INTERNATIONAL DESIGN CONFERENCE - DESIGN 2022
https://doi.org/10.1017/pds.2022.31

A Digital Twin Trust Framework for Industrial Application

J. Trauer [1,✉], S. Schweigert-Recksiek [1], T. Schenk [2], T. Baudisch [2], M. Mörtl [1] and M. Zimmermann [1]

[1] Technical University of Munich, Germany, [2] Siemens AG, Germany

✉ jakob.trauer@tum.de

Abstract

A reason for the slow adoption of digital twins in industry is a lack of trust in the concept and between the stakeholders involved. This paper presents a Trust Framework for Digital Twins based on a literature review and an interview study, including seven recommendations: (1) explain your twin, (2) create a common incentive, (3) make only one step at a time, (4) ensure IP protection and IT security, (5) prove your quality, (6) ensure a uniform environment, and (7) document thoroughly. Together with 20 concrete measures it supports practitioners in improving trust in their Digital Twin.

Keywords: digital twin, trust, industry 4.0, socio-technical systems, organisation of product development

1. Introduction

Digital Twins (DTs) are currently amongst the most discussed topics in technical product development and the number of DTs is expected to increase massively over the next years (Eckert et al., 2019; Hallstedt et al., 2020). In the future, there will be internal and external marketplaces and ecosystems for DTs, in which a wide variety of stakeholders will create, modify, and obtain DTs, as well as exchange information about them, provide feedback, etc. (Rosen et al., 2019). As DTs are meant to cover the entire lifecycle, an inherent characteristic is their interdisciplinarity. Therefore, many parties need to collaborate in order to reach the full potential (Stjepandić et al., 2022). However, especially for DTs, but also for any other digitalisation project, people often have mistrust in the technology and other parties, with which information has to be shared (Rasheed et al., 2020; Thielsch et al., 2018). This is also valid for DTs. In a survey with 61 industry participants, Trauer et al. (2022) identified "setting realistic expectations and trust" is among the 10 most crucial factors impeding the implementation of DTs. This challenge was also identified by others, e.g. Barricelli et al. (2019), Singh et al. (2018), and Neto et al. (2020)**.** However, to date there is no solution known.
Thus, it is an inevitable task for DT providers to create trust, or at least minimize distrust. Consequently, the goals of this study are to (1) derive a definition for trust in the context of DTs, and (2) to develop an initial framework providing recommendations and insights from research and the state of the art on how to create trust in DTs.

2. State of the Art

2.1. Digital Twins

Over the last decades, many different definitions of DTs have been published and used. The discussion has not concluded in a common understanding, as DTs can be quite different depending on the context. In industry, also the terms used for DTs are inconsistent. As shown by Trauer et al. (2022), companies

often refer to Digital Shadows, Digital Replicas, Digital Threads, and more instead. To create a common ground among the project partners, within this publication the definition from Trauer et al. (2020) is used:

> *"A Digital Twin is a virtual representation of a physical system, which is connected to it over the entire lifecycle for bidirectional data exchange." (Trauer et al., 2020)*

This definition is congruent with the definition of the project partner Siemens, describing DTs as a *"description of a component, product, system, infrastructure or process by a set of well-aligned, descriptive and executable models"* (Rosen et al., 2019). Especially the lifecycle aspect of this definition is quite ambitious. Therefore, Trauer et al. (2020) as well as Rosen et al. (2019) identified subcategories of DTs - Engineering Twins, Production Twins, and Operation Twins. These categories are differentiated by the lifecycle phase a DT use case is contributing to the most. The main difference of the two referenced definitions lays in the terminology of the subcategories, as Siemens is referring to Product Twins, Production Twins, and Performance Twins instead (Rosen et al., 2019). These terms can be used synonymously to the previously mentioned.

2.2. Trust

Also, regarding the definition of trust, manifold definitions in different contexts exist. In the context of organizational trust, Mayer et al. (1995) defined trust as:

> *"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"*

This definition focuses on the willingness to accept a certain vulnerability in the interaction with other parties. Other researchers rather focused on the mental state of persons trusting in someone or something, such as Lee and See (2004) defining trust as

> *"[…] the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability".*

According to Hoff and Bashir (2015), common in these two, and most of the other definitions, are three basic components. A party giving trust - the trustor, a stakeholder accepting trust - the trustee, and something which is at stake. So, trust is especially needed in untransparent, complex, unstable, and uncertain situations - situations which occur more often due to the increasing digitalization and automation (Lee and See, 2004; Liu and Loper, 2018). With a sufficient level of trust, it enables people to accommodate to the challenges of this increasing complexity and uncertainty and therefore supports also the adoption of novel technologies such as DTs (Lee and See, 2004).

However, as stated by Lee and See (2004), it is essential to facilitate an appropriate level of trust. If users put too little trust in a system - i.e., they expect less than the system would be capable of - they will not use the system to its full extent. This is common when facing new technologies like DTs. On the other hand, when people "overtrust" systems, they place more trust in a system than its capabilities could provide, therefore the user would misuse the system. For example, if an engineer trusts blindly in a topology optimization result provided by a DT without checking the assumptions and data behind, this can lead to wrong conclusions resulting in overengineering or failure of the product.

According to Ba and Pavlou (2002), there are three basic sources of trust - familiarity, calculativeness, and values. The first effect refers to experiences that can be made by repeated interaction with a trustee. This familiarity then results in trust or mistrust. Calculativeness creates trust, enabling the trustor to assess the costs and benefits of the trustee when it abuses the given trust. This can be achieved e.g. by strong liability agreements. The last source feeds trust by supporting confidence in the trustworthiness and goodwill through institutional structures such as standards and norms.

In the literature review, several general frameworks to increase trust can be found (e.g. Ba and Pavlou, 2002; Hoff and Bashir, 2015; Lee and See, 2004; Liu and Loper, 2018; Wang and Burdon, 2021; Yadav et al., 2019). Some of them focus on automated systems, others on online systems. Nevertheless, there

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

is no specific framework to support companies in creating an appropriate level of trust in their DT initiatives to be found.

3. Methodology

3.1. Project Scope

This research project was conducted in close collaboration with the Siemens AG. Siemens is an international large-scale technology company focused on industry, infrastructure, transport, and healthcare. In these different domains, Siemens is often both: A manufacturer and supplier of real products and systems and thus the creator of their DTs on the one hand and a vendor of a huge digitalization portfolio of commercial tools and available solutions to build, validate and apply DTs on the other hand. The project was kicked-off in July 2021 with seven senior DT experts of Siemens. In an interactive workshop, initial directions, a general vision and a project vision as well as expected project results were defined. The vision reads as follows: *"Siemens has taken extensive measures to build trust in its products and is an established, trusted stakeholder of digital twins. Digital twins are widely applied, and numerous best practices are available."*

3.2. Literature Review

The underlying literature review was conducted using forward and backward search. For the forward search, a research strategy plan, depicted in Table 1, was applied. To create search strings, the synonyms were combined using an OR operator and the aspects using an AND operator. These search strings were then entered to Scopus and Google Scholar to identify relevant literature.

Table 1. Research strategy plan guiding the literature review

	Aspects			
Synonyms	Digital Twin	Trust	Framework	Classification
	Simulation	Distrust	Concept	Quality*
	Digital Transformation	Mistrust	Process	Certification
	Digital*			Validation
	Technology Acceptance / Adoption			Verification
	Transformation			Traceability

3.3. Market Research

The characteristics of DTs are comparable with simulations and to some extent also with software elements. In addition, since the vision of this project entails a platform for DTs, market research was conducted to identify general measures simulation and software vendors and marketplaces offer to create trust. In this review, the most common stores were analysed, namely Apple Appstore (www.apple.com/de/app-store/), Google Playstore (www.play.google.com/), Microsoft Store (www.microsoft.com/en-gb/store/apps), Steam (www.store.steampowered.com/), Amazon Marketplace (www.sell.amazon.de/), and simercator (www.simercator.com/).

3.4. Interview Study

The main part of this research is based on an interview study. Out of an initial list of 41 potential experts from the network of the authors with experience in DTs, digitalization, and/or trust, 17 were prioritized as most relevant and invited. Of this list, 10 persons confirmed to participate in the interview study. The interviewees are employed in 9 different companies and cover a broad range of industries (see Figure 1). All of them have profound knowledge in the development or usage of DTs. Prior to the interviews, the participants were asked to fill out a survey with basic background questions. The majority stated that they have had doubts in DTs at some point and also their colleagues already have distrusted this concept (see Figure 1). All of them gained own experiences with DTs before the survey.

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

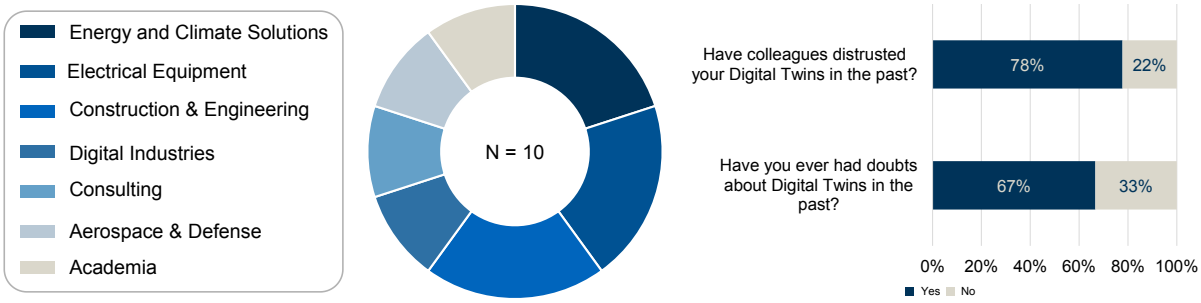


Figure 1. Background of interview participants

The interviews were conducted from July 2021 to September 2021. They lasted about an hour each and were semi-structured following an interview guide including eleven open questions (see Table 2). Since all participants were German native speakers, the questions were posed in German to avoid language barriers. After these questions on stakeholders, user stories, and solution elements, the interviewees were asked to assess the solution elements of the framework regarding impact and effort.

Table 2. Interview guideline

ID	Question
1	When we first contacted you about trust and DTs, what was the first thing that came to your mind?
2 (opt.)	You indicated that you are actively working on DTs - Please specify.
3 (opt.)	You indicated that you use DTs in your everyday work. For which tasks and in what context?
4	Which use cases do you currently work on in your company?
5	You indicated that you have never/already doubted DTs. Can you explain why?
6	You indicated in the survey that colleagues have (never) distrusted DTs / simulations. Can you explain why?
7	From your point of view, what could generally be solution elements to increase trust in DTs?
8	What is being done in your company to increase trust in simulations / DTs?
9	Which objective do you consider more promising / necessary: building trust or covering risks?
10	Which stakeholders are there in the context of trust & DTs? Who needs to trust whom?
11	What situations/use cases can you think of in which trust-building methods would be needed? What do you think the collaboration between the stakeholders should look like?

4. The Digital Twin Trust Framework

4.1. Overview

In this chapter, the combined results of the research elements presented in the previous sections are shown. The Digital Twin Trust Framework (DTTF) has three main components - Stakeholders, User Stories, and Solution Elements. The framework was created as an interactive document to enhance the usability. The overview and landing page of the DTTF is depicted in Figure 2. Clicking on one of the symbols will lead to a respective one pager including a detailed description, references, and testimonials of the interview partners. Users of the DTTF can choose, whether they want to be guided through this framework by first selecting one of the three stakeholder personas, which lead to three possible situations in which trust needs to be generated (the user stories). Connected to these user stories are the seven solution elements with concrete measures at the core of the DTTF. Users do not necessarily need to follow these three steps. Instead, one can also directly start with the solution elements.

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

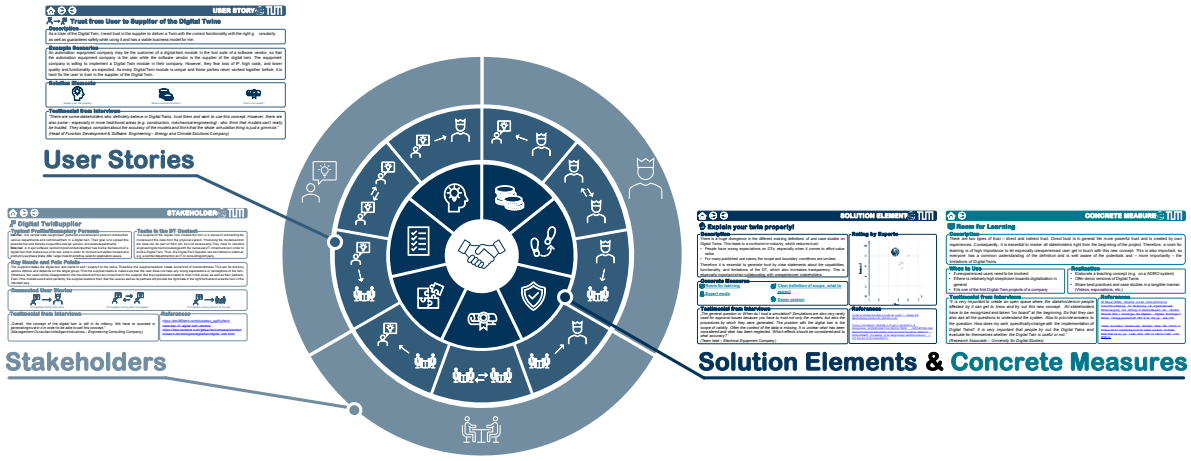


Figure 2. Overview and landing page of the digital twin trust framework

4.2. Stakeholders

There are three basic types of stakeholders in the context of a DT: A Digital Twin Supplier, a User, and Partners of the User. All three types can be either internal (different departments / disciplines / teams within the same organization) or external (business partners from different companies).

Dependent on the application scenario, one person or organization can have different roles. For instance, an automation equipment company may be the customer of a DT module in the tool suite of a software vendor, so that the automation equipment company is the user while the software vendor is the supplier of the DT. On the other hand, once the DT of a certain automation component or system is built, the automation equipment company may include the DT as an add-on to its existent product portfolio, taking the role of the DT supplier while companies buying the automation equipment are now taking the role of the user of the DT in a sense of (directly) paying for the benefits the twin offers.

The same is true for the creation of models. In some cases, the supplier may provide the abstract model types (e.g., regression models, FEM modules), while the user has to provide the concrete instances (e.g. input and output data or CAD models).

Digital Twin Supplier: The supplier of the DT creates the twin in a sense of connecting the models of and the data from the physical system. Producing the model (type) and/or the data can be part of their job, but not necessarily. They have to combine engineering domain knowledge with the necessary IT infrastructure in order to build a DT and sell it to the user. Thus, the DT Supplier can be internal or external, e.g., a central department or an IT or consulting company.

User of the Digital Twin: The user is the customer of the supplier and pays for the DT. In many cases, the users are not even interested in the interior and functionality of the twin, but more in the results of its simulations. Therefore, the user sometimes (especially for operation twins) does not necessarily have to have an engineering background. For the engineering twin, on the other hand, the user in some cases has to deliver the simulation models of the system to the supplier in the first place, as they are part of their domain knowledge. Or they deliver the necessary data, e.g., in the role of customer service or sales. The user can be part of the same organization as the supplier or from another company. They can be e.g., decision makers, salespeople, or design, production, and simulation engineers.

Partners of the User: There is a large number of possible partners of the user. One might be independent regulatory bodies or certification agencies. Another is the actual end customer (consumer) that makes use of the system the DT is supposed to mirror. There can be supplier-OEM relationships in a sense that a supplier has to use the DT or provide data and models for it.

4.3. User Stories

Trust between the beforementioned stakeholders needs to be created in various situations. Since these stakeholders need to collaborate in all possible combinations, the user stories were structured accordingly. An overview of all nine combinations of stakeholders and the resulting user stories is

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

depicted in Figure 3. To create trust in these situations, solution elements are required, which are described in the following chapter.

Digital Twin Supplier	As a DT supplier, I need to trust othersuppliers of DTs or Twin modules, that my interfaces to them are not dangerous.	As a DT supplier, I have to trust the user that they • use the Twin in the right way, so that I do not run into liability issues and • do not make improper use of my knowhow.	As a supplier of the DT, I have to trust in the quality of the data and the models the partners of the user provide.
User of the Digital Twin	As a user of the DT, I need trust in the supplier to • deliver a Twin with the correct functionality • with the right granularity • as well as guarantees safety while using it, and • has a viable business model for me.	As a user of the DT, I need to trust in other users of the same DT to use the Twin the right way, also with regards to its (in)capabilities, especially when scaling use cases.	As a user of the DT, I have to trust my partners to • be able to provide compatible models for my twin and • guarantee safety in the data exchange.
Partner of the User	As a partner of the Twin user, I need to trust the supplier not to use my know-how in an improper way after providing my part in building the Twin.	As a partner of the DT user, I need to trust the user that they protect my know-how when exchanging data.	As a partner of the Twin user, I need to trust other partners of the Twin user that my interfaces to them are not dangerous.

Figure 3. User stories in which trust needs to be created

One of the most common user stories is gaining the trust of DT users in the products a DT supplier is offering: *As a User of the Digital Twin, I need trust in the supplier to deliver a Twin with the correct functionality, with the right granularity as well as that they guarantee safety while using it and have a viable business model for me*. For example, an automation equipment company may be the customer of a DT module in the tool suite of a software vendor, so that the automation equipment company is the user while the software vendor is the supplier of the DT. The equipment company is willing to implement a DT module in their company. However, they fear loss of IP, high costs, and lower quality and functionality as expected. As every DT module is unique and those parties never worked together before, it is hard for the user to trust in the supplier of the DT. This user story is also justified by one of the interview partners stating: *"There are some stakeholders who definitely believe in Digital Twins, trust them and want to use this concept. However, there are also some - especially in more traditional areas (e.g., construction, mechanical engineering) - who think that models can't really be trusted. They always complain about the accuracy of the models and think that the whole simulation thing is just a gimmick."* (Vice President Methods, Analyses & Materials – Aerospace & Defense Company)
Based on a pairwise comparison among the solution elements, trust can be created in this situation by explaining the DT properly, by sharing a common incentive, and by proving the quality to the customer. These solution elements are described in more detail in the following chapter.

4.4. Solution Elements and Concrete Measures

Seven solution elements are at the core of the DTTF (see Figure 4). Each one of these solution elements is connected to up to three concrete measures. The intention of these elements is to increase applicability and to guide practitioners in the implementation of trust in digital twins.

Figure 4. Solution elements and connected concrete measures

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

Explain your twin properly! There is a huge divergence in the different existing definitions of and case studies on DTs (Trauer et al., 2020; Jones et al., 2020; Neto et al., 2020). This leads to a confusion in industry, which reduces trust:

- People have wrong expectations on DTs, especially when it comes to effort-value ratios.
- For many published use cases, the scope and boundary conditions are unclear.

Therefore, it is essential to generate trust by clear statements about the capabilities, functionality, and limitations of the DT, which also increases transparency. This is especially important when collaborating with unexperienced stakeholders. It can be achieved, e.g., by offering an expert mode, i.e., that if requested by the user, detailed insights in the source code of the DTs can be provided. This possibility conveys that one is playing with open cards and thus increases the trustworthiness. Another option is to offer a room for learning. There are two types of trust – direct and indirect trust. Direct trust is in general the more powerful trust and is created by own experiences. Consequently, it is essential to involve all stakeholders right from the beginning of the project (Meyer, 2020). Therefore, a room for learning is of high importance to let especially unexperienced users get in touch with this new concept.

Create a common incentive! When the motivation of the involved stakeholders is not clear, mistrust can remain as stakeholders fear to be left alone once the transaction is finished. From reviewing appstores and marketplaces, it becomes clear that a common economic incentive is a proven concept to generate trust. This ensures that all stakeholders invest effort and resources over the whole life cycle in order to make the DT a success and thereby all parties benefit from it. This solution element could be realized for example by offering a "Digital Twin as a Service" (Aheleroff et al., 2021) and/or a Digital Twin Lifecycle Management (Durão et al., 2018; Singh et al., 2020).

Make one step at a time! As the concept of a DT is often regarded as very broad and hard to grab, mistrust can result from stakeholders not seeing a way how to realize this goal. It is therefore of high importance to proceed in small steps, so that also the risk of each step is reduced to a manageable amount. Further, it is easier for stakeholders to understand the functionality and to get involved in regular gates and check points. As a result, frequent feedback can be incorporated, and emerging mistrust can be tackled right away. One measure to achieve this is to use the shell model of Trauer et al. (2020). Another option is to implement a refund system. The implementation of a DT will inevitably lead to a high amount of financial investment from the user. Additionally, it is often associated with a high risk concerning its business cases. Therefore, a refund system, as offered by Steam (Steam Refunds, 2021) for example could improve trust.

Protect the Intellectual Property (IP) & ensure safety! For the DT to work and incorporate all necessary models and data, it is inevitable for stakeholders to exchange a high amount of information. Especially in security-relevant areas, IT security and IP protection are a must. Once stakeholders do not trust in the security of their IP, no collaboration is possible. Therefore, measures have to be taken right from the beginning of the project so that mistrust in this area cannot even come up in the first place. This can be done by developing IT safety protocols and virus checks applying the recent enabler for data security (Rasheed et al., 2020). As one of our industry partners stated, this is also more important than to have strong liability agreements: *"It is quite clear that merely clarifying liability issues is not the right direction; it is a blunt sword. The concept must be such that a very high level of safety is established, ensured and also continuously maintained from the start. Anything else is just a plaster on a wound that is too big and cannot repair the damage."* (Vice President Methods, Analyses & Materials – Aerospace & Defense Company)

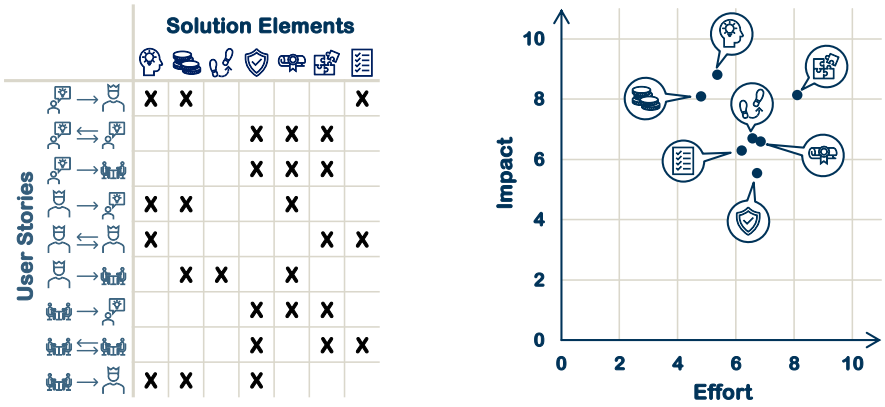
Prove your quality! Once the market for DTs has evolved, there will be a variety of stakeholders, users, and third-party partners that collaborate in order to build a DT. Therefore, stakeholders compete with others and have to show their qualities. As trusts heavily depends on positive experiences, it has to be built be continuously proving that it is justified. This is true for all stakeholders as trust is necessary in all directions before information and data can be shared. To prove your quality, it can be helpful to show best practices and to offer ratings, rankings, and customer experiences as known from other marketplaces and appstores. Trust can be built indirectly by publishing credible experiences others made when collaborating with a stakeholder. Previous studies even showed that customer reviews have a stronger impact on the trustworthiness of online stores than assurance seals (Utz et al., 2012).

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

Ensure a uniform environment! As models and data for a DT will have to come from different sources, a lack of transparency may emerge, which results in mistrust in the DT and its capabilities as well as the security. However, when a basic form of trust in the environment is present, this also increases the trust in the DT module that was developed or is offered in it. This solution element is also well known from appstores, where a standardized platform for developers ensures a basic level of quality. Therefore, stakeholders should make sure to use one coding language and environment, they should have a standardized reviewing process, and in the best case offer Digital Twin Building Blocks.

Document thoroughly! As many stakeholders have to contribute to the DT, a certain level of complexity is inevitable. This will make it necessary to have a set of proper documentation also for stakeholders joining the process in later stages or using already existent twin modules. By documenting in a thorough way, understanding of the twin as well as its functionality is supported, maintenance is enabled, and transparency is created. A standard for documenting DTs might be the DT Use Case template (Schweigert-Recksiek et al., 2020; Trauer et al., 2021). Further a standardized modelling and simulation process description could help (Sauer et al., 2021).

In general, any element is applicable in all user stories. However, in order to increase the usability of the DTTF, only the three most relevant solution elements are connected to the user stories. To identify these, a pairwise comparison was conducted together with the research project partners. All elements were compared against each other with respect to their usefulness in a specific user story. The three elements selected for each user story are presented in Figure 5a. Moreover, as a part of our interview study, we asked the interviewees to rate the impact a solution element has on trust and the effort required to implement it. The result is depicted in Figure 5b. Explain your twin properly, common incentive, and a uniform environment achieved the highest scores for the impact. The highest effort is estimated for implementing a uniform platform.



(a) (b)

Figure 5. (a) Result of the pairwise comparison to connect solution elements and user stories. (b) Estimated impact and effort of the solution elements as rated by the interview partners

5. Initial Evaluation

At the end of the research project, the DTTF was presented to twelve international DT experts working at Siemens, which were not part of the interview study, to initially evaluate the DTTF. For that, the participants were asked to anonymously submit strengths and weaknesses of the DTTF and to subjectively rate applicability and usefulness on a scale from zero to ten. As a strength of the framework, the participants particularly emphasized the comprehensive overview and the diversity and interconnectedness of the facets considered. Further, the general applicability as well as providing clear inspirations as a starting point while leaving space for individualization, was complimented. On the contrary, some attendees experienced this generic approach as a weakness of the DTTF as it is no "ready-to-use" solution to create trust. In addition, the lack of implementation of the framework was criticized. Also, some attendees demanded for quantitative metrics to assess the level of trust. On average, however, the DTTF was considered useful and applicable (see Figure 6).

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

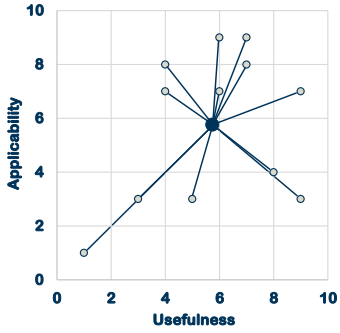


Figure 6. Initial evaluation of usefulness and applicability of the digital twin trust framework

6. Conclusion

6.1. Discussion

This research project was based on a literature review, a market study, and an interview study. In this interview study, a broad range of expertise could be covered, which increases applicability. Further, the presented DTTF is independent from the DT use case. Although DT use cases are highly individual, it is possible to apply the DTTF. However, only ten experts were considered in the interview study. Moreover, the DTTF was not yet used for a real-world project. Therefore, a final evaluation is not possible yet. But the initial evaluation already indicates medium to high level of applicability and usefulness. After the initial implementation, further adjustments of the framework might be needed.

6.2. Outlook

In this paper, a Digital Twin Trust Framework was presented. In the future, a pilot study should be conducted to implement and further concretize the DTTF. As mentioned in the initial evaluation, quantitative metrics to assess trust would be helpful. Lastly, a platform offering DT building blocks including trust measures, such as ratings and customer experiences, IT safety protocols, demo versions, refund systems, etc. would be the next big step towards a broad application of DTs in industry.

References

Aheleroff, S., Xu, X., Zhong, R.Y. and Lu, Y. (2021), "Digital Twin as a Service (DTaaS) in Industry 4.0: An Architecture Reference Model", Advanced Engineering Informatics, Vol. 47, p. 101225. https://doi.org/10.1016/j.aei.2020.101225.

Ba, S. and Pavlou, P.A. (2002), "Evidence of the Effect of Trust Building Technology in Electronic Markets: Price Premiums and Buyer Behavior", MIS Quarterly, Vol. 26 No. 3, p. 243. https://doi.org/10.2307/4132332.

Barricelli, B.R., Casiraghi, E. and Fogli, D. (2019), "A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications", IEEE Access, Vol. 7, pp. 167653–167671. https://doi.org/10.1109/ACCESS.2019.2953499.

Durão, L.F.C.S., Haag, S., Anderl, R., Schützer, K. and Zancul, E. (2018), "Digital Twin Requirements in the Context of Industry 4.0", in Chiabert, P., Bouras, A., Noël, F. and Ríos, J. (Eds.), *Product Lifecycle Management to Support Industry 4.0, 2018, Cham*, Springer International Publishing, Cham, pp. 204–214.

Eckert, C., Isaksson, O., Hallstedt, S., Malmqvist, J., Öhrwall Rönnbäck, A. and Panarotto, M. (2019), "Industry Trends to 2040", Proceedings of the Design Society: International Conference on Engineering Design, Vol. 1 No. 1, pp. 2121–2128. https://doi.org/10.1017/dsi.2019.218.

Hallstedt, S., Isaksson, O. and Öhrwall Rönnbäck, A. (2020), "The Need for New Product Development Capabilities from Digitalization, Sustainability, and Servitization Trends", Sustainability, Vol. 12 No. 23, p. 10222. https://doi.org/10.3390/su122310222.

Hoff, K.A. and Bashir, M. (2015), "Trust in automation: integrating empirical evidence on factors that influence trust", Human Factors: The Journal of the Human Factors and Ergonomics Society, Vol. 57 No. 3, pp. 407–434. https://doi.org/10.1177/0018720814547570.

Jones, D., Snider, C., Nassehi, A., Yon, J. and Hicks, B. (2020), "Characterising the Digital Twin: A systematic literature review", CIRP Journal of Manufacturing Science and Technology, Vol. 29, pp. 36–52. https://doi.org/10.1016/j.cirpj.2020.02.002.

https://doi.org/10.1017/pds.2022.31 Published online by Cambridge University Press

Lee, J.D. and See, K.A. (2004), "Trust in automation: designing for appropriate reliance", Human Factors: The Journal of the Human Factors and Ergonomics Society, Vol. 46 No. 1, pp. 50–80. https://doi.org/10.1518/hfes.46.1.50_30392.

Liu, L. and Loper, M. (2018), "Trust as a Service: Building and Managing Trust in the Internet of Things", in 2018 *IEEE International Symposium on Technologies for Homeland Security (HST), 10/23/2018 - 10/24/2018, Woburn, MA*, IEEE, pp. 1–6. https://doi.org/10.1109/THS.2018.8574169.

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995), "An Integrative Model of Organizational Trust", The Academy of Management Review, Vol. 20 No. 3, p. 709. https://doi.org/10.2307/258792.

Meyer, U. (2020), "Industrie 4.0 als sozio-technische Zukunftsvorstellung. Zur Bedeutung von organisationaler Sinnerzeugung und -stiftung", in Maasen, S. and Passoth, J.-H. (Eds.), *Soziologie des Digitalen - Digitale Soziologie?*, Nomos Verlagsgesellschaft mbH & Co. KG, pp. 349–378. https://doi.org/10.5771/9783845295008-349.

Neto, A.A., Deschamps, F., da Silva, E.R. and Lima, E.P. de (2020), "Digital twins in manufacturing: an assessment of drivers, enablers and barriers to implementation", Procedia CIRP, Vol. 93, pp. 210–215. https://doi.org/10.1016/j.procir.2020.04.131.

Rasheed, A., San, O. and Kvamsdal, T. (2020), "Digital Twin: Values, Challenges and Enablers From a Modeling Perspective", IEEE Access, Vol. 8, pp. 21980–22012. https://doi.org/10.1109/ACCESS.2020.2970143.

Rosen, R., Fischer, J. and Boschert, S. (2019), "Next Generation Digital Twin: an Ecosystem for Mechatronic Systems?", IFAC-PapersOnLine, Vol. 52 No. 15, pp. 265–270. https://doi.org/10.1016/j.ifacol.2019.11.685.

Sauer, C., Schleich, B. and Wartzack, S. (2021), "A data model for linking testbed and field test data", in Krause, D. and Paetzold, Kristin, Wartzack, Sandro (Eds.), *DS 111: Proceedings of the 32nd Symposium Design for X, September 27-28*. 2021, The Design Society. https://doi.org/10.35199/dfx2021.01.

Schweigert-Recksiek, S., Trauer, J., Engel, C., Spreitzer, K. and Zimmermann, M. (2020), "CONCEPTION OF A DIGITAL TWIN IN MECHANICAL ENGINEERING – A CASE STUDY IN TECHNICAL PRODUCT DEVELOPMENT", Proceedings of the Design Society: DESIGN Conference, Vol. 1, pp. 383–392. https://doi.org/10.1017/dsd.2020.23.

Singh, S., Shehab, E., Higgins, N., Fowler, K., Reynolds, D., Erkoyuncu, J.A. and Gadd, P. (2020), "Data management for developing digital twin ontology model", *Proceedings of the Institution of Mechanical Engineers*, Part B: Journal of Engineering Manufacture, 095440542097811. https://doi.org/10.1177/0954405420978117.

Singh, S., Shehab, E., Higgins, N., Fowler, K., Tomiyama, T. and Fowler, C. (2018), "Challenges of Digital Twin in High Value Manufacturing", in *SAE Technical Paper Series*, NOV. *06*, 2018, SAE International400 Commonwealth Drive, Warrendale, PA, United States. https://doi.org/10.4271/2018-01-1928.

"Steam Refunds" (2021), available at: https://store.steampowered.com/steam_refunds/ (accessed 2 November 2021).

Stjepandić, J., Sommer, M. and Stobrawa, S. (2022), "Digital Twin: Conclusion and Future Perspectives", in Stjepandić, J., Sommer, M. and Denkena, B. (Eds.), *DigiTwin: An Approach for Production Process Optimization in a Built Environment*, *Springer eBook Collection*, 1st ed. 2022, Springer International Publishing; Imprint Springer, Cham, pp. 235–259. https://doi.org/10.1007/978-3-030-77539-1_11.

Thielsch, M.T., Meeßen, S.M. and Hertel, G. (2018), "Trust and distrust in information systems at the workplace", PeerJ, Vol. 6, e5483. https://doi.org/10.7717/peerj.5483.

Trauer, J., Mutschler, M., Mörtl, M. and Zimmermann, M. (2022), "CHALLENGES IN IMPLEMENTING DIGITAL TWINS - A SURVEY", In Review, in Volume *2: 42nd Computers and Information in Engineering Conference (CIE), 14.-17.08.*2022, American Society of Mechanical Engineers.

Trauer, J., Pfingstl, S., Finsterer, M. and Zimmermann, M. (2021), "Improving Production Efficiency with a Digital Twin Based on Anomaly Detection", Sustainability, Vol. 13 No. 18, p. 10155. https://doi.org/10.3390/su131810155.

Trauer, J., Schweigert-Recksiek, S., Engel, C., Spreitzer, K. and Zimmermann, M. (2020), "WHAT IS A DIGITAL TWIN? – DEFINITIONS AND INSIGHTS FROM AN INDUSTRIAL CASE STUDY IN TECHNICAL PRODUCT DEVELOPMENT", Proceedings of the Design Society: DESIGN Conference, Vol. 1, pp. 757–766. https://doi.org/10.1017/dsd.2020.15.

Utz, S., Kerkhof, P. and van den Bos, J. (2012), "Consumers rule: How consumer reviews influence perceived trustworthiness of online stores", Electronic Commerce Research and Applications, Vol. 11 No. 1, pp. 49–58. https://doi.org/10.1016/j.elerap.2011.07.010.

Wang, B.T. and Burdon, M. (2021), "Automating Trustworthiness in Digital Twins", in Wang, B.T. and Wang, C.M. (Eds.), *Automating Cities*, *Advances in 21st Century Human Settlements*, Springer Singapore, Singapore, pp. 345–365. https://doi.org/10.1007/978-981-15-8670-5_14.

Yadav, A., Chakraverty, S. and Sibal, R. (2019), "A framework for classifying trust for online systems", World Wide Web, Vol. 22 No. 2, pp. 1499–1521. https://doi.org/10.1007/s11280-018-0626-6.