Human Factors in Cybersecurity, Vol. 208, 2026, 75–85
https://doi.org/10.54941/ahfe1007414

Assessing Trust in Digital Service Engineering: An Empirical Case Study of Public CCTV Analytics in Germany

Steven Schmidt

DB InfraGO AG, Berlin 10557, Germany

ABSTRACT

In the fields of digital Service Engineering and Requirements Engineering, trust is a crucial factor in ensuring the acceptance and adoption of technology by its users. This study conducts an empirical examination of trust factors in public video analytics systems in Germany to examine, how trustworthiness factors can be implemented in actual services. The study explores general perceptions of trustworthiness, trust-building factors, concerns, and benefits of these systems as they relate to public safety and security. The results of the study provide an empirical view and interpretation of predefined trust determinants for public video analytics, benefiting a higher acceptance rate by individuals. Conclusions include the importance and distribution of these determinants for this exemplary socio-technical system as well as general findings regarding the perception of trustworthiness of these systems. Additionally, the study validates a trust-indicating logo and assesses its impact on perceived trustworthiness of the system. This work adds to the ongoing discussion of Requirements Engineering for trustworthy digital services.

Keywords: Requirements engineering, Sociotechnical systems, Systems engineering, Trust engineering, CCTV

INTRODUCTION

Digital services manifest the prevalent characteristics of modern service systems. Following the general service definition of a utilization of abilities on the service providing and service consuming side via interactional processes to generate effects on the consumers side (Donabedian, 1980); (Donabedian, 1966) in: (Bullinger et al., 2006), digital services enhance this by an automated use of heterogeneous, technical, hardware-agnostic systems (Pakkala and Spohrer, 2019); (Immonen et al., 2016). In times of rising digitalization, this characteristic becomes more important in respect to the growing complexity of the digital world. The discipline of Service Engineering incorporates many different characteristics regarding a sufficient service conception, by incorporating different engineering disciplines such as Product Engineering, Industrial Engineering, Software Engineering, Information Engineering and Systems Engineering as well as business administrations aspects by considering Service Management, Service Production and Marketing, Service Quality and Innovation Management (Bullinger et al., 2006).

Received February 3, 2026; Revised April 1, 2026; Accepted April 20, 2026; Available online July 20, 2026

The definition of the term "requirement" is commonly found in the ISO/IEC/IEEE 24765 (IEEE, 2017). This definition is supported by various sources, including the International Requirements Engineering Board (Glinz, 2020), the ISO/IEC/IEEE 291488 (IEEE, 2018a) and the works of (IEEE, 2018b); (Sommerville, 2016); (Wiesner et al., 2015) and (Macaulay, 1996). While these definitions come mainly from the field of software engineering, they can also be adopted by Service Engineering. Essentially, a requirement should contain all the necessary information, including need or capability, constraints and conditions, to fulfil the criteria and obligations of a technical system, physical product or service and to meet an agreement, standard, specification, or other formally imposed documents. There are various forms and activities within the scope of Requirements Engineering to manage requirements, depending on the type and scope of the requirement and its associated properties and context field. For this purpose, there are different distinctions of requirements, last discussed in (IEEE, 2018b); (Glinz, 2020); (IEEE, 2018a); (Hull, 2011).

Yet, the complexity of systems – especially of those adapting AI aspects – becomes less comprehensible, to engineers as well as to individuals involved in those services. Trust is a crucial factor regarding the acceptance of digital services by professionals and by the public. By definition, trust means "a willingness by a trustor to make himself vulnerable to the possibility will act on his detriment" (Patrick et al., 2004). From a sociotechnical viewpoint, according to (Hill et al., 2005) trust forms a reduction of the system complexity and therefore serves as a form of abstraction. To understand the formation of this abstraction, (Luhmann, 2015); (Hoffmann et al., 2012) formed the discipline *Trust Engineering,* whereas the cited research forms the last attempt at this matter and practical application and validation is not further documented.

Following the approach of integrating trust generating requirements into Service Engineering activities in the form of Requirements Engineering acts as the guideline of this novel investigation on how to close the gap of assessing trust determinants in the practical world, subsequent to proposals in (Söllner et al., 2012) and (Hartenstein et al., 2020). Utilizing trust dimensions and determinants from (Hoffmann, 2014) by (Hoffmann et al., 2012) and (Schmidt, 2022a). as shown below in Table 1, their empirical relevance and distribution must be further investigated, since (Hoffmann et al., 2012) and (Schmidt, 2022a) argue the requirements engineer may chose relevant trust determinants and therefore provoking selection bias.

Table 1: Trust dimensions and corresponding trust determinants, as seen in (Hartenstein et al., 2021).

Dim.	Determinant
Performance	Eligibility of the system for achieving the target (Muir, 1994) (*Elig*)
	Reliability of the system (Muir, 1994) (*Reli*)
	Correctness of information (Muir and Moray, 1996) (*Corr*)
	Completeness of the required functional scope (Muir, 1994) (*Comple*)

(Continued)

Table 1: Continued.

Dim.	Determinant
Process traceability	Authenticity of the system (Muir, 1994) (*Auth*)
	Consistency of system behaviour (Muir and Moray, 1996) (*Cons*)
	Comprehensibility of the system's function (Zuboff, 1998) (*Compre*)
	Control over the system (Shankar, 2002) (*Contr*)
	Predictability of system behaviour (Muir, 1994) (*Pred*)
Purpose clarity	Communication of the system's purpose (Muir, 1994) (*Purp*)
	Benevolence of the developers (Muir, 1994) (*Bene*)
	Faith in the system (Muir, 1994) (*Faith*)

This research along other works such as (Hartenstein et al., 2021) as part of (Söllner et al., 2012) aims to close the gap regarding an empirical evaluation of these trust determinants as shown in (Hartenstein et al., 2021) in general and in dependence to the service they are evaluated for, to be utilizable for Requirements Engineering activities for trustworthy, digital services

Adding to the outlined goals of this investigation, the evaluation of a potential trust enabling approach has been tested due to the special character of the chosen service of public video analytics. By designing and presenting a trust seal, the impact of two different versions on the trustworthiness of the system has been conducted and will be presented alongside general results regarding the current trustworthiness of public video analytics systems in Germany, trust factors and the relevance of the predefined trust determinants. The digital service aspect is assumed for the reason, that these analytics always follow a purpose on the service consuming side, whereas the system itself is often provided by a service providing side. Since customer, user and stakeholder are distinct terms, all those roles are considered within Requirements Engineering activities, which this research aims to support through empirical insights.

METHOD

Together with the corresponding institutions, an online survey has been implemented and made available to a closed, controlled pool of probands of potential citizens affected by this kind of service, which was then distributed respecting statistical meta data such as age, gender, educational level, income, and region to gain a representative demographic result for the Federal Republic of Germany. Each number of valid responses is given in the following figures.

The questionnaire concentrates on perceptions, opinions and reasons for acceptance or disagreement regarding aspects of a secure and trustworthy analysis of public video material. For this, the general perception of security in public spaces and corresponding reasons, as well as security improving aspects were asked for. This section is followed by the stance towards video analytics of video footage of public places, reasons for denial, and acceptance

aspects for different public areas and different motives. In the following part, trust inducing aspects in form of predefined trust determinants are evaluated in the same manner as in (Hartenstein et al., 2021) to gain additional insights into relevance, importance and distribution.

In regard of the extended scope on this matter, the probands' stance towards data privacy seals in general and in the context of video analytics is then conducted. Therefore, two exemplary trust seals have been designed in a group workshop with attention to trust inducing elements derived from the trust determinants and general aesthetical viewpoints. They are presented in a contextual setup to provide better relation to the hypothetical situation the probands would be facing, as shown in Fig. 1, reading *Every Identity Protected – certified by Europrise*, which originates from the design workshop and the requirement to reference a certification for a potential software solution with the European Privacy Seal (Europrise, 2023).

Fig. 1: Exemplary trust seals A and B and context examples as shown in the survey.

The characteristic of the seals follows two approaches, one being more graphical and one being more informational through provision of an integrated QR code leading to an explanatory website.

All options of the questionnaires have been randomized to prevent order bias and all answers have been anonymized. The questionnaire took about 20 minutes to complete.

RESULTS

Regarding contextual responses concerning the general security perception in public areas, around 60% feel not secure, with a higher grade of perceived security in the morning (53%) and throughout the day (58%) than in the evening (22%) and the night (10%). The lowest grade of security concerns public transport systems (31%) and public transport stations (22%). Main reasons are to be found in subjectively suspicious groups of people (68%) or individuals (66%), darkness and badly lit areas (66%). It is noteworthy, that the lack of or insufficient video surveillance only concerns 27.00%

or respondents. Also, the difference between male and female respondents accounts for a mean of 13% with the highest spread being fear of sexual harassment (15% of males and 43% of females) and fear of sexual assault (16% of males and 42% of females).

Aspects providing the highest increase in perceived security by individuals contain stronger strikes against unlawful behaviour (76%), the presence of or ability to reach out to security personnel (72%) as well as improved illumination (66%) and video surveillance (56%). Signs pointing out behavioural rules are perceived as least effective towards improved security (13%). All these responses have their highest values amongst citizens aged 50 years and above making them the most vulnerable group, with citizens aged between 16 and 35 years being on the other side of the spectrum.

Narrowing down the evaluation on public video analytics systems, most respondents are open towards this matter (63%) and perceive implementation and execution as trustworthy (58%) and secure (58%), again with lower scores amongst younger respondents and higher scores of probands aged 50 years and above ($\bar{x}$ = 15.66%). The highest acceptance for video analytics concentrates on public transport stations (83%) and public transport systems (74%), followed by streets and public areas (71%). It is accepted the least in bars and clubs (41%) and restaurants (26%). It is important to combine this insight with the video analytics' purpose to gain a more complete picture of video analytics' acceptance: The highest support can be found for securing proof of crimes (81%) and deterrence of crimes (79%). The ability of timely detection of impending crimes is rated the third highest acceptance for a purpose (77%), benefiting from the core characteristics of video analytics. To optimize personnel disposition (57%) and to identify highly frequented areas in public spaces is just above indecisive. Evaluating busy times (47%), optimizing visitor paths (43%) and the general evaluation of movements (38%) are not accepted by respondents, with advertising and marketing goals being the least accepted at 10%, as visualized in **Fig. 2**.

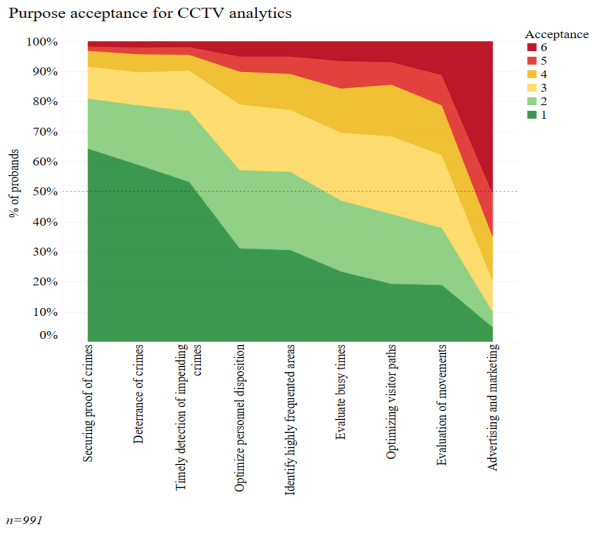

Fig. 2: Acceptance of different purposes of CCTV analytics in Germany.

Reasons for denial occur through perceptions of control and surveillance of individuals (25%) and the loss of privacy (20%). Additionally, data misuse (17%) and a lack of data protection (14%) form concerns too. Acceptance is met, when video analytics are used for prosecution (76%), providing security (65%) and usage solely for the predefined use (57%). Securing data privacy while using video analytics (48%) and protection against unauthorized access (45%) are considered the least effective measures to raise acceptance of video analytics regarding this selection (see **Fig. 3**).

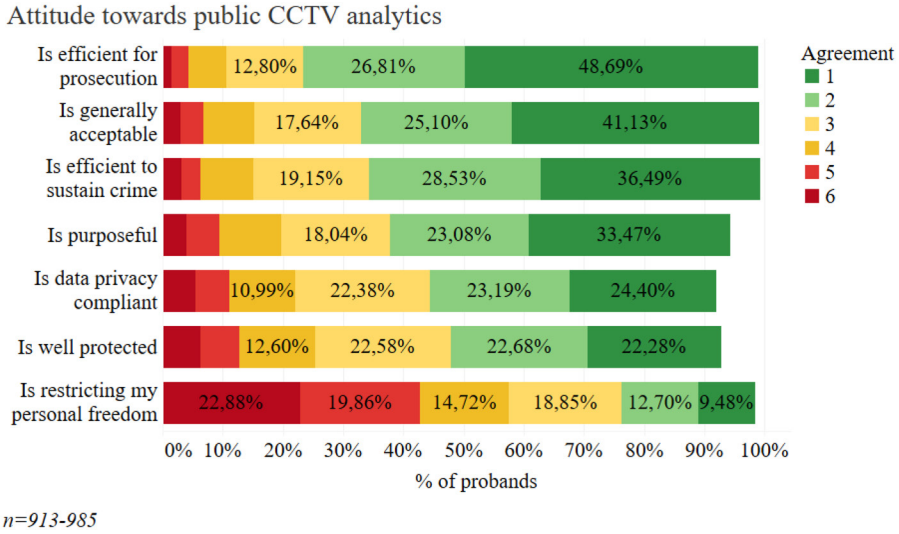

Fig. 3: Attitudes regarding public CCTV analytics in Germany.

Enhancing the evaluation of acceptance by considering trust aspects, data privacy and security measures gain 13% of all top-of-mind mentions, followed by the indication of the clear intention to use video analytics solely for prosecution and deterrence of crimes (11%) together with transparency concerning the purpose and usage of gained material and algorithms (6%). 8% indicate use by authorized personnel only as another trust building factor for public video analytics systems. Lastly, it is important to take into account, that 5% replied, that they already fully trust video analysis systems in addition to 24%, that cannot phrase trust enhancing factors top-of-mind.

The variables are named indicating their relevance regarding public video analytics systems (*V*). Ranking the trust determinants in respect to the individuals' perception of video analytics systems for public areas, parallels can be drawn comparing the results to those of a sample of different digital services as shown in (Hartenstein et al., 2021). Within the trust determinants there is no significant correlation, since they are measuring different, distinct aspects of trustworthiness. Following the interpretation of Cronbach's Alpha by (Blanz, 2021), assumptions about reliability would not be possible. Yet, low inter-item correlation provokes a low alpha value, leading to a similar interpretation as in (Hartenstein et al., 2021), which assumes that each determinant is understood differently by probands complying with the

socio-psychological factor of trust determinants for socio-technical systems such as digital services.

Regarding the statistical distribution of the trust determinants, parallel coordinates diagrams have been used and visualize the matter with the aid of a density layer for better readability (**Fig. 4**).

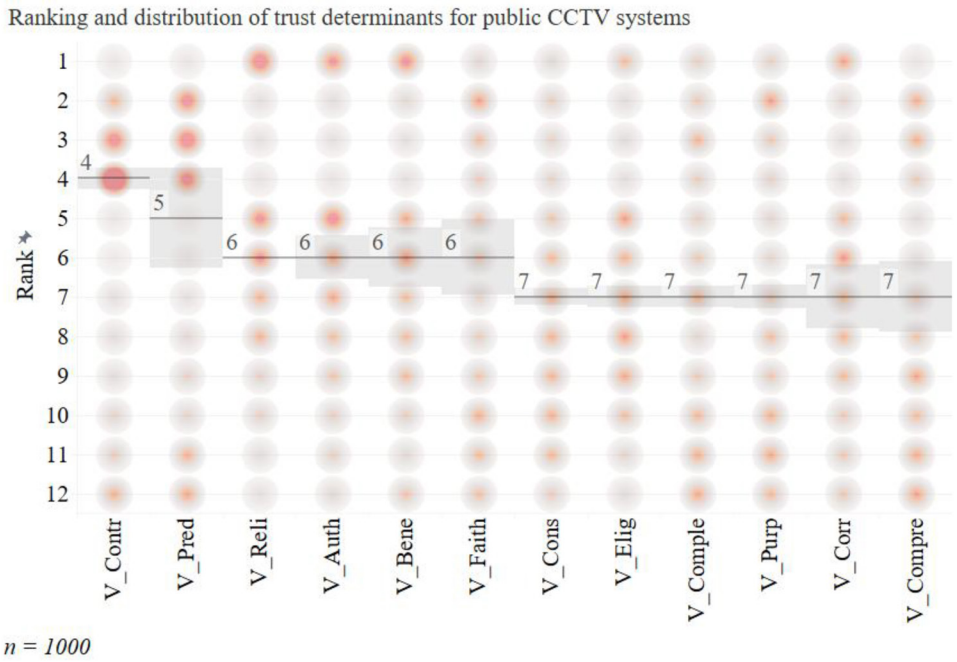

Fig. 4: Distribution of trust determinants for public CCTV analytics systems in Germany.

The related statistical data is shown below.

Statistics

		V_Auth	V_Bene	V_Comple	V_Compre	V_Cons	V_Contr	V_Corr	V_Elig	V_Faith	V_Pred	V_Purp	V_Reli
N	Valid	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000
	Missing	0	0	0	0	0	0	0	0	0	0	0	0
Median		6.00	6.00	7.00	7.00	7.00	4.00	7.00	7.00	6.00	5.00	7.00	6.00
Std Dev		3.32	3.44	3.53	3.50	3.29	3.49	3.39	3.20	3.50	3.69	3.57	3.31
Variance		11.04	11.85	12.43	12.27	10.83	12.20	11.46	10.22	12.26	13.62	12.78	10.94

Fig. 5: Median and variance of trust determinants of public video analytics systems in Germany.

The closeness of the different medians again supports the interpretation of different interpretations by individuals with an overall spread of 3 in relation to a scale variety of 12. There also is a possibility for a weaker distinction between ranks of trust determinants, putting them at a potentially identical level of importance for the service in evaluation from the perspective of the proband.

The evaluation of the use of privacy seals as a trust building component of applicable digital services shows, that just for 46% of participants the acceptance for data processing is raised, and just for 44% the conviction is

built, that data processing remains within the scope of the original purpose. Furthermore, only 44% state, that privacy seals generate a positive feeling concerning the digital service the seal is provided for, 39% hold privacy seals credible, maintaining the gap across age group throughout all named aspects ($\bar{x}$ = 5,90%).

Applying the two exemplary privacy seals mentioned above, most participants responded with similar scores for an overall positive impression (A: 39%, B: 45%), appealing message (A:43%, B: 48%) and interesting design (A: 39% B: 47%). B also provides higher values relating to reliability (47%), security (47%) and credibility (47%), although only given by less than half of probands. Same applies to the suggestions of a trustworthy handling of data (46%) and transparency (41%).

In direct comparison of the seals, B also collects the tendencies concerning overall impression (47%), trustworthiness (48%), trust generation for public video analytics systems (39%) and public video analytics acceptance (36%), see **Fig. 6**.

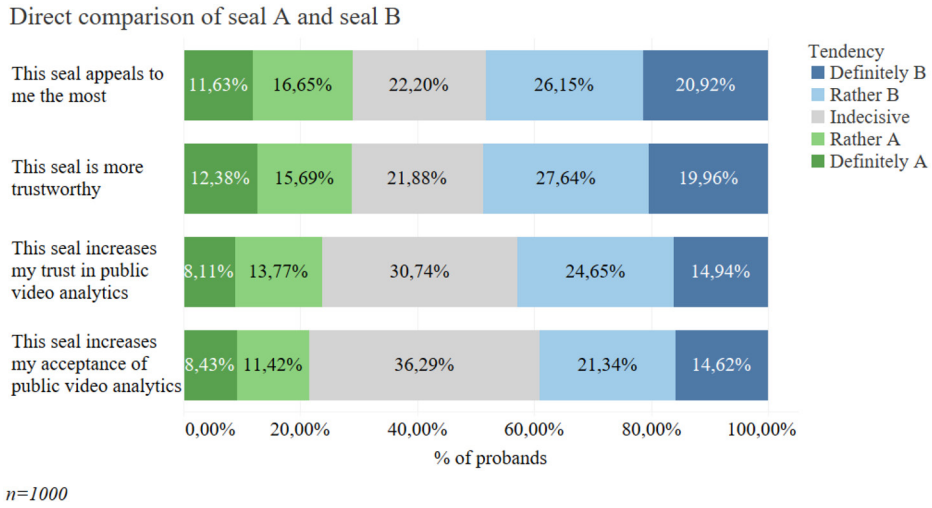

Fig. 6: Direct comparison of the exemplary seals.

Commentary by participants on either choice can be summarized as follows:

Table 2: Comparison of probands commentaries for both seals.

Seal	Commentary
Seal A	- It is kept simple - Seems more serious - Better readable - The person suggests relation to personal data - The person creates a human aspect to the message
Seal B	- More modern and professional - QR Code suggests more transparency - Suggests higher authority because of the more present shield - Pixel suggest anonymization - Conveys higher grade of quality

The used data (Schmidt, 2022c) as well as the questionnaire (Schmidt, 2023) are published online.

CONCLUSION

The results characterize the current situation of public video analytics systems' trustworthiness and related factors, which has not been examined using this methodology before. Most citizens in Germany are open towards this kind of systems, if the purpose is clearly stated and complied to, if the purposes concern security, safety and optimization of personal and public area conception. Regarding actual fears of citizens, these kinds of systems also gain raising attention and need.

Assessing the preselected trust determinants in regard of this service for public area operators, security personnel police etc., the summarization can be made, that all the 12 factors are more or less of same relevance for a trustworthy conception of these systems as well as this novel approach proves beneficial for gathering insights into trust building factors of a service, theoretically and practically. Eligibility, authenticity, consistency, comprehensibility of the system and the communication of the systems purpose as well as the service providers benevolence also relate to findings concerning the previous discoveries stated above. The reliability of the analytics system and related events as well as the correctness of gathered information and conclusions are considerably of same importance to citizens. Same applies to the completeness of required functions and corresponding predictability of the analytics systems results as trust building factors. Through comprehensibility together with the aspect of control over the system, aspects focused on the affected individuals need to be considered too. Intrinsically, the faith in the system is of importance as well.

Adding these results to findings in (Hartenstein et al., 2021), the conclusions support the thesis for digital services in general, which can be sum up as an almost equal relevance of the selected trustworthiness determinants for digital services in general and their acceptance by users and affected individuals. Therefore, further research need could not be of need, as several diverse service systems have now been evaluated.

Concerning the general idea of a Generic Requirements Engineering Framework for Trustworthy Digital Services (GREF4TS, (Schmidt, 2021)), these concluded findings will be adapted for conception and validation using an exemplary digital service (Schmidt, 2022b).

Regarding the reception and effectiveness of trust seals for digital services, it can be concluded, that the two provided exemplary seals have a positive effect for a minority of citizens with a higher tendency towards a more informative presentation. Regarding the current acceptance and trustworthiness of video analytics systems it remains open, if this kind of seal needs to be adopted to gain higher values in perception. Yet, providing this kind of information relates to trust determinants such as authenticity, comprehensibility, purpose communication and provider benevolence and therefore could be seen as a trust-supporting component of the system.

REFERENCES

Blanz M. (2021). Research Methods and Statistics for Social Work: Foundations and Applications. 2nd edition. Stuttgart: W. Kohlhammer Publishing House.

Bullinger H-J, Scheer A-W, editors. (2006). Service Engineering: Development and design of innovative services; with 24 tables. 2nd, completely revised and expanded edition. Berlin: Springer; 2006.

Donabedian A. (1966). Evaluating the quality of medical care. 1966. Milbank Quarterly 2005; 83(4): 691–729 [https://doi.org/10.1111/j.1468-0009.2005.00397.x][PMID: 16279964]

Donabedian A. (1980). Explorations in quality assessment and monitoring. Ann Arbor, Mich.: Health Administration Press 1980.

EuroPriSe Cert GmbH (2023). EuroPriSe; 2023 [cited 2023 March 26] Available from: URL: https://www.euprivacyseal.com/.

Glinz M. (2020) A Glossary of Requirements Engineering Terminology; 2020. Available from: URL: https://www.ireb.org/content/downloads/2-cpre-glossary-2-0/ireb_cpre_glossary_de_2.0.1.pdf [cited 2021 October 15]

Hartenstein S, Schmidt S, Schmietendorf A. (2020). Towards an Empirical Analysis of Trustworthiness Attributes in the Context of Digitalization. In: Towards an Empirical Analysis of Trustworthiness Attributes in the Context of Digitalization; 2020. IARIA XPS Press; 112–6.

Hartenstein S, Schmidt S, Schmietendorf A. (2021). Empirical Analysis of Trustworthiness Attributes in the Context of Digitization. In: International Journal on Advances in Security 2021; 48–58.

Hill CA, O'Hara O'Connor EA (2005). A Cognitive Theory of Trust. SSRN Journal 2005 [https://doi.org/10.2139/ssrn.869423]

Hoffmann A, Söllner M, Hoffmann H. (2012) Twenty Software Requirement Patterns to Specify Recommender Systems that Users Will Trust. SSRN Journal 2012 [https://doi.org/10.2139/ssrn.2484462]

Hoffmann A. (2014). Requirements pattern for the specification of socio-technical systems: Standardized requirements for trustworthiness and legal compliance. Kassel, Germany: Kassel University Press 2014.

Hull E. (2011). Requirements Engineering. London: Springer London 2011.

IEEE (2017). 24765-2017 - ISO/IEC/IEEE International Standard - Systems and software engineering–Vocabulary. 2017th ed. Piscataway, NJ, USA: IEEE; 2017 2017 Aug 28. Available from: URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8016712.

IEEE (2018a). 29148-2018 - ISO/IEC/IEEE International Standard - Systems and software engineering – Life cycle processes – Requirements engineering. Piscataway, NJ, USA:

IEEE (2018b). 2018 2018 Nov 30. Available from: URL: https://ieeexplore.ieee.org/servlet/opac?punumber=8559684 [cited 04.09.20121]

Immonen A, Ovaska E, Kalaoja J, Pakkala D. (2016). A service requirements engineering method for a digital service ecosystem. SOCA 2016; 10(2): 151–72 [https://doi.org/10.1007/s11761-015-0175-0]

Lee JD, See KA (2004). Trust in automation: designing for appropriate reliance. Hum Factors 2004; 46(1): 50–80 [https://doi.org/10.1518/hfes.46.1.50_30392] [PMID: 15151155]

Luhmann N. (2015). Trust: A mechanism for reducing social complexity. Reprint of the 4th ed. Stuttgart: Lucius & Lucius 2015.

Macaulay LA (1996). Requirements Engineering. London: Springer 1996.

Muir BM, Moray N. (1996). Trust in automation. Part II. Experimental studies of trust and human intervention in a process control simulation. Ergonomics 1996; 39(3): 429–60

Muir BM. (1994). Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems. Ergonomics 1994; 37(11): 1905–22

Pakkala D, Spohrer J. (2019). Digital Service: Technological Agency in Service Systems. In: Digital Service: Technological Agency in Service Systems; 2019. Hawaii International Conference on System Sciences.

Patrick A., Marsh S., Briggs P. (2004). Designing Systems That People Will Trust. [https://doi.org/10.1080/00140139408964957]

Rupp C., editor (2021). Requirements Engineering and Management: The Handbook for Requirements in Every Situation. 7th, updated and expanded edition. Munich: Hanser; 2021.

Schmidt S. (2021). On the perception and relevance of trustworthiness in public wireless networks. In: Daimi K, Arabnia HR, Deligiannidis L, Hwang M-S, Tinetti FG, editors. On the perception and relevance of trustworthiness in public wireless networks; 2021. Cham: Springer International Publishing.

Schmidt S. (2022a). On the Need for a Generic Requirements Engineering Framework for Trustworthy IT Services. In: Arai K, editor. Advances in Information and Communication. Cham: Springer International Publishing 2022; 832–42.

Schmidt S. (2022b). Entwicklung eines generischen Requirements Engineering Frameworks für digitale Services unter Berücksichtigung der Rolle der Vertrauenswürdigkeit; 2022 [cited 2022 October 21] Available from: URL: https://www.researchgate.net/publication/359262146_Entwicklung_eines_generischen_Requirements_Engineering_Frameworks_fur_digitale_Services_unter_Berucksichtigung_der_Rolle_der_Vertrauenswurdigkeit?channel=doi&linkId=6231e347d37dab4f96e8ad8a&showFulltext= true.

Schmidt S. (2022c). Questionnaire on the trustworthiness of video analysis, 2022 [cited 2026 April 10] Available from: URL: https://www.researchgate.net/publication/403689967_Fragebogen_Vertrauenswurdigkeit_von_Videoanalysen.

Schmidt S. (2023). Study data on the acceptance of video analytics at train stations in Germany, 2023 [cited 2026 April 10] Available from: URL: https://www.researchgate.net/publication/403689890_Studiendaten_zur_Erhebung_der_Akzeptanz_von_Videoanalyse_an_Bahnhofen_in_Deutschland.

Shankar V. (2002). Urban GL, Sultan F. Online trust: a stakeholder perspective, concepts, implications, and future directions. The Journal of Strategic Information Systems 2002; 11(3-4): 325–44 [https://doi.org/10.1016/S0963-8687(02)00022-7]

Sommerville I. (2016). Software engineering. Tenth edition, global edition. Boston, Columbus, Indianapolis, New York, San Francisco, Hoboken, Amsterdam, Cape Town, Dubai, London, Madrid, Milan, Munich, Paris, Montreal, Toronto, Delhi, Mexico City, São Paulo, Sydney, Hong Kong, Seoul, Singapore, Taipei, Tokyo: Pearson 2016.

Söllner M, Hoffmann A, Hoffmann H, Leimeister JM. (2012) Trust support for socio-technical ubiquitous systems. Z Betriebswirtsch 2012; 82(S4): 109–40 [https://doi.org/10.1007/s11573-012-0584-x]

Wiesner S, Peruzzini M, Hauge JB, Thoben K-D (2015). Requirements Engineering. In: Stjepandić J, Wognum N, J.C. Verhagen W, editors. Concurrent Engineering in the 21st Century: Foundations, Developments and Challenges. Cham, s.l.: Springer International Publishing 2015; 103–32.

Zuboff S. (1998). In the age of the smart machine: The future of work and power. Paperback ed. Oxford: Heinemann Professional 1989.