**Status:** Updated the points from development team

**Approved by: To be approved by CAC Team**

**Released by:** Grow Digital Twin IAPM

**Internal**

**Document Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Ver.** | **Date** | **Changed by** | **Modifications** |
| 1.0 | 11/10/2023 | Ashok Mallya | Initial Version for PPGPL |
| 1.1 | 16/11/2023 | Kar Krishnendu, Dhanapal, Satish Bhatt, Vivek, Ashok Mallya | Updates specific to PPGPL MVP deployment & Standards Updates |
| 1.2 | 21/02/2024 | Ashok Mallya, Dhanapal, Satish Bhatt | Updates specific to Scope of Work, Updates from PC Checks completed and Cyber security SOTA added |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Project Details

|  |  |
| --- | --- |
| **Project Name** | PJ-109491\_PPGPL\_01 - DT-IAPM\_PPGPL |
| **PIF ID** | PJ-109491\_PPGPL\_01 - DT-IAPM\_PPGPL |
| **Related product part numbers** | NA |
| **Product Group/Name** | GROW/PAD |
| **Project Manager** | Ashok Mallya (GROW/PAD-PD) |
| **Other Details if any** | Gas Turbine, Pump, Cooling Fan |

# Product scope

## Intended use of the product

This software product/ solution is aimed at providing Integrated Asset Performance Management (IAPM) platform for 3 Assets under Scope as documented in SOW2 with PPGPL which is driven by a Digital Twin.

The Digital Twin IAPM is a dynamic software model that relies on sensor and instrumentation data to understand its state, respond to changes, predict outcomes, improve operations, and aid judgements for business decisions.

## Interfaces of the product

Built based on Sensors – Software – Services framework, the product accepts inputs from various sensors mounted on the assets used in PPGPL, processes these inputs to assess the health/ state of asset and predict the impending faults. Various insights generated by the solution are then presented to the user via IAPM visualizations which is a web-based dashboard. Any events detected on the assets is relayed to the user via email notifications as well.

## Target markets of the product

Target Market: PPGPL Plant, Trinidad & Tobago (Port of Spain, West Indies)

Target Market: US (since Azure cloud is in East US for PPGPL T&T Region)

## Known further relevant contractual commitments

The contractual agreement signed by RBNA & PPGPL

# State of the Art Report

## Legal requirements

As part of the current release scope, solution needs to adhere to the Data Protection requirements of the regions for the personnel data being processed.

## Standards, guidelines, and rules on which solution has been built

* ISO 13374 – Condition monitoring and diagnostics of machines
* ISO 55000 - Asset management - Overview, principles and terminology
* ISO 13373 Provides guidelines for vibration condition monitoring and diagnostics of machines.
* ISO 10816: Offers guidelines for evaluating machine vibration by measurements on non-rotating parts, specifically focusing on ISO 10816-1 (general guidelines) and ISO 10816-3 (vibration measurements on rotodynamic pumps).
* API 670 – Machinery protection system
* IEC 60034 - Standard for rotating electrical machinery.
* Bosch internal standards aligned with ISO 27001 (ISMS)
* The solution is hosted on Azure cloud which is certified for the following security standards:
* ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, MTCS, IRAP, and ENS
* [B1. Cybersecurity SOTA Document - Digital Twin IAPM - Docupedia (bosch.com)](https://inside-docupedia.bosch.com/confluence/display/DTIAPM/B1.+Cybersecurity+SOTA+Document)

## Industry standard requirements

* User Authentication: The front-end solution is authenticated via single sign on based on Azure Active directory. The back-end API’s are authenticated through JWT tokens. In addition to this, certain features of the solution that are used for configuration activities are accessible only to select users. However, as this solution is hosted on PPGPL tenancy, the customer would be given the option to choose the best suited methods to operate.
* Cloud and Data Security: All relevant cloud and data security aspects of the service provider will be evaluated, and a detailed TARA report generated.
* Data Twin: Display of time series raw sensory data that is being captured from the asset is made available in charts. In addition to this, there is a possibility to have a view of the historic data based on time selection.
* Fault Detection: The solution is equipped detecting the typical faults observed in the asset class. These faults are detected by the algorithms which are based on Model based & first principles. These faults classifications are then converted into insights bucketed as Engineering Insights, Operational Insights and Business Insights.
* 3D Visualization: The solution offers an immersive 3D view – Digital Twin of the asset with an overlay of sensor data on it. It is also designed to highlight subsystems in which faults are detected. This feature is not in scope for PPGPL
* Event History: A heat map view of the asset listing all the faults/ event captured in it is made available to the user. Each even captured has a cause and effect associated to it.
* Indication of KPI: A framework has been developed to configure and display the required KPI of the asset as required by the user.

## Safety requirements (Standard and State of Art)

|  |  |  |
| --- | --- | --- |
| **Sl. No.** | **Concept** | **Requirement** |
| SN-R1 | Privileged/Restrictive/Selective access to the assets | All database/assets protected against unauthorized access. |
| SN-R2 | Data verification/validation | Correctness of data maintained |
| SN-R3 | Logging and auditing | Logging and auditing enforced, and related data kept secure |
| SN-R4 | Data Retention in Database | Cloud level data retention on the Database for 1 month has been applied as its used for near real time visualization. Moreover archiving of data is taking place on a BLOB for 90 days . |
| SN-R5 | Privileged/Restrictive/Selective access to the assets | User will have privilege to PPGPL dashboard via AAD |
| SN-R6 | Role-Based Access Control (RBAC) | Access to run any action on a ADX , COSMOS , ML Studio , Key vault resource is restricted by assigning the appropriate Role-Based Access Control (RBAC) roles to only those needing the privileges has been ensured. the principle of least privilege has been followed. |
| SN-R7 | Input validation/Query handling | Not applicable |
| SN-R8 | Firewall/DMZ/Web App Firewall to ensure availability | Azure Firewall has been kept in place, any traffic from PPGPL/Internet will traverse via Azure Fire Wall. |
| SN-R9 | Security of important data at rest | AES 256 is enabled. Enabling encryption at rest on cluster to provide data protection for stored data has been considered |
| SN-R10 | Encrypted and authenticated communication | TLS 1.2 Encrypted. Restricted view access policy shall be enabled on tables in database which contain sensitive information and only principals with Unrestricted Viewer with role in the database shall be able query that data |
| SN-R11 | Security of important data at rest | JWT Token implementation valid for 1 Hour. Application shall specify cookie definition and ensure security of that. |
| SN-R12 | Security of data in transit | Ensuring secure communication via vpn tunnel using tls 1.2 encryption |
| SN-R13 | Autonomy to the system | solution is designed to give only recommendations to the user and the solution does not have any direct control of the asset. Hence there is not autonomous decision that is taken by the solution which influences the physical asset. |

## Residual Risks

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl. No.** | **Concept** | **Requirement** | **Risk** | **Mitigation Plan** |

NIL , as per TARA and same will be updated after validation and verification.

## Conformity of the Function & Usage - General

* Normal / expected behavior / functionalities: Intended use of the product is clearly defined in the user manual. At the current stage of the product maturity, there is no autonomy given to the system. This will to a certain extent prevent unintended use of the solution. Also, these aspects would be clearly identified and defined in the customer agreement at the beginning of a deployment.
* Interaction with environment: This is a complete software solution, hence there is no direct interaction with the environment. ( Cloud related security solutions and best practices have been adopted )
* Handling of product: There is no physical product involved in the solution.
* Azure compliance offering checked by Solution Architect

## Product Safety

## Safety of the intended functionality

* Avoidance of false positives & negatives: To the extent possible, the solution is developed to avoid false positives and negatives, however, the customer agreement would define these aspects and document the liabilities if any of both the parties in case of such situations.
* Handling performance limitations, incorrect / invalid assumptions & uncertainties: In the current release, the usage of the solution will be restricted to a limited functionality. Also, the insights provided by the system shall only be considered as recommendations and not mandates. Over a period, in future release, when there is closed loop system in place, specific limitation, uncertainties shall be handled on case-to-case basis.
* Recognition of system boundaries: Has been clearly defined in the user manual and will articulated in the contractual agreement.

1 2 3 4

## Functional Safety

* Avoiding systematic hardware & software failures: A through SW validation would be done to avoid systematic software failures.
* Dealing with random hardware failures: Not Applicable, this is a complete software solution.
* Safety in emergency situations: This solution does not have any influence on the hardware/ asset either in normative or emergency situations. It only provides insights to the user. It is at the discretion of the user whether to consider the insight or not.

# . Identification of the state of the art

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **S.No** | **Legal requirements, normative requirements, Safety requirements etc.** | **Related hazard / or safety concern** | **Safety Concepts according to Standard Industry Practice** | | **Applied methods, test engineering and production methods** | **Which solutions/methods are used in this project in order to reach the state of the art?** |
| **Known solution to reach State of the Art / Variants** | **Affected components (which have to implement solution, optional)** |
| 1 | Access to the solution | Manipulation of Recommendations/ Insights generated by the solution | Implement User Authentication | Front end | AD based User Authentication + Role based access to some administrative aspects of the solution | AD based User Authentication + Role based access to some administrative aspects of the solution |
| 2 | DB Access | 1. Data loss due to DB Corruption  2. Unauthorized access  3. Unintended deletion of collections & Documents | Exposure of DB only through endpoints | Backend (AKS), Frontend, Algorithms | WAP, Ingress Protection, API based exposure | Ingress Protection, API based exposure |
| 3 | File Storage | 1. Data loss due to DB Corruption  2. Unauthorized access  3. Unintended deletion of files from Blob containers | Access through Secure channels | Blob Storage | Service Endpoints | Encryption and back up of important database |
| 4 | Solution Insights | 1. Unintended usage  2. Unintended action by the system | NA | Insights generated by the solution | Such kind of autonomy is provided after a long testing period of the solution in practical scenarios + Vetting of the SMEs | MFA and Azure Active Directory +SSO |
|  |  |  |  |  |  |  |