Cloud-based Platform to facilitate Access to Manufacturing IT

Daniel Stocka, Matthias Stöhra, Ursula Rauscheckera, Thomas Bauernhansla*

*Fraunhofer Institute for Manufacturing Engineering and Automation IPA, 70569 Stuttgart, Germany

1. Introduction

Cloud computing and the associated concepts offer numerous approaches to overcome a wide range of challenges, also in various production-related application areas. By virtualising manufacturing resources and implementation of service-oriented concepts, production facilities and even complete factories can be managed and controlled using appropriate infrastructures, including cloud-based environments. Especially SMEs benefit from cloud-managed production systems because this services can be adapted to the current production situation and the effort of setting up an own infrastructure and running expensive dedicated production control systems can be avoided. To participate, an organisation just has to setup a standardized manufacturing service bus to enable the cloud systems to access factory resources and systems in a standardized way.

Also the advantages of such an infrastructure become clear on considering the lack of information available about manufacturing equipment operated by SMEs. The potentials of these systems and their high technical capabilities are not fully exploited in most cases. This is usually due to a deficit regarding ways of obtaining current information, for example about relevant conditions and process parameters. Additionally, there is a costly time discrepancy between planning and operation, such as arranging maintenance measures late or not recognising short-notice machine availability. This is mainly caused by the fact that in typical daily IT operations, these companies are forced to implement personalised isolated solutions (e.g. diagnosis systems) in order to address the most urgent challenges. Other solutions are often put to a low priority wait list.

This article introduces the cloud approach as a promising solution to such problems and defines a cloud architecture based on a requirement catalogue. Information from a wide range of sources within a factory, such as cyber physical systems (CPS), manufacturing execution systems (MES), databases, tools, equipment, etc., are integrated into the cloud. Together with the IT services offered on a cloud platform, these are then linked by means of structured, personalised
workflows in order to provide individual engineering applications (hereafter called e-apps). The provision of such features will enable responsible engineers, production planners, etc. to develop their own e-apps configured to their individual company requirements without the need for special IT knowledge by using the e-app Standard Development Kit (SDK).

The most important criterion concerning the acceptance of such a platform, which administrates and links up company data across production sites and company boundaries, is the implementation of sufficient security mechanisms. For this reason, this aspect is also addressed in the paper.

2. State of the art

In practice, when a facility is in operation, data which can be used for the monitoring of equipment, operations, quality, and performance is available via heterogeneous information systems and interfaces. Depending on the task range and planning horizon concerned, respective IT systems enable the manufacturing level, manufacturing control level and company management level to be classified [1]. If the current technological ability of IT-assisted tools for the optimisation of products, processes, etc. in manufacturing enterprises is considered, it can be seen that the number and complexity of tools used decreases in relation to the size of an enterprise [2]. This goes in parallel with a discrepancy between large-sized and medium-sized companies with regard to the availability of digital data to be used for optimisation measures. Among other factors, the difference in the quantity of available data and IT tools implemented depends on the requirements of medium-sized enterprises, which vary somewhat from those of large companies. This point becomes clear on considering the use of knowledge management systems, for example: medium-sized companies attach great importance to the simplicity and user-friendliness of their solutions concerning their structure, method of function and operation. Besides those usability criteria, the reduction of complexity, i.e. the ability of SMEs to control and manage such systems, is also important. As managers generally want to keep control of processes, the various steps involved need to be straightforward and understandable [3]. Furthermore, additional resources (financial and human) for non-value-adding processes are often unavailable, which is why large comprehensive IT management solutions often fail to be implemented and administered in a small company environment [4].

In factories where planning, control and optimisation tasks are not executed by conventional IT tools due to the reasons mentioned above, concepts such as cloud manufacturing are an option to exploit the potential of these tools, though. Such cloud solutions are often based on the virtualisation and management of manufacturing resources on a cloud computing platform [5], [6], [7]. However, such solutions are usually not configurable to address individual company requirements.

Furthermore, solutions focusing on specific process and user interface adaptation as described in [8] are currently not available in the manufacturing environment.

According to forecasts, the introduction of mobile IT infrastructures in manufacturing companies will push business efficiency and transformation in productions [9]. The simplified development of e-apps for the manufacturing sector by means of a standardised software/hardware infrastructure will thus strongly contribute towards improving efficiency because it will be possible to aggregate cloud manufacturing concepts with individualised workflows.

3. Use cases and requirements

Before being in a position to define the IT architecture of a cloud platform for the facilitated integration, linking and distribution of manufacturing data, resources and processes, a requirement catalogue has to be compiled by deriving the main challenges and requirements from the respective use cases.

On the basis of an application scenario, the benefits of such a platform are identified and the most important stakeholders and use cases are described. In the process, a differentiation is made between functional and non-functional uses. In order to be able to give a sound overview on the overall platform and related features, only the core requirements are considered at this stage.

3.1. Application scenario: optimized execution of maintenance measures

In order to individually forecast the rate of wear of various tools used in wood-processing (cutter, saw blade, etc.), a wide range of data has to be recorded, e.g. machine operating data, tool identification data and tool class, MES data and high-resolution photos of the tools. This information may originate from numerous different data sources, such as machine control units, MES, data banks, CPS, camera systems, etc. To supply the person responsible (internal member of staff or tool supplier) for maintenance of the tools (e.g. sharpening) with all the information needed to perform the task (e.g. milling parameters), the data first has to be provided by the cloud in a standardised format, and then appropriately prepared by coupling it intelligently to forecast models. The link is not made by IT experts but instead by engineers involved in the process who define their own engineering apps.

The scenario not only addresses the integration of various data sources into the cloud (real cross-company data) but also the development of engineering apps with an easy-to-use development kit. This provides access to services integrated in the cloud, thus enabling the necessary information to be obtained and aiding definition of the required sequences in order to generate the forecast models (workflow definition) as well distributing the results to the relevant worker (workflow execution).

The data that is accessible via the cloud may originate directly from the factory or be requested from applications or services compiled via the cloud. On top of the above-mentioned maintenance example, the information also offers engineers a wide range of other application possibilities that can be quickly realised (e.g. condition monitoring, remote
maintenance, cause analysis in the event of a problem, tool comparison, process optimisation). At the same time, the tool supplier in the described scenario can use the intelligently-networked information and systems to find out the exact service life of certain customer tools, thus enabling him to provide customers with optimum maintenance support or similar.

Without the possibilities of a cloud platform that is adapted to the manufacturing environment and offers the relevant engineering development tools, engineers would have to resort to isolated solutions such as Excel spreadsheets.

### Differentiation of the term “service”

Services are the building blocks of cloud applications, and are capable of interacting with other services as part of a defined workflow. There are different types of service:

1. **Integration services**: integration of systems linked to the cloud (e.g. factory machines, equipment, etc.)
2. **CPS services**: services with special sensors and actuators that can form a highly dynamic part of processes. Examples include work piece carriers and machines.
3. **Software services**: IT services that provide defined, clearly delineated features. Examples include data archiving, specific analyses, scheduling mechanisms, etc.
4. **Aggregated services**: services which use the features of other services to create their own function, e.g. the ability to ascertain indicators by acquiring data with the aid of integration services and accessing archived data and analyses.
5. **E-app/solution**: a service including a suitable user interface which is offered directly to users via a marketplace.

### 3.2. Main stakeholders

In the following, the platform stakeholders are described and placed into groups. In some cases, the aims and roles of the various stakeholders may overlap.

1. **ISV (Independent Service/Solution Vendor)**: ISVs offer services/solutions via the cloud; they may have very different functions or aggregation levels. For example, there are integration services for integrating data sources such as machines, factory systems and databases, or aggregated services for linking integration services with intelligent bundles and workflows or offering them as a solution to end-users. This group also includes organisations offering their factory resources/capabilities/products via the cloud, as well as users implementing software solutions to develop/extend these services.

2. **User**: Users implement the services/solutions/e-apps/advantages offered by the cloud and are correspondingly authorised to utilise the development tools provided in order to set up their own services.
   a) **Engineer**, responsible for the process
      
      With the aid of the application development tools, engineers generate e-apps to deal with highly-specific problems that are typically encountered in small and medium-sized mechanical engineering enterprises. The engineers value the fact that they can adapt quickly and easily to company-specific requirements in order to support a wide range of changing workflows.
   
   a) **Person involved in the process**: worker, plant manufacturer/operator
      
      Users involved in the process implement the e-app provided by the engineer, or are a part of the workflow contained within it. For example, a workflow step could be simple user input data or the results of a complex calculation carried out by the plant operator, or services/solutions provided by the plant operator.
   
   b) **End-customer**
      
      End customers are the buyers of the solutions offered (e.g. e-apps), which they select and configure as required according to their business processes, or have them configured by a customising service offered via the ISV.

3. **Platform vendor/operator**:

   Among other things, the platform vendor/operator is responsible for the provision/secure operation of the cloud basis. This includes basic services and solutions, hardware, management, security, marketplace, etc. as well as providing development tools for ISVs (or possibly engineers in conjunction with e-apps).

### 3.3. Use cases / activity flows

The main use cases are grouped into three levels: integration level, cloud basis level and e-app development level. Figure 1 gives an overview on these levels and the detailed descriptions following in this chapter. Other possible sub-groups, e.g. for collecting use cases and requirements concerning classical cloud computing topics - are not considered here.

![Fig. 1. Main levels of the platform concept](image-url)
Level 1: Integration (CPS, machines, equipment, factory)

1) Integration of CPS, machines, equipment, factory systems
   The basis for including real data and factory features in a cloud service/solution and thus also in an e-app is firstly a standardised link to information carriers and internal factory systems, such as CPS, machines, equipment and other factory systems/software.
   a) Standardised integration process
      Using a standardised integration process, the highly diverse factory-specific data formats and protocols are transferred to a domain-specific, application-specific, etc. data format and protocol. Without this, other services/solutions in the cloud would be unable to access or integrate these sources.
   b) Access to real data
      During the integration process, not only the volumes of data to be transferred need to be taken into account but also how quickly the data has to be uploaded. Depending on the case in question, there may be enormous differences, e.g. between simple status messages and large image data files, access to equipment controls (within seconds) or calling up indicators (once a day), etc.
   2) Flexible adaption to changing general conditions
      In order to compete in a highly dynamic environment, it is essential that services can be rapidly adapted to changing general conditions, from integrating factory resources and systems right up to embedding services in higher-level workflows and services/solutions/e-apps, for example, should the need arise to extend various features such as process monitoring in order to request additional parameters or include a new piece of equipment.
   3) Caching in the event of communication breakdowns
      In cases where data is transferred to the cloud in cycles or on request, defined caching mechanisms have to take over if there is a communication failure in order to prevent data or other information, such as commands, from being lost (caching in the cloud and caching in the factory).

Level 2: Cloud-based features, especially management of cloud services and solutions

1) Standard use cases/features
   As examples of cloud-based features, standard use cases and features are listed below which are generally needed in a cloud platform and through which services - also in the form of e-apps/solutions - are offered:
   a) Registration process
   b) Role management/rights management
   c) User/organisation management/client management
   d) Cloud service repository
   e) IT cloud administration

2) Service description on the basis of cloud data models
   Services have to be described in the cloud using a standardised format in order to ensure that they will function together with other services (or as part of a solution) and to enable them to be integrated using a standardised development tool. Corresponding descriptions contain information about (standardised) service interfaces, domain-specific data models, pricing models, communication sequences, service level agreements (SLAs), etc. Depending on the type of service (integration service, CPS service, solution, e-app), descriptions may vary. For example, marketplace information providing customers with marketing support is also included in the description of a solution, whereas in the case of CPS services, the focus is more on their dynamic entry into and exit from processes.

3) Administration of a service repository
   All services registered on or offered via the platform need to be administrated in a service repository, which manages their descriptions and versions and also supports the search for services and their incorporation into other services or workflows/solutions. In the process, the roles/rights of the user accessing them also need to be considered appropriately. The repository also has to be able to deal with dynamic services, which are never completely described but log on and log off the platform constantly (e.g. magazines with sensors and actuators as a CPS service).

4) Workflow definition
   The definition of workflows, i.e. the description of several different services collaborating with one another, as well as further elements involved in the process, is a key enabler regarding the generation of high-quality services/solutions/e-apps which are capable of providing a more complex functionality and of simplifying the overall workflow from the aspect of the user. To achieve this, when defining workflows, the services that can be accessed via the service repository are linked with a supplied development tool for specific use case services/solutions/e-apps. Here, the term service aggregation could be used instead of workflow definition.

5) Onboarding services
   Before a service/solution with a valid service description and, where applicable, valid workflow definition can be successfully authorised and offered via the cloud, it must first go through a so-called onboarding process. This ensures that the service/solution can be implemented correctly. The various process steps are as follows:
   a) Devising and implementing development tools to create a service/solution, including integrating further services or defining workflows.
   b) Executing the developed service/solution in a test environment; this simulates real scenarios in a test cloud.
   c) Based on the results of the test runs as well as other aspects such as security and quality criteria, the service is then validated or refined.
   d) In order to assure later customers (service aggregators or end-customers) that specified guidelines have been observed, there should also be a possibility of having the service/solution certified
by a service company that has been authorised by the platform operator.

6) Order process
Validated (possibly certified) and authorised solutions/e-apps can be bought and sold on the marketplace. Depending on the type of solution/e-app ordered, it is instantiated for the customer and supplied in a bundle with the necessary cloud resources.

7) Customised configuration of the solution/e-app
If necessary, the solutions/e-apps ordered and supplied are tailored to customer requirements. If, for example, an MES is offered as a solution via the cloud, the customer’s controllable factory resources need to be coupled to the cloud with the aid of integration services and integrated into the cloud software solution, in this case the MES, by defining workflows accordingly.

8) Workflow execution
After commissioning a solution/e-app, it is executed according to the workflow defined. In order for them to be processed by a workflow execution engine, workflow definitions must be available in a standard format. As an example, extensions of the Business Process Modelling Notation (BPMN) can be used to do this. A workflow belonging to a solution can be initiated in several different ways.

a) Cyclical workflow execution
b) Execution initiated by an explicit call (by user, consuming connected systems/solutions, …)
c) Execution initiated by an implicit call, e.g. exception handling

To safeguard the security of data and functions, all context information regarding rights, roles, contracts, types of transaction, etc. has to be observed and verified when executing workflows.

9) Monitoring services/solutions
Together with any integrated services, the solutions supplied to the customer need to be monitored in accordance with a range of criteria. As well as criteria such as availability, reply times and capacity, protocols about all calls executed also have to be kept. Their information content varies according to the pricing model used.

10) Billing on the basis of cost and pricing models
According to the corresponding cost and pricing model, the customer-specific use data acquired through monitoring is used as a basis for the cost calculation.

Level 3: Developing an e-app

This last section considers use cases that focus particularly on the development of e-apps. These can be understood as detailed examples of possible uses of specific solutions.

1) Obtaining an e-app development kit
To develop an e-app, registered engineers are eligible to download a development tool. The aim of the development tool is to provide the engineer with optimum cloud support and offer personalised access to the services he is entitled to use and thus also access to the real factory data integrated into the cloud, for example.

2) Developing an e-app
The development tool enables engineers to aggregate a wide range of user-specific services without the need for in-depth IT knowledge. The resulting workflows are made available to the user via diverse interfaces such as mobile end-devices or terminals. These workflows can also integrate services as well as input data from the user or other people involved in the process. Modeling is designed to be as simple as possible and is graphically assisted.

3) Selling an e-app
E-apps are not only developed by engineers to carry out highly-specific tasks but also offered to other engineers on the marketplace. E-apps bought this way have to be easily configurable to individual customer tasks. If the e-app supports the adaption process, it is easier to control the diverse business processes and workflows encountered in small and medium-sized enterprises.

4) Adapting an e-app to changing general conditions
It not only has to be possible to configure an e-app or solution when it is bought or implemented for the first time, but also at a later stage in line with changes in workflows. This ensures that the e-app implemented can be re-configured to changing general company conditions at any time and remain useful to the user for a much longer period of time.

Figure 1 briefly illustrates the events taking place in Level 3 - integration into a factory environment (right), cloud platform (center) and e-app development or workflow definition (left).

3.4. Non-functional requirements

1) Scalability
The cloud not only has to be able to cope with a fast increase in the number of companies linked to it but also with a highly dynamic resource utilisation rate triggered by use patterns of e-apps and solutions.

2) Performance
All operations executed via the cloud have to be performed according to the respective contract. Reliable caching mechanisms are required should stakeholders involved in the process be unattainable for any reason.

3) Usability
All systems with user interaction need to fulfill general usability conditions. A particular challenge in this regard is implementing an easy-to-use development tool to generate e-apps because it conceals the complexity of the underlying IT framework. Workflow definitions should also permit the use of different user interfaces to allow interaction between the stakeholders involved in the process. Depending on user disabilities caused by difficult production environments and requirements, different additional interface could necessary such as gesture control, voice control or brain computer interface.
4) Portability
Whenever possible, the cloud - including all subsystems - should remain independent of a specific platform, from the underlying IT cloud through service interfaces right up to user interfaces.

5) Security
Data and communication security as well as availability are essential in order to guarantee acceptance of a cloud architecture. To benefit from the full potentials of the cloud, it has to be possible to transmit even sensitive data safely to the services/solutions/e-apps used and, if required, to memorise it in the cloud. It must also be possible to exchange defined data and features with linked companies to enhance collaboration. On all three levels (factory, cloud platform and user applications/interfaces, that is, e-apps/solutions), security plays a major role not only with regard to the infrastructure but also to the applications implemented on it and the data managed there.

4. Platform components and features

From the requirements and use cases, a comprehensive system architecture for a cloud-based platform is derived which allows ISVs to offer services with manufacturing-related IT features, turn them into solutions and thus enable e-apps to be efficiently developed and implemented in the manufacturing and engineering sectors.

The component diagram in Figure 2 depicts an abstract view of the platform architecture. The logical layers and functionalities of the various components are explained below.

The platform portal (Front-End) is the point of entry for users and vendors of services and solutions. It contains:
- The public website, on which the user can find general information about the platform, the various services on offer, examples of use cases and best practices.
- The shop, which gives an overview of all available services, solutions and e-apps. As well as the ordering mechanism, there are also ways of giving feedback and evaluating services, solutions and e-apps. This social feature adds a community aspect, which increases transparency and communication both for the user and the vendor, and also helps services to be further optimised. In the case of the wood processing plant, an engineer would visit the website’s shop to look up if there are any services available which are suitable to be used monitor the data from the machines and tools.
- Registration, or login after registration, enables platform users to go onboard, presenting themselves and be active on the platform either as a user, organisation or company.
- The user control panel allows users to update their profile information, manage the e-apps/solutions they have ordered as well as set up and administer user rights and roles. Service vendors are able to display the services and solutions they offer in the shop or on the marketplace, which is also used for order management and billing.
- The administration section is responsible for the management of the entire platform. This includes, for example, the administration of user and service rights, administration of hardware infrastructures, configuration of the basic components and basic platform services, etc.

The base components (Back-End) include supplementary services, which enable onboarding, management, configuration, execution, monitoring and billing the services and solutions. Details of these are given below:
- The basic features of the platform are responsible for user and organisation management related to rights of access and roles regarding the use of solutions and services. The costing broker ensures that billing information about various services and solutions is correctly aggregated according to their orchestration and use. The message broker safeguards communication between the various services.
- Service and solution management comprises the repository, in which the services offered are registered and described. Onboarding allows new services and solutions to be added to the repository; it functions as a tool to accompany the onboarding process and validation. Versioning enables any necessary updates regarding operating security and stability or additional versions of services to be installed without the previous version of that service being affected. This prevents an e-app or solution
that incorporates a particular service into a workflow from malfunctioning. The components of the workflow definitions required to orchestrate services are ascertained and made available for execution. The specific billing options of the various services are filed here and can be appropriately managed.

- **Service and solution instance management** is responsible for instantiating and managing services and solutions as soon as they are requested by a user. In order to do this, the user must first be able to find these services so that he can orchestrate them to create a solution as an ISV, or implement them directly as a user. Through the instantiation procedure, the relevant information about the service and solution order is forwarded to the order execution and billing components. Active services and solutions are monitored both from the aspect of functionality and from the aspect of billable activity.

- An **InterOp service bus** is utilised to integrate the basic platform services, manufacturing services and integration services. It is based on an Enterprise Service Bus (ESB) to which specific factory and service interoperability modules have been added. The workflows of the orchestrated services of a solution are also executed in the workflow definition that has been filed.

The **factory layer** represents an abstract layer and depicts the integrated equipment, CPS and also the sensors and actuators of a user’s production facility. All components should be integrated via a manufacturing service bus but still be directly responsive via integration services. This also allows the user to integrate his manufacturing equipment on the platform in the form of manufacturing services and thus incorporate them directly in an orchestration or solution.

The **infrastructure layer** encompasses all other layers of the platform. The components contained within it are primarily responsible for security mechanisms, which guarantee both the operational security and data security of the manufacturing data concerning all components managed on the platform. The infrastructure is realised in the form of a classical Infrastructure as a Service (IaaS) layer, which automatically supplies the necessary hardware for the solutions and scales them as required.

### 4.1. Equipment integration and integration framework

Standardised interfaces are utilised to integrate the equipment. Using a suitable adapter, legacy equipment may have to be added to map readable information on a standardised interface. This can also be achieved using so-called integration services, which take over these functions. However, standardised interfaces have to be designed and implemented so that they can be addressed by each service and supply the necessary information. To ensure this, an Integration Framework is needed to precisely define the interfaces and required data models. Furthermore this Integration Framework should contain documented sources for basic services, such as integration services, to demonstrate best practices and give ISVs and users a guideline, how to effectively create and integrate their services, solutions and e-apps.

#### 4.2. IT service repository

The service repository contains the services offered on the platform, their description - which represents a virtual image of the resources - and administers access rights at data level. This enables services to be found using the discovery function so that they can be orchestrated and implemented. Care must be taken here to ensure that the description of the service is both efficient and flexible. Possible concepts for a suitable description language are generally ontology-based; this enables them not only to take the specific characteristics of the services into account but also knowledge about their possible implementation, any dependencies with other services, use restrictions, the meaning of filed parameters, etc.

#### 4.3. Workflow definition and IT service composition

An IT service principally offers a specific feature. In order to combine the features of several different services to create more complex features and aggregated services of higher value, these services need to be orchestrated. To achieve this, a workflow is defined that logically links the platform’s basic services, such as monitoring and billing, integration services, integrated CPS or equipment and services from different ISVs, with one another and enables them to be executed. A graphic specification language, such as Business Process Modelling Notation (BPMN) for example, can be used to do this. BPMN allows services to be depicted as processes and coupled with one another. Apart from the sequence used to call up services, the information flow also has to be defined for each service module, for example in the form of input and output parameters. By configuring the corresponding user interface, the workflow or orchestrated service defined in this becomes an e-app or solution, which can then be implemented in practice by the end-user.

#### 4.4. Workflow execution

The defined workflows are executed by an integrated workflow engine. As it is part of the InterOp service bus, this enables problem-free access to the numerous services provided by a solution (generally distributed among different components within the overall architecture) via a common execution component. The workflow engine is not only responsible for executing the defined workflows but also for the management of triggers. These may be initiating events or take the form of the termination of pre-configured time periods, and trigger the execution of additional workflows. Workflow execution is also monitored, i.e. the system checks that workflows are running smoothly. Appropriate troubleshooting measures are initiated if any problems arise, e.g. links to the factory layer are interrupted.
4.5. Configuration of user specific user interfaces

Depending on the user concerned, the specific features of the services and solutions offered may require a different user interface or adapted function or application environment on a desktop computer or a mobile device, for example. To make this possible in a relatively simple and quick way, an SDK (Standard Development Kit) is needed which also covers the Integration Framework. The SDK enables the necessary e-apps to be partly generated in a simple form and implemented in a more complex form.

5. Security aspects

In addition to the functional requirements to be derived from the described use cases, there are also non-functional requirements which apply for the interface component to be developed. The most important of them are related to security issues since this is the major acceptance criterion for industrial users of the described cloud platform. Security plays a major role throughout all levels of the platform architecture, i.e. from the factory level with CPS, equipment, etc. right up to the e-app offered to the user via the cloud platform. On the one hand, it must always be possible to execute the features available without any problems or risks. On the other hand, the data transmitted during platform use has to be protected against misuse by unauthorised third parties. To achieve this, the security mechanisms implemented at infrastructure, communication, and application level are addressed below.

5.1. Infrastructure security

Suitable backup mechanisms and redundant systems are the main elements ensuring the availability and fail-safe use of the platform, and herewith prevent data losses. To do so, the backup mechanisms make copies of the productive platform operation at regular intervals – in extreme cases, continuously – or synchronise several platform instances with one another. Additional components monitor the system status of the infrastructure by means of certain method calls which are executed continuously, and take countermeasures in the event of a failure, e.g. if certain parts of the platform infrastructure react incorrectly.

For the implementation of appropriate backup and monitoring mechanisms, mainly configuration an of existing commercial cloud computing platform has been executed which includes the definition of backup time frames, dependencies and data exchange among virtual machines for which also their physical location has to be considered, functionalities to be checked during monitoring, such as availability of the machines and, in addition to this, availability of the applications deployed on the machines.

Further measures include suitable firewall configurations, such as segmenting the network within the infrastructure in order to restrict rights of access to the platform infrastructure. Monitoring the network or all accesses taking place within it also helps to recognise and repel potential attacks from outsiders. For this task, also a commercial platform has been used in order to efficiently manage network security aspects.

5.2. Communication security

Data loss can also occur if the internet connection via which the information exchange among factory adapter and manufacturing cloud takes place is not sufficiently available. For this reason, there should a caching mechanism be implemented which enables to temporarily store the information to be exchanged if the connection is not available and which continues messaging as soon as the connection is established again.

To do so, a message queue has been implemented based on JMS (Java Messaging Service) technologies which e.g. include configuration of communication endpoints and interfaces, format and maximum number and size of messages, as well as rules for exception handling.

Since manufacturing clouds are handling confidential information about companies, their customers, products, processes, and orders, it has to be sure that no unauthorised parties can access these data. This also concerns the transfer of data from company internal IT systems, computers, and mobile devices to the cloud platform where the software services to handle and use the data are provided.

In order to make the message transfer from and to the platform secure, messages can, in a first step, be signed and encrypted which ensures that unauthorised parties cannot create or read them. Furthermore, managed sessions can be used to prevent unauthorised duplication etc. of messages which could cause exceptions.

To realise message level security, state-of-the-art encryption has been used, i.e. SSL (Secure Sockets Layer) encryption in combination with PKI (Public Key Infrastructure). For some application cases also VPN (Virtual Private Network) connections where set up.

5.3. Application level security

In addition to data protection on message level, application and data level security has also to be implemented. In order to protect confidential data against unauthorised access at this level, access to these functionalities and information which are available on the cloud platform or via interfaces to company-specific IT systems or user interfaces has to be restricted to authorised components and users. To achieve this, different aspects like data encryption, database level security, and well-defined management of access rights is necessary. Furthermore, it can be useful to exchange or provide only data which is really needed on cloud level, since data which is not available there cannot be accessed in case of unauthorised system usage.

The related features have been implemented using encryption mechanisms for sensitive data such as passwords on database level, e.g. using one-way encryption such as MD5 (Message Digest Algorithm 5) or SHA (Secure Hash Algorithm). Furthermore, the data structure has been designed to include access rights for certain user roles or users for each
data set. Those access rights are represented by means of ACLs (Access Control Lists).

To ensure that the amount of data transferred is restricted to the needed information in order to avoid unnecessary data exchange and herewith lower the risk of unauthorised system usage, for each kind of data transfer (e.g. of equipment or measurement data), it has to be analysed which data is really necessary on cloud level. According to this, the data structure can be adapted to fulfil this respective requirement since it is based on an extensible standardised format.

Altogether, the implementation of security mechanisms within the described platform, also provides an opportunity for SMEs to ensure that the IT tools and infrastructure they use is secure since many SMEs, do not have sufficient know-how or resources to do so by themselves.

6. Conclusion and outlook

The full potential of IT systems is often not exploited in small and medium sized manufacturing enterprises. In order to overcome this issue, this paper suggests a cloud-based infrastructure to provide individualised engineering apps (e-apps) for the production domain. Those e-apps can be configured specific to the worker’s, engineer’s, or company’s needs while integrating data sources (such as tools, equipment, factory-internal IT systems) and software services deployed via the cloud platform.

In order to implement such a platform, relevant use cases and requirements are described as a basis for the platform design for which the platform components and features are explained. Since a major acceptance criterion for such a cloud platform towards industrial stakeholders is security, a separate section describes, how this aspect is to be addressed.

However, research on this topic is not finished yet. There is a need for further improvement of the e-app configuration process. In order to really achieve intuitive customisation of manufacturing IT applications according to company-specific processes, it is necessary to better support data source and service integration. This could take place by considering the following aspects:

- Semantically supported service and data source search and aggregation in order to enable integration and assembly of the intended functionalities without detailed knowledge about service features and interfaces.
- Easy integration of data sources and company-internal IT systems by means of appropriate adapters which provide this functionality in combination with a minimum configuration effort.
- Integration of services which do not only execute monitoring and analysis tasks but also actively contribute to manufacturing execution. To do so, further requirements such as time restrictions, additional security features, etc. have to be considered.

The work explained within this paper represents a sound basis for dealing with those challenges.

7. Acknowledgments

The related research and development project is funded by the German Federal Ministry of Education and Research (BMBF within the Framework Concept “Research for Tomorrow’s Production” (funding no. 02PJ2565) and managed by the Project Management Agency Karlsruhe (PTKA). The author is responsible for the contents of this publication.

8. References

[1] VDI 5600 Blatt 1:2007-12 Fertigungsmanagementsysteme 2007; Meier 2011, pp. 31; DIN 62264
[2] Büllingen, Franz; Hillebrand, Annette (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Study on behalf of the German Federal Ministry of Economics and Technology. pp. 20, available online: http://www.bitkom-akademie.de/sites/default/files/pdf/it-sicherheit-studie-publikation.pdf
[3] Baier, Elisabeth (2008): Semantische Technologien in Wissensmanagementlösungen - Einsatzpotenziale für den Mittelstand. In: Fazit Forschung, Vol. 13
[4] Rubarth, Peter (2007): "Keep It Simple, Stupid" - Leichtgewichtiges Wissensmanagement mit Wikis. Community of knowledge.
[5] Xu, Xun (2012): From cloud computing to cloud manufacturing. In: Robotics and Computer-Integrated Manufacturing 28 (1), pp. 75–86.
[6] Zhang, L.; Guo, H.; Tao, F.; Luo, Y. L.; Si, N. (2010): Flexible management of resource service composition in cloud manufacturing. In: 2010 IEEE International Conference on Industrial Engineering and Engineering Management: IEEE, pp. 2278–2282.
[7] Jang, J.; Jeong, B.; Kulvatunyou, B.; Chang, J.; Cho, H. (2008): Discovering and integrating distributed manufacturing services with semantic manufacturing capability profiles. In: International Journal of Computer Integrated Manufacturing, Vol. 21, Iss: 6, 2008, pp. 631-646.
[8] Weirauch, Philipp (2013): Get smart! CheckMobile macht Prozesse mobil. In: LogReal.direkt, 4/2013, pp. 40
[9] Lunani, Mahesh (2011): Enterprise Mobile Apps - How Role-Based Apps Will Drive Productivity and Transformation in Manufacturing Companies, available online: http://www.cognizant.com/InsightsWhitepapers/.