Author version. To be presented at WorldS4 Conference, London, UK, July 28th 2026
Final version will be available from https://link.springer.com/ - Copyright 2026 Springer Nature

# FIDES: A Trust Assessment Framework for IT Systems

Noah Holmdin[1] ✉ and Martin Gilje Jaatun[2]

[1] Swedish Defence Research Agency, Linköping, Sweden
n.holmdin@outlook.com
[2] SINTEF Digital, Trondheim, Norway
martin.g.jaatun@sintef.no

**Abstract.** The increased reliance on IT has resulted in a need for decision support for IT system usage scenarios. This is often done through risk assessment, where events are evaluated based on their likelihood of consequences and the severity of consequences. However, this may be difficult in scenarios when there is limited, uncertain, conflicting, or changing information about the IT system's behaviour. A complementary approach for this is evaluating the system based on a Decision Maker's (DM) trust in it. This paper introduces a subjective trust assessment framework for IT usage decisions.

**Keywords:** Trust · Decision support · Assessment · Evaluation · IT

## 1 Introduction

This paper introduces FIDES as a framework for post-adoptive trust assessment, building on previous research in trust modelling, while attempting to bridge existing gaps in the literature. Section 2 outlines the established design requirements. FIDES was developed as a layered architecture of three layers. A conceptual framework that establishes how FIDES interprets trust and provides meaning to the rest of the design is presented in Section 3. The evidence layer is subsequently introduced in Section 4, producing evidence from trust indicators that are relevant for the context. The layer serves as an enabler to the subsequent belief and decision layer, by producing meaningful evidence representative of the DM. Section 5 introduces the belief layer, aggregating evidence into a trust estimate which preserves probabilistic information from the evidence. Lastly, the decision layer is covered in Section 6. It uses the trust estimate, as well as utility functions, to produce context-based action recommendations for the DM.

## 2 Design Requirements

FIDES was developed with the following set of design requirements:

1. **Explicit Trust Definition** FIDES shall have a clear Definition of trust grounded in post-adoptive trust literature.

2. **Meaningful Operationalisation of Trust** FIDES shall ensure that the operationalisation of trust remains consistent with the provided Definition, such that the operationalisation is reflective of the DM.
3. **Explicit Representation of Uncertainty and Probabilistic Information** FIDES shall ensure that probabilistic information is included in the trust estimate, and that the estimate does not collapse to an expected value.
4. **Flexible Evidence Types** FIDES shall allow different types of evidence, to ensure that the evidence relevant for the DM's trust is included.
5. **Context-Dependent Trust Assessment** FIDES shall explicitly produce a trust assessment per context.
6. **Dynamic Updating of Trust** FIDES shall update the estimated trust dynamically, from observed behaviour of the IT system.
7. **Lifetime of Evidence Handling** FIDES shall ensure that operationalised evidence is updated when new evidence is available, and for adding ageing factors that reflect the loss of influence from evidence with time.
8. **Decision-Support for usage Decisions** FIDES shall include mechanisms for making post-adoptive IT usage decisions based on the trust assessment.
9. **Separation of Trust and Decision-Making** FIDES shall separate the decision layer from the trust evaluation process, such that decisions are not made solely from the trust evaluation.
10. **Support for Bounded Rationality** FIDES shall be able to operate under bounded rationality by allowing trust assessments to be made with incomplete information, uncertainty, and limited cognitive capacity.

## 3 Conceptual Framework

Trust has been studied in various fields of research, including psychology, economics, sociology, and information systems, resulting in a diverse set of Definitions and interpretations of trust [McKnight and Chervany, 2000, Rousseau et al., 1998, Kramer, 1999]. This variety reflects the fact that trust is an abstract concept that is used to explain certain aspects of human judgment. There is no universally correct definition, and different views on trust can provide value in different ways, depending on the definitions used and the context it is used in [Rousseau et al., 1998].

### 3.1 Concept of Trust

FIDES adopts Mcknight et al. [2011]'s construct of trust in a specific technology, and denotes it as *trust in an IT system*. The construct is grounded in three belief dimensions: functionality, helpfulness, and reliability, which represent the DM's beliefs about the system's ability, assistance, and consistency in behaviour. As trust is evaluated in scenarios of risk and vulnerability, the construct is extended with Castelfranchi and Falcone [2000]'s Definition of beliefs in relation to goals and actions. To formalise, this paper defines trust conceptually as denoted in Definition 1 and operationally as denoted in Definition 2.

**Definition 1 (Trust in an IT system - Conceptual)** *Trust in an IT system is a psychological state in which a human accepts vulnerability based on the expected behaviour of an IT system performing an action to achieve a goal, and when there is uncertainty regarding whether the outcome will affect the human positively or negatively.*

**Definition 2 (Trust in an IT system - Operational)** *Trust in an IT system is the subjective probability that an IT system will perform the expected action needed to achieve a goal. The expectation is grounded in a human's belief regarding the IT system's functionality, helpfulness, and reliability.*

The conceptual definition describes what trust is interpreted to mean in FIDES, while the operational definition specifies how this interpretation is represented for modelling purposes.

FIDES adopts the Bayesian interpretation of probability, which reflects an agent's degree of belief in a specific outcome in an event, based on the available information [De Finetti, 1992]. FIDES aligns with Lewicki et al. [1998], that trust and distrust are two distinct concepts, formed through different sets of beliefs in an agent. FIDES is restricted to evaluating trust, and not distrust; indicating that the evaluation of trust as low does not necessarily imply distrust. FIDES views trust as inherently subjective and context-dependent, as it reflects an agent's belief-based interpretations of prior experience, the task, and the potential impact.

### 3.2 Trust Indicators and Trust Assessment

In FIDES, a trust indicator is a property, attribute, or metric that affects the trust in an IT system. It is observed through observations that provide information on the indicator. In order to model the observations, they need to be translated into evidence before being input to the trust model.

Due to the subjective and context-dependent interpretation of trust, the trust indicators need to be chosen based on (i) the goal of using the IT system, and (ii) what affects the DM's trust in the system.

Furthermore, the trust indicators need to be explicitly tied to the belief it is connected to: functionality, helpfulness, and reliability, which in FIDES are defined as adapted from Mcknight et al. [2011]:

**Definition 3 (Functionality Belief)** *The belief that the IT system is able to perform the actions needed to achieve a goal.*

**Definition 4 (Helpfulness Belief)** *The belief that the IT system can provide the assistance needed for achieving the goal.*

**Definition 5 (Reliability Belief)** *The belief that the IT system behaves consistently in performing the actions for achieving the goal.*

Trust assessment is defined according to Definition 6.

**Definition 6 (Trust Assessment)** *Trust assessment is the overall process in which a decision-maker establishes or updates trust in an agent or an IT system, based on available information about the target's behaviour.*

## 4 Evidence Layer

The role of the evidence layer is to transform observations from an IT system into subjective evidence that reflects how the system's behaviour is affecting the DM's beliefs about the IT system's functionality, helpfulness and reliability.

FIDES evaluates trust from evidence that either supports or contradicts the functionality, helpfulness, and reliability beliefs in an IT system. The beliefs are represented as a set of belief dimensions:

$$\mathcal{K} = \{f = \text{functionality}, h = \text{helpfulness}, r = \text{reliability}\}.$$

For each belief $k \in \mathcal{K}$, $\mathcal{I}_k$ denotes the set of belief-specific trust indicators that are associated with the belief $k$. Each trust indicator $i \in \mathcal{I}_k$ represents a measurement type that is deemed relevant for assessing belief $k$. An observation from indicator $i$ is denoted as $x_i$. If the same observation is relevant to multiple beliefs, it is treated as separate belief-specific trust indicators. For each indicator $i \in \mathcal{I}_k$, the observation $x_i$ is translated into a pair of supportive and contradicting evidence points $(e^+_{k,i}, e^-_{k,i})$.

Observations are translated into evidence through a multi-step elicitation process. For each indicator $i \in \mathcal{I}_k$, two relative influence functions are elicited:

$$\psi^+_{k,i} : \mathcal{X}_i \to [0,1], \quad \psi^-_{k,i} : \mathcal{X}_i \to [0,1], \tag{1}$$

where $\psi^+_{k,i}(x_i)$ represents the extent to which observation $x_i$ supports belief $k$, $\psi^-_{k,i}(x_i)$ represents the extent to which observation $x_i$ contradicts belief $k$, and $\mathcal{X}_i$ represents the observation domain of indicator $i$. These are elicited as relative to three anchoring points: a positive saturation point $(x_i^{sat+})$, a negative saturation point $(x_i^{sat-})$, and a neutral anchoring point $(x_i^0)$, where:

$$\psi^+_{k,i}(x_i^{sat+}) = 1, \quad \psi^-_{k,i}(x_i^{sat+}) = 0, \tag{2}$$

$$\psi^+_{k,i}(x_i^{sat-}) = 0, \quad \psi^-_{k,i}(x_i^{sat-}) = 1, \tag{3}$$

$$\psi^+_{k,i}(x_i^0) = 0, \quad \psi^-_{k,i}(x_i^0) = 0. \tag{4}$$

They are further restricted such that $\psi^+_{k,i}(x_i) \cdot \psi^-_{k,i}(x_i) = 0$, to ensure that an observation is not affecting beliefs positively and negatively simultaneously.

For each belief $k \in \mathcal{K}$, a positive and a negative evidence scaling parameter are defined: $E^+_k, E^-_k$. These control the rate of evidence accumulation for the beliefs, and are retrieved through eliciting the DM's confidence in the assessment. Higher values of $E^\pm_k$ therefore make observations contribute with more evidence, leading to more concentration in the belief assessment. Lower values, in turn, lead to greater uncertainty in the belief assessment. The evidence scaling parameters

are restricted such that $E_k^{\pm} \geq 0$, as FIDES only operates with non-negative supportive and contradicting evidence.

FIDES further uses parameters for controlling the contribution of trust indicators to the assessment. The normalised weights $\tilde{w}_{k,i}^{+}$ and $\tilde{w}_{k,i}^{-}$ represent the relative importance of an indicator $i$ as compared to the other indicators affecting the same belief. The coverage parameters $\rho_k^{+}$ and $\rho_k^{-}$ represent the extent to which the chosen indicators for belief $k$ are adequate for belief assessment, and relevant for the trust assessment. Both of these parameters are constrained on the interval $[0, 1]$, and are elicited from the DM.

These variables are combined with the evidence scaling parameters to produce observation-to-evidence scaling factors:

$$\lambda_{k,i}^{+} = \tilde{w}_{k,i}^{+} \rho_k^{+} E_k^{+}, \quad \lambda_{k,i}^{-} = \tilde{w}_{k,i}^{-} \rho_k^{-} E_k^{-}. \tag{5}$$

The factors $\lambda_{k,i}^{+}$ and $\lambda_{k,i}^{-}$ represent the maximum supportive and contradicting evidence that an indicator $i$ can contribute to belief $k$. The evidence produced by an observation $x_i$ can therefore be retrieved as:

$$e_{k,i}^{+}(x_i) = \lambda_{k,i}^{+} \psi_{k,i}^{+}(x_i), \quad e_{k,i}^{-}(x_i) = \lambda_{k,i}^{-} \psi_{k,i}^{-}(x_i). \tag{6}$$

### 4.1 Temporal Evidence Handling

FIDES further incorporates lifetime handling methods for including the potential loss of relevance of observations with time. Each indicator is set to operate through either the replacement mode or the window mode. In the replacement mode, the newest evidence replaces previous evidence, while in the window mode, evidence is retained within a fixed time window, and can optionally be discounted through a decay function.

For an assessment performed at time $z$, the retained evidence pairs for indicator $i$ and belief $k$ are modelled as:

$$H_{k,i}(z) = \{(\tau_j, e_{k,i,j}^{+}, e_{k,i,j}^{-})\}_{j=1}^{m_{k,i}(z)}, \tag{7}$$

where $\tau_j$ is the time at which the evidence pair $j$ was generated, and $m_{k,i}(z)$ are the number of evidence pairs for indicator $i$ and belief $k$ for the assessment at time $z$.

If decay is used, the older evidence is weighted by a decay factor $d_j(z)$, and the updated evidence pair is then calculated as:

$$\tilde{e}_{k,i}^{+}(z) = \frac{\sum_{j=1}^{m_{k,i}(z)} d_j(z) e_{k,i,j}^{+}}{\sum_{j=1}^{m_{k,i}(z)} d_j(z)}, \qquad \tilde{e}_{k,i}^{-}(z) = \frac{\sum_{j=1}^{m_{k,i}(z)} d_j(z) e_{k,i,j}^{-}}{\sum_{j=1}^{m_{k,i}(z)} d_j(z)}. \tag{8}$$

FIDES then outputs updated evidence pairs $(\tilde{e}_{k,i}^{+}(z), \tilde{e}_{k,i}^{-}(z))$ for all indicators to the subsequent belief layer.

## 5 Belief Layer

The role of the belief layer is to aggregate the evidence into beliefs and produce a trust estimate that maintains probabilistic information. FIDES measures trust in accordance with Definition 2. Trust is assumed to influence humans in using an IT system in accordance with the findings in post-adoptive trust literature [Thatcher et al., 2011, Mcknight et al., 2011]. Based on the findings in post-adoptive trust literature, FIDES does not directly model trust from the observation, but instead models the beliefs $k \in \mathcal{K}$ from the observations, which are then aggregated to produce a trust estimate.

FIDES evaluates trust per context $C$, which is defined from a relationship between a DM and an IT system, and a goal ($G$)

$$C = \{DM, IT, G\}.$$

Trust is modelled as the context-specific variable $T_C$, derived from belief distributions associated with functionality, helpfulness, and reliability.

The belief distributions are represented as the DM's uncertainty regarding the beliefs and the evidence. FIDES models these as Beta distributions composed of supportive and contradicting evidence towards the proposition that the belief is supported. These are derived through parameterising a beta distribution with the sum of all supportive and contradicting evidence for each of the beliefs independently. The beta accumulation technique was chosen as it is interpretable, coherent with Bayesian probability, and has been widely used in trust modelling literature [Jøsang and Ismail, 2002, Fang et al., 2016].

For each belief dimension $k \in \mathcal{K}$ at time $z$, the belief-level evidence is retrieved as:

$$S_k^+(z) = \sum_{i \in \mathcal{I}_k} \tilde{e}_{k,i}^+(z), \qquad S_k^-(z) = \sum_{i \in \mathcal{I}_k} \tilde{e}_{k,i}^-(z). \tag{9}$$

These are then used as parameters to form three belief dimensions for the beliefs $k \in \mathcal{K}$, combined with a Beta(1,1) prior. The Beta(1,1) prior was chosen as it reflects an uninformative belief distribution, where all possible values in the interval $[0, 1]$ are treated as equally probable before evidence is added. The resulting belief distributions are therefore represented as:

$$B_k(z) \sim \text{Beta}(1 + S_k^+(z), 1 + S_k^-(z)) \tag{10}$$

To preserve uncertainty and the distribution structure in the aggregation, the chosen method for aggregating the beliefs into the trust estimate is a weighted sum with Monte Carlo sampling, where it is assumed that the belief dimensions contribute additively to the trust estimate. For each of the Monte Carlo iterations $j = 1, \ldots, N$, one value is sampled from each belief distribution:

$$b_f^j \sim B_f(z), \quad b_h^j \sim B_h(z), \quad b_r^j \sim B_r(z) \tag{11}$$

The trust estimation for each sample $j$ is then computed as:

$$t^j = v_f(z) b_f^j + v_h(z) b_h^j + v_r(z) b_r^j, \tag{12}$$

where $v_k$ represents the dynamic aggregation weight of belief $k$ at time $z$.

The dynamic weight is defined to represent the evidence strength of each belief distribution, and is therefore derived by normalising the evidential strength of each belief across the belief dimensions, where the evidential strength $q_k$ of belief $k$ is calculated as:

$$q_k(z) = S_k^+(z) + S_k^-(z), \tag{13}$$

and the dynamic aggregation weight is calculated as:

$$v_k(z) = \begin{cases} \dfrac{q_k(z)}{\sum_{a \in \mathcal{K}} q_a(z)}, & \text{if } \sum_{a \in \mathcal{K}} q_a(z) \neq 0 \\ \dfrac{1}{|\mathcal{K}|}, & \text{if } \sum_{a \in \mathcal{K}} q_a(z) = 0 \end{cases} \tag{14}$$

This ensures that beliefs with more evidential strength receive more influence for deriving the trust estimate, and beliefs with less evidential strength receive less influence in deriving the trust estimate. This is similar to CertainTrust [Ries, 2007], who uses evidential strength to derive the certainty of a trust opinion. The certainty then increases with the amount of collected evidence, and discounting of the trust estimate with certainty makes the output reflect the evidence strength in the trust assessment [Ries, 2007]. The dynamic weighting in FIDES further lessens the risk of double-counting belief preferences, as the relevance of each belief for the trust assessment is already encoded in the evidence layer through the coverage parameters $\rho_k^{\pm}$.

Repeating the Monte Carlo sampling process (see Equation 12) for $j = 1 \ldots N$ then produces the set of samples $\{t^j\}_{j=1}^N$ which is an approximation of the trust variable $T_C$ distribution. As $N$ increases, the Monte Carlo approximation of the resulting trust estimate will therefore become more stable in accordance with the law of large numbers [Metropolis, 1949].

The sampling is further done with an assumption of independence between the belief dimensions. This means that functionality, helpfulness, and reliability are modelled as separate belief distributions, without dependency relationships between them.

## 6 Decision Layer

The role of the decision layer is to produce a decision recommendation from the trust evaluation. According to normative decision theory, rational decisions are made by evaluating two components: the consequences that the decision can result in, and the likelihood of these consequences [Keeney and Raiffa, 1976]. The trust estimate $\{t^j\}$ represents the probabilistic trust estimate for the IT system. To further include the consequences of trust-based decisions in the evaluation, FIDES includes a decision layer that evaluates the outcomes of trust-grounded decisions regarding post-adoptive usage of an IT system.

In alignment with the findings in post-adoptive IT usage research, trust is assumed to influence whether a DM continues, explores, or stops the usage of an

IT system [Thatcher et al., 2011, Mcknight et al., 2011]. Therefore, the decision alternatives in FIDES are defined as the set:

$$\mathcal{A} = \{a_1 = \text{Explore}, a_2 = \text{Continue}, a_3 = \text{Monitor}, a_4 = \text{Stop}\},$$

where the alternatives correspond to the following descriptions:

- Explore: The IT system can be trusted sufficiently to justify relying on it to a further extent in the given context.
- Continue: The IT system can be trusted sufficiently to justify maintaining the current level of usage in the given context.
- Monitor: The IT system can be trusted sufficiently to justify maintaining the current level of usage, if the usage is being actively monitored in the given context.
- Stop: The IT system cannot be trusted sufficiently to justify its further usage in the given context.

The chosen decision architecture for FIDES is the use of utility theory. It provides a widely adopted normative framework for making decisions, where alternatives are evaluated according to the utility of their possible outcomes and the probabilities of those outcomes [Keeney and Raiffa, 1976]. The choice is aligned with the use of utility theory as a separate decision layer in previous trust models [Kurniawan and Kyas, 2015, Quercia et al., 2006].

Utility theory was chosen for the decision layer as it concerns how decisions should be made, providing decision recommendations that are rational from the available information in accordance with bounded rationality [Simon, 1955].

To define utility functions, two global anchors are elicited that represent the best and the worst outcome under all alternatives. These are set as:

$$\max_{a,t} U_a(t) = 1, \quad \min_{a,t} U_a(t) = 0.$$

Intermediate values are then elicited as relative to these anchors. For the intermediate values, a set of trust levels to elicit utility values from is chosen. This results in a set of utility functions $\{U_a\}_{a\in\mathcal{A}}$ that represent the DM's preferences for the decision alternative $a$ under various levels of trust.

### 6.1 Evaluating Alternatives Using Expected Utility

After eliciting the utility functions, the expected utility $EU$ of each alternative is calculated through expected utility theory [Keeney and Raiffa, 1976]:

$$EU(a) = \mathbb{E}[U_a(T_C)] \approx \frac{1}{N}\sum_{j=1}^{N} U_a(t^j) \tag{15}$$

where:

- $EU(a)$ is the expected utility for alternative $a$,
- $N$ is the number of Monte Carlo samples in $\{t^j\}$.

### 6.2 Selecting the Alternative that Maximises Utility

After calculating the *EU* for all actions, FIDES recommends the action that maximises the expected utility according to the Maximise Expected Utility decision criterion:

$$a^* = \arg\max_{a \in \mathcal{A}} EU(a) \tag{16}$$

## 7 Conclusion

We have presented FIDES: a trust assessment framework for post-adoptive IT. It was developed to provide an actionable, interpretable, and dynamic approach to trust assessment, with the aim of contributing to the TELEMETRY project's goal of capturing vulnerability indicators, managing cyber threat intelligence, and assessing cybersecurity risks [Taylor et al., 2026]. FIDES translates observations from trust indicators into subjective evidence, derives belief distributions that represent the extent to which the evidence supports the DM's beliefs about the IT system's functionality, helpfulness, and reliability, aggregates the belief distributions into a trust estimate, and produces a decision recommendation based on this estimate.

## Acknowledgement

This work has been performed in the context of the HEU TELEMETRY project, co-funded by the European Union (grant number 101119747) and by UK Research and Innovation (grant number 10087006). This paper is in part based on the first author's master's dissertation in information security, conducted at the Norwegian University of Science and Technology (NTNU).

## References

C. Castelfranchi and R. Falcone. Trust is much more than subjective probability: mental components and sources of trust. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, volume vol.1, page 10. IEEE Comput. Soc, 2000. https://doi.org/10.1109/HICSS.2000.926815.

B. De Finetti. Foresight: Its Logical Laws, Its Subjective Sources. In S. Kotz and N. L. Johnson, editors, *Breakthroughs in Statistics*, pages 134–174. Springer, New York, 1992. https://doi.org/10.1007/978-1-4612-0919-5_10.

W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan. BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks. *Journal of Network and Computer Applications*, 59:88–94, 2016. https://doi.org/10.1016/j.jnca.2015.06.013.

A. Jøsang and R. Ismail. The Beta Reputation System. In *Proceedings of the 15th bled electronic commerce conference*, volume 5, pages 2502–2511, 2002.

R. L. Keeney and H. Raiffa. *Decision analysis with multiple conflicting objectives*. Wiley& Sons, New York, 1976.

R. M. Kramer. TRUST AND DISTRUST IN ORGANIZATIONS: Emerging Perspectives, Enduring Questions. *Annual Review of Psychology*, 50(1):569–598, Feb. 1999. https://doi.org/10.1146/annurev.psych.50.1.569.

A. Kurniawan and M. Kyas. A trust model-based Bayesian decision theory in large scale Internet of Things. In *2015 IEEE Tenth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pages 1–5. IEEE, 2015. https://doi.org/10.1109/ISSNIP.2015.7106964.

R. J. Lewicki, D. J. McAllister, and R. J. Bies. Trust and Distrust: New Relationships and Realities. *Academy of Management Review*, 23(3):438–458, 1998.

D. H. McKnight and N. L. Chervany. What is Trust? A Conceptual Analysis and an Interdisciplinary Model. In *AMICS 2000*. Association for Information Systems (AIS), 2000.

D. H. Mcknight, M. Carter, J. B. Thatcher, and P. F. Clay. Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems*, 2(2):1–25, June 2011. https://doi.org/10.1145/1985347.1985353.

N. Metropolis. The monte carlo method. *Journal of the American statistical association*, 44(247):335–341, 1949.

D. Quercia, S. Hailes, and L. Capra. B-Trust: Bayesian Trust Framework for Pervasive Computing. In *Trust Management*, pages 298–312. Springer, 2006. https://doi.org/10.1007/11755593_22.

S. Ries. Certain trust: a trust model for users and agents. In *Proceedings of the 2007 ACM symposium on Applied computing*, pages 1599–1604. ACM, 2007. https://doi.org/10.1145/1244002.1244342.

D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer. Not So Different After All: A Cross-Discipline View Of Trust. *Academy of Management Review*, 23 (3):393–404, July 1998. https://doi.org/10.5465/amr.1998.926617.

H. A. Simon. A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, 69(1):99, Feb. 1955. https://doi.org/10.2307/1884852.

S. Taylor, M. G. Jaatun, A. Omerovic, R. Borgaonkar, R. Seidl, N. Goetze, J. Kuhr, D. Prosvirin, M. Leone, A. Kuznetsov, A. Gritskevich, A. Mpantis, O. G. Perales, B.-L. Wenning, and S. Duttagupta. Toward cybersecurity testing and monitoring of IoT ecosystems. *SN Computer Science*, 7(5):468, 2026.

J. B. Thatcher, D. H. McKnight, E. W. Baker, R. E. Arsal, and N. H. Roberts. The Role of Trust in Postadoption IT Exploration: An Empirical Examination of Knowledge Management Systems. *IEEE Transactions on Engineering Management*, 58(1):56–70, Feb. 2011. https://doi.org/10.1109/TEM.2009.2028320.