Supporting Virtual Aircraft Certification via Provenance

Paula Natascha Ruß
Institute of Software Technology
German Aerospace Center (DLR)
Bremen, Germany
paula.russ@dlr.de

Andreas Schreiber
Institute of Software Technology
German Aerospace Center (DLR)
Cologne, Germany
andreas.schreiber@dlr.de

Malte Christian Struck
Institute of Software Technology
German Aerospace Center (DLR)
Bremen, Germany
malte.struck@dlr.de

Alexander Weinert
Institute of Software Technology
German Aerospace Center (DLR)
Cologne, Germany
alexander.weinert@dlr.de

Abstract

Exhaustive physical testing ensures the airworthiness of an airplane and is time-consuming and costly. With the latest advancements in computational models and computing power, testing parts virtually becomes feasible. Ensuring the reliability and trustworthiness of such virtual verification processes is a critical point. We collect and assess the obligations and requirements stated by the certification authorities Federal Aviation Administration (FAA) and European Union Aviation Safety Agency (EASA) and from the contributors towards virtual certification. Then, we discuss the possible applications and benefits of using provenance data, which is the documentation of the origins and history of data. By recording detailed metadata, it can support traceability and thus reliability. We propose two provenance models, the first one captures only the workflow between the contributors and their tools. The second one shows the steps of each tool in detail so that the data flow is traceable. These models can be connected by the inputs and outputs of each tool. In the end, the certification authority can use the workflow provenance graph to request the simulation and tool provenance graphs of each contributor. The certifiers have detailed insights into the computational analyses, while the contributors do not reveal their business secrets to each other. Integration of provenance can support regulatory compliance by fulfilling many of the stated obligations and is therefore a promising approach.

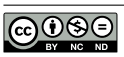
CCS Concepts

• **Information systems** → **Data provenance**; • **Applied computing** → **Aerospace**.

Keywords

Provenance, Workflows, Aviation, Virtual Certification

ACM Reference Format:
Paula Natascha Ruß, Andreas Schreiber, Malte Christian Struck, and Alexander Weinert. 2025. Supporting Virtual Aircraft Certification via Provenance.



PW' 25, Berlin, Germany

ACM ISBN 979-8-4007-1941-7/25/06
https://doi.org/10.1145/3736229.3736257

In *ProvenanceWeek (PW' 25), June 22–27, 2025, Berlin, Germany*. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3736229.3736257

1 Introduction

The certification of an aircraft includes many different tests to ensure its airworthiness. These tests can be time-consuming and depending on the results of these tests, adjustments may be required, so the tests may need to be repeated and prolonging the process. Certification is very costly, the certification process can take over one year of total flow time, which leads to cost of one billion dollar [6].

The advancement in computational power led to the possibility of using simulations and other analysis tools to test the airplane components and its behavior. The perspective of computer science on virtual certification of aircrafts include different challenges, like making the simulation data secure and traceable or storing them for reproducibility for decades.

In this work, we investigate the following research questions:

RQ 1 Which requirements do stakeholders have towards the implementation of a process for virtual certification?

RQ 2 Which of these requirements can be (partially) satisfied using provenance and which infrastructure is required for capturing that information?

This work is structured as follows: First, we give necessary background on virtual aircraft certification and provenance (Section 2). Next, we discuss the requirements for the virtual certification process and how data provenance can fulfill some of these requirements (Sections 3 and 4). Then we provide a provenance model (Section 5) as well as a description of infrastructure required to capture provenance during the certification process and evaluate this setup (Section 6). Finally, we give an overview of related work (Section 7) before concluding (Section 8).

2 Background

Digital Engineering. Before being mass-produced, new aircraft designs are certified as airworthy by *certification agencies* such as the FAA in the USA or the EASA in the EU. Certification involves numerous tests of physical aircraft prototypes and demonstrators to ensure that the aircraft complies with regulations. Virtual certification (or certification by analysis) instead aims to demonstrate compliance with the regulations via computational models using

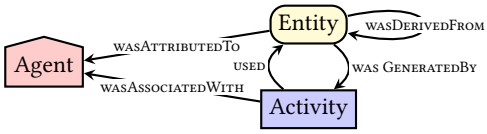


Figure 1: Subset of the W3C PROV model.

digital validation techniques instead of physical tests. A typical engineering project involves numerous *contributors*, such as companies, research institutes or individuals, who are required to collaborate.

In such projects, each contributor has an internal hardware infrastructure that communicates with a single coordination server hosted by one of the contributors. While the contributors share the goal of engineering a complete aircraft or a part thereof, they also aim to keep information about their inner workings confidential. This includes, for example, details on the number and identity of Subject Matter Experts (SMEs) working on the project, details about the software tools used, or the topography of their digital infrastructure.

Virtual Certification and the Virtual Product House (VPH). Virtual certification faces several challenges, ranging from the fidelity required of simulation and analysis methods, to digital collaboration between all involved partners, to the acceptance of digital methods by regulatory authorities. Our focus is on building the authorities' confidence in modeling and simulation techniques. This includes ensuring that computational models are accurate, verifiable, reproducible, and traceable. It is important to ensure that the simulation data, model assumptions, computational steps, and results are documented and comprehensible to enable trust in the systems.

In this context, German Aerospace Center (DLR) has established the VPH to create a platform for the virtual design and testing of aircraft components and systems with respect to certification-relevant aspects [3]. The simulations of virtual models can be done of the complete aircraft or of individual systems. Each simulation typically comprises the execution of multiple discipline-specific tools resulting in one or more Key Performance Indicators (KPIs). These KPIs are crucial for certification as they ensure that an aircraft complies with safety and performance standards.

Provenance. A provenance graph is a directed acyclic graph labeled with nodes and edges, where each node represents an entity, an activity, or an agent [4]. The node type entity is used to describe the current state of a thing that are used in the process. The activities represent processes and events, which uses, changes, or creates entities. Finally, nodes of type agent show the responsibility for a process or entity. Edges represent the relationships between the entities, activities, and agents.

In our case, a provenance graph represents the data entities involved in a computational process, the activities that consume and produce those data, and the software and human agents that orchestrate these processes.

A widely used standard for the notation of provenance is the W3C PROV standard [4]. In this work, we use the subset of this standard (Figure 1).

3 Obligations in Virtual Certification

The engineering of aircraft is a collaborative process involving multiple contributors and certification agencies from various professions. All stakeholders involved in this process have obligations regarding virtual certifications, as well as restrictions on how to track and verify simulation data. In this section, we list the obligations of the two most relevant stakeholders: the certification agencies (Section 3.1) and the SMEs (Section 3.2).

3.1 Certification Agencies

There are multiple certification agencies in countries around the world. However, to our knowledge, only EASA and FAA have published obligations related to virtual certification. Both agencies list the data to be collected and stored during the engineering process, but do not prescribe technical means of doing so.

3.1.1 EASA. The EASA proposed a certification memo in 2020, in which they listed some documentation obligations[1]. EASA demands that the following information be stored during the process of digital engineering:

EO1 All relevant aspects of the method and simulation: pre-processing, solution, post-processing
EO2 All information to retrace the decisions, to understand the assumptions, and limitations
EO3 Description of the analytical models, input data and results, processes and tools
EO4 Experience level of staff
EO5 Software and hardware, OS overview, versions of the tools and software programs, also changes during the process

EASA requires this information to be documented and stored for all activities of partners and subcontractors. As mentioned, EASA does not prescribe technical methods to create or store this documentation. Instead, they formulate additional obligations towards the method of data storage.

First, the data shall be stored as long as the aircraft model is in use. In practice, this means that the information is likely be accessible for multiple years or decades (**EO6**). Moreover, EASA states that the documentation includes the required information shall "easy to access, read and understand" (**EO7**). Furthermore, EASA requires that, in the case of an aircraft issue, the engineering process is not only traceable but also reproducible (**EO8**). This includes the obligation that all software used in the engineering process must be able to run after an issue has occurred.

3.1.2 FAA. The FAA has published a recommendation on virtual certification, using aircraft seats as an example[2]. The FAA demands that the following information be stored during the digital engineering process:

FO1 Software and hardware overview: computer hardware, OS, software, finite element binary specifics
FO2 Computer model: Detailed description with input data
FO3 Engineering assumptions with rational support
FO4 The source of the external data

[1] https://www.easa.europa.eu/en/document-library/product-certification-consultations/proposed-certification-memorandum-modelling
[2] https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-146A.pdf

FO5 General analysis control parameters with justifications for the parameters

The FAA does not set obligations for contributors responsible for storing data, nor does it set obligations for the manner of data storage or access.

3.2 Subject-Matter Experts (SMEs)

In the previous section, we have listed the obligations towards virtual certification formulated by the certifying agencies. These focus on the post-hoc analysis of the engineering process. Fulfilling these obligations is essential for any virtual engineering process. Moreover, following user-centric design principles, the virtual design process has to take into account the obligations formulated by the people working with it, namely the SMEs.

As part of general software development work at VPH we have conducted unstructured regular interviews with SMEs. These SMEs work in multiple fields ranging from university research via applied research to industrial engineering and come from a variety of contributing disciplines. Structured interviews with all involved SMEs are beyond the scope of this work and part of future research, as we focus on the obligations posed by certifying agencies.

The unstructured interviews resulted in the following obligations formulated by SMEs:

SO1 The process shall store structured data in a standardized way
SO2 There shall be traceability between inputs, parameters and outputs
SO3 Detailed metadata of the simulation shall be stored, e.g. runtime or resource usage
SO4 The processes shall easily integrate with existing systems with limited overhead
SO5 Safety, security, and privacy shall be ensured
SO6 Trade secrets and intellectual property shall be protected
SO7 The process shall be easy-to-use
SO8 It shall be possible to query and filter the data for interactive exploration
SO9 It shall be possible to visualize the collected data

4 Turning Obligations into Requirements

Our collected obligations posed by the certifying agencies must be satisfied for the resulting aircraft design to be certified. The obligations formulated by SMEs, in contrast, influence the adoption of the system in practice and even their partial fulfillment yields a benefit for the contributors. Moreover, the obligations of the certifying agencies address data to be collected for a post-hoc analysis, while the SMEs formulate requirements towards an interactive support system for virtual engineering. In this section, we address the first research question through the consolidation of obligations into technical requirements (RQ 1).

After consolidating and analyzing the obligations of certifying agencies and SMEs, we have identified the following technical requirements for a system supporting virtual certification:

R1 The system must store heterogeneous data in a structured way.
R2 The system must allow for manual and automated data entry and retrieval.
R3 The system must store data in a human-readable way.
R4 The system must not use proprietary data formats nor proprietary software.
R5 The system must allow users to trace the origin of data artifacts and to reproduce the computations producing them.
R6 The system must provide functionality even if only partial data is accessible.
R7 The system must offer interfaces for purpose-made analysis tooling.

We derived the above requirements from the obligations that were explicitly formulated by contributors. In addition, the very process of competing contributors collaborating on a single engineering artifact imposes security requirements upon the process of digital engineering. In particular, no contributor wants their competitors to gain more information than absolutely necessary about their respective work in order to not disclose intellectual property. We formalize this implicit obligation in the following requirement:

R8 Each user of the system may only access data that they entered themselves or that is absolutely necessary for their work.

The rest of this section briefly describes each requirement and explains why it is included, noting the obligations it satisfies. Table 1 summarizes the relationship between requirements and obligations.

Structured Storage of Heterogeneous Data (R1). The obligations given by EASA and by FAA go into detail regarding the nature of the data that needs to be stored for subsequent certification of digital artifacts. Analysis shows that the data to be stored are very heterogeneous, ranging from software versions (EO5, FO1) over personal information of employees (EO4) to documentations of the rationale behind design decisions (EO2, FO3). Further, data from digital engineering and simulations can be in a variety of formats, ranging from an aircraft design in an XML-format [1], over CAD models, to binary data such as images and videos. Thus, it is necessary for the system to support the storage of almost arbitrary input data, with respect to limitations posited by R3 and R4.

Automated and Manual Entry and Retrieval (R2). As mentioned in the previous paragraph, the data is highly heterogeneous. Much of this data can be recorded automatically, such as the hardware and software overview (EO5, FO1) or the meta-data about the process (SO3). But some need to be added manually, such as the experience level of staff (EO4). Therefore, a system should support manual as well as automated recording (SO7). Furthermore, the data must be accessible to humans (R3) as well as to other tools for possible analyses (R4).

Human-Readable Data (R3). EASA states that the data need to be easily accessible and readable (EO7). To understand the information in the data, it should be visualized in a way that humans can easily retrieve and understand it (SO9). Moreover, the data needs to be stored for a long term, up to decades (EO6), such that the available software will change overtime. Therefore, to ensure the accessibility of the data, it should be stored in an encoding that can be read by humans.

Non-proprietary Data Formats (R4). EASA poses the obligation that the stored data shall be easily accessible for years and decades after the certification (EO6, EO7). Many software products store

Table 1: Matching Obligations with Requirements

	EO1	EO2	EO3	EO4	EO5	EO6	EO7	EO8	FO1	FO2	FO3	FO4	FO5	SO1	SO2	SO3	SO4	SO5	SO6	SO7	SO8	SO9
R1	X	X	X	X	X				X	X	X	X	X	X								
R2		X		X							X		X	X		X	X			X	X	
R3						X	X															X
R4						X	X															
R5								X							X							
R6																		X	X			
R7						X		X													X	X
R8																		X	X			

data in proprietary formats that are only readable by that particular software. There is, however, no guarantee that the vendors publishing and maintaining that software will still exist after decades have passed, nor that they still offer software capable of reading the data. If the used data formats are not freely documented, it will be impossible to interpret the data decades after initial certification, either due to lack of knowledge or due to legal complications. Hence, we require the data to be stored in openly accessible and non-proprietary data formats.

Traceability and Reproducibility (R5). Both agencies stated obligations that the traceability of the methods and the simulations. A system must provide detailed information about the analytic and computational models and all relevant aspects of the simulations (EO1, EO3, FO2, SO2). The results should even be traceable to the source of external data (FO4). Further, each decision and assumption made need to be traceable (EO2, FO3).

Additionally, the EASA stated explicitly that the results need to be reproducible as long as the aircraft is in service (EO6).

Usable with Partial Data Access (R6). Due to the confidentiality of some data, to ensure the trade secrets are secured, the data should also be possible to use and understand if parts are cumulated or omitted (SO5, SO6).

Interfaces for Analyzes (R7). Collecting and storing the data is one part, another part is the analysis of them. As designing an aircraft involves many different disciplines, the data will be analyzed by a range of different tools (SO8, SO9). This supports the reproducibility and verifiability of results (EO8).

Confidentiality (R8). The safety, security and confidentiality of the designs, processes and results is of high importance for the contributors (SO6, SO5). We have to assume that they only want to exchange the most necessary data with other parties and at the same time have to rely on the accuracy of the data they receive. A system needs to protect the intellectual property of each contributor, without creating a barrier to cooperation. Therefore, we recommend that a system uses the principle of least knowledge, where each party can only access the required data.

While these requirements define the foundation for trustworthy virtual certification, a structured approach is needed to ensure that the data remains traceable and verifiable for the agencies.

5 Provenance Models

In the previous section we have discussed the requirements derived from stakeholder's obligations imposed on the process of digital engineering. In this section, we present an architecture for a system supporting digital engineering that fulfills the requirements using data provenance, addressing the second research question (RQ 2).

Typically, one would now develop a provenance model that specifies which data to collect during the engineering process. Whenever a contributor would perform an engineering task, they would query the collected data for the provenance of their input data. After completing the task, the company would append the data collection to record the provenance of their payload data. Such a data collection would, however, contravene the confidentiality requirement (R8): Each contributor would be able to gather information about the inner workings of other contributors.

Hence, we construct two provenance models of differing granularity, which we call the *workflow model* and the *simulation model*. While the workflow model describes the relation of the contributors, the simulation model records detailed information about the process at each contributor. We describe the workflow model and the simulation model in more detail in Section 5.1 and in Section 5.2, respectively.

5.1 Workflow Model

The workflow model aims to satisfy the requirements of the certifying agencies without disclosing intellectual property of the contributors. To this end, it records information about the relation of the individual simulation models. Certifying agencies can use this information to assemble the complete engineering workflow using the data provided to them by the simulation models.

In the workflow model, each activity represents a top-level engineering step performed by some contributor, each of which is represented as an agent. The data exchanged between the contributors is represented by entities that hold a hash value of the data. As we need to have unique identifiers, a suitable hash function must be chosen, especially one should be preferred, which does not have known collisions. Thus, the actual data exchanged is not stored in the model, but only "pointers" to it. The model is stored in some central location, where each contributor can access it.

Using the hash values, the certifying agencies can verify that the correct input data was used in each step. An *example of the workflow for digital engineering* (Figure 2) has five contributors that

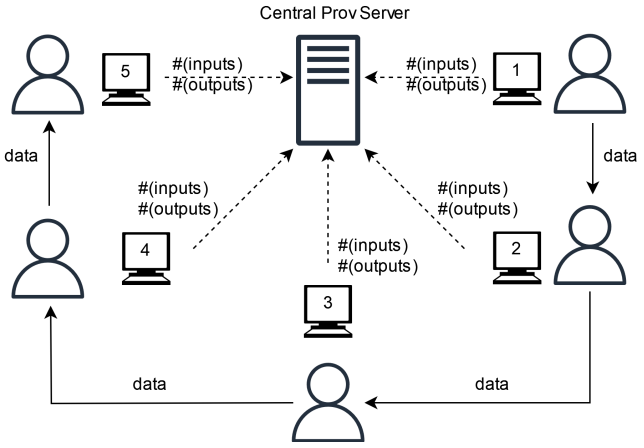


Figure 2: In our workflow, data is passed from contributor to contributor. The hashes of the received data (#inputs) and the computed output data (#outputs) are sent to a central server that stores the workflow's provenance.

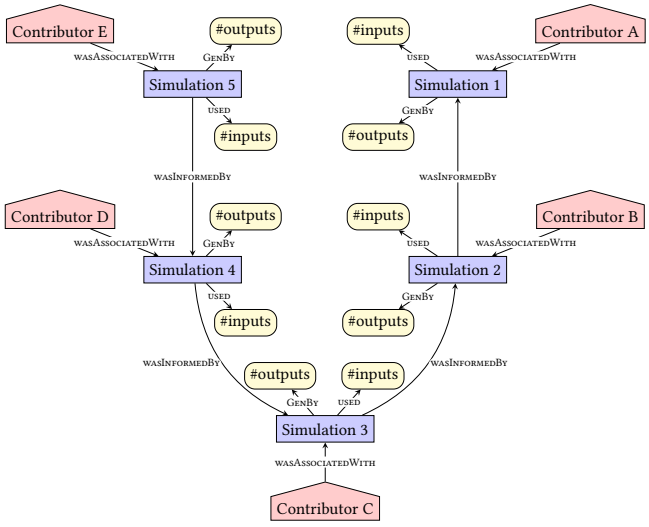


Figure 3: The provenance graph stored by the central PROV server (Figure 2). This provenance graph is passed on to the certifier, who can then contact each agent associated with a simulation to obtain its provenance graph. For better readability, "wasGeneratedBy" was shortened to "GenBy".

send the hashes of the input and output to the central workflow provenance server (Figure 3), while the real data are passed on directly.

The entities represent the connections between the workflow and the simulation model. Starting with the input entities, the simulation can be traced through the workflow model as activity nodes, and finally the results are stored in the output entity nodes, which are connected to the simulation's activity node. Furthermore, by grouping together activity nodes, different levels of detail can be constructed to provide a human-readable overview of the simulation. Depending on the simulation and its complexity, for example, this level could show only the function calls from the main class or only the self-written functions, abstracting the low-level operations.

5.2 Simulation Model

The main purpose of the simulation model is to serve the requirements of the engineers. To this end, it contains detailed description of individual calculations and engineering steps. The data recorded using the simulation model remains with the contributor, as it contains detailed information about their working and must not be accessible to competitors.

Since each contributor has their own engineering processes and documentation formats, we cannot prescribe a general-purpose model that fits the requirements of each company. The only hard requirement we impose upon the simulation model of any given company is it models the data received from other companies as well as the data given to other companies as entities. We moreover discuss possible uses of the provenance node types in the following.

Agent. Recall that agent nodes are used to model both human agents and software agents. Each contributor should use agent nodes to model information that is unlikely to change with incoming data or during the engineering process. This includes, e.g., the experience levels of engineers and developers, or the versions of software packages. Some of this information may need to be added manually. Contributors must include information as stipulated in obligations EO3, EO4, and EO5 as well as in obligations FO1 and FO2.

Activity. Each activity represents an individual operation performed during digital engineering. In theory, every operation, like addition and multiplication, can be represented by an activity node. Similar to agent nodes, the decision on the required level of granularity lies with each contributor. Each contributor needs to ensure that the recorded data fulfills obligation EO1 and EO3 as well as FO2 and FO5.

Entity. Entities model the data that is used. Again, each contributor needs to decide how much information to record about the data itself. Similar to agent and activity nodes, they must take care to fulfill obligation EO3 as well as FO2. Moreover, each contributor needs to agree on data representation for exchanged data with other contributors with which it directly interacts.

6 Evaluation

Having described the provenance models in the previous section, we now evaluate it. Due to the long development time of aircraft and aircraft parts, it is infeasible to compare design processes with and without using our model. Instead, we evaluate our system in two ways: First, in Section 6.1, we describe how a certifying agency would use the collected data to certify the finished artifact. Second, in Section 6.2 we evaluate the provenance models against the requirements collected in Section 4.

6.1 Use Case: Certification

Evaluating the tools and simulations for certification purposes will be done by the employees of the certification agencies.

Given the workflow provenance graph, they can demand the provenance graph of the simulation from the related contributor,

which should be stated in the corresponding agent node, and using the hash values of the input and output data. Therefore, the provenance graphs can be unambiguously identified, and the certifier can verify that the correct inputs were used. Step by step, the certifying agency can collect the provenance graphs of all tools and simulations used and can check the hashes if always the correct data was used. Following the data through each step and tool, the certifying agency can examine the behavior of the systems used and evaluate their computations.

Therewith, they can inspect if the simulations and analysis were correct and are according to the guidelines. The granularity of each provenance graph and the added metadata will be different between different tool providers, but as provenance is a standardized model, it will be compatible with the others and the connection points will be the output/input relation of the data.

6.2 Fulfillment of the Requirements

We now evaluate our system against Requirement R1 through Requirement R7. We omit an evaluation against Requirement R8 as we have already discussed this in Section 5.

Most of our requirements are satisfied by our choice of provenance graphs as a data storage format. In particular, provenance graphs can store arbitrary data in a structured way (R1) and there exist numerous openly documented provenance storage formats such as JSON, XML, etc. [2]. Moreover, there exist freely distributable software libraries for accessing these formats, both via automated scripting and via viewers for human consumption. Thus, Requirement R2, Requirement R3, Requirement R4, and Requirement R7 are satisfied as well. Finally, as described in Section 6.1, our model allows certifying agencies to trace the flow of data throughout the process, satisfying Requirement R5. This holds true even if partial data is still accessible, satisfying Requirement R6.

7 Related Work

There have already been endeavors introducing provenance for virtual aircraft certification. In particular, Dressel et al. introduced a provenance-based data and development environment and a provenance container that stores the data together with its provenance information [3]. While this work enables the transport of payload data together with its provenance data, it does not discuss the structure of the provenance data required for subsequent certification.

Mirabella et al. developed a framework for automatic generation of certification reports [7]. The purpose of this framework is to align test results with the obligations posed by certifying agencies. It is not concerned with eliciting or storing data, but instead focuses on preparing the data for certification. Moreover, the framework does not take confidentiality requirements into account. In contrast, our system allows competing contributors to store their simulation data confidentially. The data stored in our system could subsequently be used by the framework to generate certification reports.

NASA is working on virtual certification under the term Certification by Analysis (CbA) [6]. They focus on increased fidelity of simulations that allows for simulations that capture real-world behavior. Our work, in contrast, focuses on gathering the data created by such simulations as well as by other digital engineering steps and making it available to certifying agencies.

Blockchain technology is another approach for making workflows and simulations in aviation traceable in a decentralized way. Santos et al. [8] investigated how blockchain could be used for the traceability of records and certificates in the aviation sector. They pointed out that blockchain can be used to maintain the data immutability for protecting and securing the data for building trust. In contrast to our work, the authors do not consider the confidentiality required for collaboration between competing contributing companies. The study by Kocadag et al. [5] explores the use of blockchain technology to securely store provenance data. The study reviews current research on blockchain-based storage strategies, highlighting their advantages and challenges. The authors developed a system based on this literature and noted that provenance data can be very large due to its complexity.

8 Conclusion

Virtual design and certification of a complete aircraft is still a long-term goal of the aviation industry. In this work we have developed a method for storing information relevant to virtual certification such that the intellectual properties of contributors are kept confidential, but accessible to certifying agencies. This aims to raise the confidence of the certifying agencies in the eventual result of the certification. Moreover, our system does not prescribe particular data formats or storage mechanisms for the contributing companies, but instead allows them to store as much or as little data as they deem necessary for the certification process.

As a next step, we are looking to deploy our system in a limited development process to investigate its usability in a real-life engineering process. Experience shows that usability and user experience plays a major role in the adoption of novel processes. Hence, we aim at integrating our process more deeply with existing engineering processes. This will allow our system to simplify digital engineering and certification processes and thus make the development of novel aircraft and aircraft parts easier, cheaper and faster.

References

[1] Marko Alder, Erwin Moerland, Jonas Jepsen, and Björn Nagel. 2020. Recent Advances in Establishing a Common Language for Aircraft Design with CPACS. In *Aerospace Europe Conference 2020*. https://elib.dlr.de/134341/

[2] Trung Dong Huynh, Paul Groth, and Stephan Zednik. 2013. PROV Implementation Report. https://www.w3.org/TR/prov-implementations/

[3] Frank Dressel, Martin Rädel, Alexander Weinert, Malte Christian Struck, Tobias Haase, and Matthias Otten. 2022. Common source & provenance at virtual product house: Integration with a data management system. (2022).

[4] Paul Groth and Luc Moreau. 2013. An Overview of the PROV Family of Documents. https://www.w3.org/TR/prov-overview/

[5] Steven Kocadag, Matthias Pohl, and Andreas Schreiber. 2025. Trusted Provenance with Blockchain Technology: A Systematic Literature Review. In *Balancing Software Innovation and Regulatory Compliance*. Springer Nature Switzerland, 93–105. https://doi.org/10.1007/978-3-031-89277-6_6

[6] Timothy Mauery, Juan Alonso, Andrew Cary, Vincent Lee, Robert Malecki, Dimitri Mavriplis, Gorazd Medic, John Schaefer, and Jeffrey Slotnick. 2021. *A guide for aircraft certification by analysis.* Technical Report. NASA.

[7] Claudio Mirabella, Michele Tuccillo, Pierluigi Della Vecchia, et al. 2024. A Model-Based System Engineering Approach Towards Aircraft Digital Certification. In *ICAS PROCEEDINGS*.

[8] Luis F. F. M. Santos, José António Costa, Duarte Valério, Nelson Batista, and Rui Melicio. 2022. Blockchain Information Based Systems in Aviation: The Advantages for Aircraft Records Management. In *2022 International Conference on Control, Automation and Diagnosis (ICCAD)*. https://doi.org/10.1109/ICCAD55197.2022.9853888