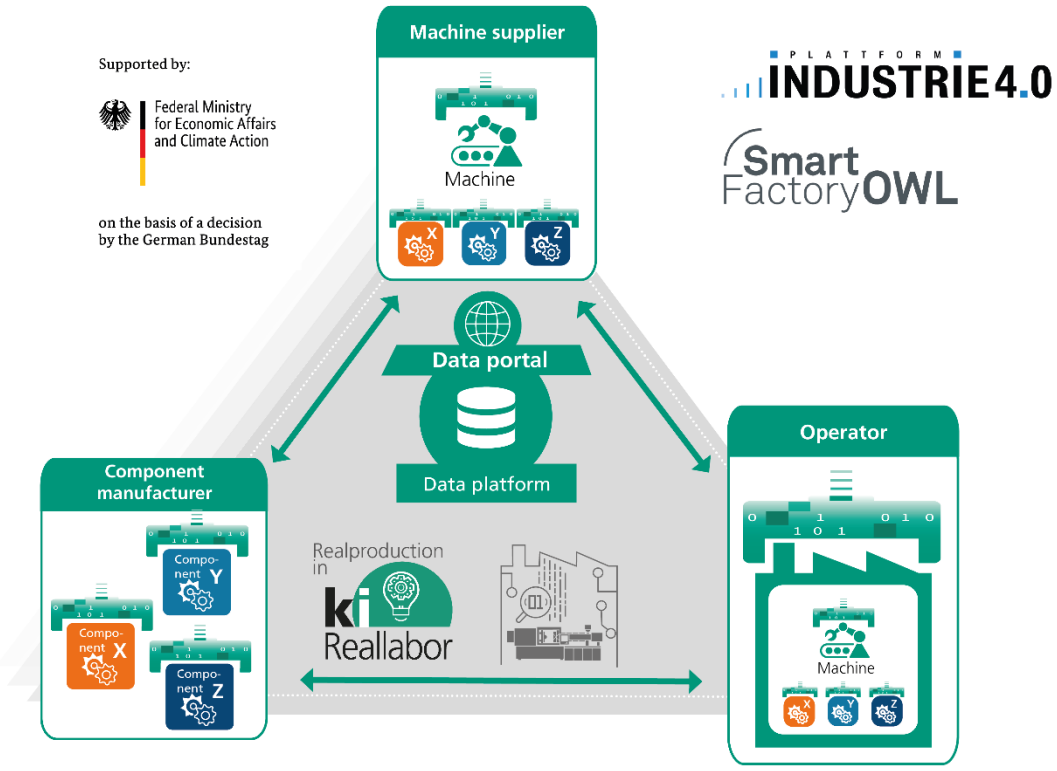
Use Case: Collaborative Condition Monitoring (CCM) in the AI Real Lab of the SmartFactoryOWL



Source: Based on Plattform Industrie 4.0

Share and use data across company boundaries

- Creating added value through multilateral data sharing
- Share and use operational data in the form of time series
- Testing of Gaia-X Federation Services[1] based on W3C[2] technologies in a realistic production environment
- Authentication via Gaia-X Identity & Trust using Decentralised Identifiers (DID) and Verifiable Credentials (VC)
- Increase discoverability and usability of data (Gaia-X Federated Catalogue & AAS Registry)

[1] Gaia-X Federation Services - www.gxfs.de

[2] World Wide Web Consortium (W3C) - www.w3.org

Industrial Digital Twin Association e.V.
Lyoner Straße 18 — 60528 Frankfurt am Main
Germany

Phone +49 69 6603 1939
Email info@idtwin.org
www.industrialdigitaltwin.org

The use case "Collaborative Condition Monitoring" (CCM) deals with the collection and multilateral sharing and use of operating data, among other things, to optimise the reliability and service life of machines and their components in a value network consisting of component manufacturers, machine manufacturers and machine operators. Machines typically contain different components from different manufacturers. One of the challenges is to find the components in operation in the IIoT and to be able to access their generated data easily and securely.

AAS enables cross-manufacturer data exchange and reduces data engineering efforts

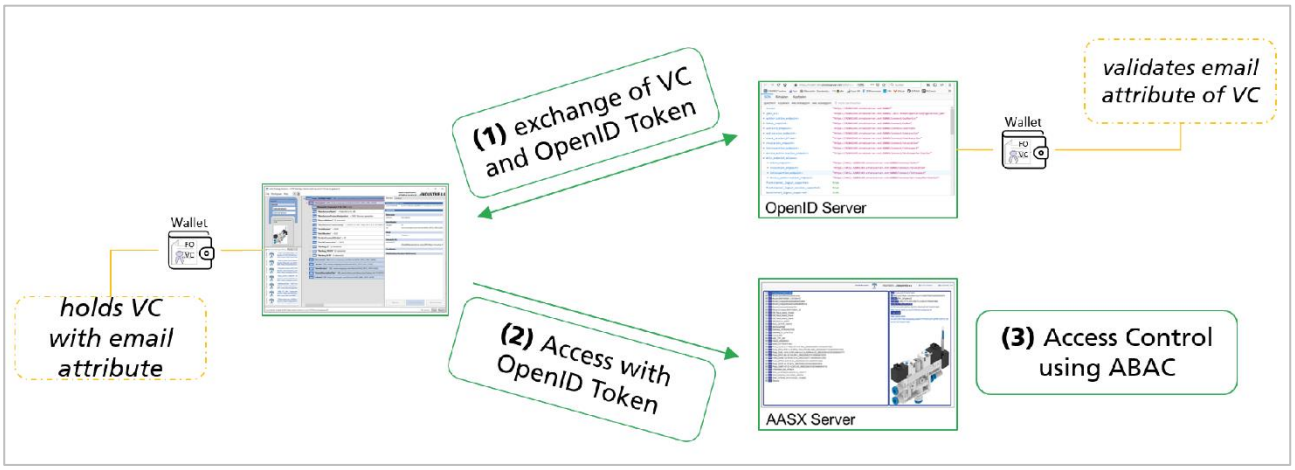
The variety of products in operation leads to a high degree of heterogeneity in terms of communication technologies and information models. This is accompanied by high efforts for so-called data engineering (data integration, building up data understanding, data pre-processing, etc.). The Asset Administration Shell (AAS) reduces these efforts: As a standardised Industrie 4.0 interface, it enables simple data integration (e.g. via REST API) and as a standardised Industrie 4.0 information model, it offers the possibility to semantically annotate operational data and make it machine-interpretable. This enables new services such as AI solutions to automatically connect data sources with the appropriate services.

GAIA-X Federation Services enable a trusted data space for Industry 4.0

In addition to the basic requirement of interoperability by means of an Asset Administration Shell (AAS), multilateral data exchange is based on a trusted data space. The Gaia-X Federation Services describe a toolbox consisting of the areas "Identity & Trust", "Federated Catalogue", "Sovereign Data Exchange" and "Compliance" to build trust and interoperability and ensure that participants retain sovereignty over their data. They form the basis for the Industry 4.0 data space. In the area of Identity & Trust, CCM relies on Self Sovereign Identities (SSI) [3]and the Trust over IP (ToIP) [4]stack, for example. Access control uses attributes from so-called *Verifiable Credentials*, which can be issued and verified decentrally and sovereignly by the parties involved in the value network. This makes it possible to include new types of attributes that could not previously be mapped with the X.509 standard. AAS applications exchange this information via so-called SSI digital wallets. It is even conceivable that each asset or its AAS has its own wallet to hold, issue or verify required proofs and further attributes. The only basic requirement is a connection to a corresponding SSI digital wallet. In order to exchange historised data as a CSV file in a performant, sustainable and interoperable way, a tailored sub-model defines important semantic enrichments to exclude implicit interpretations and to define an explicit mapping between operational data and column entries. The AAS Registry is another building block that enables the discovery of administrative shells. Conceptually, however, the Gaia-X Federated Catalogue is also considered, which is an even more powerful tool that allows complex queries.

[3] Self-Sovereign Identity (SSI) - en.wikipedia.org/wiki/Self-Sovereign_Identity

[4] Trust over IP (ToIP) - trustoverip.org



Access control using SSI technology with existing OpenID authentication infrastructure
The OpenID server can verify that the VC was issued by the component manufacturer and has not been modified.