OT Security and Operations –

OT Platform Solution

Mash4GUARD

Assessment services, implementation and modular platform (ACCESS, INSIGHT, RESCUE)

Mashfrog Group

Summary

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

1. Executive Summary

This document describes the main features of the Mashfrog OT platform. The platform is an **integrated and modular solution** based on Edge components that ensures:

- Secure access to OT plants, bound to corporate identity, passkey/WebAuthn, and an Edge-based session broker;
- Passive and continuous visibility of OT traffic through network sensors and DPI engines, integrated with corporate SIEM systems;
- Protection and versioning of PLC, SCADA and network device configurations, with backup orchestration, automated validation and verifiable rollback.

The standard implementation model of the solution is structured in two phases.

The initial **assessment phase** produces the inventory of OT assets and related IT systems, the mapping of sites and networks, the classification of devices and protocols, communication flows and operational dependencies; it also defines baselines, control criteria and integration requirements with IdM/SSO, SIEM, CMDB/ITSM and existing backup systems.

Following the assessment, the platform composed of the ACCESS, INSIGHT and RESCUE modules is activated: ACCESS implements privileged access control and session traceability, leveraging strong authentication (SSO, passkey/WebAuthn) and an Edge gateway that opens sessions towards plants only after identity, context and authorization checks; INSIGHT provides passive visibility of OT traffic with industrial protocol DPI, contextual enrichment (assets, sites, lines) and generation of events/alerts natively integrable into SIEM systems; RESCUE manages backup orchestration, versioning and configuration validation with change workflows, approval and automated rollback.

Modularity enables selective adoption: it is possible to implement one or more modules, without the obligation to activate them all, for example starting from remote access control only or network visibility only.

The integration of the three modules reduces tool fragmentation, standardizes interfaces and processes, and enables the adoption of “security by design” controls within existing processes (IdM/SSO, SIEM/SOAR, CMDB/ITSM, ticketing). The result is centralized control, automated configuration validation and measurable operational management, with audit

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

evidence and natural alignment with regulatory and compliance requirements for OT security.

2. Context and Challenges

Modern industrial environments face increasing challenges related to the complexity of **OT (Operational Technology)** networks. The coexistence of heterogeneous systems, often distributed across multiple sites, makes it difficult to achieve **unified visibility of assets** and communication flows.

In many cases, access is not centrally managed and structured processes for operation **control and traceability** are lacking, with the risk of unauthorized or undocumented interventions. In addition, the absence of **configuration versioning** leads to unvalidated manual changes and limited rollback capability in case of error or failure.

These conditions result in concrete risks:

- **Unplanned downtime**, with direct impacts on production.
- **Expanded attack surface**, exposing the infrastructure to potential intrusions or malware.
- **Difficulty in complying** with security regulations and industrial standards.
- **Increased operational costs** due to inefficiencies and fragmented tool management.

To address these challenges, it is necessary to adopt an approach that combines **assessment services** and an **integrated platform** capable of delivering control, automation and security by design.

3. Phased Approach

The implementation of the solution is designed to follow a **gradual and non-disruptive** path, minimizing plant impact and ensuring safe and progressive adoption.

The timeline is jointly defined during project **kickoff** and documented in a Project Plan.

The solution includes the joint definition of scope through a scoping workshop guided by **operational impact** and **cyber risk**.

Together we identify the most representative/critical “reference” plants and verify technical prerequisites (SSO/PAM, SPAN/TAP/NetFlow, management reachability).

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

For each plant, a profile sheet is completed with device classes, protocols, access patterns, change types, safety constraints and operational windows.

The scope is then frozen with entry/exit stage-gates, RACI definition and baseline KPIs to measure value and **reusability** across ACCESS, INSIGHT and RESCUE.

The plan is structured into three main phases:

➤ **Phase 1 – Assessment**

- **Survey of OT/IT/IoT sites, networks and devices:** A team of experts conducts a comprehensive analysis to identify and map sites, networks and all OT/IT/IoT devices, including the industrial protocols in use.
- **Population of the asset database with structured and correlated information**: The collected data will be entered into a central database to create a structured and dynamic inventory of assets, complete with information on risks and vulnerabilities.
- **Definition of an operational baseline as a reference point for subsequent phases:** an operational "baseline" is established, providing a reference point for normal system performance and for future monitoring.

➤ **Phase 2 – Edge Implementation**

- **Installation and configuration of Edge devices in pilot sites:** Installation and configuration of Edge devices at pilot sites (in case of INSIGHT or ACCESS module), which will act as gateways for industrial data collection.
- **Integration of standard and proprietary protocols**: Integration with standard (such as Modbus, OPC-UA) and proprietary protocols is implemented to initiate network traffic collection and ensure full operational visibility.
- **Activation of network traffic collection** to enable visibility and monitoring.

➤ **Phase 3 – Operations**

- **Progressive activation of ACCESS, INSIGHT and RESCUE modules**: The modules are progressively activated and configured for the pilot site, making the solution fully operational.
- **Enablement of centralized tracking and control of privileged access**: Enable centralized management of privileged access. Every control and modification session is tracked and monitored in real time.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

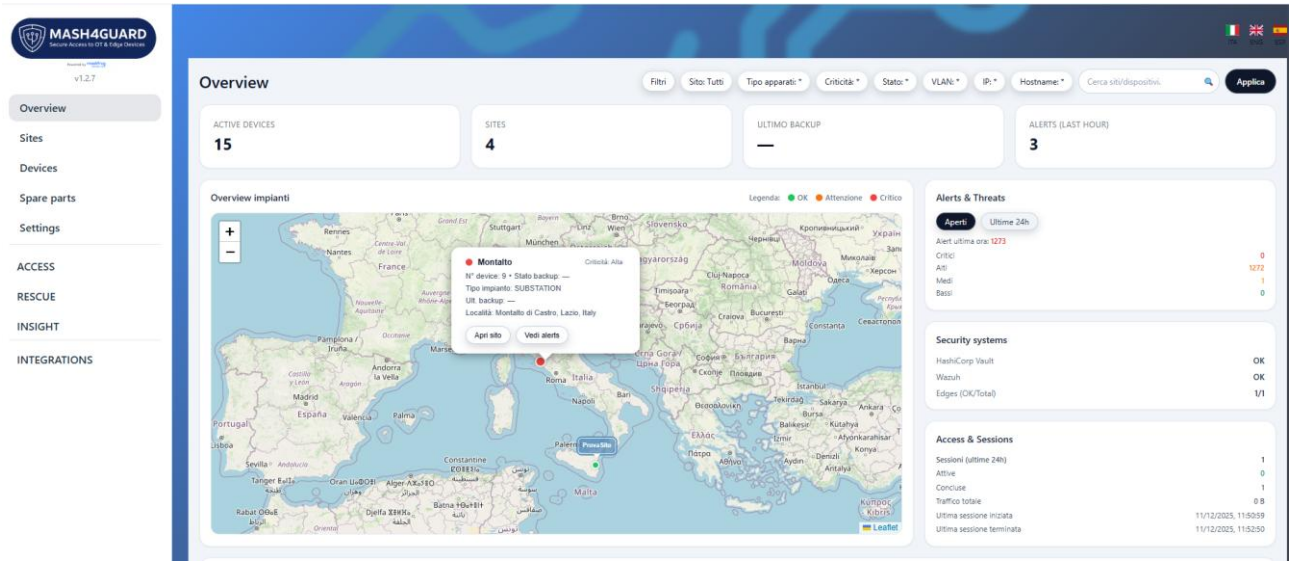
- **Continuous monitoring of OT traffic with alert generation and reporting:** The platform starts monitoring OT traffic, identifying anomalies and generating alerts and detailed reporting for timely response.
- Implementation of **configuration versioning**, with validation processes and rollback capability in case of anomalies: Automatic versioning of device configurations is implemented. This includes enabling validation processes (approval of changes) and the ability to immediately **rollback** to a previous, secure version in the event of problems, ensuring operational continuity.

4. Platform Mash4GUARD

4.1 Overview

The platform represents a single, **centralized dashboard** for integrated management of **OT, IT and IoT** environments. Through one interface it consolidates and manages asset inventory, users and access profiles, sessions and activity logs, and device configurations.

This approach eliminates tool fragmentation and guarantees **complete visibility of the entire technological ecosystem**, improving operational efficiency, security posture and overall governance. The platform acts as a "single source of truth" for all security and operational data.



Picture 1- Centralized Dashboard

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

4.2 ACCESS Module

The **ACCESS** module manages secure privileged access to OT plants and systems, acting as a single entry point for internal operators, maintainers and external vendors. It integrates natively with identity services such as Active Directory, LDAP and Entra ID, leveraging corporate SSO, multi-factor authentication and passkey/WebAuthn.

Access to plants occurs through an Edge-based session broker (not by direct connection or shared credential). The user authenticates on the platform, requests access to a specific OT asset, and only upon positive authorization is a controlled session opened (RDP, SSH, VNC, web) from Edge through the device. Technical credentials are managed and protected by the platform (avoiding their exposure to operators and third parties and reducing the risk of misuse).

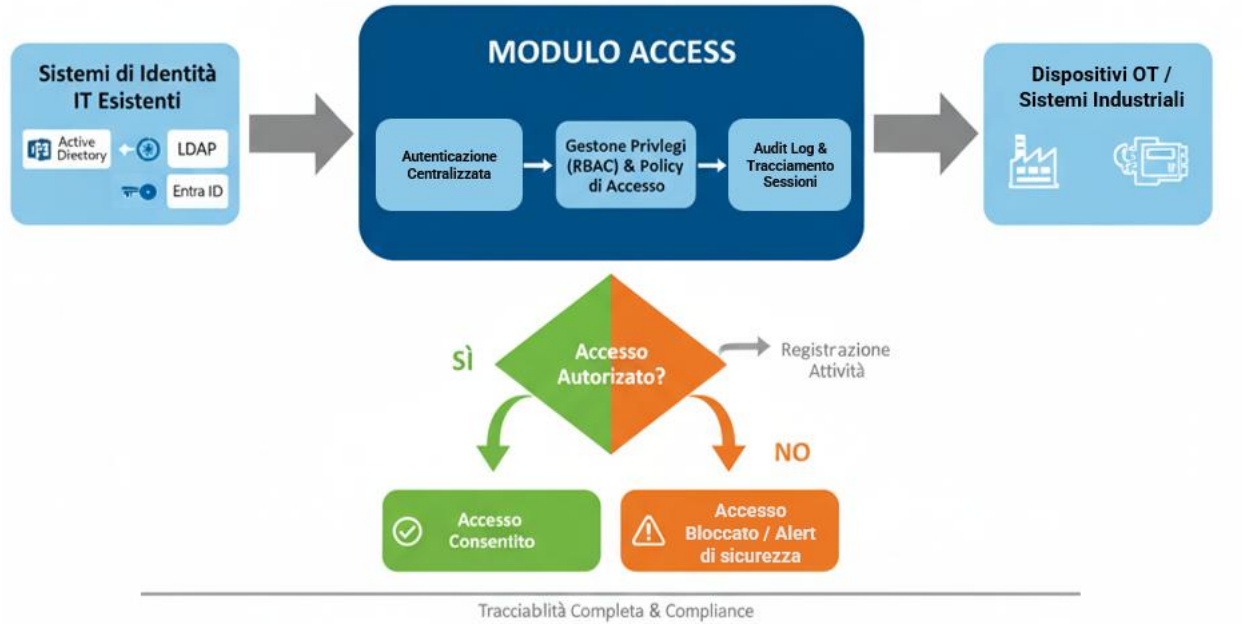
Granular RBAC control, time scopes, maintenance windows, separation of duties (SoD) and approval workflows are supported (e.g. opening access only if associated with a ticket or an authorized change)

Control is granular and role-based (RBAC), with the ability to define time scopes, maintenance windows, separation of duties (SoD) and, where required, approval workflows (e.g. opening accesses only if associated with a ticket or an authorized change). Each session can be tracked and, where required, recorded, generating detailed logs for audit and compliance purposes (who did what, when and on which devices).

The main value is the ability to always maintain a clear and centralized overview of access to OT systems, drastically reducing the risk of unauthorized or untraceable access. A strong logging and auditing system also provides the evidence needed for compliance and reporting to internal and external auditors.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com



Picture 2 – Access process

4.3 INSIGHT Module

The **INSIGHT** module collects and analyzes OT network traffic in real time, providing deep visibility into communication flows among PLCs, SCADA, HMIs, network devices and supervision systems. The solution is based on passive sensors installed on Edge devices using advanced DPI engines (e.g., Suricata, Zeek and industrial protocol parsers) to decode major OT protocols (Modbus, OPC-UA, Ethernet/IP, etc.) and enrich events with operational context.

INSIGHT builds a dynamic asset map, identifying which devices talk to whom, over which protocols and with which traffic patterns. Based on this map, it generates events/alerts in case of anomalies (new unregistered devices, sudden changes in flows, non-standard commands, anomalous access attempts) that can be filtered and correlated to reduce noise and focus on truly significant scenario.

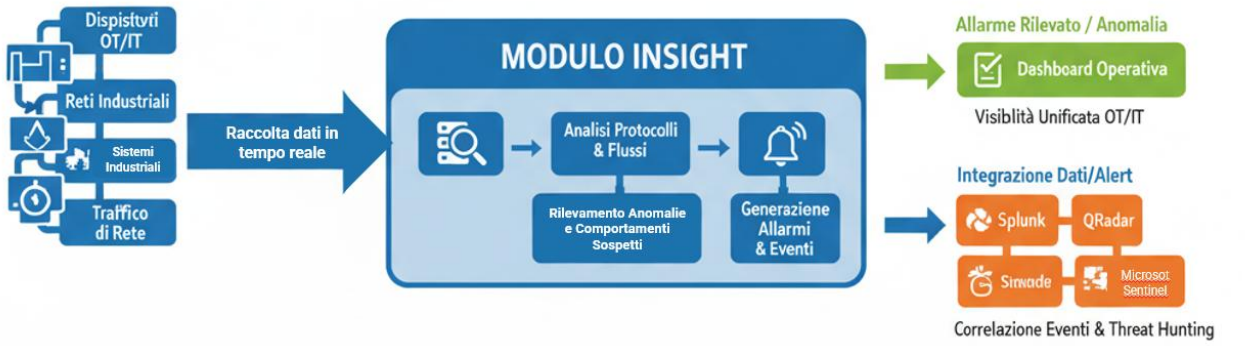
It integrates with major **SIEM** systems already configured in company (e.g., Wazuh, Splunk, QRadar, Microsoft Sentinel) to correlate OT and IT events within a single view. This way, the security team gains a comprehensive understanding of the threat landscape and can adopt use cases and playbooks specific for industrial environment (e.g., detection of scanning on OT ports, potentially destructive commands, lateral propagation from IT to OT).

INSIGHT represents the NDR (Network Detection and Respons)/visibility component of the OT platform: It allows you to move from partial and fragmented visibility to continuous, structured

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

monitoring aligned with the detection, analysis and response requirements set out in the OT security standards.



Picture 3 – Inspection Process

4.4 RESCUE Module

The **RESCUE** module introduces an advanced level of configuration management and protection, bringing the principles of Change Management, versioning and continuous validation typical of CI/CD processes in the IT world to the OT environment. Its goal is to ensure business continuity and consistency of configurations across PLCs, RTUs, HMIs, network equipment, and supervisory systems, preventing human error and non-compliant changes that could compromise production. The module was born from a cyber requirement (integrity, traceability, separation of duties) that generates a direct and measurable impact on operations (quality of changes, recovery times, reduction of errors).

RESCUE acts as a central orchestrator of backup and OT configurations: configurations are extracted in a structured way from the equipment, stored in a versioned repository, related to the plants and associated changes. This lets you know at all times which configuration version is in production, who approved it, and what checks were performed before release.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

Key features include:

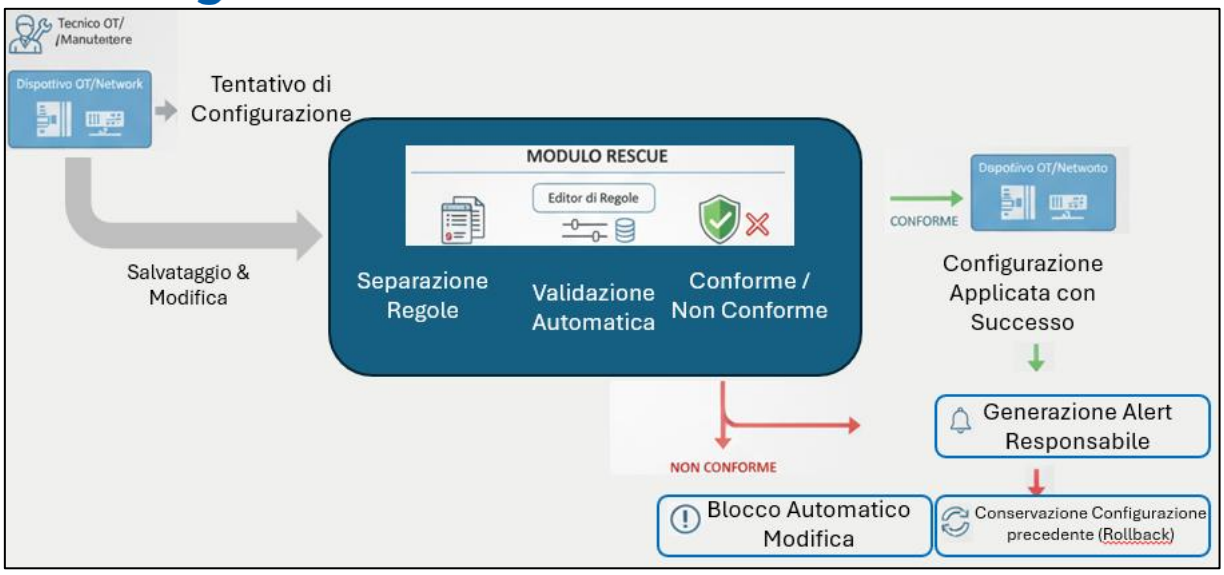
- **Rules and Policies Editor**: Define standardized configuration policies and compliance policies for all device classes. Rules act as a digital change management process, structuring changes before they are applied and ensuring that each operation is aligned with company security and operational standards.
- **Management of Allowed Variables and Ranges**: each configurable parameter (IP addresses, subnets, ports, time-outs, security settings, etc.) can be defined with allowed values or numerical/logical ranges. This ensures that all settings are consistent and compatible, eliminating the risk of risky or non-standard configurations.
- **Automatic Validation and Controlled Deployment**: before application, each change is automatically checked against the defined rules. In the event of non-compliance, the system blocks the change, generates an alert and keeps the previous configuration active, preventing negative impacts on operations. The same logic enables progressive rollouts (by line, site, cluster of equipment) with pre and post change controls.

RESCUE transforms configuration management from a manual activity to a controlled process: each change is versioned, "lint" by a dedicated Syntactic Validation Module, approved by a third party and released with signed evidence. In the event of an anomaly or incident, a secure rollback to the baseline is available and, if necessary, rapid recovery of known and validated backups.

In this way, RESCUE does not only act as a backup system, but as a real OT Element Manager: the Operator works faster and with fewer errors, the ICT obtains control and proof of conformity. Same process, two benefits: continuity and control.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com



Picture 4 – Configuration/Versioning Management process

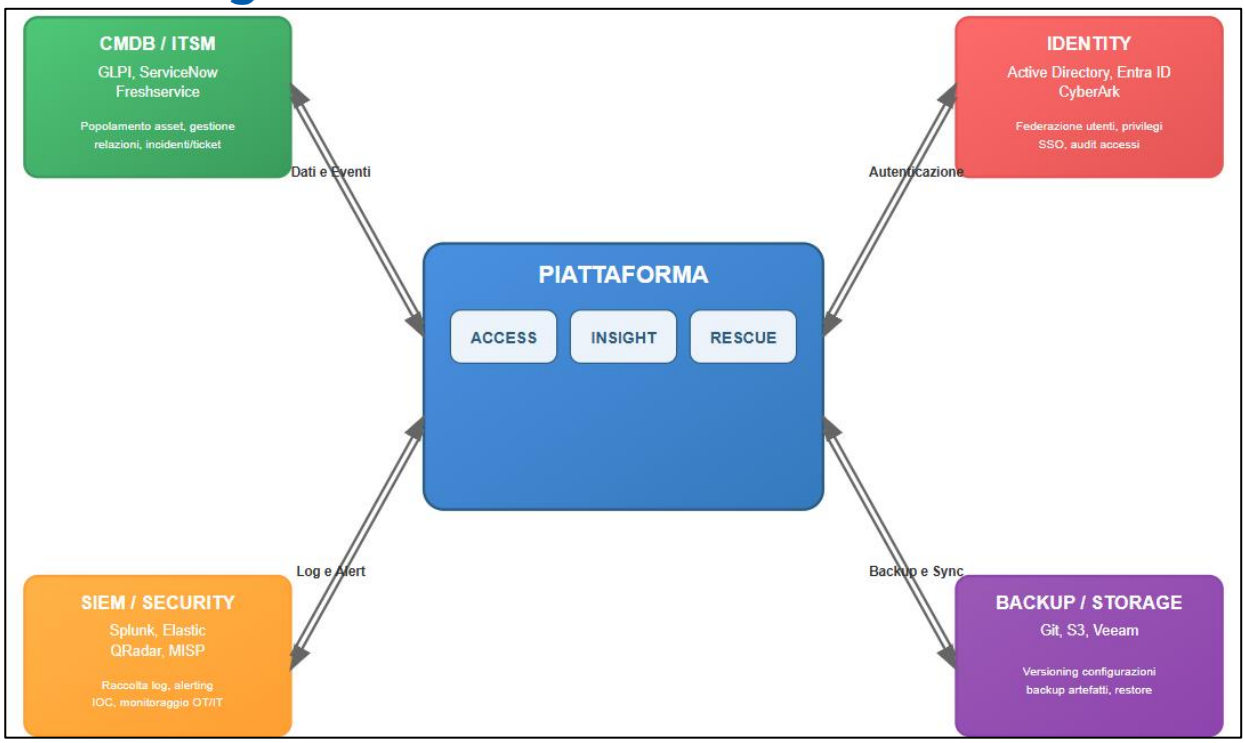
RESCUE is the **OT Element Manager** that brings the CI/CD discipline to plant configurations: the Operator works faster and with fewer errors, the ICT obtains control and conformity tests. Same process, two benefits: continuity and control.

5. Integration with external systems

Our platform is designed with an open and modular architecture, which does not aim to replace existing systems, but to enhance them and extend their functionality. Thanks to the use of standard **APIs** and connectors, the solution integrates natively and bi-directionally with the tools already present in the IT and OT ecosystem. This approach maximizes the value of past investments and enables safer, more consistent and efficient workflows.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com



Picture 5 - Integration with external systems

The strength of our architecture lies in its ability to act as a bridge between different technological worlds. This allows the use of existing tools, enriching workflows with data specific to the OT environment. All of this is done through **standard APIs**, **webhooks,** and **native connectors**, ensuring that existing operational flows are not interrupted.

Integration with external systems, such as CMDB/ITSM, consolidates asset inventory and automates management processes. Similarly, connecting to identity management and SIEM systems enhances the overall security posture, providing unified visibility and centralized control. Finally, integration with Backup and Storage systems ensures resiliency and business continuity, which are crucial in any industrial environment.

6. Deliverable

Upon completion of the implementation, the expected technical and operational deliverables (documentation, configurations, runbooks and test evidence) will be delivered, necessary for an autonomous and secure management of the OT environment.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

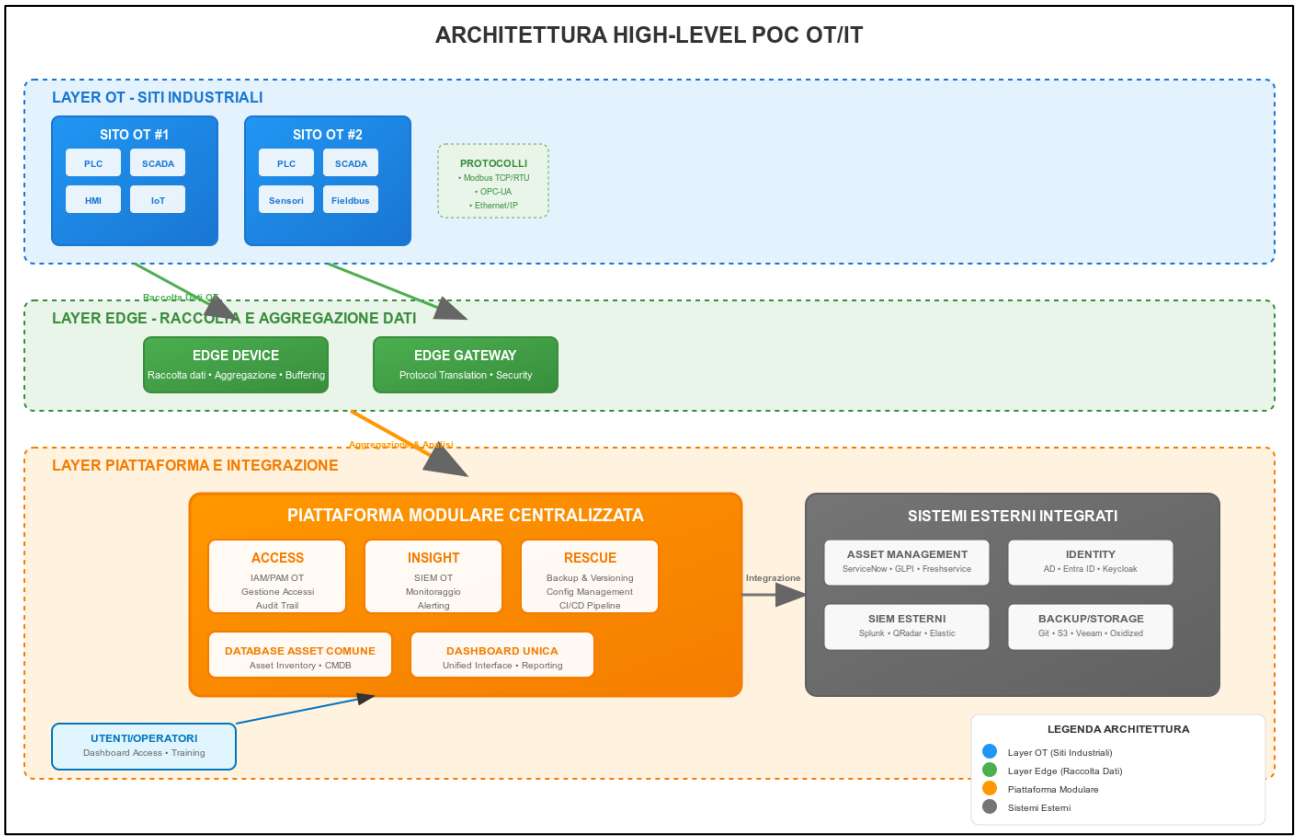
info@mashfrog.com
www.mashfrog.com

Deliverable	Description
Asset Assessment and Inventory Report	Detailed document highlighting the current status of OT/IT/IoT assets, their classification, vulnerabilities found, and recommendations for improvement.
Functional Operational Dashboard	An active, populated interface with real-time data from the pilot site, ready for monitoring, analysis, and centralized management.
Platform and Operating Modules	The complete platform, with **ACCESS**, **INSIGHT** and **RESCUE** modules, implemented and tested on the pilot site, ready for daily use.
Configuration Validation Report	A report that certifies the effectiveness of the versioning and validation process (CI/CD type), demonstrating the security and consistency of the configurations applied.
Operational Training and User Manual	Dedicated training sessions for IT and OT staff, accompanied by a detailed manual to ensure full autonomy in using the platform.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

7. Logic architecture and high-level diagram



Picture 6 – High-Level Diagram

The diagram shows how the solution via our OT/IT platform operates directly on the industrial site. At **OT** sites (**blue** layer), machines, PLCs, SCADAs, and IoT sensors generate data constantly during daily operations.

This data is collected by **Edge Devices** (**green** layer), locally positioned devices that aggregate machinery traffic, translate industrial protocols (such as Modbus and OPC-UA) and ensure that the information is secure and ready for processing.

From the Edge layer, data is sent to the **central Modular Platform** (**orange** layer), where the ACCESS, INSIGHT and RESCUE modules allow access management, OT infrastructure monitoring, backup and configuration versioning respectively.

The platform has a **common asset database** and a **single dashboard**, giving operators a complete and up-to-date view of the status of their plants. Finally, the platform integrates with **external systems** such as asset management tools, identity, SIEM, or backup solutions, enabling synchronization and interoperability with enterprise IT. In practice, the operational

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

flow is clear: the data is born in the OT site, is collected and prepared by the Edge, analyzed and managed by the platform, and finally integrated with external systems, allowing operators and managers to always have reliable information, in real time, without interrupting production.

8. Roadmap

The implemented platform defines the technical baseline for managing the security and operation of the OT environment. The results of the pilot phase enable the extension to a multi-site model, with uniform application of policies, standardization of processes and centralized visibility across all plants.

Planned evolutions include multi-site extension with collector scalability and policy templatization; the automation of changes (canary deploy, progressive rollout); the expansion of the library of DPI rules with support for additional protocols (TBD); the evolution of the API to version 2 with subscription mechanisms, advanced queries and exports in additional formats; and improved HA/DR with reduced RPO/RTO and storage optimization.

Our future roadmap includes:

- **Multi-site expansion**: Replicate the successful model in other production sites.
- **Evolution to Manufacturing Solution**: Transition the system to a complete manufacturing infrastructure, with a continuous maintenance and upgrade plan.
- **Ongoing Support**: Offering technical support and consulting services to maximize the return on investment in the long term.

Picture 7 - Next steps & benefits

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

9. Regulatory alignment (NIS 2 / IEC 62443)

The proposed OT platform is designed to concretely support the adoption of the main regulations and guidelines in the industrial field:

- the NIS 2 Directive and its national transposition, with particular reference to the obligations of risk management, access control, continuous monitoring and incident management;
- the IEC 62443 series of standards, which define requirements for industrial automation and control systems, with a focus on access management, communications security, configuration management and recovery capabilities.

The platform's contribution is organized around the three modules ACCESS, INSIGHT and RESCUE, which act as technological "bricks" to support the controls required by regulations.

9.1 General Approach

From a regulatory point of view, the platform does not limit itself to introducing new technologies, but structures OT processes in a "cyber by design" key:

- governance: traceability of accesses, configuration changes and maintenance activities on OT plants and networks;
- technical measures: strong authentication, segregation of access paths, passive monitoring, centralized management of backups and configurations;
- Evidence and audits: automatic production of logs, reports and baselines that form the documentary basis for internal audits, inspections and compliance checks.

This results a natural alignment with the requirements of NIS 2 and IEC 62443 principles relating to risk management, defence in depth and separation between control plane and data plane.

9.2 Contribution of the ACCESS module

ACCESS addresses identity, privileged access, and traceability requirements:

- Authentication and management of user identities
  - integration with company IdM/SSO (AD, Entra ID, LDAP);
  - use of passkeys/WebAuthn and MFA for access to the systems;
  - Reduction of local credentials on OT assets in favor of a centralized access broker.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

- Manage and log privileged remote access to assets
  - session broker based on Edge gateway, which opens sessions only after identity and authorization verification;
  - binding between session, identity, assets involved and motivation (ticket, change, maintenance intervention).
- Separation of Roles and Duties (SoD)
  - definition of distinct roles for operators, maintenance technicians, OT/IT administrators and service providers;
  - Ability to introduce multi-level approvals for the most critical accesses.
- Logging, Advisory & Vulnerability Management
  - generation of complete access logs, exportable to SIEM and audit systems;
  - integration with ticketing/ITSM tools to link access and changes to remediation and vulnerability management plans.

In this way, **ACCESS** directly contributes to the identity and access management, logging and accountability controls required by NIS 2, ACN and IEC 62443.

9.3 Contribution of the INSIGHT module

INSIGHT meets the requirements for monitoring, threat detection, and centralized logging:

- Continuous monitoring of OT assets and communication flows
  - passive network sensors based on PPE engines, installed on the Edges;
  - Discovery and dynamic mapping of industrial devices, lines, cells and protocols.
- Logging and analysis of OT logs and events
  - normalization of OT network events and sending to SIEM;
  - correlation with IT events for an integrated view of threats;
  - construction of behavioral baselines with which to compare new activities.
- Threat detection and alerting mechanisms
  - rules and use cases specific to the OT (anomalous commands, scanning, new devices, deviations from expected flows);
  - alerts to SOC/CSIRT or to OT contact persons for coordinated response actions.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

INSIGHT enables the transition from manual and partial monitoring to a structured logging and detection system, in line with NIS 2 and ACN requirements for continuous monitoring, incident detection and early reporting, and IEC 62443 requirements for communications protection and abnormal condition detection.

9.4 Contribution of the RESCUE module

RESCUE covers the requirements related to configuration management, health and recovery capabilities:

- Centralized backup of OT configurations
  - extraction and storage of configurations of PLC, RTU, HMI, switches, firewalls, etc.;
  - Versioned repository, with traceability of who made the last modification and when.
- Optimization of change management
  - structured workflows for proposal, validation, approval and deployment of changes;
  - automatic compliance checks against company rules and policies before the changes are applied.
- Preserving the integrity of configurations
  - syntactic and logical validation (linting) of configurations;
  - separation of duties between those who propose, approve and apply the changes;
  - historical evidence that allows us to demonstrate that the configuration "in production" is known and under control.
- Recovery solutions
  - Ability to quickly roll back to a known baseline configuration in the event of a failure or incident;
  - support for business continuity and disaster recovery plans for the OT environment.

These capabilities directly address NIS 2 and ACN requirements for backup, business continuity, and configuration management, and IEC 62443 objectives for asset lifecycle management, security levels, and protection against unauthorized changes.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com

9.5 Coverage Summary

In summary:

- **ACCESS** provides the "identity and access pillar", making OT remote accesses strongly authenticated, authorized, tracked and traceable to people and business processes.
- **INSIGHT** creates the "visibility and monitoring pillar", guaranteeing logging, detection and OT flow analysis capabilities integrated with the company SOC.
- **RESCUE** introduces the "configurations and resiliency pillar", transforming backup and OT changes into controlled, versioned and verifiable processes.

The joint adoption of the three modules allows the organization to demonstrate a level of maturity consistent with the requirements of NIS 2, with the technical and organizational measures indicated by ACN and with the security principles described in the IEC 62443 series, building a robust, sustainable and auditable industrial safety framework.

Sede legale
Via G. Peroni, 400/402
00131 - Roma
C.F. e P.IVA 02534640905

info@mashfrog.com
www.mashfrog.com