Arquitectura del Sistema ACQC: Diseño e Integración OT Segura

Arquitectura técnica para la Célula Autónoma de Calidad en Repsol Puertollano

Mariano Millañanco Fernández
Puertollano. Ciudad Real, España
Universidad de Sevilla — Máster en Microelectrónica
UTAMED — Máster en Inteligencia Artificial
github.com/tangodelta217/ACQC
mariano.millananco@gmail.com

2026

Resumen

La Célula Autónoma de Calidad Circular (ACQC) es una solución para estimar y optimizar en tiempo real la calidad de producto en la refinería de Repsol Puertollano. En este documento se detalla la arquitectura técnica del sistema, integrando sensores analíticos en línea, modelos de inferencia de calidad (soft sensors) y un módulo de recomendación de setpoints operativos seguros. Se describe el alcance limitado al modo asesor (operador en el bucle), enfatizando la naturaleza *read-only* de la integración con los controladores de planta. Además, se definen los requisitos funcionales y no funcionales clave, las distintas vistas arquitectónicas (contexto, contenedores, despliegue), la arquitectura de datos (fuentes de información, sincronización y calidad de datos), los flujos operativos normales y degradados (fallback ante fallos o deriva), así como los mecanismos de observabilidad (registros, métricas, alertas) para la operación confiable. También se abordan la integración con entornos OT existentes bajo principios de ciberseguridad (segmentación en DMZ, credenciales, firma de firmware) y se enumeran riesgos técnicos identificados junto con sus mitigaciones.

Abstract

The Autonomous Circular Quality Cell (ACQC) is a solution to estimate and optimize product quality in real-time at the Repsol Puertollano refinery. This document details the technical architecture of the system, integrating inline analytical sensors, predictive quality inference models (soft sensors), and a safe setpoint recommendation module. The scope is limited to an advisory mode (human-in-the-loop), emphasizing the read-only integration with existing plant controllers. Key functional and non-functional requirements are defined, and various architectural views (context, containers, deployment) are presented. The data architecture (data sources, synchronization, quality), normal and degraded operational flows (fallback in case of sensor failure or model drift), and observability mechanisms (logging, metrics, alerts) are described to ensure reliable operation.

Keywords: soft sensors; PAT; optimización segura; seguridad OT; edge computing

Resumen ejecutivo (entregables medibles)

- Sistema de inferencia en tiempo real de calidad: sensor analítico (NIR/Raman) acoplado con modelos de ML (soft sensor) que logra un error esperado inferior al 5 % respecto al laboratorio.
- Modo *fallback* documentado: sensores virtuales suplen fallos del instrumento principal, con detección automática de deriva y recalibración periódica.
- Módulo de optimización robusta en modo asesor: recomienda ajustes de setpoint garantizando cero violaciones de restricciones de seguridad o calidad.
- Integración OT endurecida: el sistema edge emplea *secure boot*, firmware firmado y registra de forma auditable todos los datos, modelos y recomendaciones.
- Interfaz para el operador: *dashboard* con visualización de la calidad estimada, alarmas de confianza, histórico por lote y reportes de métricas de desempeño del sistema.

1. Alcance y contexto

La variabilidad de las materias primas circulares (como aceites de pirólisis plástica) dificulta mantener la calidad de los productos finales, introduciendo contaminantes e incertidumbre en el proceso **Lim2025**. En refino, la calidad del *feedstock* reciclado puede fluctuar ampliamente en términos de contaminantes y propiedades físicas, complicando la obtención de productos consistentes. Los métodos tradicionales dependen en gran medida de análisis de laboratorio *off-line*, que generan latencias significativas: los resultados llegan tarde y limitan la capacidad de ajuste proactivo. La tendencia moderna es implantar *Process Analytical Technology* (PAT) para monitorización en tiempo real, sustituyendo el control reactivo por un enfoque proac-

tivo **Sathiyapriyan2025**. Sin embargo, muchas plantas aún operan con visibilidad reducida en línea, lo que obliga a fijar márgenes operativos conservadores (setpoints subóptimos) para asegurar la especificación de calidad, a expensas de eficiencia energética y productividad. La idea de emplear *soft sensors* data-driven en la industria de proceso ha sido investigada desde hace décadas, demostrando su utilidad para complementar o reemplazar mediciones físicas tradicionales **Kadlec2009**.

En este contexto, el sistema **Autonomous Circular Quality Cell (ACQC)** surge como propuesta para integrar sensores analíticos en línea y analítica de datos avanzada con los sistemas de control de la planta. El objetivo es estimar en tiempo real las variables críticas de calidad del producto mediante *soft sensors* (modelos predictivos basados en datos) y complementar la operación con recomendaciones de ajuste que optimicen el rendimiento sin comprometer la seguridad.

El **alcance del proyecto TFM** se limita explícitamente a la monitorización y asesoramiento. La ACQC funcionará en modo *read-only* respecto al sistema de control: generará alertas y recomendaciones al operador, pero no actuará automáticamente sobre las válvulas o consignas del proceso. Cualquier implementación de control autónomo en lazo cerrado queda fuera de alcance y requeriría procedimientos formales de gestión de cambios (*Management of Change, MOC*) y validaciones adicionales.

2. Requisitos del sistema

Requisitos funcionales (RF)

- **RF-01: Ingestión de datos en tiempo real.** El sistema debe conectarse a las fuentes de datos de planta y obtener lecturas en tiempo real o casi tiempo real. La ingestión debe realizarse en modo lectura utilizando protocolos industriales estándar (p. ej. OPC UA o MQTT).
- **RF-02: Inferencia de calidad mediante *soft sensors*.** El sistema debe estimar continuamente los valores de las variables de calidad objetivo a partir de los datos de proceso y analíticos. Se espera lograr una precisión tal que el error promedio de las predicciones sea $< 5\,\%$ respecto al valor de laboratorio **Stanisic2024**.
- **RF-03: Detección de desviaciones y modo *fallback*.** El sistema debe monitorizar la calidad de los datos y el rendimiento de los modelos en línea para detectar anomalías.
- **RF-04: Optimización y recomendación de setpoints.** La ACQC debe calcular recomendaciones de ajuste de setpoints garantizando no violar límites de seguridad ni especificaciones de producto **Krishnamoorthy2023**.
- **RF-05: Interfaz de usuario y alertas.** El sistema debe proporcionar una interfaz visual (*dashboard*) accesible para el operador de planta.
- **RF-06: Registro y trazabilidad de decisiones.** El sistema debe registrar en un histórico todas las recomendaciones emitidas y las acciones del operador.

Requisitos no funcionales (RNF)

- **RNF-01: Latencia de inferencia.** Cada ciclo completo de inferencia debe ocurrir en segundos o sub-segundo.
- **RNF-02: Disponibilidad y robustez.** Se busca una disponibilidad mínima del 99 % durante el periodo de operación continua.
- **RNF-03: Seguridad informática.** El sistema debe cumplir con las políticas de ciberseguridad industrial, incluyendo autenticación robusta y comunicaciones cifradas.
- **RNF-04: Mantenibilidad y modularidad.** La arquitectura debe ser modular para facilitar su mantenimiento y evolución.
- **RNF-05: Observabilidad y diagnóstico.** El sistema debe exponer mecanismos de observación de su estado interno **Rani2024**.
- **RNF-06: Escalabilidad horizontal.** El diseño debe poder escalar a múltiples unidades o plantas.

3. Vistas de arquitectura

3.1 Vista de contexto

En la Figura 1 se ilustra la ACQC en relación con los sistemas y usuarios del entorno de Puertollano. Los principales actores son:

- **PLC/DCS de planta:** Proporciona las variables de proceso en modo solo lectura mediante OPC UA **Hirsch2023**.
- **Sensores analíticos en línea:** Instrumentos NIR o Raman que generan datos espectrales.
- **Historian / BBDD de proceso:** Base de datos histórica (p.ej. OSIsoft PI).
- **Laboratorio (LIMS):** Sistema de información de laboratorio con resultados de calidad medidos *off-line*.
- **Operador de planta:** Usuario final que visualiza estimaciones y recibe recomendaciones.

3.2 Vista de contenedores

A nivel interno, la ACQC se compone de varios módulos (Figura 2):

- **Módulo de Ingestión de Datos:** Comunicación con fuentes OT mediante OPC UA.
- **Módulo de Inferencia de Calidad:** Implementa los modelos ML/analíticos **Dietrich2025**.
- **Módulo de Detección de Anomalías y Fallback:** Supervisa calidad de entradas y salidas.
- **Módulo de Optimización Robusta:** Resuelve el problema de optimización para sugerir mejoras.
- **Módulo de Interfaz de Usuario:** Servidor web con *dashboard*.
- **Módulo de Registro & Monitoreo:** Persistencia de datos y observabilidad.

3.3 Vista de despliegue

La arquitectura de despliegue se basa en el modelo Purdue de redes industriales. El dispositivo **edge ACQC** se ubica en una zona de red segregada (DMZ industrial) intermedia entre la red de control de planta (nivel 2/3) y la red corporativa (nivel 4). El edge se conecta hacia la red de control OT únicamente para leer datos, a través de puertos específicos aprobados (por ejemplo, puerto TCP 4840 para OPC UA).

4. Arquitectura de datos

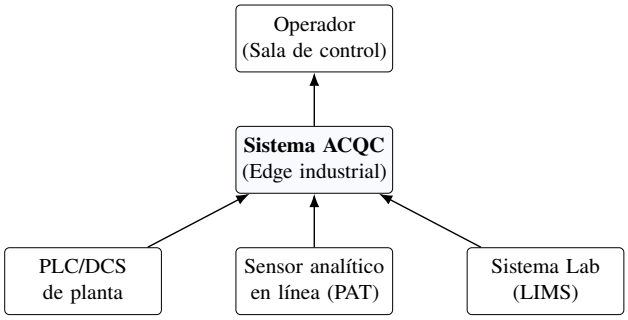

Figura 1: Vista de contexto: interacción de la ACQC con sistemas de planta y operador.

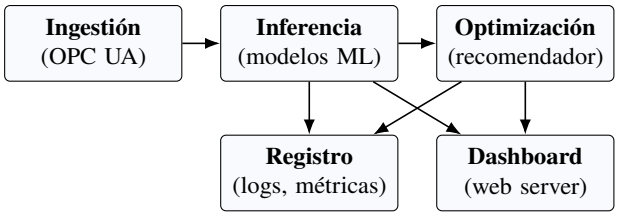

Figura 2: Vista de contenedores: principales módulos lógicos dentro del sistema ACQC.

4.1 Fuentes de datos integradas

- **Señales de proceso en planta:** Variables del PLC/DCS (temperaturas, presiones, caudales).
- **Datos de sensores analíticos:** Espectros NIR/Raman a intervalos regulares.
- **Resultados de laboratorio:** Propiedades de calidad medidas en muestras.
- **Metadatos de producción:** Identificador de lote, tipo de materia prima.

4.2 Calidad de datos y validación

Se define un **contrato de datos** para cada señal indicando sus unidades, rango físico plausible y significado. El sistema de ingestión aplica validaciones contra ese contrato **Teh2020**.

5. Flujos operativos

5.1 Flujo normal de operación

En condiciones normales, el sistema sigue un ciclo continuo:

1. *Adquisición de datos:* El módulo de ingestión lee periódicamente las variables de proceso.
2. *Inferencia de calidad:* El módulo de *soft sensors* ejecuta los modelos ML.
3. *Publicación en dashboard:* Las estimaciones se muestran en tiempo real.
4. *Optimización y recomendación:* El módulo optimizador evalúa oportunidades de mejora.
5. *Notificación de recomendación:* La recomendación aparece destacada para el operador.
6. *Acción del operador:* El operador decide implementarla o no.

5.2 Flujo de fallo de sensor (modo degradado)

Si ocurre un fallo en el sensor analítico principal:

1. El módulo de ingestión detecta la ausencia de nuevas lecturas.
2. El sistema activa una alarma de *Sensor Fault*.
3. Se activa el **modo degradado (fallback)**, empleando un modelo virtual alternativo.
4. Si el sensor vuelve, el sistema retorna a Estado Normal.

6. Observabilidad y operación

Cada módulo de la ACQC emite logs estructurados con distintos niveles (info, warning, error). Se exponen métricas para monitorización (latencia de inferencia, disponibilidad de datos, uso de CPU/memoria). Se preparan *runbooks* para diagnosticar y resolver problemas rápidamente.

7. Integración OT y seguridad

Se siguen principios de *defense-in-depth*, alineados con estándares ISA/IEC-62443 **Cheminod2013**:

- **Modo solo lectura:** La ACQC no envía comandos al DCS.
- **Credenciales y autenticación:** Cuentas de servicio dedicadas con permisos restringidos.
- **Cifrado de comunicaciones:** OPC UA en modo *SignAndEncrypt*, HTTPS para la interfaz web.
- **Segmentación de red:** Reglas de firewall estrictas en DMZ.
- **Hardening de la plataforma:** OS reducido, secure boot, firma de contenedores.

8. Riesgos técnicos y mitigación

1. **Datos insuficientes para entrenar modelos:** Planificar campañas de muestreo adicionales.
2. **Desviaciones de los modelos:** Implementar detección temprana de deriva y recalibración periódica.
3. **Fallo del sensor analítico principal:** Desarrollo del modelo de respaldo.
4. **Latencia excesiva en inferencia:** Optimizar código y modelos.
5. **Integración con DCS/historian falla:** Probar conectividad con anticipación.
6. **Resistencia de operadores:** Involucrar a operadores desde etapas tempranas.
7. **Ataque cibernético a la ACQC:** Medidas de seguridad robustas.

9. Anexos

9.1 Diccionario de tags (extracto)

Tag	Unidad	Rango	Notas
FI_101	t/h	0–100	Caudal alim.
TI_101	°C	300–380	Temp. reactor
NIR_Absorb	–	0–3	Absorbancia
Lab_Visc40	cSt	0.5–5.0	Viscosidad

9.2 Variables de calidad objetivo

- **Densidad @15°C (kg/m^3):** Indicador básico de calidad de hidrocarburo.
- **Viscosidad cinemática @40°C (cSt):** Resistencia al flujo del producto.
- **Índice de acidez (mg KOH/g):** Cantidad de ácido en el producto.

- **Contenido de Cloro (ppm):** Presencia de cloro, crítico por corrosión.

9.3 Puertos/protocolos principales

- **OPC UA:** Puerto TCP 4840 – Suscripción a datos de proceso.
- **HTTPS Dashboard:** Puerto TCP 443 – Servidor web del edge.
- **NTP:** Puerto UDP 123 – Sincronización horaria.
- **SSH:** Puerto TCP 22 – Acceso remoto (opcional).

9.4 Glosario de términos

- **ACQC:** *Autonomous Circular Quality Cell*.
- **PAT:** *Process Analytical Technology*.
- **PLC:** *Programmable Logic Controller*.
- **DCS:** *Distributed Control System*.
- **Historian:** Base de datos histórica de proceso.
- **LIMS:** *Laboratory Information Management System*.
- **DMZ:** *Demilitarized Zone*.
- **Soft sensor:** Modelo que estima una variable de difícil medición directa.
- **CQA:** *Critical Quality Attribute*.
- **KPI:** *Key Performance Indicator*.