ESTABLISHING DIGITAL TRUST

Towards a Strategic Roadmap for Industrial Companies

White Paper
February 2022

Digital Trust Forum

Charter of Trust

Authors

Prof. Dr. Felix Wortmann
Scientific Director
Bosch IoT Lab at University of St. Gallen & ETH Zurich
Dufourstrasse 40a
CH-9000 St. Gallen

Fabian Schäfer
Research Associate
Bosch IoT Lab at University of St. Gallen & ETH Zurich
Dufourstrasse 40a
CH-9000 St. Gallen

Dr. Wolfgang Bronner
Managing Director
Bosch IoT Lab at University of St. Gallen & ETH Zurich
Dufourstrasse 40a
CH-9000 St. Gallen

Dirk Slama
VP Co-Innovation and IT/IoT Alliances
Bosch Group
Ullsteinstraße 128
DE-12109 Berlin

Dr. Christoph Peylo
Senior VP Digital Trust
Bosch Group
Borsigstraße 4
DE-70469 Stuttgart-Feuerbach

Natalia Oropeza
Global Chief Cybersecurity & Chief Diversity Officer
Siemens AG
Trautenaustr. 10
DE-38114 Braunschweig

Publisher

Digital Trust Forum
www.digitaltrustforum.org

1. Executive Summary

The convergence of the Internet of Things (IoT), with its smart connected products, and Artificial Intelligence (AI) is collectively referred to as AIoT. For industrial companies, AIoT is an important enabler for the innovation of processes, products and services. Within the realm of AIoT, industrial companies collaborate and compete in digital ecosystems. Hence, sharing and exchanging data becomes a key driver for value creation in AIoT business models. However, data sharing and exchange is heavily dependent on digital trust – the willingness to engage in a digital value exchange that bears potential risk. Ultimately, customers only use digital offerings they consider trustworthy and that build upon systems which are reliable, robust, and transparent in the way they process data. As Tanja Rückert, CDO of Bosch, explains, the Digital Trust Forum wants to support companies in the creation of products and services that meet these requirements: "We have to ensure that our products and services are trustworthy across their entire lifecycle. And this is what we are working on in the Digital Trust Forum."

"We have to ensure that our products and services are trustworthy across their entire lifecycle. And this is what we are working on in the Digital Trust Forum."

Tanja Rückert
CDO
BOSCH

From an AIoT provider perspective, digital trust is the result of a diverse set of activities that span different domains such as cybersecurity, privacy, data sovereignty, and AI ethics. Cedrik Neike, Member of the Managing Board of Siemens AG and CEO of Siemens Digital Industries, emphasizes the importance of digital trust and the activities required in the related domains: "I am convinced that trust is the necessary condition for technological innovation to thrive. And this trust is unthinkable without reliable cybersecurity. By securing our innovative products, solutions and services, we build trust – in technologies, in the people behind them and in digital development."

"I am convinced that trust is the necessary condition for technological innovation to thrive. And this trust is unthinkable without reliable cybersecurity. By securing our innovative products, solutions and services, we build trust – in technologies, in the people behind them and in digital development."

Cedrik Neike
Managing Board Member
& CEO Digital Industries
SIEMENS

Companies that successfully engage in the realm of digital trust can outperform their competition, especially in markets where customers have growing concerns about the processing and use of their data. Michael Dell, Chairman and CEO of Dell Technologies, summarizes: "In the age that we are in, customers are sharing more and more data and customer trust is a significant differentiator for companies. Security, privacy, resilience, all have to be central considerations when we're designing and providing digital solutions. And the Digital Trust Forum, that we're proud to be a part of, is a great way to drive this forward."[1]

"In the age that we are in, customers are sharing more and more data and customer trust is a significant differentiator for companies. Security, privacy, resilience, all have to be central considerations when we're designing and providing digital solutions. And the Digital Trust Forum, that we're proud to be a part of, is a great way to drive this forward."

Michael Dell
Chairman & CEO
DELL Technologies

[1] Extracted from BCW.on Session 4 on June 9, 2021: Webinar with Michael Dell, Dell Technologies. Retrieved June 10, 2021, from https://bosch-connected-world.com/bcw-on/#session-4-dell.

In light of this complexity, the managers of digital OEMs face the challenge to drive digital trust without compromising data exploitation and corresponding AIoT opportunities. They must align digital trust initiatives across multiple business units and develop a clear vision and strategy towards digital trust. In essence, they need to develop and implement a digital trust roadmap. Thus, companies must prioritize and adopt digital trust initiatives in alignment with the requirements of their industry and business model.

The purpose of this white paper is to support industrial companies in their development and implementation of a digital trust roadmap that is geared towards three fundamental questions:

- Why is digital trust desirable for customers, and what is the customer value of digital trust?
- What is the competitive advantage for companies that invest in digital trust?
- Where is the optimum between a company's engagement and added customer value?

The underlying study is based on insights from desk research as well as semi-structured expert interviews. The interviews were conducted with senior executives from participating companies in the Digital Trust Forum.

Figure 1: Strategic digital trust roadmap for industrial companies

Industrial companies address the challenge of digital trust in three core steps (cf. Figure 1). First, they work towards mastering individual trust domains. In the last decade, they have heavily invested in cybersecurity. Moreover, with the emergence of a new generation of privacy regulations, companies devoted significant resources to data privacy. Lately, alongside security and data privacy, data sovereignty and AI ethics have gained momentum.

In the second step, companies integrate the different trust domains to create a coherent digital trust foundation. After outlining the Digital Trust Forum (Chapter 2) and digital trust essentials (Chapter 3), this white paper presents six trust initiatives that industrial companies conduct to create a solid digital trust foundation (Chapter 4). The trust initiatives are derived on the basis of a digital trust framework (House of Digital Trust) and six core digital trust principles that industrial companies pursue.

Third, companies drive trust in the specific digital ecosystems they engage in. In these ecosystems, companies must participate in joint endeavors to facilitate trust. For example, it is no longer about individual companies creating a code of conduct for themselves, but about jointly creating a code of conduct for all stakeholders in an ecosystem. Chapter 5 of this white paper outlines three fundamental questions that must be addressed to bring trust and prosperity to ecosystems. “Why?” is all about business cases. “What?” covers the actual smart services and how the business cases are realized. Finally, the third question (“How?”) addresses how the services are enabled by fundamental rules (code of conduct) and regulations as well as common standards and technologies.

2. Digital Trust Forum and Its Vision

The Digital Trust Forum (DTF) is a global, open, and independent initiative with a focus on enabling trusted digital solutions for connected, intelligent, physical products utilizing AI and the IoT (collectively referred to as AIoT in this context). The DTF is inspired by the EU initiatives on AI and trust. The inaugural DTF was held in May 2019 in Berlin, hosted by the former Bosch Group-CDO Michael Bolle and EU Commissioner Mariya Gabriel (cf. Figure 2). The participating organizations included BDI, DIGITALEUROPE, Eclipse Foundation, Enisa, ETSI, IEEE, Industrial Internet Consortium, ISO/IEC JTC 1/SC 42, Platform Industrie 4.0, and Trusted IoT Alliance.

Figure 2: Digital Trust Forum at Bosch Connected World

Technology is evolving at a – sometimes breathtakingly – high speed. The rapid advancements in AI and the IoT, and their massive utilization (AIoT), are causing not only enthusiastic responses, but also many concerns. These concerns relate to security and data privacy, but they also sometimes relate to dystopic visions of failing civil infrastructure, criminally abused information technology (IT) systems, or even out-of-control autonomous systems. To ensure that the many opportunities presented by these innovative technologies continue to achieve a high level of customer acceptance, trust between all related stakeholders must be established. The trustworthy behavior of technical systems and all related stakeholders, thus meeting end-users' expectations, must be ensured on many levels.

The DTF is bringing together representatives from the relevant stakeholder groups to ensure that end-users develop an ongoing high level of trust in AI- and IoT-based solutions. For novel solutions to continue to attract new customers and users, a trustworthy environment is required. The DTF will therefore help its partners and supporters to take a proactive role in setting and managing expectations regarding trust in such digital solutions. To provide this support, the DTF will equip industrial companies with a digital trust governance framework and a roadmap to address digital trust strategically. Moreover, it will make trust policies explicit and transparent, and build the required trust management mechanism directly into digital solutions.

3. Digital Trust and Digital Ecosystems

3.1 The Concept of Digital Trust

Two Perspectives on Digital Trust

Without trust, there is no value exchange between market participants. This fundamental principle of economics is true for both physical and digital markets. Hence, there is a significant body of knowledge on trust and its impact in existing research. In the realm of digital value exchange, for example, there are various definitions for digital trust. On the basis of these definitions, Figure 3 depicts two fundamental perspectives on digital trust.

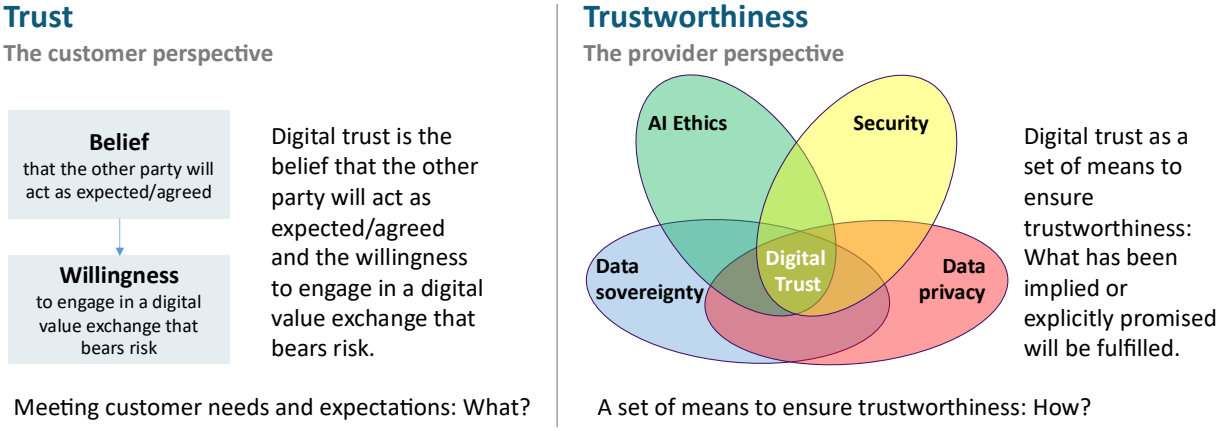

Figure 3: Two perspectives on digital trust

From a customer perspective, digital trust is the belief that the other party will act as expected or agreed within a digital value exchange. Thereby, it is important to realize that trust is always related to risk. Without risk, there is no need to trust. In the context of digital services, for example, there is the risk that data is actively misused or treated in an insecure manner; thus, it can get lost or stolen. As such, digital trust is ultimately the willingness to engage in a digital value exchange that bears risk.[2] From a provider perspective, trust is about ensuring that promises, which have been made implicitly or explicitly, are fulfilled. It is about trustworthiness and a set of means to facilitate trust. More specifically, these means span the core domains security, data privacy, data sovereignty, and AI ethics (see also Section 4.1).[3]

The Challenge of Digital Trust

The most fundamental challenge of digital trust is that it often cannot be seen or experienced. When you see a shiny green apple, you know that it is not rotten. Upon seeing a nice-looking app, you do not know if the app missuses the data entered into it. In essence, digital trust most often relies on credence attributes rather than search or experience attributes.

What are search, experience, and credence attributes? Marketers distinguish these attributes in the realm of product quality.[4] Search attributes can be evaluated prior to purchase or usage. Take the

[2] Gefen et al. (2003); Luhmann (1979); Lui & Jamieson, 2003; Mayer et al. (1995); Shrier & Krigsman (2019); Thiesse (2007).
[3] Abraham et al. (2019); van den Dam (2017).
[4] Nelson (1970); Darby & Karni (1973).

Bosch 360° indoor camera[5] as an example. As the camera lens retracts fully mechanically into the housing, the user can be certain that the camera is really not recording in this retracted setting. This camera can thereby guarantee privacy, and a potential user can immediately understand this even before buying the camera.

In contrast, experience attributes can only be evaluated after usage. For instance, if you buy a bike on eBay and receive the bike in the promised quality, you only know after the transaction that the quality was as promised. However, you still do not know if your data is in good hands. Your credit card information might be misused months later. Hence, this transaction is based on credence attributes that cannot be evaluated even after usage. Most digital offerings rely on credence attributes. Apple, for example, promises their customers to use on-device intelligence to improve the recognition of a user's face to unlock their device instead of uploading the user's data and processing it on Apple servers.[6] However, users cannot evaluate this promise, neither before nor after usage. They must instead trust Apple. Figure 4 summarizes the outlined examples.

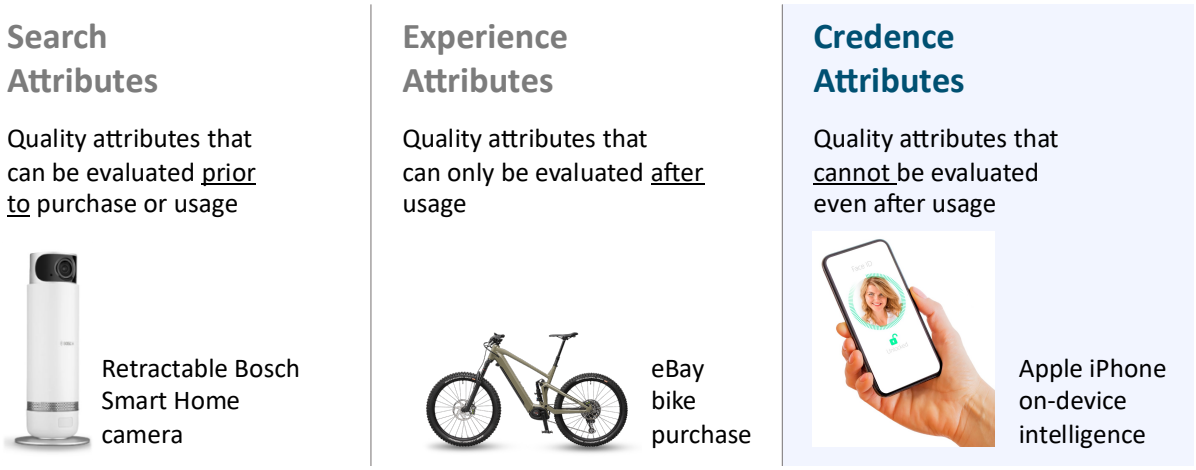

Figure 4: Digital trust most often relies on credence attributes

For industrial companies, it is essential to realize that digital trust is, in essence, about credence attributes. Why? Building a secure product on the basis of privacy by design and incorporating the latest AI ethics is simply not enough. Customers cannot see or experience the built-in quality.

The Dual Nature of Creating Digital Trust

As described in the previous section, in the digital age, it is not sufficient to implement only privacy or security features. Industrial companies must communicate and proof them. They need to make and assure promises (A) while also keeping those promises (B) (cf. Figure 5).

[5] https://www.bosch-smarthome.com/uk/en/products/devices/360-indoor-camera/ [Accessed on September 13, 2021].
[6] https://support.apple.com/en-us/HT208108 [Accessed on September 14, 2021].

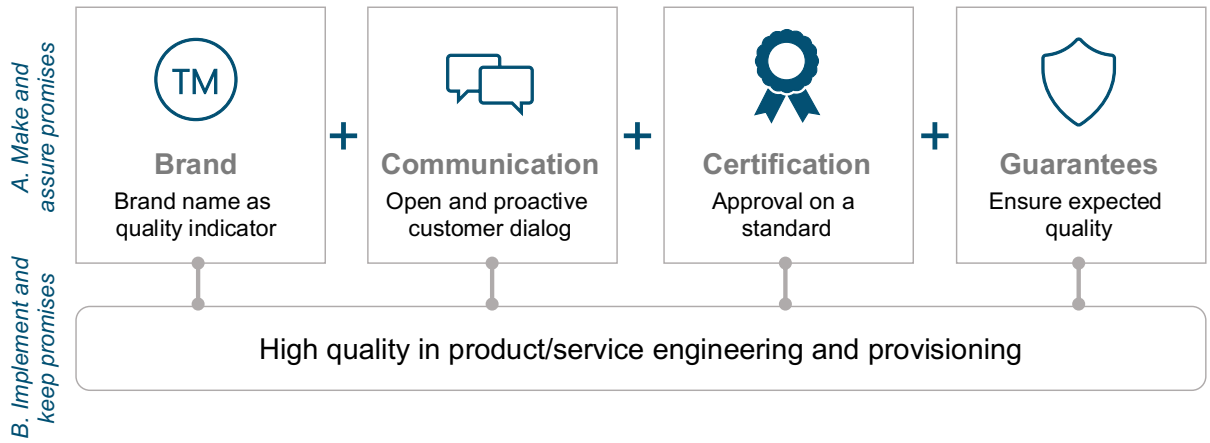

Figure 5: The dual nature of creating digital trust: making and keeping the promises

Implementing and keeping promises (B) includes high-quality product/service engineering and provisioning. It relies on the competence of a diverse set of contributors such as UX and product designers, privacy and AI engineers as well as data security officers. Making and assuring promises (A) includes a set of well-established means to create trust in markets:

- *Brand:* The brand of a company serves as an important quality indicator for customers. Customers trust brands and hence buy and adopt their products and services. Within the last years, Apple, for example, has invested heavily into its brand on the basis of a data privacy campaign. "Data Minimization" and "On-Device Intelligence" were core messages they communicated.[7] Apple was presented as the opposite of Google and Facebook in taking care of its customers' data privacy.
- *Communication:* Despite large brand campaigns, proactive customer communication is central for achieving digital trust. One example is Google Chrome and its privacy mode. If customers only find out later in public press that data was recorded even if they assumed it was not, customer trust is severely damaged.[8] However, by carefully explaining security and privacy features and practices to customers, companies can benefit accordingly. Once again, Apple invested significantly in customer communication and its very comprehensive privacy website (www.apple.com/privacy).
- *Certification:* In various industries, certification standards have been established to serve as instruments of quality assurance. Core to a certification system is that inspections are conducted by independent bodies (third-party certification) on the basis of standards that are laid down by external organizations. In the realm of digital trust and security, for example, ISO/IEC 27001 has gained significant momentum as an international standard on how to manage information security in enterprises. Customers value certifications as a sign of assured quality[9].
- *Guarantees:* A very common means to overcome trust challenges is guarantees. Warrantees, as a specific form of guarantees, for example, are key in established markets such as the used-car market. Practices like ensuring certain qualities of digital services (availability, security) and paying in the case of underperformance and incidents have even led to the creation of

[7] https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf [Accessed on September 13, 2021].
[8] https://www.reuters.com/article/us-alphabet-google-privacy-lawsuit-idUSKBN23933H [Accessed on September 13, 2021].
[9] Albersmeier et al. (2009).

corresponding insurance products such as cybersecurity insurances. Hence, the providers of digital services can create trust by providing guarantees.

3.2 Digital Trust as a Key Success Factor for Ecosystems

The convergence of the IoT with its smart connected products and AI is collectively referred to as AIoT, which is a key enabler for the innovation of products, processes and services of industrial companies. Within the realm of AIoT, industrial companies collaborate and compete in digital ecosystems such as production and consumption ecosystems.[10] The former extend the traditional value-generation across the supply chain. The latter opens new cross-industrial business opportunities. For instance, data from connected cars may be important to the car manufacturer, but also insurance companies or workshops. Ultimately, sharing and exchanging data in ecosystems becomes a key driver for the value creation of AIoT business models.

Executives from leading technology companies recognize digital trust as a key success factor for digital ecosystems. Digital trust lays the foundation for cross-organizational and cross-industry data sharing and value creation. Recent studies underline the importance of trust for digital ecosystems.[11] In 73% of digital ecosystems, trust was a matter for success. Moreover, in 52% of ecosystems, trust-related issues were a core reason for failure. Digital ecosystems often involve a diverse set of stakeholders. Accordingly, trust must be established between all the involved stakeholders in the ecosystem. While customers want to share their data with a trusted service and platform provider, the service and platform provider themselves may need to store their data securely in the databases of an infrastructure provider.

To establish and increase trust in such ecosystems, technology alone is not sufficient. Recent evidence reveals that several complementary instruments are required to create trust (cf. Figure 6). In 90% of ecosystems, a combination of instruments was essential for success. Such instruments include monetary incentives, standards, rules, and digital solutions like trust-enabling technology (e.g., multiparty computation). The success of a digital ecosystem depends on the identification of the best combination of these instruments.[12]

Technology only

According to the BCG Henderson Institute the "rise of digital platforms has led to the facile conclusion that technology is sufficient to ensure trust in an ecosystem".

Their study shows, that this is "far from true" instead "there's no single instrument or technology that can create trust in an ecosystem".

Trust-building instruments

In 90% of ecosystems a combination of instruments was essential for the success.

Such instruments include monetary incentives, standards, rules, and digital solutions (e.g., ratings and trust-enabling technology).

In ecosystems a combination of instruments that leads to the cooperation of all participants must be identified.

Figure 6: A combination of complementary instruments is required to build trust (Source: Aguiar et al., 2021)

[10] Subramaniam et al. (2019).
[11] Aguiar et al. (2021); Keller et al. (2021).
[12] Aguiar et al. (2021).

4. Creating the Foundation for Digital Trust

Industrial companies that want to engage successfully in digital ecosystems must address the topic of digital trust. Based on insights from desk research as well as semi-structured expert interviews with senior executives from participating companies in the DTF, fundamentals for creating digital trust were identified. These fundamentals are outlined in the following.

4.1 Actionable Domains of Digital Trust

The House of Digital Trust (cf. Figure 7) decomposes the complex topic of digital trust into actionable domains. The digital trust framework consists of three layers: the digital trust foundation, digital trust strategy layer, and digital trust operating model layer.

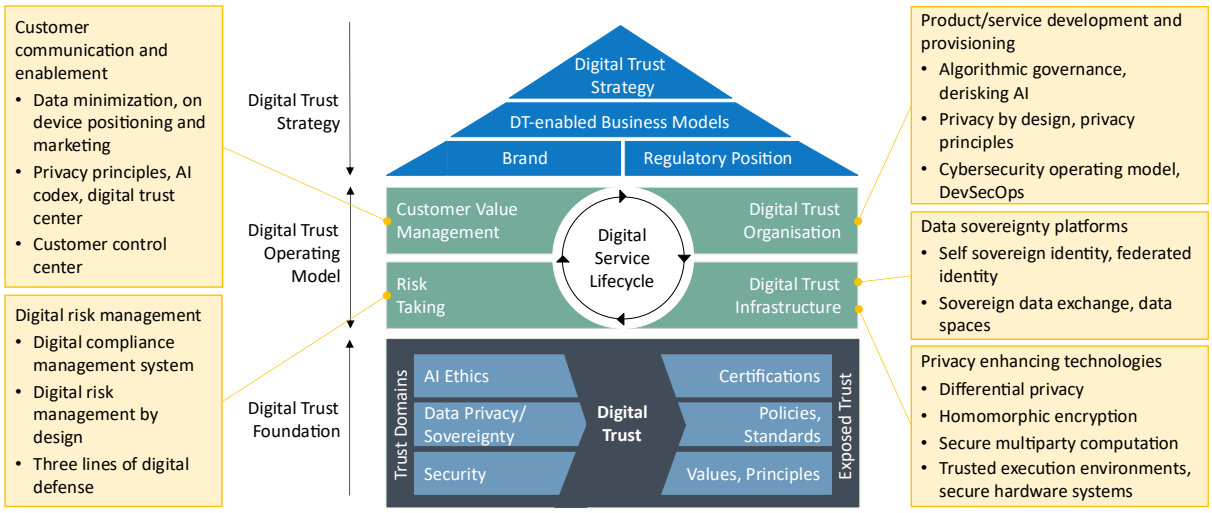

Figure 7: House of Digital Trust

Digital Trust Foundation

The digital trust foundation builds the basis for a company's ability to create digital trust. Hence, companies must address this domain early. Three key digital trust domains form the foundation for digital trust:

- *Cybersecurity:* Cybersecurity is about protecting digital information from unintended access and maintaining confidentiality, integrity, and availability of digital assets.[13]
- *Data privacy and data sovereignty:* Data privacy and data sovereignty ensure the ability of an individual or organization to control information about itself.[14]
- *AI ethics:* AI ethics addresses the practices and technologies of designing, implementing, and using AI in an ethical manner.[15]

Digital trust must be formalized and exposed so that it can be operationalized. Most companies have explicit principles that expose core trust values. In the realm of digital trust, common principles are privacy principles and AI principles. For instance, Bosch has established ethical "red lines" for the use of AI in its "Code of Ethics for AI". The code of ethics contains principles such as "Trust is one of our

[13] ISO/IEC 27032:2012; Von Solms & von Solms (2017).
[14] Stone et al. (1983); Westin (1967).
[15] Leslie, D. (2019); Mittelstadt (2019).

company's fundamental values. We want to develop trustworthy AI products".[16] The principles provide a fundamental orientation for employees, partners, and customers and inform more specific policies and standards. Finally, third-party certifications can demonstrate the compliance with standards and serve as a quality assurance instrument.

Digital Trust Strategy

From a strategic viewpoint, industrial companies have four core domains in which they must take action:

- *Digital trust strategy:* Companies must first and foremost set strategic priorities in respect to digital trust. They might make digital trust a strategic theme, just as Apple has done to differentiate itself from the competition. Alternatively, they might decide that digital trust is rather a mandatory, non-differentiating aspect of their industry. In both cases, companies have to identify essential trust initiatives they want or have to implement.
- *DT-enabled business models:* Companies must ensure that they approach digital trust in a way that is consistent with their business model. Digital trust approaches and technologies can also enable new business models and lead to a competitive advantage. Device manufactures, for example, can gain a competitive edge against Big Tech service providers by promoting business models that rely on data minimization and on-device intelligence.
- *Brand:* In light of the ongoing digitization, even well-respected industrial players must evolve their brand. Customers can value a brand very highly but consider the digital competence of the corresponding company to be low. Furthermore, a brand might need to be extended to reflect digital values in respect to data privacy, security, and AI ethics.
- *Regulatory position:* The regulatory engagement of a company is increasingly important, as many regulations are currently evolving around data privacy, security and AI ethics. On the one hand, companies need to anticipate upcoming regulations to prepare themselves. On the other hand, companies can get actively involved to assure that viable and meaningful regulations and standards are developed.

Digital Trust Operating Model

To integrate digital trust into their operating models, companies must address four areas:

- *Customer value management:* Customer value management is about customer communication and providing customer value on the basis of digital trust. As of today, companies are expected to take a stance on data privacy, security, AI ethics, and data sovereignty. Hence, most companies have privacy, data sovereignty, and AI principles, either as a dedicated website or as part of a compressive code of conduct or charter of trust. Moreover, data privacy or security features are often neither visible nor experienceable for customers. Hence, these features must be communicated and explained to the customer to be effective. Finally, in the context of data privacy and data sovereignty, customers should have the ability to set preferences and control the data that is processed by the service provider, for example, in dedicated environment such as a trust center.
- *Risk taking:* Over the last decades, established industrial companies have had to master a fundamental shift with respect to their internal and external digital services. While in the past digital services were developed and deployed in rather protected and closed environments, the transition to the cloud and ecosystems has challenged existing practices. Moreover, complex and demanding regulations (e.g., GDPR) increase the need for careful decision-

[16] https://www.bosch-ai.com/industrial-ai/code-of-ethics-for-ai/ [Accessed on September 13, 2021].

making (digital compliance management). Furthermore, the use of AI provides new emerging risks for companies. To thrive in this open and much more complex world, a well-reflected risk culture and risk management is necessary to facilitate trust and balance business opportunities with business risks (risk management by design). Today, it is about empowering decentralized decision-making rather than enforcing centrally managed checklists.

- *Digital trust organization:* A major operational enabler for digital trust is the digital trust organization that includes processes, roles and responsibilities. Although development processes for digital services across industrial companies are different, every company needs to adopt privacy by design, state of the art cybersecurity approaches (DevSecOps), and algorithmic governance during the development and provisioning of digital services. The importance of these topics increase as more data becomes available and as algorithms become increasingly powerful. In established industrial companies, the different digital trust domains (i.e., security, privacy, AI ethics) are usually owned by different organizational departments including legal, compliance, cybersecurity, and specific AI departments. Within their processes and business units, industrial companies must ensure that the diverse set of digital trust principles, policies, and standards are implemented. At the same time, they have to take care that these requirements are integrated and well-balanced so that they can be implemented in an efficient way rather than becoming a serious burden.
- *Digital trust infrastructure:* Emerging digital trust infrastructures open new opportunities; therefore, companies must reflect, explore, and leverage their business potential. In the realm of data sovereignty, for example, self-sovereign identity (SSI) technology promises individuals and organization control over their digital identities. Moreover, a new generation of sovereign data exchange is facilitated by emerging solutions such as the Industrial Data Spaces or Gaia-X. Furthermore, trust policy management systems for AIoT products allow companies to enable intelligent autonomous systems to self-monitor themselves and align with formalized and standardized trust policy definitions. Finally, technologies such as secure multiparty computation or differential privacy facilitate new ways of ensuring privacy.

4.2 Core Principles to Facilitate Trust

Our interviews revealed six core principles (cf. Figure 8) vital for companies to facilitate trust in their digital ecosystems.

Figure 8: Core principles to facilitate trust

1. Customers First

Putting the customer and the user in the center of thinking is core to digital trust. Although "customers first" sounds like a natural starting point, digital trust is often driven with a technology or compliance agenda. Lately, digital trust initiatives such as Gaia-X have received tremendous attention, but the focus is often on technology without keeping the customer and business case in mind. Companies need to realize that solving actual customer problems (use cases) is the necessary condition, and digital trust is the sufficient condition for success in digital ecosystems. Peter Weckesser, EVP and CDO of Schneider

Electric, highlights that companies first need to have a compelling value proposition that cannot be taken for granted: “If customers believe that we can really add value, they entrust us their data and pay for our services.” Maciej Kranz, EVP and CTO of Kone, emphasizes the importance of trust in today’s ecosystems: “Our customers are increasingly asking us for comprehensive solutions that require us to work with a large number of partners. And trust is absolutely foundational here.”

> *“Our customers are increasingly asking us for comprehensive solutions that require us to work with a large number of partners. And trust is absolutely foundational here.”*
>
> 
>
> Maciej Kranz
> EVP & CTO
> KONE

2. Charter of Trust

For established industrial companies specifically, digital trust is not a stand-alone domain. In this context, Vera Schneevoigt, CDO of Bosch Building Technologies, highlights that principles from the digital world must be embedded in a company's existing value set: “We have to integrate digital trust into our Bosch values. Digital trust is not an isolated topic.” Established companies have proven values, principles, and policies to ensure trust. Often, core values and principles are publicly available in the form of a comprehensive code of conduct or charter of trust. Digital trust values, principles, and policies have to be integrated into existing principles and policies. A comprehensive but concise charter of trust that also addresses security, data privacy, and AI ethics is necessary.

3. Standards and Conformity Assessments

Standards can be a viable means to capture best practices, ensure interoperability, speed up development, and create trust by laying the foundation for conformity assessments such as certification. Moreover, they can be an integral part of tenders, orders, or contracts.[17] However, standards can also be a burden that creates complexity, slows processes, and serves as a basis for costly third-party certifications, especially if the number and complexity of available standards is growing. To ensure the viability of standards and their alignment with internal practices and processes, companies must actively engage in standardization and determine a portfolio of core standards (security, privacy, data sovereignty, AI ethics) that the company builds upon – specifically in times of disruption and change, where new standards are emerging.

4. Risk Management

In recent years, the need for collaboration has significantly increased (e.g., collaboration in ecosystems, cloud usage). Furthermore, through inter-organizational collaboration, business risk has significantly grown. Vera Schneevoigt, CDO of Bosch Building Technologies, emphasizes the transition: “We come from very closed ecosystems and now we are operating in open ecosystems. In open ecosystems we can't control everything. That's just over. Now, it is all about taking well-calculated risks.“ The established means of addressing risks, such as centrally managed checklists, are not sufficient anymore. Moreover, due to regulatory and technological uncertainty, for example, in respect to GDPR and the potential biases of AI algorithms, companies must make risk-related decisions more frequently. Hence, all these decisions cannot be made by top management or a specialized central department, as doing so would significantly inhibit innovation and time-to-market. Ultimately, empowering decentralized, risk-aware decision-making and adopting existing risk management systems to new realities is becoming mandatory.

[17] Thomsen (2018).

"We come from very closed ecosystems and now we are operating in open ecosystems. In open ecosystems we can't control everything. That's just over. Now, it is all about taking well-calculated risks."

Vera Schneevoigt
CDO Building Technologies
BOSCH

5. Global Divide

Companies have to be aware that there are dedicated regions and countries with a very specific understanding of digital trust. Vera Schneevoigt, CDO of Bosch Building Technologies, states that "it is really challenging to have a global footprint today. Digital trust in Asia means something different than in North America, Europe or Africa." Moreover, companies must understand that there are red lines in each region that can be crossed very easily, for example, by integrating components into a product that come from a "no go" region. This also has severe implications for IT and digital service provisioning, as IT was always about centralization and operating globally. Now there is a growing need for local and even completely isolated digital service delivery. Peter Weckesser, EVP and CDO of Schneider Electric, explains: "20 years ago, the philosophy was 'we build global factories and export worldwide'. Now we are transitioning into a new era with multi-local operations for resilient, sustainable, and agile production."

"20 years ago, the philosophy was 'we build global factories and export worldwide'. Now we are transitioning into a new era with multi-local operations for resilient, sustainable, and agile production."

Dr. Peter Weckesser
EVP & CDO
Schneider Electric

6. Unique Ecosystems

Trust is not a static concept; each ecosystem has its own players, setting, and requirements. Companies must be sensitive to these trust requirements and their change over time. Thus, for example, the choice of infrastructure varies from ecosystem to ecosystem. Dr. Bernhard Eschermann, CTO of ABB Process Automation, explains: "While public cloud has gained significant momentum, there are also customers who insist on their critical systems to remain on-premise. They would like to have as little connection of these systems to the external world as possible based on their risk perception." The ultimate goal for participants in an ecosystem is to reach consensus on the required trust and appropriate means in each ecosystem. Vera Schneevoigt, CDO of Bosch Building Technologies, explains that companies must therefore be sensitive and identify specific trust opportunities, while also challenging idealistic propositions: "At the end of the day, each partner has its red line. While we in Europe are very sensitive about data protection, our customers in the U.S. and Asia also have their red lines and code of values. They are just different. We have to be sensitive about these differences and also recognize changes over time."

4.3 Fundamental Digital Trust Initiatives

The interviews revealed six fundamental digital trust initiatives vital for addressing the identified core principles (cf. Figure 9). Two initiatives (A, B) are essential for establishing a solid trust foundation. Four initiatives (C-F) fall within the digital trust operating model.

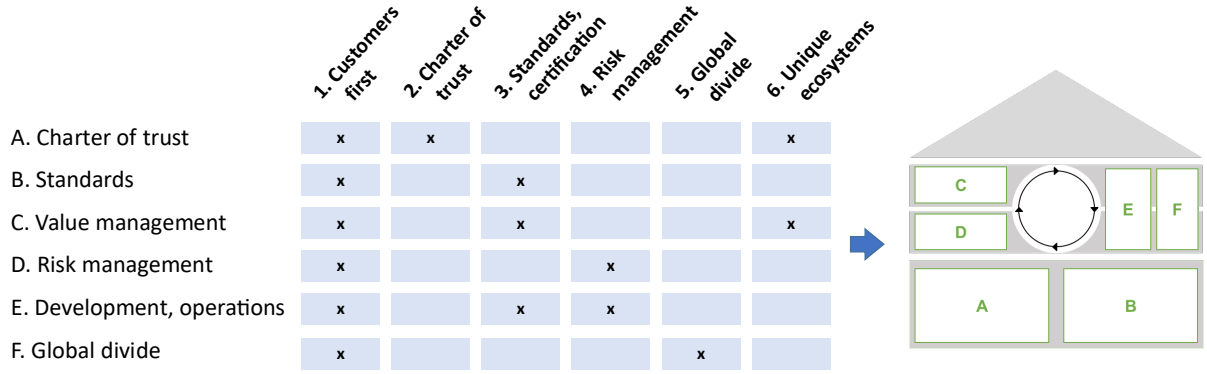

Figure 9: Fundamental digital trust initiatives (A-F) and their positioning

A. Charter of Trust

The first initiative addresses creating a concise, public, and credible charter of trust that underlines a company's willingness to act compliantly and ethically. A charter of trust establishes the fundamental values and principles for an industrial company's analog and digital business activities, addressing all digital trust domains. It should serve as a guide for every person and team regarding ethics and compliance. The charter of trust serves as a basis for more detailed policies that formally express specific directions and rules. A charter should be integrated into a governance system to enforce its principles. The governance system should also include an alert system so that whistleblowers can report transgressions without the fear of persecution. Ultimately, it is about setting fundamental boundaries rather than extensive detailed regulations. Heiko Damboldt, Head of Digital Governance at BASF, summarizes, "I don't want to constrain agility by prescribing everything in detail top-down. I want to provide a framework in which you can move. That means, however, that the framework must be clearly described. I also have to communicate it and monitor whether it is being adhered to."

"I don't want to constrain agility by prescribing everything in detail top-down. I want to provide a framework in which you can move. That means, however, that the framework must be clearly described. I also have to communicate it and monitor whether it is being adhered to."

Heiko Damboldt
Head of Digital Governance
BASF

B. Standards

Companies must identify a relevant and consistent set of standards that they integrate into their processes and technologies. Moreover, industry leaders specifically might take an active role in the development of standards. Concerning digital trust, Dr. Bernhard Eschermann, CTO of ABB Process Automation, explains that companies benefit from engaging in the development of standards to ensure that they are meaningful: "We need standards that are well-aligned. As an example, standards regarding safety need to cover all aspects that are relevant for a system and not just a specific technology used when building the system. Overlapping or competing standards increase the cost of developing products and solutions without providing value to customers."

"We need standards that are well-aligned. As an example, standards regarding safety need to cover all aspects that are relevant for a system and not just a specific technology used when building the system. Overlapping or competing standards increase the cost of developing products and solutions without providing value to customers."

Dr. Bernhard Eschermann
CTO Process Automation
ABB

C. Value Management

Value management is about understanding customer needs and addressing them. Within their privacy, security, and AI ethics efforts, companies should always validate their alignment with customer needs, which can be subject to dramatic change. While data privacy, for example, was not a core issue in B2C five years ago, the tide has turned. Additionally, value management is about communication and explaining what measures a company is taking to ensure trust. Furthermore, it is about transparency and giving users control over their data. Finally, it can also include helping customers within their challenges of secure and trustful service provisioning. Peter Weckesser, EVP and CDO of Schneider Electric, for example, outlines that digital service providers can offer security services to their customers, highlighting competence and creating trust: "We have a cybersecurity business, which is where we offer IT/OT cybersecurity services to our customers."

D. Risk Management

Companies have to redesign their risk management approaches to be able to cope with risks in the digital world. Christoph Peylo, SVP Project Digital Trust at Bosch Group, emphasizes that most often, a fundamental paradigm shift is necessary: „We have to rethink and revise our risk management policies for AIoT software systems. Traditionally, certification schemes and security procedures are designed for first-party software. However, data driven software supply chains and the software itself are getting more complex. We need a balanced interplay of regulation, standardization and cooperation between companies to establish digital trust." Especially in established industrial companies, a very common but unrealistic "control everything" mindset must be overcome regarding digital offerings. Building the highest level of defense around everything is costly, time consuming, and often ineffective, as it does not prioritize limited resources. Companies must instead focus on "defeat the most significant threats", make risks visible and prioritize investments to reach their target risk levels. In particular, during the development process of AIoT products and digital services, companies need to facilitate a continuous risk management that includes an immediate discovery of risks.[18] Risk management structures must be introduced to allow the management of risks across different hierarchy levels and well-defined escalation paths. However, in a first step, individual employees should be trained to recognize and take appropriate risk-related decisions. This decentralization contributes to a more effective and efficient risk management.

„We have to rethink and revise our risk management policies for AIoT software systems. Traditionally, certification schemes and security procedures are designed for first-party software. However, data driven software supply chains and the software itself are getting more complex. We need a balanced interplay of regulation, standardization and cooperation between companies to establish digital trust."

Dr. Christoph Peylo
SVP Project Digital Trust
BOSCH

[18] Boehm et. al (2019).

E. Development and Operations of AIoT Solutions

Companies need to establish AIoT development and operations processes that enable trust by design. More specifically, within their processes and business units, they must ensure that the diverse set of digital trust principles and policies from the diverse digital trust domains (i.e., security, data privacy, data sovereignty, AI ethics) are implemented. However, they also have to ensure that these requirements are integrated and well-balanced so they can be realized in an efficient manner without unnecessary overhead and bureaucracy. Furthermore, development and operations processes should reflect the best or common practices captured in industry standards, and the risk management system must be closely tied to the product development process. Risks need to be identified early and evaluated appropriately to foster calculated risk-decisions instead of naïve risk and innovation avoidance. In all these activities, it is central to put customers first and integrate them tightly into the product creation and validation process, as Said Tabet, Technology Lead AI and IoT at Dell Technologies, emphasizes: "We work collaboratively with our customers. After all, you can't build trust when a relationship is purely transactional. We spend time with our customers exploring their challenges so that we can genuinely help them achieve long-term outcomes."

"We work collaboratively with our customers. After all, you can't build trust when a relationship is purely transactional. We spend time with our customers exploring their challenges so that we can genuinely help them achieve long-term outcomes."

Said Tabet
Technology Lead AI, IoT
DELL Technologies

F. Global Divide

In light of the rising global tensions (e.g., between the USA and China), industrial companies must reconsider to what extent they can still scale their digital offerings across markets. Global companies are used to having dedicated IT operations in China, as China has always been very strict with adopting digital services that are operated outside of China. However, in recent years, the USA has also become much more careful with products or services from abroad. Additionally, Europe has raised strong concerns against the US-based hyperscalers and their offerings. In essence, companies must prepare proactively for this ongoing global divide. They might have to deploy dedicated data centers or use distinct cloud providers in these different regions that run isolated deployments of similar digital services tailored to the privacy and security requirements of those regions. The thoughts of Dr. Peter Weckesser, EVP and CDO of Schneider Electric, underline this phenomenon: "We face a more fragmented world that we have to address. And as we're focusing on more local production, it affects the data infrastructure as well."

5. Driving Trust in Dedicated Ecosystems

The presented initiatives are central to establishing a viable foundation for digital trust. However, to build trust in a comprehensive ecosystem and enable digital business models therein, a change in perspective is necessary. In these ecosystems, companies must shift their focus from an individual company view to an ecosystem perspective. It is not about a single House of Digital Trust, but we are talking about multiple houses or orchestrating a whole city.

To bring trust and prosperity to this city, three fundamental questions must be addressed. "Why?" is all about business cases. Without compelling business cases, there is no digital value exchange in ecosystems. Every stakeholder of an ecosystem must have a business case to stay in that ecosystem. While this sounds trivial, many discussions about digital trust in ecosystems focus on rules, regulation, and technology, neglecting the most fundamental ingredient of ecosystems. "What?" addresses smart services and how the business cases are realized. The final question ("How?") covers how services are

enabled by fundamental rules (code of conduct) and regulations as well as common standards and technologies (cf. Figure 10). The three fundamental questions are directly related to each other and hence must be addressed cohesively.

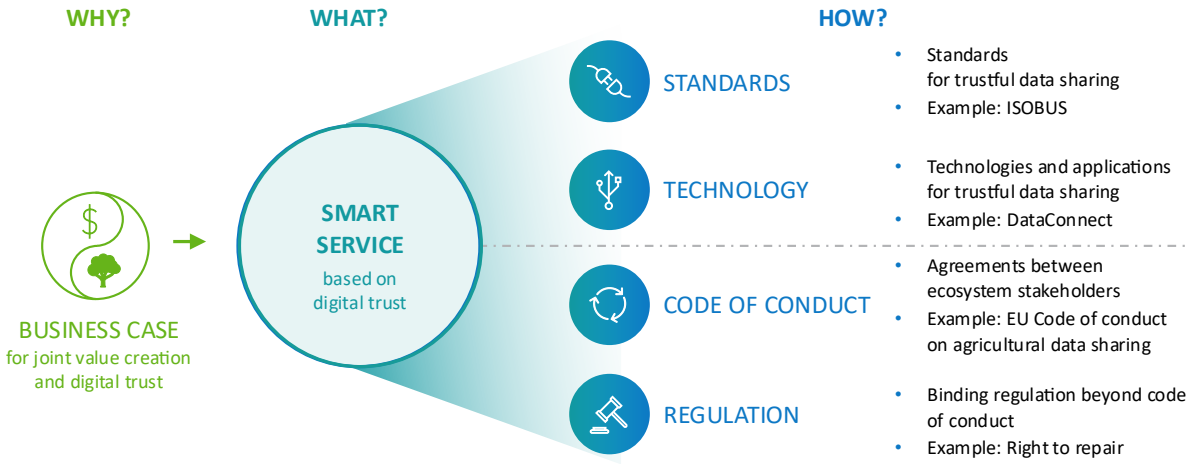

Figure 10: Driving trust in dedicated ecosystems – three fundamental questions: Why? What? How?

The agricultural industry is one of the most advanced AIoT domains driving ecosystem initiatives like smart farming and Agriculture 4.0. The industry was also the first to establish an industry code of conduct "to ensure that data-sharing leads to a prosperous agri-food chain."[19] Hence, in this chapter, the agricultural industry is used to further elaborate on the question of "how?", including the rules (code of conduct), regulations, standards, and technology.

Code of Conduct

In every ecosystem, there are essential questions that must be answered. In the realm of digital ecosystems, the most fundamental question is "who owns which data?" The answer to this question has severe consequences in respect to rights, responsibilities, and ultimately, the monetization of value propositions. Developing a joint code of conduct is one way of establishing a shared understanding of the most fundamental questions, values, principles, and rules that underly an ecosystem. The agricultural industry, for example, agreed on the "EU Code of conduct on agricultural data sharing by contractual agreement."[20] This non-binding code of conduct defines key principles that refer to the rights and obligations of processing and sharing data and focuses thereby in particular on non-personal agricultural data.

Regulation

Regulations go way beyond a code of conduct and are legally binding. As they are a rigid means to enforce rules, it takes time to develop them, and their legal enforcement and implementation can be costly. Hence, Maciej Kranz, EVP and CTO of Kone, outlines that "a consortium of companies that are like minded should first put their own framework in place and start battle testing it before engaging regulatory bodies. Then regulators can build upon the gained experience and adopt proven practices or address exiting issues." Despite existing code of conducts, legislators might need to establish legislation to protect certain ecosystem stakeholders. A recent example is the so called "right-to-repair" in the agricultural industry. In 2018, the Equipment Dealer Association and John Deere

[19] https://www.cema-agri.org/images/publications/brochures/EU_Code_of_conduct_leaflet.pdf [Accessed on September 13, 2021].
[20] https://fefac.eu/wp-content/uploads/2020/07/EU_COD1.pdf [Accessed on September 13, 2021].

voluntarily agreed on the right of farmers to be able to repair their own machinery and get appropriate access to tools, software, and diagnostic equipment from John Deere.[21] However, there was increasing dissatisfaction among farmers. From their perspective, John Deere failed to implement its promise. Hence, farmers in several US states joined a movement for the legislative implementation of a right-to-repair.

Standards

Industry standards facilitate and improve access to data in ecosystems and enable trusted data sharing and exchange. Standards are central to exploiting the potential of digitization in ecosystems, like the well-known ISOBUS standard in agriculture illustrates. ISOBUS is the communication protocol for equipment manufacturers in agriculture. It enables computers, vehicles, and implements to “talk” to each other regardless of their brand; thus, it is a viable enabler of precision farming. Essentially it ensures that a John Deere tractor is capable of operating a Claas large square baler and that all machine data can be processed in subsequent steps, for example, to analyze yield and determine subsequent fertilization.

Technology

Reference implementations of standards, open-source software, or infrastructure that is jointly developed and operated by multiple ecosystem stakeholders extends beyond specifications, norms, and requirements. These technologies help companies to realize digital services that require a shared technology stack (infrastructure) to address a diverse set of ecosystem stakeholders. One such example is DataConnect. DataConnect is a direct, cloud-to-cloud machine data solution. With DataConnect, farmers and contractors operating fleets of machinery from different manufacturers can securely exchange and view machine data through a common interface. More specifically, they can control and monitor their entire machinery fleet using their telematics platform of choice, without the need to switch between portals or transfer data manually from one system to another.[22] Thomas Hahn, Chief Expert Software at Siemens, explains that within the industrial context, he focuses on the development of the digital infrastructure Gaia-X: "Currently I am active with the policy rules and data spaces especially with respect to Industry 4.0 or more general user aspects. With Gaia-X we are on a good way, but still enough remains to be elaborated together with the partners of the ecosystem!“

"Currently I am active with the policy rules and data spaces especially with respect to Industry 4.0 or more general user aspects. With Gaia-X we are on a good way, but still enough remains to be elaborated together with the partners of the ecosystem!“

As its Gaia-X board member, Thomas Hahn is responsible for the ecosystem that is driving the cooperation of Gaia-X with other initiatives and governments.

Thomas Hahn
Chief Expert Software
SIEMENS

[21] https://www.extremetech.com/electronics/320183-john-deere-fails-to-uphold-right-to-repair-agreement-signed-in-2018 [Accessed on September 13, 2021].
[22] https://www.deere.com/en/our-company/news-and-announcements/news-releases/2019/agriculture/2019nov05-dataconnect/ [Accessed on September 13, 2021].

6. Summary and Outlook

This Digital Trust Forum white paper describes how industrial companies address the challenge of digital trust in three fundamental steps. In a first step, companies work towards mastering individual trust domains. In the last years, most companies have made substantial progress in terms of security and data privacy. Furthermore, several enterprises have recently invested in data sovereignty and AI ethics. In a second step, industrial companies have to integrate the different trust domains to create a coherent digital trust foundation. This white paper presents six essential trust initiatives that industrial companies conduct to create a solid digital trust foundation. The trust initiatives are derived on the basis of a digital trust framework (House of Digital Trust) and six core digital trust principles that industrial companies pursue. In a third step, industrial companies have to widen their perspective. They need to drive trust in the specific digital ecosystems they engage in jointly with other stakeholders. This includes, for example, the collaborative creation of a code of conduct for all stakeholders in an ecosystem. To bring trust and prosperity to ecosystems, three fundamental questions must be addressed. The “Why?” question is all about business cases. “What?” covers smart services and how the business cases are realized. Ultimately, “How?” discusses how services are enabled by fundamental rules (code of conduct) and regulations as well as common standards and technologies.

As of today, there is a strong push towards digital trust from a regulatory as well as from a technological perspective. The Gaia-X initiative, for example, aims at developing “the next generation of a European data infrastructure: a secure, federated system that meets the highest standards of digital sovereignty.”[23] More specifically, it develops standards and technologies in the realm of identity and trust, sovereign data exchange, federated catalogues, and compliance. The European Commission drives digital trust with a strong agenda from a regulatory side. The Commission has already released the Data Governance Act, the Digital Market Act, and the Implementing Act (under the Open Data Directive), and ultimately, the Data Act will follow. As depicted in this white paper, to drive innovation and facilitate a prosperous digital economy, actionable solutions are necessary, integrating technology and regulation and placing a specific perspective on economic and societal value.

[23] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Dossier/gaia-x.html [Accessed on September 13, 2021].

7. References

Abraham, C., Sims, R. R., Daultrey, S., Buff, A., & Fealey, A. (2019). How digital trust drives culture change. *MIT Sloan Management Review*, *60*(3), 1-8.

Aguiar, M., Pidun, U., Lacanna, S., Knust, N. & Candelon, F. (2021). Building trust in business ecosystems. *BCG Henderson Institute*.

Albersmeier, F., Schulze, H., Jahn, G., & Spiller, A. (2009). The reliability of third-party certification in the food chain: From checklists to risk-oriented auditing. *Food Control*, *20*(10), 927-935.

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2019). The risk-based approach to cybersecurity. *McKinsey, New York.*

Darby, M. R., & Karni, E. (1973). Free competition and the optimal amount of fraud. *The Journal of law and economics*, *16*(1), 67-88.

Gefen, D., Rao, V. S., & Tractinsky, N. (2003). The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications. In *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS'03)*.

ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity. International Organization for Standardization, Geneva, Switzerland.

Keller, J., Tennison, J., & Thereaux, O. (2021). The economic impact of trust in data ecosystems: Report prepared for the ODI. *Frontier Economics*.

Leslie, D. (2019). Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. *The Alan Turing Institute*.

Luhmann, N. (1979). *Trust and Power*. Wiley.

Lui, H.K., & Jamieson, R. (2003). Integrating trust and risk perceptions in business-to-consumer electronic commerce with the technology acceptance model. *European Conference on Information Systems (ECIS 2003), Naples*.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review, 20*(3), 709-734.

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence, 1*(11), 501-507.

Nelson, P. (1970). Information and consumer behavior. *Journal of political economy*, *78*(2), 311-329.

Shrier, D., & Krigsman, M. (2019, January 4). Futurist David Shrier: Blockchain, AI, FinTech, Digital Identity and You. CXO Talks. Retrieved from https://www.cxotalk.com/episode/futurist-david-shrier-blockchain-ai-fintech-digital-identity-you [Accessed on September 13, 2021]

Subramaniam, M., Iyer, B., & Venkatraman, V. (2019). Competing in digital ecosystems. *Business Horizons, 62*(1), 83-94.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of applied psychology*, *68*(3), 459-468.

Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems, 16*(2), 214-232.

Thomsen, T. (2018). Technische Probleme durch Industriestandards gemeinsam lösen. *ATZextra, 23*(2), 50-53.

Van den Dam, R. (2017). The trust factor in the digital economy: Why privacy and security is fundamental for successful ecosystems. *14th ITS Asia-Pacific Regional Conference, Kyoto*.

Von Solms, B. & von Solms, R. (2017). Cybersecurity and information security – what goes where?. *Information and Computer Security, 26*(1), 2-9.

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.