password complexity, preventing attackers from successfully guessing credentials through brute-force methods. **O.AUDIT** ensures that all failed login attempts are logged, providing traceability and detection of brute-force attacks.

**T.MISCONFIG**

This threat is mitigated by **O.*MNGMNT***, which ensures that only authorized administrators can modify critical security attributes, and ***O.AUDIT***, which records all security-relevant configuration changes, enabling detection of unauthorized or erroneous modifications.

**T.SESSION_HIJACK**

This threat is addressed by ***O.SESSION_CONTROL***, which enforces secure session management, including automatic termination after inactivity, user-initiated termination, and restrictions on concurrent sessions, thereby reducing opportunities for session takeover by an attacker.

**T.DATA_EXPOSE**
This threat is countered by ***O.DATA_PROTECT***, which protects TSF data from disclosure and modification during transmission between TOE components, ensuring that sensitive information is not exposed to unauthorized parties in transit.

In addition, this threat is also addressed through ***OE.NETWORK*** and ***OE.SEC_ENV***, which ensure that all external communications occur over trusted and protected channels.
The operational environment establishes secure communication paths (such as **IPsec tunnels** or equivalent mechanisms) and enforces firewall and access-control measures to maintain the confidentiality and integrity of data exchanged between the TOE and external systems.
Furthermore, ***OE.SEC_ENV*** guarantees that the TOE and its supporting infrastructure reside within a **controlled and physically secure environment**, preventing unauthorized access to communication interfaces and network components.

Together, these measures ensure that sensitive information remains protected against disclosure or alteration both within the TOE and when interacting with external systems.

**P.NETWORK**

***OE.NETWORK*** ensures that appropriate network-layer protection is enforced, with a firewall permitting access only through the required ports.
In this context, **external users** refer to authorized TOE users (administrators or operators) who access the TOE from a different subnet or remote site **via a secure VPN/IPSec channel** that is part of the operational environment. Any untrusted external connections outside the protected network are denied.

**A.PROTECT**

This assumption is addressed by ***OE.SEC_ENV***, which ensures the physical and environmental security of the TOE and its components, including secure management of hardware configurations and network devices to protect confidentiality and integrity of transmitted data.

**A.PHYSICAL**
This assumption is addressed by ***OE.SEC_ENV***, which ensures that the TOE's hosting environment is physically protected against unauthorized access. Only authorized personnel are allowed to access critical components.

**A.TIME**

This assumption is addressed ***by OE.RELIABLE_TIME_SOURCE***, which ensures that the operational environment provides the TOE with access to a reliable and accurate time source. This supports trustworthy timestamps in audit data and proper sequencing of security-relevant events.

**P.AUDIT_BACKUP**
*OE.AUDIT_BACKUP* ensures that audit logs generated by the TOE are regularly backed up and securely retained. This prevents the risk of storage exhaustion on the host machine due to unbounded log growth and ensures audit data remains available for accountability, incident investigation, and compliance purposes. By enforcing backups either at regular intervals or upon reaching defined storage thresholds, the operational environment supports continuous availability and reliability of audit information.

**A.ADMIN_TRUST**

This assumption is addressed by OE.ADMIN_TRUST, which ensures that the IT environment assigns only trustworthy and competent personnel as Linux system administrators responsible for managing the server infrastructure on which the TOE is deployed. The operational environment implements vetting procedures, provides appropriate training, and establishes accountability mechanisms to ensure administrators follow documented security procedures and do not attempt to compromise the security of the TOE or its underlying platform.

**A.CERT_TRUST**

This assumption is addressed by **OE.CERT_TRUST**, which requires the operational environment to ensure that the TOE's self-signed TLS certificate is pre-installed in the trusted certificate store of all client workstations. This enables proper TLS server authentication and certificate validation, preventing man-in-the-middle attacks through certificate substitution

# 5 EXTENDED COMPONENT DEFINITION

*There are no extended components.*

# 6 SECURITY REQUIREMENTS

## 6.1 SFR Formatting

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from Common Criteria Version 2022, Part 2 providing functional requirements and Part 3 providing assurance requirements.

The following formatting conventions are used:

- **Assignment:** Depicted using **bolded text** surrounded by square brackets: [**assignment**]
- **Selection:** Depicted using *italicized text* surrounded by square brackets: [*selection*]
- **Refinement:** Additions shown in **bold**, deletions shown with ~~strikethrough~~
- **Iteration:** Shown with identifier suffix: FDP_ACC.1/IDENTIFIER

## 6.2 SECURITY FUNCTIONAL REQUIREMENTS (SFR)

| Requirement Class | Requirement Component |
|---|---|
| FAU: Security Audit | FAU_GEN.1: Audit Data Generation<br>FAU_GEN.2: User identity association |
| FDP: User Data Protection | FDP_ACC.1: Subset Access Control<br>FDP_ACF.1: Security Attribute Based Access Control |
| FIA: Identification and Authentication | FIA_ATD.1: User attribute definition<br>FIA_AFL.1: Authentication failure handling<br>FIA_UID.2: User identification before any action<br>FIA_UAU.2: User authentication before any action<br>FIA_SOS.1: Verification of secrets |
| FMT: Security Management | FMT_MSA.1: Management of Security Attributes<br>FMT_MSA.3: Static Attribute Initialization<br>FMT_SMF.1: Specification of Management Functions<br>FMT_SMR.1: Security Roles |
| FTA: TOE Access | FTA_SSL.3: TSF-initiated termination<br>FTA_SSL.4: User-initiated termination<br>FTA_TSE.1: TOE session establishment |
| FPT: Protection of Security Functionality | FPT_ITT.1: Basic Internal TSF data transfer protection<br>FTP_ITC.1 Inter-TSF trusted channel |

*Table 4: Security Functional Requirements*

### 6.2.1 Security Audit

**FAU_GEN.1 Audit data generation**

*Hierarchical to:* No other components.

*Dependencies:* FPT_STM.1 Reliable time stamps

**FAU_GEN.1.1** The TSF shall be able to generate an audit data of the following auditable events:

a) Start-up and shutdown of the audit functions.

b) All auditable events for the [*not specified]* level of audit.

c) [**Operational commands, user authentication events, Security management actions, Communication failures, System configuration changes**]

**FAU_GEN.1.2**

The TSF shall record within the audit data at least the following information:
a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.

b) For each auditable event type, based on the auditable event definitions of the functional components included in the ~~PP, PP-Module, functional package or~~ ST, [ **Source IP address, Object involved in the action (if applicable)**].

**FAU_GEN.2 User identity association**

*Hierarchical to:* No other components.

*Dependencies:* FAU_GEN.1 Audit data generation, FIA_UID.1 Timing of identification

**FAU_GEN.2.1** For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

### 6.2.2 User Data Protection

**FDP_ACC.1 Subset access control**

*Hierarchical to:* No other components.

*Dependencies:* FDP_ACF.1 Security attribute-based access control

**FDP_ACC.1.1** The TSF shall enforce the [**Command and Control Access Policy**] on [**subjects: Users with assigned roles (Administrator, Operator, or custom-defined roles); objects: operational data, telemetry data, system configuration, user profile data; operations: read, write, execute, delete**].

**FDP_ACF.1 Security attribute-based access control**

*Hierarchical to:* No other components.

*Dependencies:*

FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute

**FDP_ACF.1.1** The TSF shall enforce the **[Command and Control Access Policy]** to objects based on the following:

- **[subjects and SFP-relevant attributes: Users with assigned roles (Administrator role, Operator role, or custom-defined roles), account status (enabled/disabled), assigned operational roles]**
- **[objects and SFP-relevant attributes: operational data (data classification level), telemetry data (data classification level), system configuration (configuration type), user profile data (profile owner identity)]**
- **[operations: read, write, execute, delete]**

**FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

**[1. Access is permitted only if the user account status is enabled. 2. Users assigned to the System Administrator role may read, write, execute, and delete operational data, telemetry data, and system configuration. 3. Users assigned to the Operator role: read operational data and telemetry data and execute pre-approved operational commands only. 4. Users assigned to administrator-defined roles may perform operations as specified by the System Administrator for that role. 5. All authenticated users may read and write their own user profile data. Access to another user's profile data is denied.]**

**FDP_ACF.1.3** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

**FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

### 6.2.3 Identification and Authentication

**FIA_AFL.1 Authentication failure handling**

*Hierarchical to:* No other components.

*Dependencies:* FIA_UAU.1 Timing of authentication

**FIA_AFL.1.1** The TSF shall detect when **[[*5*]]** unsuccessful authentication attempts occur related to [**user attempting to authenticate**].

**FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**disable the user account until System Administrator re-enables it**].

**FIA_ATD.1 User attribute definition**

*Hierarchical to:* No other components.

*Dependencies:* No dependencies.

**FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users: [**user roles, authentication credentials, account status**].

**FIA_SOS.1 Verification of secrets**

*Hierarchical to:* No other components.

*Dependencies:* No dependencies.

**FIA_SOS.1.1** The TSF shall provide a mechanism to verify that secrets meet [**the following requirements:** a) **Minimum length of 8 characters** b) **Contains at least one uppercase letter** c) **Contains at least one lowercase letter** d) **Contains at least one numeric digit** e) **Contains at least one special character**].

**FIA_UAU.2 User authentication before any action**

*Hierarchical to:* FIA_UAU.1 Timing of authentication

*Dependencies:* FIA_UID.1 Timing of identification

**FIA_UAU.2.1** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

**FIA_UID.2 User identification before any action**

*Hierarchical to:* FIA_UID.1 Timing of identification

*Dependencies:* No dependencies.

**FIA_UID.2.1** The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user

### 6.2.4 Security Management

**FMT_MSA.1 Management of security attributes**

*Hierarchical to:* No other components.

*Dependencies:* [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

**FMT_MSA.1.1** The TSF shall enforce the **[Command and Control Access Policy]** to restrict the ability to [*modify*, *delete,* **[create]**] the security attributes **[user roles and account status (enabled/disabled)]** to **[System Administrator and explicitly authorized administrative roles]**.

**FMT_MSA.3 Static attribute initialization**

*Hierarchical to:* No other components.

*Dependencies:* FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

**FMT_MSA.3.1** The TSF shall enforce the [**Command and Control Access Policy**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2** The TSF shall allow the [**System Administrator and explicitly authorized administrative roles**] to specify alternative initial values to override the default values when an object or information is created.

**FMT_SMF.1 Specification of Management Functions**

*Hierarchical to:* No other components.

*Dependencies:* No dependencies.

**FMT_SMF.1.1** The TSF shall be capable of performing the following management functions: [**create, modify, delete, and view user accounts; assign and revoke roles; configure parameters; manage security policies**].

**FMT_SMR.1 Security roles**

*Hierarchical to:* No other components.

*Dependencies:* FIA_UID.1 Timing of identification

**FMT_SMR.1.1** The TSF shall maintain roles**, including predefined roles** [**Administrator role**, **Operator role**].

**FMT_SMR.1.2** The TSF shall be able to associate users with roles**, either directly or via group assignment**.

Note: FMT_SMR.1 is satisfied with TOE's role-based access model. Instead of restricting users to fixed roles, the TOE defines and enforces roles. Predefined roles (Administrator and Operator) exist, but administrators may also define new roles. Access control enforcement is consistently applied regardless of whether roles are predefined or custom. This model provides flexibility while maintaining security assurance.

### 6.2.5 TOE Access

**FTA_SSL.3 TSF-initiated termination**

*Hierarchical to:* No other components.

*Dependencies:* FMT_SMR.1 Security Roles

**FTA_SSL.3.1** The TSF shall terminate an interactive session after **[a configurable period of inactivity, with a default value of 15 minutes]**.

**FTA_SSL.4 User-initiated termination**

*Hierarchical to:* No other components.

*Dependencies:* No dependencies.

**FTA_SSL.4.1** The TSF shall allow user-initiated termination of the user's own interactive session.

**FTA_TSE.1 TOE session establishment**

*Hierarchical to:* No other components.

*Dependencies:* No dependencies.

**FTA_TSE.1.1** The TSF shall be able to deny session establishment based on [**disable status of the user, and concurrent session limit which is [1] or the authentication credentials provided are incorrect**].

### 6.2.6 Protection of Security Functionality

**FPT_ITT.1 Basic internal TSF data transfer protection**

*Hierarchical to:* No other components.

*Dependencies:* No dependencies.

**FPT_ITT.1.1** The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

**FTP_ITC.1 Inter-TSF trusted channel**

*Hierarchical to:* No other components.

*Dependencies:* No dependencies.

**FTP_ITC.1.1** The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

**FTP_ITC.1.2**
The TSF shall permit [*the TSF, another trusted IT product*] to initiate communication via the trusted channel.

**FTP_ITC.1.3**
The TSF shall initiate communication via the trusted channel for [**data persistence operations between the Backend and the Database (MongoDB), including user authentication credential storage and validation, operational data storage and retrieval**].

**Note:**

The TOE establishes trusted communication channels **between its internal components**, specifically between the **Frontend (Electron/React-based user interface)** and the **Backend (Spring Boot–based application services)**.
These internal connections are protected using **TLS 1.3**, ensuring confidentiality, integrity, and authenticity of all TSF data exchanged between the frontend and backend.

Communication between the **Backend** and the **Database (MongoDB)** is likewise secured through **TLS 1.2** connections managed within the TOE's configuration.

Communication with **external systems** (such as sensors, effectors, or third-party subsystems) is **outside the TOE boundary**. Those external links are protected by **site-to-site IPsec tunnels** or equivalent mechanisms implemented in the **operational environment**, not by the TOE itself.

Therefore, **FTP_ITC.1 applies exclusively to TOE-internal communications (Frontend ↔ Backend ↔ Database)**, while protection of external channels is ensured by the operational environment.

## 6.3 SECURITY ASSURANCE REQUIREMENTS (SAR)

The TOE meets the security assurance requirements for EAL2. The following table summarizes the requirements:

| Assurance Class | Assurance Components | Dependency | Dependency Met ? |
|---|---|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description | ADV_FSP.1, ADV_TDS.1 | Yes, by ADV_FSP.2, ADV_TDS.1 |
| | ADV_FSP.2 Security-enforcing functional specification | ADV_TDS.1 | Yes |
| | ADV_TDS.1 Basic design | ADV_FSP.2 | Yes |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance | ADV_FSP.1 | Yes, by ADV_FSP.2 |
| | AGD_PRE.1 Preparative procedures | None | - |
| ALC: Life-cycle support | ALC_CMC.2 Use of a CM system | ALC_CMS.1 | Yes, by ALC_CMS.2 |
| | ALC_CMS.2 Parts of the TOE CM coverage | None | - |
| | ALC_DEL.1 Delivery procedures | None | - |
| | ASE_CCL.1 Conformance claims | ASE_INT.1, ASE_ECD.1, ASE_REQ.1 | Yes, by ASE_REQ.2 |

|  |  |  |  |
|---|---|---|---|
| ASE: Security Target evaluation | ASE_ECD.1 Extended components definition | None | - |
|  | ASE_INT.1 ST introduction | None | - |
|  | ASE_OBJ.2 Security objectives | ASE_SPD.1 | Yes |
|  | ASE_REQ.2 Stated Security Requirements | ASE_OBJ.2, ASE_ECD.1 | Yes |
|  | ASE_SPD.1 Security problem definition | None | - |
|  | ASE_TSS.1 TOE summary specification | ASE_INT.1, ASE_REQ.1, ADV_FSP.1 | Yes, by ADV_FSP.1and ASE_REQ.2 |
| ATE: Tests | ATE_COV.1 Evidence of coverage | ADV_FSP.2, ATE_FUN.1 | Yes |
|  | ATE_FUN.1 Functional testing | ATE_COV.1 | Yes |
|  | ATE_IND.2 Independent testing - sample | ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1 | Yes |
| AVA: Vulnerability Assessment | AVA_VAN.2 Vulnerability analysis | ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1 | Yes |

*Table 5: Security Assurance Requirements*

## 6.4 SECURITY REQUIREMENTS RATIONALE

### 6.4.1 SFR Rationale

#### SFR Dependency Rationale

The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included.

| SFR | Dependency | Dependency Met? |
|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | NO |
| FAU_GEN.2 | FAU_GEN.1<br>FIA_UID.1 | YES<br>YES(FIA_UID.2 is hierarchical to FIA_UID.1) |

| | | |
|---|---|---|
| FDP_ACC.1 | FDP_ACF.1 | YES |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | YES<br>YES |
| FIA_ATD.1 | - | - |
| FIA_UID.2 | - | - |
| FIA_UAU.2 | FIA_UID.1 | YES(FIA_UID.2 is hierarchical to FIA_UID.1) |
| FIA_AFL.1 | FIA_UAU.1 | YES(FIA_UAU.2 is hierarchical to FIA_UAU.1) |
| FIA_SOS.1 | - | - |
| FMT_MSA.1 | [FDP_ACC.1 or FDP_IFC.1]<br>FMT_SMR.1<br>FMT_SMF.1 | FDP_ACC.1,<br>YES<br>YES |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | YES,<br>YES |
| FMT_SMF.1 | - | - |
| FMT_SMR.1 | FIA_UID.1 | YES(FIA_UID.2 is hierarchical to FIA_UID.1) |
| FTA_SSL.3 | - | - |
| FTA_SSL.4 | - | - |
| FTA_TSE.1 | - | - |
| FPT_ITT.1 | - | - |
| FTP_ITC.1 | - | - |

*Table 6 SFR-Dependency Rationale Table*

The dependency on **FPT_STM.1 Reliable time stamps** is satisfied by the operational environment. The TOE relies on the environment to provide an accurate and reliable time source as defined in Assumption **A.TIME** and Objective **OE.RELIABLE_**TIME_SOURCE. Therefore, this dependency is not implemented within the TOE itself.

### SFR- Objective Rationale

| | O.AUTH | O.AUDIT | O.SESSION_CONTROL | O.ACCESS_CONTROL | O.DATA_PROTECT | O.MNGMNT |
|---|---|---|---|---|---|---|
| FAU_GEN.1 | | X | | | | |
| FAU_GEN.2 | | X | | | | |
| FDP_ACC.1 | | | | X | | |
| FDP_ACF.1 | | | | X | | |
| FIA_AFL.1 | X | | | | | |
| FIA_ATD.1 | | | | X | | |
| FIA_UID.2 | X | | | | | |
| FIA_UAU.2 | X | | | | | |
| FIA_SOS.1 | X | | | | | |
| FMT_MSA.1 | | | | | | X |
| FMT_MSA.3 | | | | | | X |
| FMT_SMF.1 | | | | | | X |
| FMT_SMR.1 | | | | X | | |
| FTA_SSL.3 | | | X | | | |
| FTA_SSL.4 | | | X | | | |
| FTA_TSE.1 | | | X | | | |
| FPT_ITT.1 | | | | | X | |
| FTP_ITC.1 | s | | | | X | |

*Table 7 SFR-Objective Rationale Table*

**O.AUTH:**

O.AUTH is satisfied through ***FIA_UID.2*** and ***FIA_UAU.2. FIA_UID.2*** requires that each user be uniquely identified before any TOE-mediated action can occur, while ***FIA_UAU.2*** requires successful authentication of the identified user before granting access to TOE resources. In addition, the TOE enforces account lockout after five unsuccessful authentication attempts, requiring administrator intervention to re-enable the account. The TOE also restricts users to a maximum of one active session at a time, preventing concurrent logins. Furthermore, the TOE enforces secure session handling by allowing user-initiated logout and automatically terminating sessions after 15 minutes of inactivity.

Together, these requirements ensure that only authenticated users can access TOE resources, repeated authentication failures are mitigated, and active sessions are securely controlled.

The TOE enforces password complexity and robustness requirements defined in **FIA_SOS.1**, ensuring that secrets meet organizational policy for length and composition. Additionally, **FIA_AFL.1** provides authentication failure handling by locking accounts after repeated failed login attempts, thereby mitigating brute-force attacks.

**O.AUDIT:**

***FAU_GEN.1*** generates the required audit data with a reliable timestamp*.* Audit logs are associated by users by ***FAU_GEN.2***.

**O.MNGMNT:**

O.MNGMNT is satisfied through ***FMT_SMF.1, FMT_MSA.1***, and ***FMT_MSA.3. FMT_SMF.1*** defines the management functions that administrators can perform, including user account management, role assignment, and security policy configuration***. FMT_MSA.1*** ensures that only authorized administrators can create, modify, or delete security attributes such as user roles, access control attributes, and operational assignments. ***FMT_MSA.3*** ensures that newly created security attributes are initialized with restrictive default values, thereby reducing the attack surface. Together, these requirements ensure that management functions and security attributes are securely controlled and restricted to authorized administrators*.*

**O.ACCESS_CONTROL:**

The TOE enforces a role-based access control policy in accordance with **FDP_ACC.1** and **FDP_ACF.1**, ensuring that access to objects such as operational data, telemetry, system configuration, and audit logs is only granted based on defined security attributes. **FIA_ATD.1** defines and maintains user attributes, while **FMT_SMR.1** specifies the security roles, guaranteeing that users can perform only those actions permitted by their assigned role.

**O.SESSION_CONTROL:**

The TOE enforces secure session handling as specified in **FTA_SSL.3** by terminating inactive sessions after a defined period, and **FTA_SSL.4** allows users to voluntarily terminate their sessions. Additionally, **FTA_TSE.1** prevents session establishment for disabled accounts and enforces a limit on concurrent sessions, preventing unauthorized session hijacking or parallel logins.

**O.DATA_PROTECT:**

The TOE ensures the confidentiality and integrity of TSF data transmitted between its components in line with **FPT_ITT.1** and **FTP_ITC.1**, protecting against disclosure and modification during internal transfers.

### 6.4.2 SAR Rationale

The chosen assurance level EAL2 is appropriate for the operational environment and threat level. EAL2 provides increased confidence through structural testing and independent vulnerability analysis, which is suitable for a Command and Control system.

# 7 TOE SUMMARY SPECIFICATION

## 7.1 Security Audit

The TOE generates comprehensive audit logs for all Command and Control operations, including operational commands, operator authentication, and security management actions. All audit data include reliable timestamps and user identity information.

**TOE Security Functional Requirements Satisfied:** *FAU_GEN.1, FAU_GEN.2*

## 7.2 User Data Protection

The TOE implements role-based access control to protect control data, telemetry data, and system configuration information. Access is granted based on user role based model with default roles (System Administrator, Operator) and specific assignments. The system enforces the Command and Control Access Policy to ensure only authorized users can access sensitive information and operational control.

Access control enforcement is implemented using Spring Security framework with method-level security annotations (@PreAuthorize) applied to service layer methods. These annotations enforce role checks before allowing access to protected operations. For example, administrative functions are protected with @PreAuthorize("hasRole('ADMIN')"), while user-specific operations verify ownership through role-based expressions. This method-level enforcement ensures that the access control policy defined in FDP_ACC.1 and FDP_ACF.1 is consistently applied across all TSF interfaces.

To prevent Insecure Direct Object Reference (IDOR) attacks, all objects managed by the TOE (user accounts, groups, operational data, system configurations) are identified using UUID (Universally Unique Identifier) values. UUIDs are non-sequential and cryptographically random, eliminating the predictability of object identifiers and preventing unauthorized access through identifier guessing. Even if an attacker obtains a valid UUID, the access control mechanisms described above ensure that roles checks are enforced before any object can be accessed or modified.

**TOE Security Functional Requirements Satisfied:** *FDP_ACC.1, FDP_ACF.1*

## 7.3 Identification and Authentication

The TOE requires authentication for all users, including username/password for high-security operations. The system maintains comprehensive user attributes including user roles, operational assignments, authentication credentials, and account status. Authentication failures are handled by disabling accounts after five unsuccessful attempts until System Administrator intervention.

The TOE verifies that user passwords meet complexity rules, such as minimum length and inclusion of uppercase, lowercase, numbers, and special characters. User passwords are stored using BCrypt hashing algorithm, which automatically applies a cryptographically strong random salt before hashing. Passwords are never stored in plaintext. During authentication, the provided password is hashed using the same salt and compared against the stored hash value.

**TOE Security Functional Requirements Satisfied:** *FIA_AFL.1, FIA_ATD.1, FIA_UAU.2, FIA_UID.2, FIA_SOS.1*

## 7.4 Security Management

The TOE provides mechanisms to govern which users can access with resources or functions. The Security Management function allows the Administrator user to properly configure this functionality. Administrators can create and manage roles, assign them to individual users, or group them into roles. The TOE enforces security consistently across all roles, regardless of whether they belong to predefined roles (Administrator, Operator) or custom-defined roles. This flexible role based model allows administrators to implement least-privilege access while ensuring accountability.

In FMT_MSA.1, the way the system manages security is by changing and giving access rights to different plugins. This feature lets Administrator user adjust role in detail. It means Administrator user can limit or allow access to different parts of the system depending on what each user needs to do according to FMT_MSA.3. This thorough method makes sure the system follows security rules properly. It helps control who can access what and strengthens the overall security setup of the system. Users can perform management functions as defined in FMT_SMF.1 as applicable to their role FMT_SMR.1.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

## 7.5 TOE Access

The TSF provides a method for controlling the establishment of a user’s (or administrator’s) session based on a termination of session after a specified period of user inactivity. Interactive sessions are logged out. The users are automatically logged out and returned to the login page. The session termination period is configurable, and the default value is 15 minutes. The TOE also allows user-initiated termination of the user's own interactive session. The TOE can deny session establishment of users with disabled status. To authenticate again, administrator allows user by changing user status. The TOE also enforces a limit on the number of concurrent sessions a user can establish, preventing multiple active logins.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FTA_SSL.3, FTA_SSL.4, FTA_TSE.1

## 7.6 Protection of Security Functionality

The TOE protects critical security data and TSF communications while being transmitted between its internal components and trusted IT products.
Data exchanged between the **Frontend (User Workstation)** and the **Backend Server** is protected through **TLS 1.3**, fulfilling the requirements of **FPT_ITT.1**, which ensures confidentiality and integrity of TSF data transferred within the TOE boundary.

In addition, the TOE secures communication between the **Backend** and the **Database (MongoDB)** using **TLS 1.2**, thereby fulfilling **FTP_ITC.1**, which provides a trusted channel ensuring authenticated and encrypted communication between the TOE and another trusted IT product.

Communication with **external systems** (such as sensors, effectors, and third-party subsystems) lies **outside the TOE boundary** and is protected by the **operational environment** through mechanisms such as IPsec tunnels or equivalent network-layer protections.

These combined measures ensure that all TSF data transferred internally and across trusted interfaces remain protected against unauthorized disclosure or modification, while external link security is managed by the operational environment.

**TOE Security Functional Requirements Satisfied:** FPT_ITT.1, FTP_ITC.1

# GLOSSARY

**SEMS**: Sensor/Effector Management System

**TSF**: TOE Security Functions

**TOE**: Target of Evaluation

**SFR**: Security Functional Requirement

**SAR**: Security Assurance Requirement

# REFERENCES

Common Criteria for Information Technology Security Evaluation Part I: Introduction and General Model; Version 2022

Common Criteria for Information Technology Security Evaluation Part II: Security Functional Requirements; Version 2022

Common Criteria for Information Technology Security Evaluation Part III: Security Assurance Requirements; Version 2022

Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; Version 2022