

Detección de eventos anómalos en un entorno industrial mediante el uso de técnicas de Federated Learning.

**Darío Martín García Carretero**

Máster Universitario en Ciencia de Datos

Área 2

**Raúl Parada Medina**

**Jordi Casas Roma**

08/01/2020

Creative Commons License

This work is licensed under a [Creative Commons Attribution 4.0 International License](http://creativecommons.org/licenses/by/4.0/).

**FICHA DEL TRABAJO FINAL**

|  |  |
| --- | --- |
| **Título del trabajo:** | *Detección de eventos anómalos en un entorno industrial mediante el uso técnicas de Federated Learning.* |
| **Nombre del autor:** | *Darío Martín García Carretero* |
| **Nombre del consultor/a:** | *Raúl Parada Medina* |
| **Nombre del PRA:** | *Jordi Casas Roma* |
| **Fecha de entrega (mm/aaaa):** | 01/2020 |
| **Titulación:** | *Máster en Ciencia de Datos* |
| **Área del Trabajo Final:** | *Área 2* |
| **Idioma del trabajo:** | *Español* |
| **Palabras clave** | *eventos anómalos, entorno industrial, federated learning* |
| **Resumen del Trabajo (máximo 250 palabras):** *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.* | |
| Un evento anómalo es aquel que se produce de forma repentina y sin previsión. En un entorno industrial estos eventos (generalmente fallos en las máquinas) pueden provocar grandes daños por lo que su detección puede ayudar a prevenir situaciones críticas.  El objetivo del proyecto es mostrar como detectar las posibles anomalías que se pudieran producir en los equipos industriales mediante el uso de un modelo de aprendizaje automático. Para enseñar a distinguir a un modelo entre un comportamiento normal y otro anormal se necesitan datos, contra más datos, mejor.  Hoy en día la mayoría de los componentes dentro de un entorno industrial están monitorizados mediante el uso de dispositivos de medición especializados. Disponemos de los datos suministrados por nuestros dispositivos de medición para entrenar al modelo, pero ¿y si pudiéramos disponer de más datos? Muchos equipos industriales son de uso genérico y pueden ser usados para muchas tareas y en muchos tipos de instalación. Si pudiéramos tener acceso a los datos de todos esos dispositivos podríamos crear un modelo mucho mejor.  Por diversas razones a las compañías no les gusta compartir sus datos. Por este motivo en este trabajo se propone el uso del Federated Learning (FL). Gracias a el FL se pueden construir modelos aprovechando toda la información disponible manteniendo la privacidad de los datos sensibles. | |
| **Abstract (in English, 250 words or less):** | |
| An anomalous event is one that occurs suddenly and without foresight. In an industrial environment, these events (usually machine failures) can cause great damage, so their detection can help prevent critical situations.  The objective of the project is to show how to detect possible anomalies that could occur in industrial equipment using a machine learning model. To teach a model to distinguish between normal and abnormal behaviour, data is needed, the more data, the better.  Today, most components within an industrial environment are monitored by specialized measuring devices. We have the data provided by our measuring devices to train the model, but what if we could have more data? Many industrial equipment is generic and can be used for many tasks and in many types of installation. If we could have access to the data of all those devices, we could create a much better model.  For various reasons companies do not like to share their data. For this reason, this paper proposes the use of Federated Learning (FL). Thanks to the FL, models can be built taking advantage of all available information while maintaining the privacy of sensitive data. | |

**Índice**

[1. Introducción 1](#_Toc27673705)

[1.1 Contexto y justificación del trabajo 1](#_Toc27673706)

[1.2 Objetivos del Trabajo 2](#_Toc27673707)

[1.3 Enfoque y método seguido 2](#_Toc27673708)

[1.4 Planificación del Trabajo 3](#_Toc27673709)

[1.5 Breve sumario de productos obtenidos 4](#_Toc27673710)

[1.6 Breve descripción de los otros capítulos de la memoria 4](#_Toc27673711)

[2. Estudio del estado del arte 5](#_Toc27673712)

[2.1 Detección de eventos anómalos 5](#_Toc27673713)

[2.2 Federated Learning 10](#_Toc27673714)

[2.3 Novedades propuestas 11](#_Toc27673715)

[3. Escenario 12](#_Toc27673716)

[4. ¿Qué es Federated Learning? 14](#_Toc27673717)

[5. Diseño 16](#_Toc27673718)

[5. Implementación 17](#_Toc27673719)

[5.1 Preparación del entorno de trabajo 17](#_Toc27673720)

[4.3 Simulación de un entorno industrial 17](#_Toc27673721)

[4.3.1 Introducción 17](#_Toc27673722)

[4.3.2 Caracterización de la degradación de las máquinas 18](#_Toc27673723)

[4.3.3 Evolución de las condiciones operacionales 19](#_Toc27673724)

[4.3.4 Proceso de simulación 22](#_Toc27673725)

[4.3.5 Configuración de la simulación 23](#_Toc27673726)

[4.3.6 Resultados de la simulación 23](#_Toc27673727)

[4.4 Creación de un modelo para la detección de eventos anómalos 25](#_Toc27673728)

[4.4.1 Adquisición de los datos 25](#_Toc27673729)

[4.4.2 Análisis de los datos 25](#_Toc27673730)

[4.4.3 Elección del tipo modelo 28](#_Toc27673731)

[4.4.4 Procesado de los datos 28](#_Toc27673732)

[5. Conclusiones 34](#_Toc27673733)

[6. Glosario 35](#_Toc27673734)

[7. Bibliografía 36](#_Toc27673735)

[6. Anexos 38](#_Toc27673736)

**Lista de figuras**

[Fig. 1 Los fallos no controlados pueden tener resultados catastróficos 1](file:///D:\Master%20Data%20Science\TFM\PEC\PEC3\doc\TFM_PEC3_v5.docx#_Toc27673743)

[Fig. 2 Planificación del trabajo 3](#_Toc27673744)

[Fig. 3 IRESE framework 5](#_Toc27673745)

[Fig. 4 Arquitectura de la red propuesta 6](#_Toc27673746)

[Fig. 5 Proyecciones PCA de los datos temporales 7](#_Toc27673747)

[Fig. 6 Arquitectura GAN propuesta 7](#_Toc27673748)

[Fig. 7 Modelo híbrido propuesto 8](#_Toc27673749)

[Fig. 8 Identificación de una instancia normal (izquierda) y una anormal (derecha) 9](#_Toc27673750)

[Fig. 9 Arquitectura de una Replicator Neural Network (izquierda) y función de activación de la capa intermedia (derecha) 9](#_Toc27673751)

[Fig. 10 Cada dispositivo personaliza el modelo localmente (A). Las actualizaciones de muchos usuarios se agregan (B) para actualizar el modelo global que se compartirá con todos los usuarios (C), después de lo cual se repite el proceso. 10](#_Toc27673752)

[Fig. 11 Arquitectura de la U-Net utilizada 11](#_Toc27673753)

[Fig. 12 Esquema de funcionamiento del Federated Learning 14](#_Toc27673754)

[Fig. 13 Curvas de degradación para diferentes parámetros 18](#_Toc27673755)

[Fig. 14 Efecto de la degradación en la velocidad 20](#_Toc27673756)

[Fig. 15 Efecto de la degradación en la temperatura 21](#_Toc27673757)

[Fig. 16 Efecto de la degradación en la presión 22](#_Toc27673758)

[Fig. 17 Ejemplo de un archivo de configuración de una simulación 23](#_Toc27673759)

[Fig. 18 Representación gráfica de los datos operacionales 27](#_Toc27673760)

[Fig. 19 Datos operacionales junto con los datos de mantenimiento 27](#_Toc27673761)

**Lista de ecuaciones**

(Ecuación 1) 18

(Ecuación 2) 19

(Ecuación 3) 19

*(Ecuación 4)* 20

(Ecuación 5) 20

(Ecuación 6) 21

**Lista de tablas**

[Tabla 1 Fragmento de archivo de telemetría 24](#_Toc27673762)

[Tabla 2 Fragmento del registro de mantenimiento 25](#_Toc27673763)

[Tabla 3 Datos descriptivos de la máquina 26](#_Toc27673764)

[Tabla 4 Tabla de correlaciones 26](#_Toc27673765)

# 1. Introducción

## 1.1 Contexto y justificación del trabajo

Un evento anómalo es aquel que se produce de forma repentina y sin previsión. En un entorno industrial estos eventos (generalmente fallos en las máquinas) pueden provocar grandes daños por lo que su detección puede ayudar a prevenir situaciones críticas.

El objetivo del proyecto es demostrar cómo se pueden detectar las posibles anomalías que se pudieran producir en los equipos industriales mediante el uso de un modelo de aprendizaje automático. Para enseñar a distinguir a un modelo entre un comportamiento normal y otro anormal se necesitan datos, contra más datos, mejor. Hoy en día la mayoría de los componentes dentro de un entorno



Fig. 1 Los fallos no controlados pueden tener resultados catastróficos

industrial están monitorizados mediante el uso de dispositivos de medición especializados. Dispondremos de los datos suministrados por nuestros dispositivos de medición para entrenar un modelo, pero ¿y si pudiéramos disponer de más datos? Muchos equipos industriales son de uso genérico y pueden ser usados para muchas tareas en muchos tipos de instalación. Si pudiéramos tener acceso a los datos de todos esos dispositivos podríamos crear un modelo mucho mejor.

Por diversas razones a las compañías no les gusta compartir sus datos, es por este motivo por lo que en este trabajo se propone el uso del Federated Learning (FL). Con el FL se pueden construir modelos aprovechando toda la información disponible manteniendo la privacidad de los datos.

## 1.2 Objetivos del Trabajo

El objetivo es mostrar un caso de uso para la aplicación del Federated Learning en la detección de eventos anómalos en entornos industriales, en nuestro caso, fallos en máquinas. La finalidad es que la metodología aquí presentada pueda servir como base para el desarrollo e implantación de soluciones similares en diferentes tipos de situaciones y/o entornos.

## 1.3 Enfoque y método seguido

El método que se seguirá se describe a continuación:

**Preparación del entorno de trabajo**

Se instalarán las herramientas necesarias para la generación de los conjuntos de datos, la gestión y el análisis de los datos y para la creación de los modelos necesarios.

**Simulación de un entorno industrial**

Se implementará un software que permitirá simular un entorno industrial. De esta simulación será de donde se obtendrán los datos necesarios para la creación de los modelos.

**Análisis de los datos generados**

**Elección del framework Federated Learning**

Actualmente existen dos alternativas: TensorFlow y PySyft (basada en Torch) se evaluará cual es la más conveniente y se instalará el framework elegido en el entorno de trabajo.

**Elección del modelo a utilizar**

Posteriormente se decidirá sobre el tipo de modelos que se usarán basándonos en la información obtenida del análisis del estado del arte.

**Selección de los criterios de evaluación del modelo**

Se seleccionarán los métodos más convenientes para el caso de estudio (Precision, F-Score, Accuracy, etc.).

**Creación y evaluación de los modelos**

Se realizarán múltiples pruebas con los distintos conjuntos de datos generados y con los distintos modelos creados con la finalidad de evaluar la calidad de estos últimos.

**Discusión de los resultados y análisis de posibles extensiones**

## 1.4 Planificación del Trabajo

La planificación temporal del trabajo es la siguiente:

* **18 septiembre – 20 octubre**:
  + Definir el alcance del TFM.
  + Decidir el conjunto de datos a usar.
  + Decidir el tipo de modelos/ técnicas a usar en base al estudio del estado de arte.
* **21 octubre – 21 diciembre:**
  + Instalación del entorno de trabajo
  + Obtención del conjunto de datos
  + Procesado del conjunto de datos
  + Generación de los modelos
  + Análisis de la calidad de los modelos
  + Análisis de los resultados y estudio de posibles extensiones
* **22 diciembre – 8 enero:**
  + Redacción de la memoria
  + Creación de la presentación
* **9 enero – 22 enero:**
  + Defensa pública del trabajo

A continuación, se muestra un diagrama con la programación establecida:



Fig. 2 Planificación del trabajo

## 1.5 Breve sumario de productos obtenidos

Como ya se ha mencionado el objetivo del trabajo es mostrar una metodología por lo que el objetivo de los modelos aquí generados no se extiende más allá de su uso a nivel didáctico y su aplicación en entornos reales no tiene mucho sentido. Si embargo, todo el procedimiento hasta llegar a su construcción puede resultar de gran interés en la resolución de problemas similares y justamente esto, el proceso, es lo que podría considerarse como el producto obtenido de este trabajo.

## 1.6 Breve descripción de los otros capítulos de la memoria

En el apartado 2, se presenta un estudio del estado del arte con el objetivo de conocer cómo se han solucionado en el pasado problemas similares. Esto nos servirá para dos cosas: inspirarnos a la hora de construir una solución para el problema que nos ocupa y para no repetir estudios o trabajos que ya se realizaron en su momento.

En el apartado 3, se hace una detallada explicación del problema que se desea solucionar incluyendo cuales son las necesidades y restricciones a las que tendremos que hacer frente.

En el apartado 4, se realiza una breve explicación de en qué consiste y de cómo funciona el Federated Learning.

En el apartado 5, encontramos una breve descripción del procedimiento que se va a seguir a la hora de construir y evaluar de los modelos.

En el apartado 6, se detallará todo el proceso de la construcción y evaluación de estos modelos.

En el apartado 7, se evaluarán los resultados obtenidos y se reflexionará sobre las posibles extensiones o líneas de trabajo futuras.

# 2. Estudio del estado del arte

Este trabajo aborda dos temáticas que, aunque relacionas entre sí, puede ser estudiadas de forma independiente. Por este motivo se realizará el estudio del arte de manera independiente.

## 2.1 Detección de eventos anómalos

Un evento anómalo es una observación (o pequeño conjunto de observaciones) que ocurre infrecuentemente y que se desvía o es inconsistente con respecto al resto de observaciones lo suficiente como para indicar que se está produciendo una anomalía en el conjunto de datos.

La detección de este tipo de eventos se ha estudiado ampliamente en la literatura científica desde multitud de enfoques diferentes. A continuación, se muestran algunos de ellos:

**IRESE: An intelligent rare-event detection system using unsupervised learning on the IoT edge** [2]

Este documento propone un sistema de detección de eventos anómalos basado en el uso de modelos de Machine Learning no supervisados (clustering) en tiempo real. El procedimiento se divide en cuatro fases:

1. Captura de los datos.
2. Extracción de características.
3. Clustering online, se aplica el algoritmo BIRCH (Balanced Iterative Reducing and Clustering using Hierarchies) para generar micro-clusters.
4. Clustering offline, se utiliza Agglomerative Clustering que finalmente genera dos macro-clusters, uno que contiene los eventos normales y otro con los eventos raros.



Fig. 3 IRESE framework

Las principales ventajas que ofrece este framework son dos, una es que gran parte del proceso se lleva a cabo en dispositivos locales (edge devices) lo que reduce la sobrecarga en la red y la latencia del sistema. La otra es que no se necesita etiquetar los eventos anómalos debido al uso de algoritmos no supervisados. En cuanto a las desventajas, la principal sería la extracción de características ya que este procedimiento es muy dependiente del tipo de datos que se quieren procesar.

En cuanto a los resultados, el articulo menciona que se han obtenido valores de precision y de recall por encima del 90% en algunos casos.

**Anomaly detection in ECG time signals via deep long short-term memory networks** [3]

Este trabajo utiliza la detección de eventos anómalos con fines médicos. En particular se analiza el uso de redes neuronales LSTM (Long Short-Term Memory) profundas para la detección de anomalías en las señales EGC (electrocardiogramas).



Fig. 4 Arquitectura de la red propuesta

Si denotamos una señal EGC como X = {x(0), …, x(i), …, x(n)} donde cada x(i) representa un valor del EGC en el tiempo i. El procedimiento a grandes rasgos es el siguiente:

1. Se entrena la red con el siguiente objetivo: predecir los k siguientes valores del EGC para cada x(i).
2. A partir de la red construida se obtiene un conjunto de vectores de error para cada x(i). Con estos vectores de error se ajusta una distribución normal multivariante.
3. A partir de esa distribución se calcula la probabilidad de ocurrencia del vector de error obtenido y en función de un threshold se determina si ese punto anómalo o no.

Este método presenta varias ventajas sobre otros métodos:

1. No se requiere apenas preprocesamiento de los datos.
2. No se necesita saber a priori el tipo de anomalías que pueden aparecer.

El método proporciona resultados bastante buenos llegando valores para el

F-score por encima de 0.9 para varias clases de anomalías.

**Diagnosing Network-Wide Traffic Anomalies** [4]

El documento explora el uso del método PCA (Principal Analysis Components) para la detección de eventos anómalos en una red de comunicación. La idea consiste en dividir el espacio original en dos subespacios, uno que captura el comportamiento normal y otro el anómalo. El espacio normal estará formado por las componentes que capturan más varianza mientras que el espacio anómalo estará formado por los componentes que capturan menos varianza.



Fig. 5 Proyecciones PCA de los datos temporales

Gracias a esta división podremos descomponer cada instancia en sus componentes normales y anormales. Para determinar cuándo se ha producido un evento extraño se utiliza la norma del vector del espacio anómalo. Si esta norma no sobrepasa cierto threshold se considerará como un evento normal en otro caso se identificará como un evento anómalo.

Los resultados muestran altas tasas de detección y bajas tasas de falsos positivos.

**Anomaly Detection with Generative Adversarial Networks for Multivariate Time Series** [5]

Este estudio utiliza una arquitectura GAN (Generative Adversarial Network) como mecanismo para la detección de eventos anómalos en un entorno industrial informatizado. Una arquitectura GAN está pensada como un sistema generativo (dada una distribución, el sistema es entrenado para generar datos que sigan esa distribución). Un sistema GAN está formado por dos redes neuronales: una llamada generativa que es la encargada de generar datos que sigan la distribución dada y una llamada discriminante, que se encarga de ayudar al entrenamiento de la primera. El objetivo del método propuesto es entrenar la arquitectura GAN para que aprenda a generar situaciones de uso normal. A continuación, se muestra un esquema del sistema propuesto:



Fig. 6 Arquitectura GAN propuesta

Para determinar cuándo una situación es anómala el sistema se basa en una puntuación (una combinación entre en la diferencia entre el input real y el generado y el valor de salida de la red discriminante).

Una de las principales ventajas de este método es que es no supervisado por lo que no es necesario el etiquetado de las muestras. Por otro lado, su principal desventaja es su alto coste computacional. Con respecto a su rendimiento, el documento menciona que el modelo mejora el desempeño de modelos anteriores en el conjunto de datos utilizado (Secure Water Treatment Testbed).

**High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning** [6]

Los algoritmos one-class SVM (1SVM) son una herramienta que demostrado ser efectiva en la tarea de la detección de valores anómalos. El problema con este tipo de modelos es que no escalan bien. En este trabajo se propone un método que permite solventar esa limitación gracias al uso de DBNs (Deep Belief Networks). La idea es poder sustituir los kernels no lineales de las 1SVM (muy costosos de calcular) por kernels lineales (menos costosos) gracias al uso de las DBN para la generación de vectores de características.



Fig. 7 Modelo híbrido propuesto

Los resultados experimentales demuestran que el modelo híbrido mejora a los modelos 1SVMs en aproximadamente un 20% en algunos conjuntos de datos. Comparado con los métodos basados en autoencoders la diferencia es prácticamente inapreciable sin embargo el método propuesto es tres veces más rápido en el entrenamiento y hasta 1000 veces más rápido en el testing.

**Isolation-Based Anomaly Detection** [7]

Lo que diferencia a esta propuesta del resto es que, en lugar de tratar de modelar las instancias normales para luego buscar los valores anómalos, el modelo explícitamente identifica las anomalías. Esto se consigue a través de los llamados Isolation Forests. Los Isolation Forest están formados por un conjunto de árboles de decisión. Cada árbol se crea de la siguiente manera, primero se selecciona un atributo aleatoriamente y luego se establece una partición también aleatoria entre el máximo y el mínimo del atributo seleccionado. La idea detrás de este algoritmo es que los puntos que están más aislados estarán en las hojas más cercanas a nodo raíz.



Fig. 8 Identificación de una instancia normal (izquierda) y una anormal (derecha)

Este algoritmo puede tratar con conjuntos de datos grandes y de alta dimensionalidad. Sin embargo, este método presenta ciertos problemas debido a que las particiones se realizan únicamente de manera vertical u horizontal. Para solventar esos problemas se ha propuesto una modificación al algoritmo original en [8] llamado Extended Isolation Forest.

**Outlier Detection Using Replicator Neural Networks** [9]

La Replicator Neural Network utilizada en este artículo es MLP (Multi-Layer Perceptron) compuesto por tres capas ocultas. La función de esta red es la de reproducir los datos de entrada en la salida con el mínimo error posible.



Fig. 9 Arquitectura de una Replicator Neural Network (izquierda) y función de activación de la capa intermedia (derecha)

Una vez entrenada la red a cada punto se le asigna un valor que es la media de los errores de reconstrucción de cada una de las variables. Cuanto más grande sea el error más probable será que se trate de una anomalía. Este método es similar al uso de auto-encoders, la diferencia más llamativa es que este método utiliza una función de activación especial en forma de escalera la capa intermedia.

## 2.2 Federated Learning

El campo del Federated Learning es relativamente nuevo y se encuentra en pleno estudio es por este motivo que no existe tantos trabajos como en el caso del Machine Learning tradicional. Se han seleccionado tres trabajos, dos de definición e introducción a esta tecnología y uno centrado en un caso práctico de aplicación.

**Communication-Efficient Learning of Deep Networks from Decentralized Data** [10]

En este artículo se presenta un algoritmo que permite el uso de modelos de Machine Learning sobre conjuntos de datos descentralizados. En el documento no solo demuestra que esta idea es factible técnicamente presentando un algoritmo llamado *FederatedAveraging* sino que permite crear modelos de una alta calidad. Uno de los aspectos más importante de esta propuesta es que permite incrementar el nivel de privacidad de los clientes ya que en ningún momento se comparten datos entre clientes ni estos son enviados a un servidor central. A continuación, se muestra un esquema del modelo propuesto:



Fig. 10 Cada dispositivo personaliza el modelo localmente (A). Las actualizaciones de muchos usuarios se agregan (B) para actualizar el modelo global que se compartirá con todos los usuarios (C), después de lo cual se repite el proceso.

**Federated Machine Learning: Concept and Applications** [11]

Este documento presenta los conceptos básicos del Federated Learning sus principales técnicas y arquitecturas. Expone su potencial en varias aplicaciones y compara sus características con otros sistemas de aprendizaje distribuidos (Distributed Machine Learning, Federated Database Systems, etc.). Adicionalmente introduce el concepto de Data Alliance of Enterprises. Una Data Alliance of Enterprises es un conjunto de organizaciones que, mediante el uso de sus datos (sin compartirlos directamente con los demás miembros) colaboran para crear un modelo que aporte beneficios a todos los participantes. Este tipo de alianzas están llamadas a ser el futuro del Machine Learning y se espera constituyan todo un nuevo modelo de negocio [12].

**Multi-Institutional Deep Learning Modeling Without Sharing Patient Data: A Feasibility Study on Brain Tumor Segmentation** [13]

En este documento se presenta el primer uso del Federated Learning para el tratamiento de imágenes para el diagnóstico médico. En particular se usa esta tecnología para la creación de un modelo distribuido de segmentación de imágenes (U-Net) sin compartir datos de pacientes entre instituciones.



Fig. 11 Arquitectura de la U-Net utilizada

El estudio demuestra que el modelo basado en Federated Learning consigue un rendimiento prácticamente equivalente al modelo creado con el uso de datos compartidos.

## 2.3 Novedades propuestas

Aunque la detección de eventos anómalos ha sido estudiada en profundidad desde múltiples perspectivas nunca se había abordado el problema de forma colaborativa y descentralizada. Esta es la principal novedad que pretende aportar este trabajo.

# 3. Escenario

Supongamos que una empresa multinacional dispone de plantas repartidas por todo el mundo. A pesar de pertenecer a la misma compañía cada una de las instalaciones tiene sus propias particularidades en cuanto al tipo de productos que producen, la manera de fabricarlos, etc. A estas diferencias se han de añadir también las condiciones ambientales de cada lugar: temperatura, humedad, presión atmosférica, etc. A pesar de estas diferencias, las máquinas utilizadas en todas las factorías son similares.

La empresa desea implantar un sistema que pueda ayudar a detectar las posibles averías de las máquinas de sus factorías antes de que estas puedan provocar daños tanto al personal como a las propias instalaciones.

Dado que todas las instalaciones están dotadas de sensores que capturan los datos operaciones de las máquinas se dispone de gran cantidad de datos sobre su funcionamiento. Por este motivo se ha optado por la utilización de técnicas de Machine Learning para tratar de resolver el problema.

A pesar de pertenecer a la misma compañía, las plantas trabajan con un alto grado de independencia y de hecho, suelen competir entre ellas en cuestiones como la cantidad de producción, calidad, etc. Debido a esta competitividad las factorías suelen ser reacias a compartir datos sobre sus técnicas de producción, las configuraciones de sus máquinas, etc. Esto implica que el acceso a sus datos está muy restringido y estos pueden ser únicamente utilizados a nivel interno. Esto motiva que la construcción de modelos de Machine Learning solo se pueda realizar a nivel local con los datos de cada factoría de forma independiente.

Debido a las diferencias en las condiciones de trabajo y ambientales de cada instalación, un modelo construido para una factoría concreta puede no funcionar correctamente en otra instalación diferente. En principio esto no representa un problema ya que cada planta tendrá su propio modelo que será usado internamente.

La compañía está en constante expansión y es habitual que abra nuevas plantas a lo largo de mundo. Obviamente la empresa desea implantar el sistema de detección de fallos que tan bien le ha funcionado en otras factorías. Pero hay un problema, en principio no se podría confiar en que el ninguno de los modelos locales existentes fuera de utilidad en estas nuevas instalaciones. Por lo que sería necesario recolectar datos de esta nueva factoría quizás durante meses o incluso años para poder crear un modelo local.

La compañía considera esta tardanza inaceptable por lo que exige que diseñe un sistema que permita que las nuevas factorías se aprovechen de los modelos construidos previamente al vuelo, sin tantas esperas.

La forma tradicional de solucionar este problema sería almacenando los datos de todas las instalaciones existentes en un único lugar y a partir de todos los datos construir un modelo más robusto que pudiera adaptarse mejor a un nuevo comportamiento al haber aprendido de datos de diferentes fuentes.

Este tipo de solución no se puede aplicar en este caso ya los datos de cada instalación deben ser privados y es aquí es donde entra en juego el uso del **Federated Learning.**

# 4. ¿Qué es Federated Learning?

El aprendizaje federado (también conocido como aprendizaje colaborativo) es una técnica de aprendizaje automático que entrena un algoritmo a través de múltiples dispositivos o servidores que contienen muestras de datos locales, sin intercambiar sus muestras de entre ellos. Este enfoque contrasta con las técnicas tradicionales de aprendizaje automático centralizado donde todas las muestras de datos se cargan en un servidor, así como con los enfoques descentralizados más clásicos que suponen que las muestras de datos locales se distribuyen de manera idéntica.

El aprendizaje federado permite a múltiples actores construir un modelo de aprendizaje automático robusto y común sin compartir datos, abordando así problemas críticos como la privacidad de los datos, la seguridad de los datos, los derechos de acceso a los datos y el acceso a datos heterogéneos.

El aprendizaje federado tiene como objetivo entrenar un algoritmo de aprendizaje automático, por ejemplo, redes neuronales, en múltiples conjuntos de datos locales contenidos en nodos locales sin intercambiar muestras de datos. El principio general consiste en entrenar modelos locales en muestras de datos locales e intercambiar parámetros (por ejemplo, los pesos de una red neuronal) entre estos modelos locales con cierta frecuencia para generar un modelo global.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Paso 1 | Paso 2 | | Paso 3 | | Paso 4 | |
|  | | | | | | |
|  | | | | | | |
| El servidor central elige el tipo de modelo a entrenar | | El servidor central transmite el modelo a los nodos | | Lo nodos entrenan el modelo de forma local con sus propios datos | | El servidor central solicita los modelos locales y a partir de ellos genera otro modelo si acceder a ningún dato |

Fig. 12 Esquema de funcionamiento del Federated Learning

Para construir el modelo global existen varias alternativas aunque las más utilizadas son:

**Federated Stochastic Gradient Descent (FedSGD)**

El entrenamiento de modelos basado en la optimización de parámetros se suele basar en variantes del SGD (Stochastic Gradient Descent), donde los gradientes se calculan en un subconjunto aleatorio del conjunto de datos total y luego se utilizan para hacer un paso del descenso del gradiente.

El FedSGD es la traducción directa de este algoritmo a la configuración federada pero utilizando una fracción aleatoria de los nodos y utilizando todos los datos en estos nodos. El servidor promedia los gradientes proporcionalmente al número de muestras de entrenamiento en cada nodo, y se utilizan para realizar un paso de descenso de gradiente.

**Federative averaging (FedAvg)**

El FedAvg es una generalización de FedSGD, que permite a los nodos locales realizar más de una actualización de sus parámetros. Posteriormente intercambia estos parámetros con el servidor central en lugar de los gradientes. La razón de que este método funcione es que si todos los nodos locales comienzan desde la misma inicialización, promediar los gradientes es estrictamente equivalente a promediar los pesos mismos. Además, se sabe que promediar pesos ajustados provenientes de la misma inicialización no necesariamente perjudica el rendimiento promedio del modelo resultante.

# 5. Diseño del experimento

El objetivo del trabajo es mostrar la posible aplicación del aprendizaje automático federado en la detección de potenciales fallos en máquinas dentro de un conglomerado de entornos industriales monitorizados. Este tipo de entornos monitorizados hoy en día están muy extendidos gracias al auge de la Industria 4.0 y la implementación de dispositivos IoT (Internet of Things) en las fábricas. Sin embargo, es prácticamente imposible obtener un conjunto de datos real por ser este tipo de datos muy sensible para las compañías. Por este motivo no se utilizarán datos reales y en su lugar, se desarrollará un software que nos permitirá la simulación de estos datos.

Teniendo lo anterior en cuenta, se tratará de demostrar la utilidad del aprendizaje federado en situaciones como las descritas en el apartado 3 siguiendo el siguiente procedimiento:

* Se generarán 5 conjuntos de datos simulados con diferentes condiciones ambientales y de funcionamiento.
* De esos conjuntos se elegirá uno y con estos datos se construirá un modelo. Este modelo será el modelo base para todos los demás conjuntos de datos. Notar que lo que nos interesa es la estructura del modelo y no el valor de sus parámetros.
* Después se entrenará un modelo (con la estructura definida en el paso anterior) por cada uno de los conjuntos de datos.
* Se evaluarán los modelos obtenidos.
* A continuación se elegirán 4 de los 5 conjuntos de datos y se entrenará un modelo federado.
* Compararemos el modelo federado global con cada uno de los modelos locales para comparar los rendimientos.
* Finalmente evaluaremos el conjunto de datos que se quedó fuera del entrenamiento del modelo federado con este, y comparemos su desempeño con respecto a su correspondiente modelo local entrenado con anterioridad.

# 6. Implementación

## 6.1 Preparación del entorno de trabajo

La mayor parte del desarrollo del proyecto se llevará a cabo con el lenguaje de programación Python. Python ofrece, entre otras, las siguientes ventajas [14]:

* **Simplicidad.** Python ofrece la posibilidad de desarrollar programas muy potentes con muy pocas de líneas de código. Identifica y asocia automáticamente los tipos de datos y, en general, resulta un lenguaje fácil de usar y no se requiere mucho tiempo de codificación.
* **Compatibilidad.** Muchas de las tecnologías actuales relacionadas con el Machine Learning están pensadas para ser utilizadas con este lenguaje.
* **Facilidad de aprendizaje.** En comparación con otros lenguajes, Python es fácil de aprender incluso para los programadores con menos experiencia. Principalmente por tres razones:
  + Cuenta con amplios recursos de aprendizaje.
  + Garantiza un código legible.
  + Se rodea de una gran comunidad.
* **Variedad de paquetes.** Python tiene un poderoso conjunto de paquetes para una amplia gama de necesidades de análisis y ciencia de datos (numPy, Pandas, Scipy, Scikit-learn, etc.)
* **Visualización de datos.** Aunque no es el mejor lenguaje en lo que respecta a la visualización de datos. Actualmente existen APIs que pueden ofrecer resultados bastante buenos.

Nuestro entorno de trabajo estará formado por las siguientes herramientas:

* **Microsoft Excel.** Software de hojas de cálculo
* **Python.** En su versión 3.6
* **PyCharm.** Editor para el lenguaje de programación Python

## 6.2 Simulación de un entorno industrial

### 6.2.1 Introducción

El objetivo es implementar un software para la simulación de un entorno industrial cuyas instalaciones se encuentran monitorizadas mediante dispositivos IoT. Debido a las características únicas de cada tipo de instalación no nos es posible construir un software que simule cada una de las diferentes máquinas que pudieran existir en dicho entorno industrial. Por lo tanto, consideraremos únicamente un tipo de máquina: máquinas rotatorias genéricas. Basándonos en conjuntos de datos ya existentes (por ejemplo, Turbofan Engine Degradation Simulation Data Set) para cada máquina se estudiarán las siguientes variables operacionales[[1]](#footnote-1):

* Velocidad rotacional
* Temperatura
* Presión

Además de estos valores se tendrán en cuenta variables relacionadas con el entorno. En particular la temperatura del entorno y la presión atmosférica.

### 6.2.2 Caracterización de la degradación de las máquinas

Con el propósito de una generación de datos inspirada en la física se utilizará una aproximación similar a la utilizada en [15]. En particular se usará la siguiente ecuación para simular la degradación de una máquina en función de su tiempo de uso:

(Ecuación 1)

Donde, *a* y *b* son coeficientes que determinan la forma de la curva y *d* es la degradación inicial. A continuación se muestra un ejemplo de estas curvas:



Fig. 13 Curvas de degradación para diferentes parámetros

Podemos observar que la curva punteada representa una degradación repentina mientras que la curva continua representaría una degradación más constante ( aunque el fallo se produciría antes).

En nuestro caso se considerarán dos curvas de degradación para cada máquina lo que equivaldría a decir que cada máquina puede fallar por dos motivos diferentes:

* Uno estrechamente relacionado con la presión y/o la temperatura (a esta curva la llamaremos ***h1).***
* Una relacionada con la velocidad (que denotaremos por ***h2****)*

### 6.2.3 Evolución de las condiciones operacionales

Para cada uno de los parámetros operacionales se propondrá una fórmula[[2]](#footnote-2) que nos proporcionará su valor en el tiempo *t* en función de:

* Su valor en *t-1*
* Valores del resto de parámetros operacionales
* Valor de la(s) curva(s) de degradación en *t*
* Parámetros ambientales

Formalmente:

(Ecuación 2)

Donde:

* **F(t)** es el valor objetivo
* **w** valores de los parámetros operacionales actuales
* **F(t-1)** es el valor anterior
* **h\*(t)** valor de la(s) curva(s) de degradación
* **a\*(t)** condiciones ambientales

**Cálculo de la velocidad**

La velocidad en *t* será una media entre a velocidad en *t-1* y la velocidad objetivo ponderada con un coeficiente relacionado con la función de degradación***h2.***

(Ecuación 3)

A continuación, se muestra el efecto de la degradación en la evolución de la velocidad:

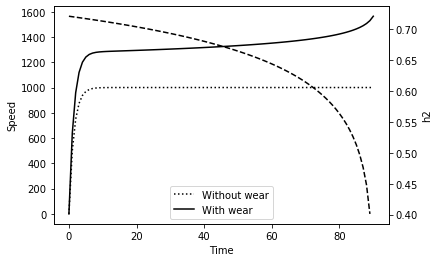


Fig. 14 Efecto de la degradación en la velocidad

En este caso, en el que la velocidad objetivo era 100, podemos ver como el efecto del desgaste afecta a la velocidad real. Al principio la diferencia se mantiene más o menos constante empezando a aumentar de forma notable al final de la vida útil de la máquina.

**Cálculo de la temperatura**

La temperatura del dispositivo estará afectada por la velocidad por lo que en este caso la temperatura estará influenciada tanto por ***h1*** como por ***h2*** (a diferencia de lo que ocurría con la velocidad a la que solo influía ***h2*** ). La fórmula utilizada para el cálculo de la temperatura es la siguiente[[3]](#footnote-3):

*(Ecuación 4)*

Donde:

(Ecuación 5)

Seguidamente se muestra gráficamente el efecto del desgaste de los componentes en la temperatura de operación:

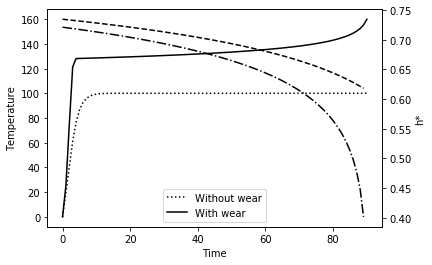


Fig. 15 Efecto de la degradación en la temperatura

Como sucedía en el caso de la velocidad vemos que la diferencia entre el caso ideal (línea punteada) y del afectado por el desgaste (línea continua) crece de forma moderada hasta que, al final de la vida útil del dispositivo, empieza a crecer de forma más pronunciada.

**Cálculo de la presión**

Igual que con la temperatura el cálculo de la presión estará influenciado por ***h1*** y ***h2.*** A continuación se muestra la fórmula usada para el cálculo de la presión[[4]](#footnote-4):

(Ecuación 6)

Donde ***g*** es la función definida en (Ecuación 5).

A continuación, se puede observar gráficamente el efecto del desgaste sobre la presión:

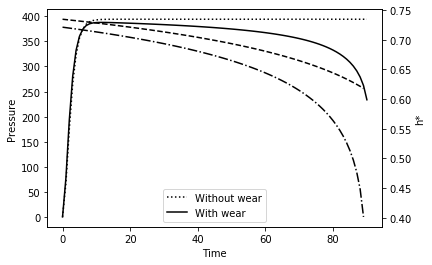


Fig. 16 Efecto de la degradación en la presión

A diferencia de lo que ocurría con la velocidad y la temperatura cuando el aparato se encuentra al final de su vida útil el valor real tiende a ser menor que el del funcionamiento óptimo.

### 6.2.4 Proceso de simulación

El objetivo es simular el funcionamiento de un conjunto de máquinas dentro de una instalación industrial y almacenar tanto los datos de telemetría como los datos referentes al mantenimiento de las máquinas.

Antes de iniciar la simulación a cada una de las máquinas que forma parte de la instalación se les asignan unas curvas de degradación (***h1***, ***h2***) cuyos parámetros son elegidos de forma aleatoria dentro de un intervalo de valores previamente establecido.

Una vez asignadas las curvas se inicia la simulación. Cada simulación (que tiene una duración determinada) se divide en lo que denominaremos periodos. En cada periodo se elige de forma aleatoria un conjunto de máquinas. Estas funcionaran durante un intervalo de tiempo elegido al azar dentro de cada periodo. La velocidad de funcionamiento de cada máquina se establece aleatoriamente dentro unos márgenes establecidos. Durante su funcionamiento se almacenarán sus datos telemétricos. Puede ocurrir, que durante su funcionamiento, en una máquina se produzca un fallo. En este caso esta máquina quedará inutilizada hasta el siguiente periodo y se creará un registro de mantenimiento indicando cuando se produjo el fallo y cuál fue la causa del fallo. Una vez finalice el periodo actual esa máquina será “reparada” asignándole un nuevo par de curvas de degradación y pudiendo participar nuevamente en la selección para el siguiente periodo.

El procedimiento anteriormente descrito se repite hasta que el tiempo de simulación finaliza.

### 6.2.5 Configuración de la simulación

Cada simulación tiene un total de 20 parámetros configurables. Esta capacidad de personalización será crucial para las siguientes fases del proyecto. Algunos de estos parámetros son:

* Duración del periodo (batch\_time)
* Duración de la simulación (simulation\_time)
* Número de máquinas en la instalación (machine\_count)
* Número de máquinas por periodo (machines\_per\_batch)
* Temperatura ambiente (temperature)
* Intervalo de velocidad de funcionamiento (operational\_speed\_min, operational\_speed\_max)

[CONFIGURATION]  
  
name = Facility A  
; three months  
simulation\_time = 7776000  
temperature = 15  
pressure = 98  
cycle\_length\_min = 1  
cycle\_length\_max = 5  
cycle\_duration = 60  
machines\_per\_batch = 5  
operational\_speed\_min = 800  
operational\_speed\_max = 900  
batch\_time = 3600  
machine\_count = 10  
ttf1\_min = 5000  
ttf1\_max = 50000  
ttf2\_min = 500  
ttf2\_max = 90000  
temperature\_max = 100  
pressure\_factor = 1.8  
telemetry\_path = ../data/generation/facility A/telemetry  
event\_path = ../data/generation/facility A/event

Fig. 17 Ejemplo de un archivo de configuración de una simulación

### 6.2.6 Resultados de la simulación

Una vez finalizada la simulación por cada máquina obtendremos dos tipos de archivos:

**Datos de telemetría**

Como su nombre sugiere contiene los datos registrados durante el funcionamiento de la máquina. La información contenida en este archivo es la siguiente:

* **id:** identificador único de la máquina
* **time:** marca temporal de la medida
* **speed:** velocidad medida
* **tgtspeed:** velocidad objetivo
* **temp:** temperatura de la máquina
* **press:** presión en la máquina
* **atemp:** temperatura ambiente
* **apress:** presión atmosférica

Tabla 1 Fragmento de archivo de telemetría

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **id** | **time** | **speed** | **tgtspeed** | **temp** | **press** | **atemp** | **apress** |
| 2e8a9c8c | 1125 | 488.79 | 873.00 | 18.22 | 98.71 | 15.08 | 98.06 |
| 2e8a9c8c | 1126 | 727.72 | 873.00 | 22.14 | 286.18 | 15.04 | 97.94 |
| 2e8a9c8c | 1127 | 848.98 | 873.00 | 26.85 | 482.01 | 14.93 | 97.98 |
| 2e8a9c8c | 1128 | 911.73 | 873.00 | 32.51 | 608.00 | 14.94 | 97.90 |
| 2e8a9c8c | 1129 | 945.71 | 873.00 | 39.37 | 730.92 | 15.08 | 97.91 |
| 2e8a9c8c | 1130 | 953.32 | 873.00 | 47.71 | 796.18 | 14.99 | 97.96 |
| 2e8a9c8c | 1131 | 965.56 | 873.00 | 57.69 | 810.21 | 14.94 | 98.02 |
| 2e8a9c8c | 1132 | 966.21 | 873.00 | 69.78 | 834.22 | 14.95 | 98.01 |

Es importante notar que durante el proceso de simulación los datos han sido contaminados añadiendo ruido para que el proceso resultara más realista.

**Registro de mantenimiento de la máquina**

Este archivo contendrá información sobre las averías de la máquina y está compuesto por los siguientes atributos:

* **id:** identificador único de la máquina
* **time:** marca temporal del evento
* **code:** código que identifica al evento (**F1** y **F2** son los códigos de cada una de las averías que se pueden producir mientras que el código **FIXED** indica que una máquina ha sido arreglada)
* **severity: CRITICAL** si estamos ante una avería **INFO** en otro caso

Tabla 2 Fragmento del registro de mantenimiento

|  |  |  |  |
| --- | --- | --- | --- |
| **id** | **time** | **code** | **severity** |
| 2e8a9c8c | 300061 | F1 | CRITICAL |
| 2e8a9c8c | 302400 | FIXED | INFO |
| 2e8a9c8c | 2301135 | F1 | CRITICAL |
| 2e8a9c8c | 2304000 | FIXED | INFO |
| 2e8a9c8c | 2893790 | F1 | CRITICAL |
| 2e8a9c8c | 2894400 | FIXED | INFO |
| 2e8a9c8c | 4113063 | F2 | CRITICAL |
| 2e8a9c8c | 4114800 | FIXED | INFO |

## 6.3 Creación del modelo base

Antes de poder aplicar técnicas de Federated Learning es necesario construir un modelo base. Este modelo base será la piedra angular de todo el proceso de aprendizaje federado. En los siguientes apartados se detallará todo el proceso necesario para la creación de este modelo.

### 6.3.1 Adquisición de los datos

Los datos han sido obtenidos gracias al software de simulación cuyo funcionamiento se ha detallado en el anterior. La simulación se corresponde a un periodo de temporal de aproximadamente seis meses. Los parámetros utilizados para realizar la simulación han sido:

* Número de máquinas: 20
* Número de máquinas por periodo:10
* Duración del periodo: 1h
* Temperatura ambiente media: 20 ºC
* Presión atmosférica media: 101 kPa
* Tiempo mínimo de actividad por periodo: 1 min
* Tiempo máximo de actividad por periodo: 10 min
* Mínima velocidad de funcionamiento: 800 rpm
* Máxima velocidad de funcionamiento: 900 rpm
* Temperatura máxima de funcionamiento: 125 ºC

### 6.3.2 Análisis de los datos

Debido a la forma de generar los datos de telemetría y de mantenimiento no será necesario realizar el análisis sobre todo el conjunto de datos. Se elegirá una máquina al azar y esta se considerará como representante de todo el conjunto. Una vez hemos seleccionado esta máquina representativa vamos a hacerle un pequeño interrogatorio a su conjunto de datos asociado:

**¿Cuál es el número de registros almacenados?**

El conjunto está formado por un total de 743144 registros

**¿Cuántos fallos se han producido en estos seis meses?**

Se han producido un total de 21 fallos de tipo **F1** y 12 de tipo **F2.** Teniendo esto en cuenta parece que son mucho más frecuentes los errores de tipo **F1**.

**¿Cuáles son sus estadísticas más relevantes?**

Tabla 3 Datos descriptivos de la máquina

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **speed** | **tgtspeed** | **temp** | **press** | **atemp** | **apress** |
| **count** | 743144 | 743144 | 743144 | 743144 | 743144 | 743144 |
| mean | 971.10 | 835.12 | 146.25 | 871.70 | 20.00 | 101.00 |
| std | 128.77 | 115.44 | 18.63 | 169.02 | 0.06 | 0.06 |
| min | 5.54 | 0.00 | 22.40 | 9.12 | 19.90 | 100.90 |
| 25% | 943.28 | 823.00 | 143.58 | 801.87 | 19.95 | 100.95 |
| 50% | 980.49 | 849.00 | 146.71 | 904.57 | 20.00 | 101.00 |
| 75% | 1014.11 | 876.00 | 151.85 | 981.73 | 20.05 | 101.05 |
| max | 1545.38 | 899.00 | 223.94 | 1753.91 | 20.10 | 101.10 |

En interesante destacar las diferencias notables que existen entre los valores medios de la velocidad (*speed*), la presión (*press*) y la temperatura (*temp*) y sus valores máximos. Estos valores extremos podrían estar relacionados con la aparición de fallos en la máquina.

**¿Qué relación existe entre las variables operacionales?**

Tabla 4 Tabla de correlaciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **speed** | **tgtspeed** | **temp** | **press** |
| **speed** | 1.000 | 0.874 | 0.153 | 0.539 |
| **tgtspeed** | 0.874 | 1.000 | -0.018 | 0.387 |
| **temp** | 0.153 | -0.018 | 1.000 | -0.061 |
| **press** | 0.539 | 0.387 | -0.061 | 1.000 |

Se puede observar una correlación alta entre la velocidad (speed) y la velocidad objetivo (tgtspeed) lo cual es totalmente lógico. Sin embargo, entre el resto de las variables no se observa ninguna relación destacable.

**¿Qué aspecto tienen los datos?**

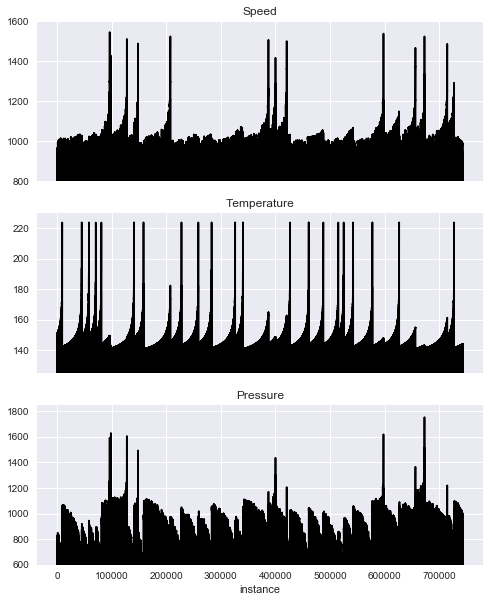


Fig. 18 Representación gráfica de los datos operacionales

Se pueden observar en todas las variables operacionales picos muy marcados. Es muy probable que estos picos estén relacionados directamente con los fallos. Para comprobar que realmente existe esa relación vamos a añadir a estas gráficas la información temporal de los fallos que se han producido:

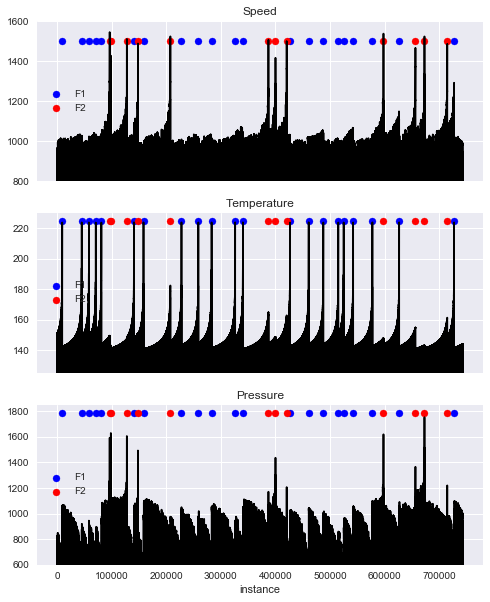


Fig. 19 Datos operacionales junto con los datos de mantenimiento

Efectivamente se puede ver que nuestra suposición era cierta en el caso de la velocidad y la temperatura. Sin embargo, en el caso de la presión se puede ver que, mientras que los fallos de tipo **F2** sí que están relacionados con los picos los fallos de tipo **F1** parece que están relacionados con los valles.

### 6.3.3 Elección del tipo modelo

Nuestro objetivo es poder decidir si en un determinado momento una máquina está en riesgo de rotura o no utilizando únicamente sus datos telemétricos. Dicho de otra manera, debemos clasificar esa máquina como potencialmente peligrosa o como segura. Teniendo en cuento esto parece claro que será necesario el uso de un modelo de clasificación. Existen multitud de familias de modelos que pueden ser usados para tareas de clasificación: árboles de decisión, máquinas de soporte de vectores, k-vecinos más cercanos, etc. Sin embargo nos hemos decidido por el uso de redes neuronales. Esta elección está motivada principalmente por dos cuestiones:

* Han demostrado tener un rendimiento excelente en multitud de problemas.
* Aunque en teoría el uso del Federated Learning es aplicable a cualquier tipo de modelo cuyo entrenamiento se base en la optimización de parámetros [15] , es cierto que al ser una tecnología relativamente nueva la mayoría de los frameworks actuales solo permiten el uso de redes neurales en sus implementaciones de aprendizaje federado.

### 6.3.4 Procesado de los datos

Disponemos del conjunto de datos pero no en el formato adecuado para sacarle el máximo partido. Para que pueda ser usado en el entrenamiento del modelo este debe pasar por un conjunto de transformaciones. A continuación, se describen las transformaciones aplicadas:

**Agregación de los datos de telemetría por ciclo**

¿Qué son los ciclos?

Muchas máquinas del mundo real funcionan en ciclos. Un ciclo puede considerarse como un período temporal que describe un estado de funcionamiento de una máquina. Por ejemplo, la operación de un motor en un avión puede describirse por los ciclos: motor en funcionamiento (avión en vuelo) o motor apagado (avión en tierra).

¿Porque es importante agregar los datos por ciclo?

Las transmisiones de telemetría sin procesar, si bien pueden ser muy útiles para tareas como el monitoreo en tiempo real, pueden causar problemas a la hora de construir modelos de detección de fallos. Es frecuente que en entornos no controlados (como puede ser una fábrica) los datos no sean del todo precisos.

Para mitigar los posibles errores en las mediciones (fallos puntuales en los equipos de medida, ruido, etc.) que pueden afectar a la calidad de los modelos construidos suele ser una buena opción considerar datos agregados por ciclo.

Se han utilizado dos operaciones de agregación para los datos operaciones (velocidad, temperatura y presión): media y máximo.

**Cruce de los datos agregados con los datos de mantenimiento**

En este punto disponemos de dos conjuntos de datos independientes. Pero es necesario juntarlos en un único archivo. Gracias a que disponemos las marcas de tiempo en las que se registró un fallo de las máquinas y que el en archivo de telemetría existen también esas marcas de tiempo es sencillo relacionar ambos conjuntos de datos y unirlos en un único dataset.

**Cálculo del RUL (Remaining Useful Life)**

En esta transformación se creará un nuevo campo numérico que nos indicará en número de ciclos que quedan antes de que se produzca un fallo. A continuación se muestra un ejemplo:

Tabla 5 Cálculo RUL

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **cycleid** | **agg1** | **…** | **aggN** | **error** | **RUL** |
| 465 | … | … | … |  | 5 |
| 466 | … | … | … |  | 4 |
| 467 | … | … | … |  | 3 |
| 468 | … | … | … |  | 2 |
| 469 | … | … | … |  | 1 |
| 470 | … | … | … | F1 | 0 |
| 471 | … | … | … |  | 3 |
| 472 | … | … | … |  | 2 |
| 473 | … | … | … |  | 1 |
| 474 | … | … | … | F2 | 0 |

En la parte de derecha de la tabla vemos el resultado de las operaciones de transformación de los anteriores pasos. Rodeado en rojo el nuevo campo.

**Etiquetado de las instancias**

El objetivo es resolver un problema de clasificación por lo que tenemos que etiquetar las instancias. Para ello nos hemos basado en el método utilizado en [16]. Lo primero será establecer un tamaño de ventana (en nuestro caso se ha utilizado el valor 7) entonces se le asignará la etiqueta 1 o 2 a una instancia cuando su valor RUL sea menor que el tamaño de ventana (1 cuando el fallo sea de tipo F1 y 2 cuando sea de tipo F2) y 0 en otro caso. Esta forma de etiquetado nos permite detectar, no solo las instancias que se corresponden con un fallo sino que también permite identificar las que están muy cerca de ser un fallo. Esto tiene dos ventajas:

* Nos permite tener más instancias de la clase minoritaria[[5]](#footnote-5)
* Detectar un estado de fallo antes de que se produzca. Esto es una ventaja muy interesante a la hora de poder realizar tareas preventivas.

**Enriquecimiento de los datos**

Una forma de añadir mayor cantidad de información al conjunto de datos disponible es lo que se conoce como feature engineering. En nuestro caso añadiremos cuatro nuevos atributos. Cada nuevo atributo se corresponderá con los datos promediados de cierto atributo de las n instancias precedentes. De forma visual:

Tabla 6 Feature engineering

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **cycleid** | **f1** | **…** | **fN** | **f1\_mean** | **…** | **fN\_mean** |
| 465 | … | … | … |  |  |  |
| 466 | … | … | … |  |  |  |
| 467 | … | … | … |  |  |  |
| 468 | … | … | … |  |  |  |
| 469 | … | … | … |  |  |  |
| 470 | … | … | … |  |  |  |
| 471 | … | … | … |  |  |  |
| 472 | … | … | … |  |  |  |
| 473 | … | … | … |  |  |  |
| 474 | … | … | … |  |  |  |

En nuestro caso se tomado n=5 y las variables involucradas han sido[[6]](#footnote-6):

* Temperatura (media y máximo)
* Presión (media y máximo)

Este procedimiento es muy interesante ya que permite añadir una cierta cantidad información histórica a cada registro. El modelo podrá, no solo tener información instantánea si no que tendrá también información sobre la tendencia.

**Balanceo del conjunto de datos**

Por la propia naturaleza de los datos que estamos manejando es normal que exista una gran diferencia entre los casos donde no se detecta ninguna anomalía (clase 0) y los casos donde es posible que se produzca una avería (clase 1 o clase 2 ). Sin embargo este tipo de conjuntos de datos suelen ser problemáticos a la hora de entrenar los modelos. Existen multitud de técnicas para balancear conjuntos de datos: oversampling, subsampling, métodos basados en pesos, etc. [17]

En nuestro caso nos hemos decantado por el uso del algoritmo SMOTE (Synthetic Minority Over-sampling Technique) [18]. Este algoritmo genera nuevas instancias a partir de las clases minoritarias dejando intacta la clase mayoritaria. Las nuevas instancias no son copias de los casos existentes si no que se calculan como combinaciones lineales de los vecinos mas cercanos de esa misma clase.

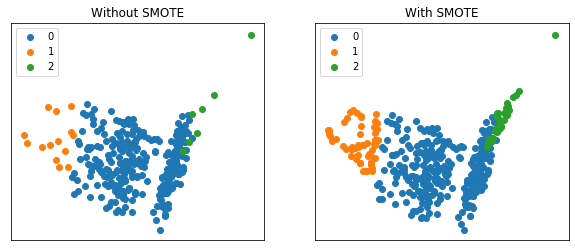


Fig. 20 Efecto de aplicar el algoritmo SMOTE sobre los datos

En nuestro caso y dependiendo de la configuración de la simulación y otros factores como el tamaño de la ventana a la hora de etiquetar los datos la proporción entre clases puede variar. Sin embargo gracias al uso de SMOTE podemos garantizar que esa proporción se mantendrá constante (en nuestro caso hemos establecido una proporción mínima de un 20% de clases minoritarias).

.

**Normalización de los datos**

A parte de del desbalanceo hay otro factor que puede provocar que los modelos no funcionen correctamente. Que los datos estén en distintas unidades y que tengan valores demasiado grandes con respecto a los parámetros que el modelo necesita ajustar, esto es especialmente cierto cuando hablamos de redes neuronales [19]. Por este motivo se han normalizado los datos (a cada atributo se le ha restado la media y se han divido por su desviación típica). De esta manera todos los atributos estarán en la misma escala y además tendrán valores similares a los parámetros del modelo.

**División de los datos para el entrenamiento y la validación del modelo**

Esta es la última fase de la preparación del conjunto de datos para el entrenamiento del modelo. Para cada instalación se construirán dos conjuntos de datos: uno de entrenamiento y otro de validación. Mientras que el primero servirá para determinar el conjunto de parámetros del modelo el segundo servirá para validar que el modelo se ha entrenado de forma satisfactoria es importante que entre ambos conjuntos no se comparta ningún tipo de información.

La forma habitual de construir estos conjuntos es a partir de un porcentaje. Se determina que porcentaje de datos de todos los disponibles se dedicará al entrenamiento y cual a la validación. Posteriormente se asignarán instancias a un conjunto u otro hasta que se cumpla con el porcentaje indicado (el proceso puede ser determinista o aleatorio).

Sin embargo en nuestro caso no se puede aplicar directamente esta técnica ya que debido a la forma de calcular algunos atributos (ver apartado de enriquecimiento de los datos) este método podría provocar una filtración entre ambos conjuntos [20].

Se utilizará la siguiente técnica:

* Se ordenarán los datos de forma temporal
* Se dividirá el conjunto de datos de la siguiente manera: 80% de datos para el entrenamiento y 20% para la validación
* Finalmente se eliminarán del conjunto de entrenamiento los últimos n casos, donde n se corresponde con el valor seleccionado en el apartado de enriquecimiento de datos (en nuestro caso 5)

Este procedimiento garantizara que no existe filtración de datos entre los conjuntos.

### 6**.3.5 Selección del framework para el desarrollo del modelo**

En la actualidad existen multitud de librerías que nos permiten la creación de modelos de Machine Learning [21]. Para tomar la decisión de cual elegir se han tenido en cuenta los siguientes factores:

1. Su soporte para trabajar con Federated Learning.
2. Que lenguaje de programación requiere.
3. Sencillez de uso.

Teniendo en cuenta esos factores no hemos decantado por el uso combinado de PyTotch (<https://pytorch.org>)y PySyft (<https://github.com/OpenMined/PySyft>).

### 6.3.6 Selección de los criterios para la evaluación del modelo

Los criterios de evaluación de un modelo de clasificación dependen mucho del tipo de problema que se esté tratando [22]. Enumeraremos a continuación los criterios más utilizados y veremos cuales son los más idóneos para nuestro problema:

**Accuracy.** Probablemente sea la medida más usada. Es muy fácil de interpretar y se puede utilizar tanto como problemas de clasificación binarios como multiclase. El problema es que su uso no es recomendable para conjuntos no balanceados donde una clase este mucho más representada que las demás.

**Precision.** Esta medida responde a la siguiente pregunta ¿Qué proporción de instancias clasificadas como “X” son realmente “X”? Este tipo de medida se utiliza cuando queremos estar muy seguros de nuestra predicción.

**Recall.** El recall responde a la siguiente pregunta ¿ De todas las instancias “X” qué proporción han sido clasificadas como “X”? Esta medida se utiliza cuando queremos capturar la mayor cantidad de clases “X” posible.

**F1-Score.** Combina las dos medidas anteriores mediante una media armónica. Es muy útil cuando nos interesa un balance entre ambas medidas.

Desde nuestro punto de vista la medida que debemos tener en cuenta por encima de las demás es el recall en las clases 1 y 2 (fallos de tipo F1 y F2 respectivamente). Por una razón: un fallo en una máquina no controlado puede provocar tanto daños materiales graves como daños personales irreparables.

-----

Dependiendo de la perspectiva desde la que tratemos el problema nos puede interesar una u otra medida:

* Si tratamos el problema desde un punto de vista económico nos interesa la mayor precisión posible en las clases 1 y 2 (fallos de tipo F1 y F2 respectivamente) ya que cada falso positivo costaría dinero a la empresa.
* Desde un punto de seguridad nos interesa el mayor recall posible en las clases 1 y 2 ya que cada

Está claro que de las 4 medidas la primera de ellas es la que menos tendremos en cuenta ya que esta muy desaconsejada para conjunto no balanceados como los nuestros.

Desde el piunto de vista de la seguridad

La medida mas importante es aquella que garantice la mayor seguridad en las instalaciones o lo que es lo mismo que detecte la mayor cantidad posible de fallos en las máquinas. Por este motivo lo que consideraremos como medida principal el recall en las clases 1 y 2 (fallos de tipo F1 y F2 respectivamente).

Desde el punto de vista economicoa

Si quisiéremos buscar un tradeoff entre ambas pero consideramos que lo más importante es la seguraidad

----

### 6.3.7 Implementación, entrenamiento y validación del modelo

# 5. Conclusiones

Este capítulo tiene que incluir:

* Una descripción de las conclusiones del trabajo: Qué lecciones se han aprendido del trabajo?.
* Una reflexión crítica sobre el logro de los objetivos planteados inicialmente: Hemos logrado todos los objetivos? Si la respuesta es negativa, por qué motivo?
* Un análisis crítico del seguimiento de la planificación y metodología a lo largo del producto: Se ha seguido la planificación? La metodología prevista ha sido la adecuada? Ha habido que introducir cambios para garantizar el éxito del trabajo? Por qué?
* Las líneas de trabajo futuro que no se han podido explorar en este trabajo y han quedado pendientes.

# 6. Glosario

Definición de los términos y acrónimos más relevantes utilizados dentro de la Memoria.

# 7. Bibliografía

|  |  |
| --- | --- |
| [1] | Z. Janjua, M. Vecchio, M. Antonini y F. Antonelli, «IRESE: An intelligent rare-event detection system using unsupervised learning on the IoT edge,» *Engineering Applications of Artificial Intelligence,* vol. 84, pp. 41-50, 2019. |
| [2] | S. Chauhan y L. Vig, «Anomaly detection in ECG time signals via deep long short-term memory networks,» de *IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, Paris, 2015. |
| [3] | A. Lakhina, M. Crovella y C. Diot, «Diagnosing Network-Wide Traffic Anomalies,» *Computer Communication Review,* vol. 34, 2004. |
| [4] | D. Li, D. Chen, J. Goh y S. k. Ng, «Anomaly Detection with Generative Adversarial Networks for Multivariate Time Series,» de *International Workshop on Big Data*, London, 2018. |
| [5] | S. M. Erfani, S. Rajasegarar, S. Karunasekera y C. Leckie, «High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning,» *Pattern Recognition,* vol. 58, pp. 121-134, 2016. |
| [6] | F. T. Liu, K. Ting y Z.-H. Zhou, «Isolation-Based Anomaly Detection,» *ACM Transactions on Knowledge Discovery From Data - TKDD,* vol. 6, pp. 1-39, 2012. |
| [7] | S. Hariri, M. Carrasco Kind y R. J. Brunner, «Extended Isolation Forest,» 2018. |
| [8] | S. Hawkins, H. He, G. Williams y R. Baxter, «Outlier Detection Using Replicator Neural Networks,» *Data Warehousing and Knowledge Discovery,* pp. 170-180, 2002. |
| [9] | H. B. McMahan, E. Moore, D. Ramage, S. Hampson y B. Agüera y Arcas, «Communication-Efficient Learning of Deep Networks from Decentralized Data,» 2016. |
| [10] | Q. Yang, Y. Liu, T. Chen y Y. Tong, «Federated Machine Learning: Concept and Applications,» 2019. |
| [11] | A. Gonfalonieri, «Towards Data Science,» [En línea]. Available: https://towardsdatascience.com/federated-learning-a-new-ai-business-model-ec6b4141b1bf. |
| [12] | M. J. Sheller, G. A. Reina, B. Edwards, J. Martin y S. Bakas, «Multi-Institutional Deep Learning Modeling Without Sharing Patient Data: A Feasibility Study on Brain Tumor Segmentation,» 2018. |
| [13] | U. I. d. Valencia, «www.universidadviu.es,» [En línea]. Available: https://www.universidadviu.es/python-para-big-data-motivos-para-elegirlo/. [Último acceso: 15 12 2019]. |
| [14] | K. G. D. S. N. E. A. Saxena, «Damage propagation modeling for aircraft engine run-to-failure simulation,» de *International Conference on Prognostics and Health Management,*, Denver, CO, USA, 2008. |
| [15] | F. Hartmann, «Federated Learning,» [En línea]. Available: https://florian.github.io/federated-learning/. [Último acceso: 15 10 2019]. |
| [16] | C. Yang y S. Létourneau, «Learning to predict train wheel failures,» de *KDD '05*, 2005. |
| [17] | machinelearningmastery.com, «8 Tactics to Combat Imbalanced Classes in Your Machine Learning Dataset,» [En línea]. Available: https://machinelearningmastery.com/tactics-to-combat-imbalanced-classes-in-your-machine-learning-dataset/. [Último acceso: 5 12 2019]. |
| [18] | K. W. Bowyer, N. V. Chawla, L. O. Hall y P. Kegelmeyer, «SMOTE: Synthetic Minority Over-sampling Technique,» *CoRR,* vol. abs/1106.1813, 2011. |
| [19] | T. Stöttner, «Why data should be normalized before training a neural network,» [En línea]. Available: https://towardsdatascience.com/why-data-should-be-normalized-before-training-a-neural-network-c626b7f66c7d. [Último acceso: 10 12 2019]. |
| [20] | Microsoft, «Azure AI guide for predictive maintenance solutions,» [En línea]. Available: https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/cortana-analytics-playbook-predictive-maintenance#time-dependent-split. [Último acceso: 5 12 2019]. |
| [21] | O. Kharkovyna, «Top 10 Best Deep Learning Frameworks in 2019,» towardsdatascience.com, 3 Jan 2019. [En línea]. Available: https://towardsdatascience.com/top-10-best-deep-learning-frameworks-in-2019-5ccb90ea6de. [Último acceso: 29 11 2019]. |
| [22] | Wikipedia, «Federated Learning, Wikipedia,» [En línea]. Available: https://en.wikipedia.org/wiki/Federated\_learning. [Último acceso: 1 12 2019]. |
| [23] | Microsoft, «Predictive Maintenance,» [En línea]. Available: https://gallery.azure.ai/Collection/Predictive-Maintenance-Template-3. [Último acceso: 16 11 2019]. |

# 6. Anexos

Listado de apartados que son demasiado extensos para incluir dentro de la memoria y tienen un carácter autocontenido (por ejemplo, manuales de usuario, manuales de instalación, etc.)

Dependiente del tipo de trabajo, es posible que no haya que añadir ningún anexo.

1. Las unidades de medida serán: kPa para las presiones, ºC para las temperaturas y rpm para las velocidades [↑](#footnote-ref-1)
2. Las fórmulas propuestas están basadas en las fórmulas presentadas en [21]. [↑](#footnote-ref-2)
3. El valor de las constantes que aparecen en la fórmula podrá variar en función de las condiciones de la instalación que se quiera simular. [↑](#footnote-ref-3)
4. Al igual que el caso de la temperatura las constantes pueden variar en función de las condiciones de la instalación que se quiera simular. [↑](#footnote-ref-4)
5. Aunque todavía no se ha mencionado, nos encontramos ante un problema de clasificación desbalanceado. Hablaremos de esta problemática en secciones posteriores [↑](#footnote-ref-5)
6. Notar que las variables temperatura ya habían sido agregadas en una transformación anterior [↑](#footnote-ref-6)