BRUCON BREWERY

Architecture Dossier

TABLE OF CONTENT

1. Introduction

1.1. Purpose of the document

The Architecture Document presents the general and detailed architecture of the target solution for the BruCON brewery. The Architecture Document formalizes the architecture description of the target solution and shows the implementation requirements of the systems in the brewery.

1.2. Scope of the document

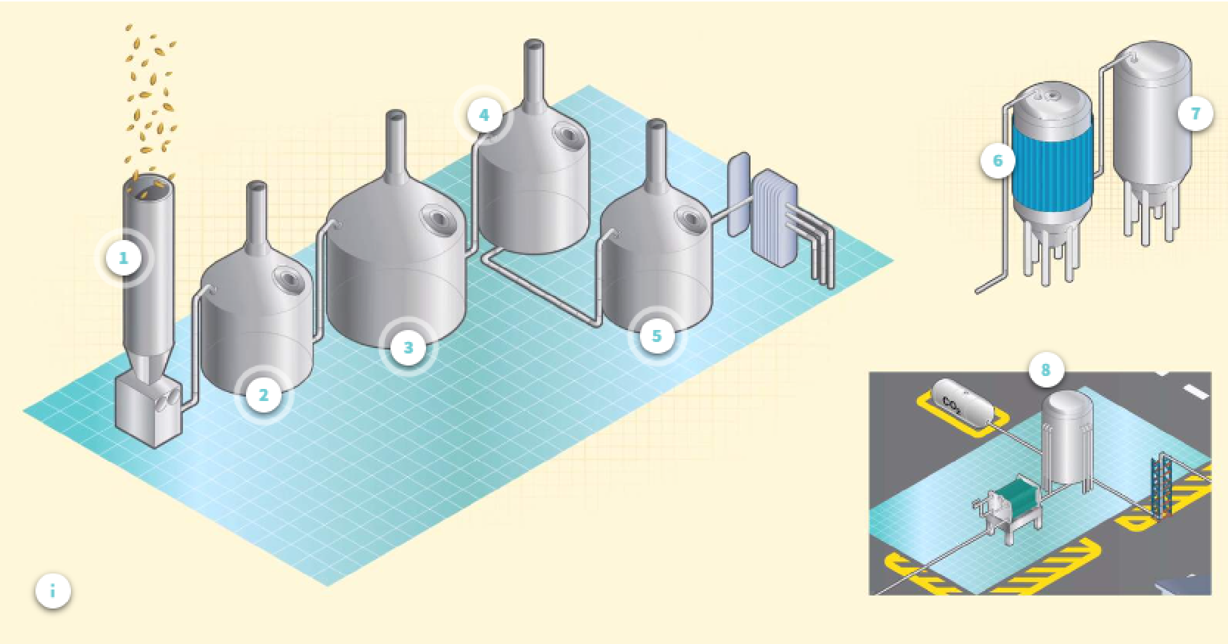
This Architecture Document focuses on the industrial systems deployment in the brewery and their interfacing with the IT infrastructure of the enterprise. The concerned security pillars in this dossier address key IAM aspects, remote access controls as well as auditing, logging and monitoring aspects.

1.3. Business Story

In an urgent response to market needs of beer production and to stay ahead of the competition, the brewery decided to perform a quick expansion of its production lines. Key elements that were taken into consideration, leverage existing infrastructure solutions where possible, be time and cost efficient in the implementation, and launch the new lines as soon as possible.

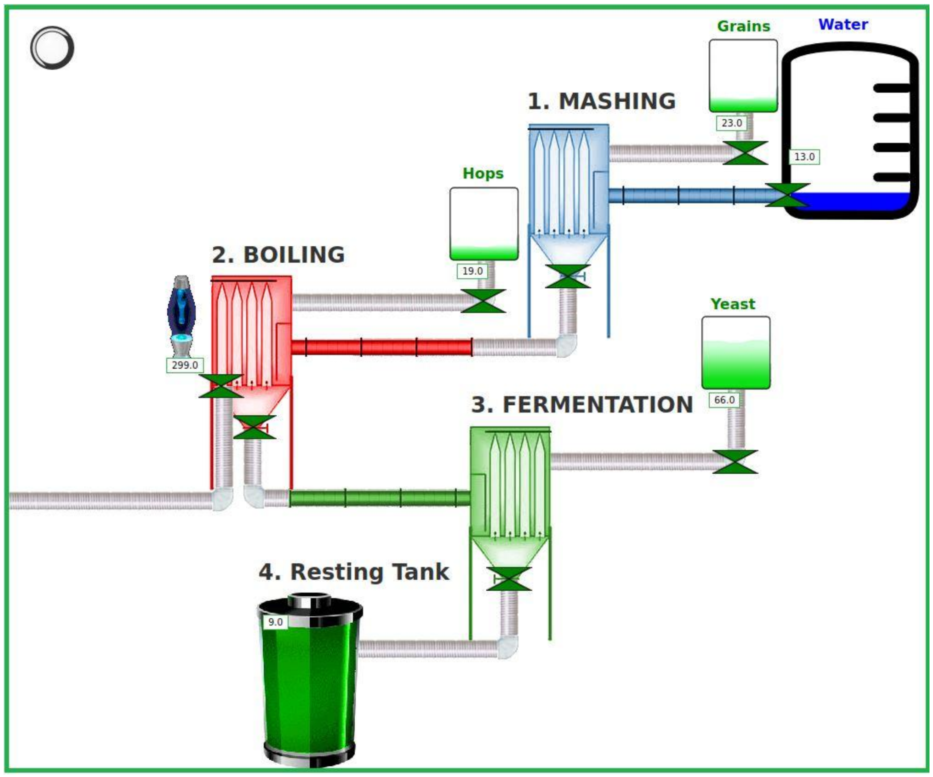
1.4. Solution Architecture Overview

1.4.1. High Level View Of Components per Brewing Line



High level view of Brewing Process

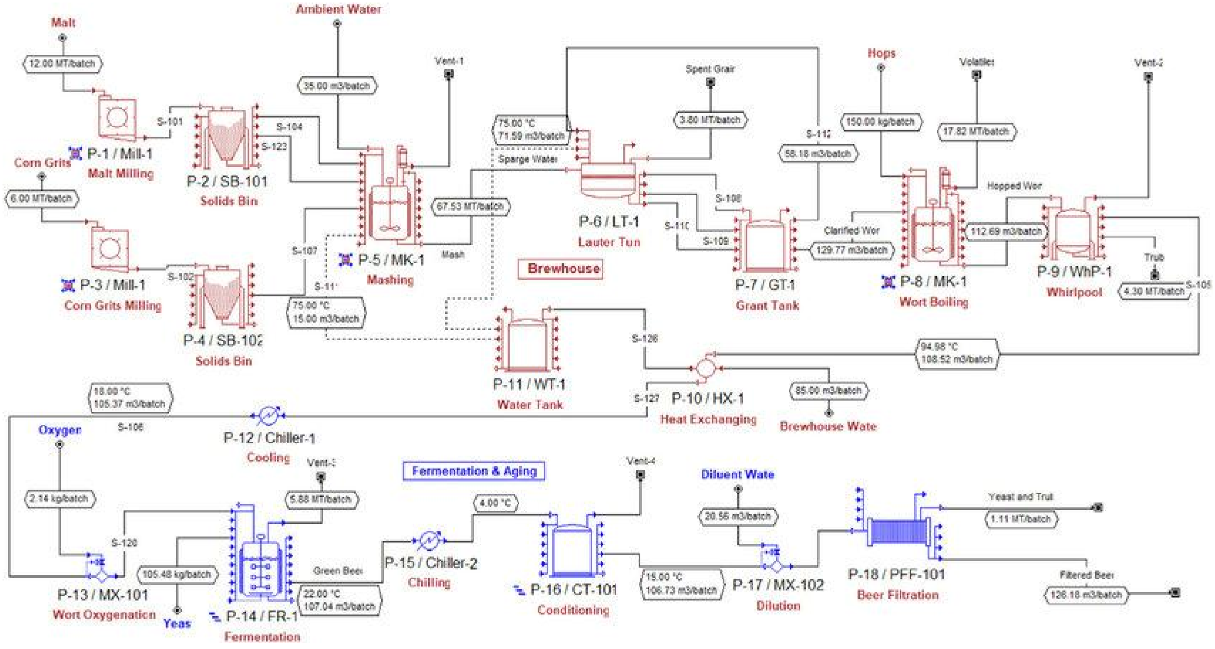
1.4.2. HMI Level Process View



HMI Process Monitoring

1.4.3. Brewery Flow Process Chart

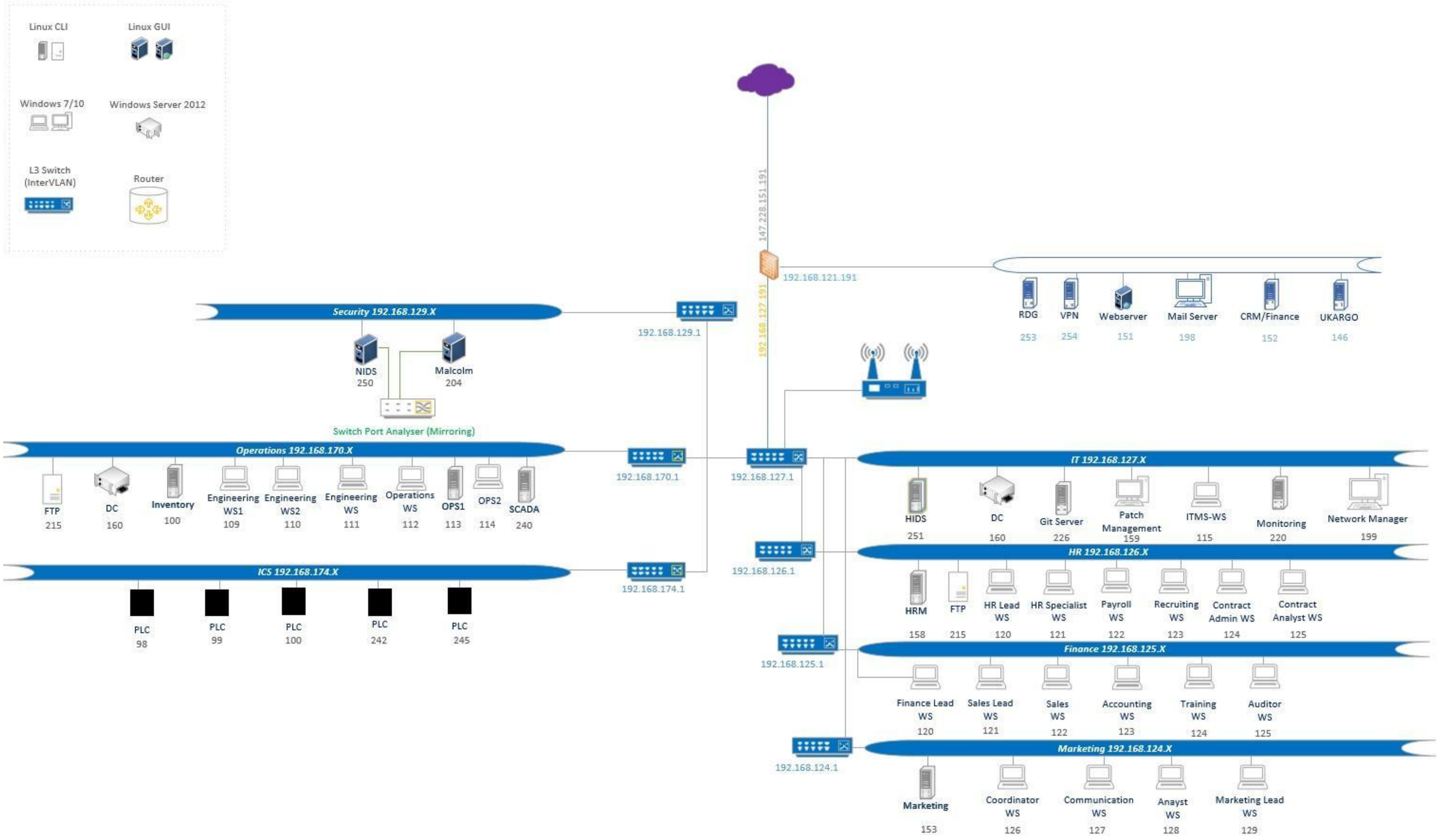
The section highlights the intended flow and component in the new implementation.



Brewing Flow Process Chart

1.4.4. Technical Architecture and Deployment Description

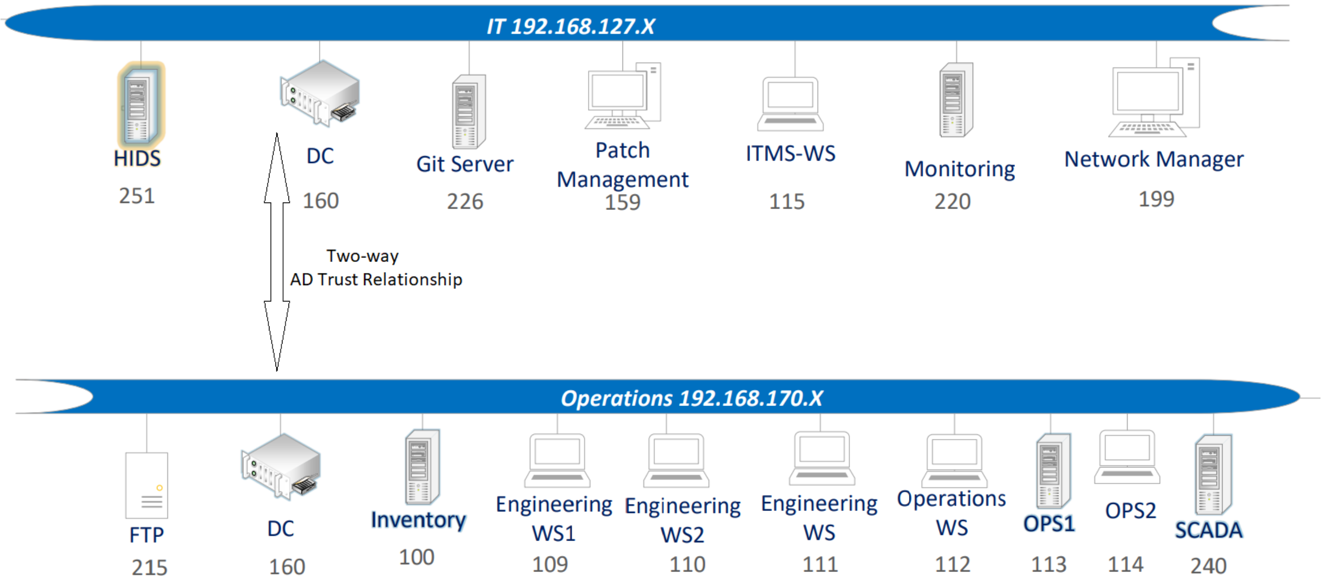
1.4.4.1. Network Architecture



Network Architecture Diagram

1.4.4.2. Industrial IDP and Directory Services Authentication

The primary Identity Provider and users directory within the industrial environment is the industrial active directory managed on a domain controller placed in the industrial operations network. It is built and designed to answer various operational and business needs for the industrial process. The industrial active directory has an established two-way trust relationship with the IT active directory. The authentication leverages directory services from the IT environment to provide user authentication services, usernames, passwords and enforces active directory policies. This can allow a faster deployment, and a seamless integration for authentication and access management across both environments.Users authenticated through IT active directory on an RBAC basis are allowed to carry necessary functions within the industrial environment.



AD Trust Relationship

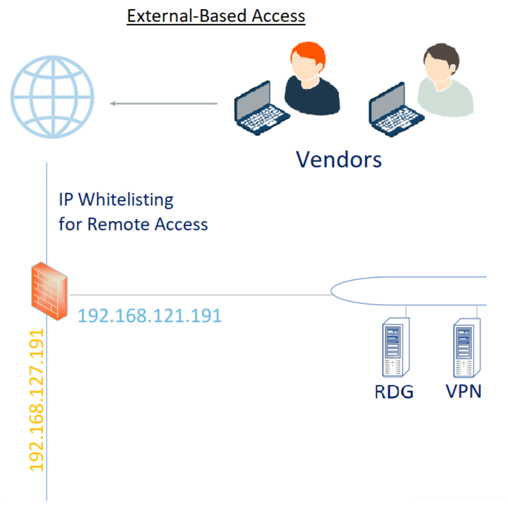
1.4.4.3. Remote Access - Internal and External-Based

Remote access provided in the architecture has the purpose of allowing authorized users to connect to industrial systems and process from external locations or networks outside of the industrial network. The accounts being created for remote access are managed by IT administrators in the brewery and created on a discretionary basis upon request on the active directory.

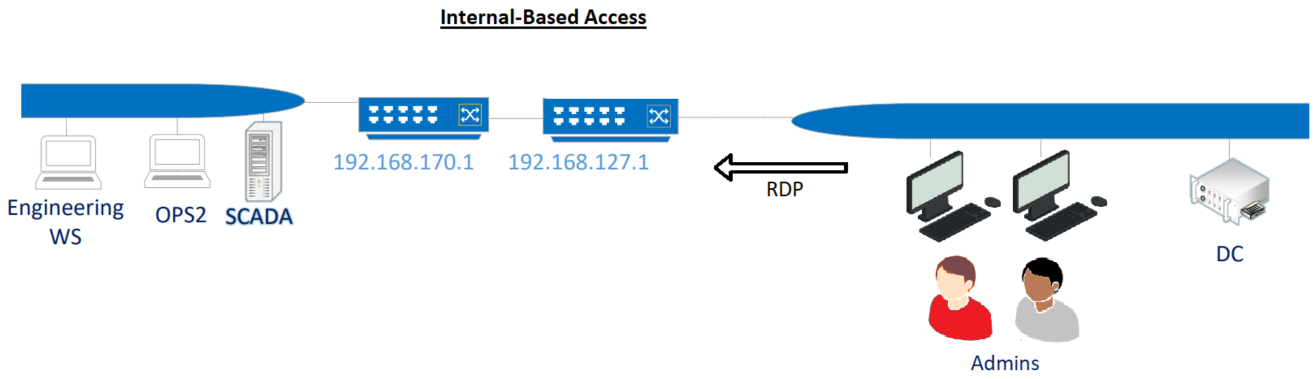
Remote access to the industrial environment is divided into two categories:

- Internal-based remote access operations refers to remote access taking place into the industrial network, having as a source any of the networks within the enterprise (hereby originating from IT network or any other business network). For ease of access, this access flows through internal networks across ATM switches and authentication takes place through the industrial active directory for any remote protocol.
- External-based access relevant to vendors and partners providing their support to industrial processes takes place over the internet through the company firewall with specific IP whitelisting for access from vendors and partners networks. The authentication then takes place through the active directory service into the IT environment, and users are routed internally to reach the designated assets for maintenance, support or operations.

For simplicity of management and operations, vendors and partners are provided with one shared account per vendor relying on a username and strong complex password, that their teams use to carry out their duties in an industrial environment.



External-Based Access



Internal-Based Access

1.4.4.4. Remote Access - Internal and External-Based

Auditing and logging is enabled on assets across the infrastructure in IT and OT environments:

- For network captured events, mirroring is leveraged for key assets and logs are stored inside the Security subnet.
- Remote access gateway and authentication logs are captured and stored locally.
- Servers and Users Endpoints' activity is being logged and captured locally on the assets including Windows Event Logs, and the logs of two security solutions installed on them which are the Anti-Malware and App Whitelisting solution.

Logs undergo periodic reviews twice a year with specific focus on authentication logs, and privileged accounts activities as well as key assets activity.

A monitoring server exists for deferred analysis of any abnormal event impacting operational resilience that takes place and focuses on critical elements for business operations, finance, emails and communication, administrative and legal functions in the company. The monitoring server is placed in an IT network with better proximity to these operations being monitored.

2. Record of Revisions and Validation

Date	Summary of Action/Revision	Stakeholder (s)	Comment
31/5/2023	**Architecture Dossier Document Creation**	Solution Architecture Team	
6/6/2023	**Finalization of Architecture Dossier and Push for Review**	Solution Architecture Team	Business urgency to increase brewing and fermentation lines count
13/6/2023	**Review of Architecture Security Posture**	Principal Security Architect	Reservations on security controls. Comments Report submitted with request to review again prior to deployment
22/6/2023	**Modifications applied on architecture**	Solution Architecture Team	Ready for deployment