

SYSTEMATIC MAPPING STUDY ON VERIFICATION AND VALIDATION OF INDUSTRIAL THIRD-PARTY IOT APPLICATIONS

Ivan Tritchkov

Siemens Corporate Technology, Günther-Scharowsky-Str. 1, 91058 Erlangen, Germany.

ivan.tritchkov@siemens.com

Submitted on 18.05.2020

© Tritchkov I., 2020

Abstract: The next industrial revolution commonly known as Industry 4.0 represents the idea of interconnected manufacturing, where intelligent devices, systems and processes exchange information, resources and artifacts to optimize the complete value-added chain and to reduce costs and time-to-market. Industrial software ecosystems are a good example how the latest digitalization trends are applied in the industry domain and how with the help of industrial IoT applications the production process can be optimized. However, the use of third-party applications exposes to a risk the systems and devices part of the manufacturing process. To address these risks a set of quality measures must be carried out in the ecosystem. This paper presents the results of a systematic mapping study carried out in the area of verification and validation of industrial IoT third-party applications. The goal of the study is to structure the scientific landscape and to provide an up-to-date snapshot of the current state of the research field.

Index Terms: industrial applications, industrial ecosystems mapping, IoT, mapping study, quality assurance, testing, verification, validation, third party

I. INTRODUCTION

Industry 4.0 is a name originally initiated in Germany and commonly used to represent the fourth industrial revolution. It addresses the latest trends in digitizing manufacturing and production, which revolutionizes the way how commodities and products are created. The core concept behind Industry 4.0 refers to the intelligent networking of machines and processes for industry with the help of information and communication technology [1], [2]. Thus, Internet and the interconnectivity it offers between different systems, devices and processes, constitutes the main driver of the fourth industrial revolution. Another common term related to that is Internet of Things (short: IoT). ITU defines IoT as “global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things” [3].

In the context of Industry 4.0 of particular interest for machine vendors, manufacturers and software providers is the possibility to connect devices from the shop floor to cloud-based IoT platforms. The combination of real-world production data and the nearly endless resources provided by a cloud allow to get the most of the production process. Using methods from the data analytics, one is able to optimize the production process, predict more accurately downtimes and

schedule maintenance, just to name a few of the application fields.

Therefore, it is not quite surprising that more and more companies are keen on creating industrial ecosystems or contributing to these. The industrial ecosystems are one of the phenomena brought by the digitalization age and one of the cornerstones of the shared economy towards Industry 4.0.

There has been no consensus to date on the definition of a software ecosystem. As per Messerschmitt and Szyperski [4], software ecosystem refers to a collection of software products that have some given degree of symbiotic relationships. According to Bosch et al. [5], a software ecosystem consists of a software platform, a set of internal and external developers and a community of domain experts in service to a community of users that compose relevant solution elements to satisfy their needs. Jansen et al. [6] defines a software ecosystem as a set of businesses functioning as a unit and interacting with a shared market for software and services, together with the relationships among them. These relationships are frequently underpinned by a common technological platform or market and operate through the exchange of information, resources and artifacts. This definition is also adopted by this paper.

Based on that, one can conclude that the major characteristics of software ecosystems, witnessed also by [7], [8] are:

- Business interests
- Common technological platform
- Common market for software and services
- Exchange of information, resources and artefacts
- Relationships among the parties involved in the ecosystem

While the common technological platform provides the underpinning software base around which the platform is built, the involvement in the ecosystem depends on the business interests. They are on the other hand usually driven by the value (both monetary and non-monetary), which the information, resources and artifacts being exchanged bring for the parties involved in the ecosystem

The items subject of exchange in a software ecosystem are usually provided in a form of applications or so called apps. The applications are software extensions which provide additional services and functions. They are published in the

ecosystem's marketplace commonly known as app store, where interested users can purchase them against a fee or for free. After that the apps are installed on the end user's device.

The more apps are offered in the marketplace, the more additional services are available and the more attractive the ecosystem is for all involved parties. Therefore, modern ecosystems offer the possibility to device owners and other interested parties to implement and publish in the app store their own applications known as third-party apps. The special thing about them is that from platform provider's and device owner's perspective, these apps are a piece of software code, developed by another company or organization.

Thus, from a software quality perspective third-party apps constitute a risk for both the ecosystem platform and the device they run on. This is even more valid for the industry domain, where the requirements with respect to functional and non-functional requirements are higher than in the entertainment domain for example. To address this risk all parties in an industrial software ecosystem have to undertake certain quality measures owing to the use of third-party apps.

Driven by the recent progress made in the area of Industry 4.0, I believe this topic will become in the next years even more important. In order to summarize the current state of work and to identify gaps and needs for further research, a study on the verification and validation of third-party apps was undertaken.

There are different methods for structuring a scientific research landscape. Two of the most common methods are systematic literature review [9] and systematic mapping study [10]. As stated by Petersen et. al [10] both methods "differ in terms of goals, breadth and depth" and "should and can be used complementary". A systematic map can be conducted first, to get an overview of the topic area. Then the state of evidence in specific topics can be investigated using a systematic review [10] Mapping studies provide the summary of the results in a visual form, a map, which eases the understanding of the current state of work. This paper aims to provide an overview of the results of this mapping study.

The reminder of this work is structured as follows: Chapter II presents the current state of research. Chapter III provides an overview of the research method used in this study. Chapter IV discusses the results of the study, while the major findings and conclusions are introduced in Chapter V. Chapter VI presents the main threads for validity and the last chapter summarizes the main contribution of study and proposes topics for future work in the research area.

II. RELATED WORK

To the best of my knowledge, there is so far no published work providing an overview of the current state of research in the area of verification and validation of third-party industrial applications. Several mapping studies have been published so far, but they all target only single aspects of the research area subject of this study.

A. Garcia-Holgado and F. Garcia-Penalvo [11] provide an overview of the software ecosystem domain as a whole, while O. Barbosa et al. [12] aims to scope the domain from three-dimensional perspective. F. Fotrousi et al. [13] conducted a study on KPIs for software ecosystems. The

current state of research in the area of requirements engineering in software ecosystems area is reported by A. Vegendla et al. [14].

A. Fontao et al. [15] conducts a mapping study focused solely on mobile software ecosystems (MSECO). It has identified during the search for relevant publications 268 records, which were reduced to 28 after sanitization. The study helped to understand better the characteristics and benefits of MSECOs and to gain an overview of the available methods, tools, processes and approaches in the technical literature with respect to MSECOs.

Wortmann et al. [16] characterizes in his mapping study on "Modeling for Industry 4.0" the state of the art of model-based software engineering for smart factories. His study has analyzed 1475 publications and out of them has qualified 199 for classification. One of the findings of his research is that "neither validation & verification, nor the human factors crucial to the success of Industry 4.0 or product modeling are investigated as much as integration and digital representation".

The aspect of verification and validation of applications is subject of talk by S. Zein et al. [17]. Out of 7356 studies they have identified 79 relevant empirical studies and have mapped them according to a classification schema. Their study reveals several gaps in the research area: need for eliciting early testing requirements, need for research in real-world development environments, testing techniques for application lifecycle conformance and mobile services testing, as well as comparative studies for security and usability testing.

Although all of the above-mentioned studies are related to the research topic subject of this study and some of them have even addressed the verification and validation aspect, none of them is focused in particular neither on the third-party applications, nor on industrial software ecosystems.

III. RESEARCH METHOD

Systematic mapping study (SMS) is as per Petersen et. al [10] a methodology that provides a structure of the type of research reports and results that have been published by categorizing them and gives a visualization of its results, usually in the form of a map. This chapter provides a step by step description of the SMS methodology used to conduct the study.

A. THE SYSTEMATIC MAPPING PROCESS

The systematic mapping process consists of several sequential steps. Every step of the process has a different purpose and outcome. The SMS starts with definition of the research field and setting up the research agenda in terms of a time frame, goals and available resources. Then, one proceeds with definition of research questions, search for relevant publications, publications screening, keywording of abstracts and mapping. These steps are the most essential ones and built the core of the process as described by [10]. The current study showed that in order to improve the quality of the search results, one has to follow a systematic approach for the definition of the research questions and for the definition of the search queries. Therefore, compared to the process proposed by Petersen et al. [10] the definition of the search strings is highlighted as a separate step here. The systematic

mapping process ends with the reporting step. Fig. 1 provides this paper and the outcomes of every process step. an overview of the systematic mapping process followed by

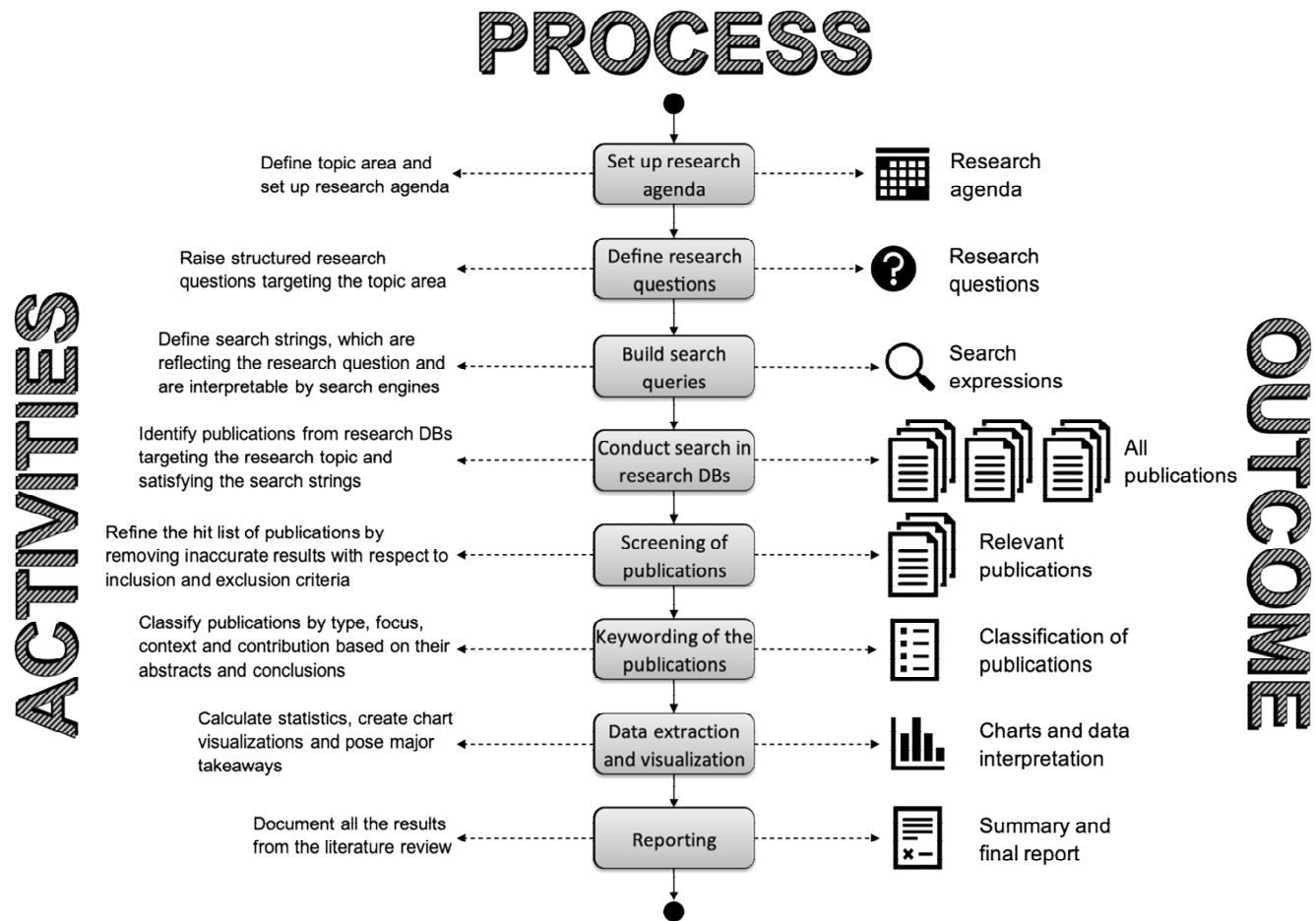


Fig. 1. The Systematic Mapping Process

The remaining part of this chapter provides more detailed information about the process steps and the activities carried out there.

B. SET UP RESEARCH AGENDA

The research process begins with setting up the research agenda and the frames of the study. This step aims to detail the schedule of the study and to specify the research field of interest, the persons involved in the study, the available and required software licenses, the overall goals of the study and the reporting format of the results.

The research field for this SMS was set to verification and validation of industrial IoT applications. The was carried out from November 2018 to April 2019 and the goal is to structure the scientific landscape, to characterize the current state of the research and to help understand and compare the results in this field. The results of the study were documented in the form of (i) a map and (ii) a report containing a detailed description of the findings.

C. DEFINE RESEARCH QUESTIONS

The definition of the research questions is one of the most important steps in every study and has a major impact on the results. Since the majority of the research databases uses search engines supporting rudimental queries, it is recommended to use a more systematic approach for the definition of the research questions (RQs).

As stated by Petticrew and Roberts [18] a good way for defining RQs in the medical domain is to break them down into population, intervention, comparison, outcome and context. This structure is also known as PICO or PICOC model. Kitchenham et. al [9] adapts these criteria and proposes a mapping, which is suitable for the software engineering domain.

provides an overview of this mapping.

Following this structure, the research question of this study was built. For every element of the PICOC model a corresponding phrase was specified as in column “Root Term”

in Table 1. Then, the phrases were grouped together resulting into the research question the study was aiming to answer.

Table 1

PICOC Model Elements and Root Term Definition

Criterion	Description	Example	Root Term
Population	People or artifacts affected by the intervention	Testers, managers, IT systems, Telecommunication companies, Small IT companies, etc.)	Third-party Edge applications
Intervention	Software methodology, technology, tool, or procedure addressing specific issues	Requirements engineering, system testing, software cost estimation, etc.	QA measures (for industrial ecosystems)
Comparison	Software methodology, technology, tool, or procedure the intervention has been compared to	Requirements engineering, system testing, software cost estimation, etc.	QA measures (for mobile ecosystems)
Outcome	Relevant outcomes	Improved reliability, short time to market, etc.	Efficient approach for verification and validation
Context	The context in which the comparison takes place	Academia vs. industry	Industrial context

The end result of this step is the research question this study aims to answer:

Which quality assurance measures are required in order to establish an efficient approach for verification and validation of 3rd party edge applications in industrial ecosystem context compared to applications in mobile domain?

D. BUILD SEARCH QUERIES

The next step in the systematic mapping process is the definition of search queries. They are used to search in research databases for relevant articles, journals, papers, scientific books and other publications contributing to the research question.

The majority of the research databases usually dispose search engines, which support and ease finding the right records. These search engines receive as input a string of words or phrases (so called keywords) which they are able to interpret. Every entry in the research database is checked against the search string and matching entries are added to the hitlist with the search results. Common search engines usually follow specific notation consisting of keywords and operators expressing the relations between the keywords

Table 2 provides an overview of the most common operators used by the search engines. Please note that this is not a comprehensive list and there might be deviating operators depending on the research database.

Search queries have strong impact on the search results and on the study itself. If a search string is too generic the search results would be inaccurate and biased by irrelevant publications. On the other hand, if the search string is too specific, relevant publications might be excluded from the hitlist, just because they did not match in the exact same way

the search string. What’s more, using semantically varying search queries in different research databases might lead to distinctive results, which is also recognized as threat to the validity of the study in Chapter VI.

To overcome this issue, it is useful to build a search string with equivalent meaning to the research question but omitting unnecessary expressions. The PICOC model previously used to formulate the research question simplifies this activity, too. First, for every term corresponding to a PICOC criterion one should define a set of related keywords. These might include synonyms, spelling variations or other related terms. Then, in the related terms are transformed with the help of logical operators into interpretable logical expressions. Adding operators allows to dedicatedly broaden the search by considering synonyms or spelling variations or to narrow it down by excluding specific terms.

The result of this process step is a search string, which is designed to repeat semantically the research question but it can be also easily interpreted by search engines:

(“3rd party” OR “third party”) OR (application* OR app* OR edge application* OR “edge app*” OR “mobile application*” OR “mobile app*”) AND

(test* OR “quality assurance” OR QA OR verification OR validation OR “verification and validation” OR “V&V” OR functional OR “non-functional” OR NFR* OR qualities OR “quality attribute*” OR “quality measure*”) AND (approach* OR method* OR methodology OR concept* OR strategy OR “test strategy” OR process* OR “test process*” OR framework*) AND

(industrial OR ecosystem* OR “industrial ecosystem*” OR mobile* OR “mobile ecosystem*” OR iOS OR android OR edge OR “edge ecosystem*”)

Table 2

List of logical operators commonly used by search engines in digital libraries

Operator	Usage	Example	Outcome
AND	This operator is used to narrow the search. It considers only unique records containing both terms.	applications AND test	The search engine retrieves only unique records containing both terms "applications" and "test".
OR	This operator is used to broaden the search. It considers either one of the terms or both of them.	applications OR apps	The database retrieves all unique records containing "applications" or "apps" or both - "applications" and "apps".
NOT	This operator is used to narrow down the search by excluding terms from the hit list.	ecosystems NOT ecology	The database retrieves all records containing "ecosystem", but not "ecology".
*	The wildcard operator serves as truncation operator. Terms match if they begin with the word preceding or following the * operator.	test*	The search engine considers all unique records containing the terms "test", "testing", "testable", etc. but also words like "testimonial", "testament", etc.
()	The parenthesis operator groups words into subexpressions, which can be also nested. Parentheses specifies the order in which the expressions are interpreted.	(third party OR 3rd party) AND (applications OR apps)	The search engine looks first for all records containing either "third party" or "3rd party" and then looks in the results for "applications" or "apps".

Table 3

Related terms used to build the search strings

Criterion	Root Term	Related Terms	Search string
Population	Third-party applications	3rd party, third party, application, app, edge application, edge app, mobile application, mobile app, IoT app	("3rd party" OR "third party") OR ("application*" OR "app*" OR "edge application*" OR "edge app*" OR "mobile application*" OR "mobile app*" OR "IoT app*")
Intervention	QA measures (with respect to industrial ecosystems)	Test, testing, quality assurance, QA, verification, validation, V&V, functional, non-functional, NFR, qualities	"test*" OR "quality assurance" OR "QA" OR "verification" OR "validation" OR "verification and validation" OR "V&V" OR "functional" OR "non-functional" OR "NFR*" OR "qualities" OR "quality attribute*" OR "quality measure*"
Comparison	QA measures (with respect to mobile ecosystems)	Test, testing, quality assurance, QA, verification, validation, V&V, functional, non-functional, NFR, qualities	"test*" OR "quality assurance" OR "QA" OR "verification" OR "validation" OR "verification and validation" OR "V&V" OR "functional" OR "non-functional" OR "NFR*" OR "qualities" OR "quality attribute*" OR "quality measure*"
Outcome	Efficient approach for verification and validation	Approach, method, methodology, strategy, process, test process, framework	"approach*" OR "method*" OR "methodology" OR "concept*" OR "strategy" OR "test strategy" OR "process*" OR "test process*" OR "framework*"
Context	Industrial context	industrial, ecosystem, industrial ecosystem, edge, edge ecosystem, software, software ecosystem, mobile, mobile ecosystem	"industrial" OR "ecosystem*" OR "industrial ecosystem*" OR "mobile*" OR "mobile ecosystem*" OR "iOS" OR "android" OR "edge" OR "edge ecosystem*"

Table 4

Search queries used to identify relevant studies		
Abbr.	Search string	Database
Q1	("3rd party" OR "third party") OR (application* OR app* OR mobile app*) AND (test* OR "quality assurance" OR verification OR validation) AND (approach* OR method* OR methodology OR concept* OR strategy OR process* OR framework*) AND (industrial OR ecosystem* OR "industrial ecosystem*" OR mobile* OR "mobile ecosystem*" OR iOS OR android OR edge OR "edge ecosystem*")	ACM arXiv
Q2	("3rd party" OR "third party") AND (application OR "edge application" OR "edge app*" OR "mobile application*" OR "mobile app*") AND (testing OR "quality assurance" OR "verification and validation") AND ("industrial ecosystem") Time range: 1994-2019	SpringerLink
Q3	(application OR app OR "edge application" OR "edge app" OR "mobile application" OR "mobile app") AND (testing OR "quality assurance" OR "verification validation") AND ("industrial ecosystem" OR "software ecosystem") Limit to: Computer Science, Engineering, Mathematics, Decision Science, Medicine Time range: 1994 – present	Scopus IEEEExplore
Q4	"third party" application "industrial application" testing validation software ecosystem "industrial ecosystem"	Google Scholar

E. CONDUCT SEARCH IN RESEARCH DATABASES

The systematic mapping process continues with the next process step, where the search string is used to conduct search for relevant publications in research databases. The search was applied to arXiv, ACM, Elsevier / Scopus, Google Scholar, IEEEExplore and Springer Link.

Since the databases use different search engines, it was not possible to use the exact same search string as defined in the previous step. As a result, the original search string was modified to preserve on the one hand its semantical meaning and to match on the other hand engine characteristics like maximum number of keywords, supported string notation or applicable search fields to name a few. In addition to the search strings in some of the digital libraries one is able to set further filters limiting the time frame of the publications or the discipline they address. Since, the concept of software ecosystems is relatively new [19], the time range of the search was set to consider publications published in the last 25 years. Table 4 provides an overview of the search query variations used with the corresponding research libraries.

Performing the search, 307 publications were found in the digital databases arXiv, ACM, Elsevier, Google Scholar, IEEEExplore and SpringerLink. In order to find papers remained unidentified by the search in research databases, exploratory search was performed in Google in addition to the systematic search. As a result, a total number of 328 publications were identified for this study. Table 5 shows a more detailed view on the search results by digital library and search query.

Table 5

List of digital libraries considered in the study			
Digital Library	URL	Search Query	Nr. of Papers
arXiv	arxiv.org	Q1	25
ACM	dl.acm.org	Q1	37
Scopus	www.elsevier.com	Q3	119
Google	www.google.com	n.a.	21
Google Scholar	scholar.google.com	Q4	7
IEEE Explore	ieeexplore.ieee.org	Q3	55
SpringerLink	link.springer.com	Q2	64
Total:			328

F. SCREENING PUBLICATIONS

In this step all identified primary studies are screened. This has a twofold sanitizing purpose: (i) removing from the hitlist duplicate records and (ii) removing records, which passed the search query, but are not relevant to answer the research question.

As first sanitizing step the hitlist with all 328 publications identified during the initial search was investigated for duplicate records. It revealed that 44 copies appeared in the hitlist of more than one digital library. The detected records were marked as duplicated and removed from the hitlist. In summary, a total number of 284 unique publications were taken qualified for further screening.

The second sanitizing step follows two basic criteria: for inclusion and exclusion. The inclusion of a study into the classification schema is based on the inclusion criteria

proposed by [16], which I found suitable for this study. Table 6 provides an overview of the inclusion rules:

Table 6

List of inclusion criteria	
Inclusion criteria	Rule Description
in1	Peer-reviewed studies published in journals, conferences and workshops
in2	Studies available in English or German
in3	Studies with full-text accessible electronically
in4	From title, abstract and keywords is evident that the publications are contributing to the research question.

The exclusion criteria aim to eliminate from the study duplicate records and records not contributing to the research question. Therefore, considered should be only publications (i) from the software engineering domain, (ii) discussion about applications from the ecosystem, cloud or edge computing domain (incl. third party code), (iii) dealing with testing and quality and (iv) addressing applications running on hardware devices. As given in Table 7 for every one of these aspects a corresponding exclusion rule is defined.

Table 7

List of exclusion criteria	
Exclusion criteria	Rule Description
ex1	Publication is not related to the software engineering discipline (e.g. publication deals with ecosystems in ecology context).
ex2	Publication is from the software engineering domain but has no relevance to (industrial) software ecosystems or cloud and edge computing.
ex3	The main contribution of the publication is not in the area of testing and quality assurance.
ex4	The publication deals with ecosystems, where the runtime environment of the applications has no hardware dependency.

The exclusion and inclusion criteria were applied on all abstracts and keywords of all records of the list with primary studies. In some cases, where it was not evident from the abstracts whether a publication was relevant or not, the criteria were applied based on the introduction and summary chapters. Further, publications whose full text was not able to be retrieved neither from the digital library, nor by searching on the internet or by contacting the authors, had to be removed from the list of relevant papers, so that the study is not bias by inaccurate classification.

After the second sanitization step of the primary studies, a total number of 232 of the 284 publications were removed from the list of publications for classification. In detail, 9 records were removed because they violated inclusion rule in1, 101 publications were removed during sanitization, because the full text was not available (in2), and it was not evident from the abstract if they contribute to the research

question. From the remaining 174 records, 13 were removed, because they were not related to the software engineering domain (exclusion criteria ex1). 85 publications were excluded because of ex2 and another 22 records, because of ex3. Only 2 publication was removed following ex4. At the end, 52 publications qualified for the next classification step.

G. KEYWORDING OF THE PUBLICATIONS

In the keywording step all relevant publications are thoroughly investigated and classified according to a classification schema. The schema itself is built towards the process proposed by Petersen [10]. In a nutshell the keywording is done by investigating the abstracts of the relevant publications and looking for keywords revealing the contribution of the paper. In the next step the keywords extracted from different papers are grouped together to develop a common understanding about the nature of the research and its contribution. The keywording process is depicted in Figure 2. Following these steps, a group of 6 facets was defined. These are shortly introduced in the remaining part of this section.

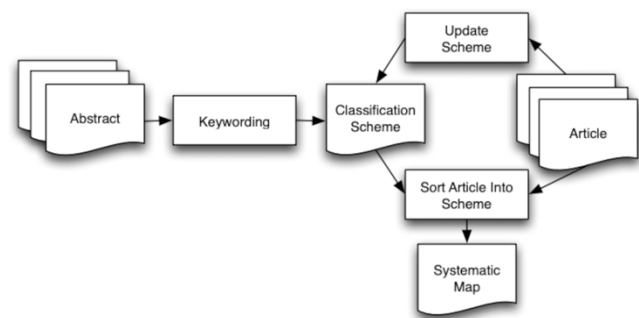


Fig. 2. Keywording schema [10]

Inspired by Wieringa et al. [20] every entry from the list of relevant studies was classified based on the types of research presented in Table 8. The “Publication type” facet shown in Table 9 classifies inspired by [21] the studies according to the way they were published. Since books were not in the scope of this study, no classification group for books and book chapters was defined for this facet. The “Contribution type” facet as given in Table 11 classifies the publications based on the type of their contribution to the research question. This classification is inspired by [22] and give insights how the research question was addressed by the identified studies. The “Focus area” facet as per Table 10 categorizes the studies towards the disciplines from the software engineering. It aims to provide information about how the contribution of the publications maps to software development phases like requirements engineering, architecture and design, development, testing and quality assurance. Security is a group of its own, because of the impact it has on software ecosystems and third-party applications. The categorization provided by this facet refers to the software engineering disciplines, where the majority of the quality assurance measures should be carried out according to the current state of research.

Table 8

Classification schema by Research type

Research type	Description
Evaluation research	Evaluates a problem or an implemented solution in practice incl. case studies, field studies & field experiments.
Validation research	Focuses on investigating a proposed solution (through mathematical analysis, experiments, simulations, prototypes).
Solution proposal	Novel or a significant extension to an existing technique.
Experience paper	Report on personal experiences and/or lessons learned from one or more real-life projects in the topic area.
Opinion Philos. paper	Everything else, which lacks preciseness, including but not limited to conceptual proposals of new ways of looking at things.

Table 9

Classification schema by Publication type

Publication type	Description
Journal	The study was published as an article in a journal
Dissertation	The study was published as a dissertation work
Conference Proceeding	The study was published as part of conference proceedings
Non-reviewed paper	The study was published as white paper, position paper, extended abstract or any other form of non-peer-reviewed work.

The “Domain” facet presented in Table 12 aims to classify the business area of the ecosystem targeted by the publications. It helps to put in a business context the contribution of the publications and to expose to what extend industrial ecosystems are subject of present research. The “Ecosystem aspect” facet as given in Table 13 categorizes the studies based on which technological part of the ecosystem they are mainly dealing with. This category observes how third-party applications are addressed in the current state of research.

H. DATA EXTRACTION AND VISUALIZATION

Once the keywording is finished and the classification scheme is in place, the actual data extraction takes place. Every relevant paper is classified following the classification scheme considering at least introduction and conclusion chapters. In some cases, where this was insufficient the complete paper was considered.

The data extracted in this step is visualized using pie charts, which provide an overview of the results per facet. Further, map charts were created to put the different facets in correlation and to provide more complete picture of the paper’s contributions with respect to the research question.

The results of this step are discussed in detail in Chapter IV of this publication.

Table 10

Classification schema by Focus area

Focus area	Description
Requirements	The publication whose main contribution is in the requirements engineering phase.
Architecture	Refers to publications addressing problems, methods and solution approaches carried out in the design and architecture phase
Development lifecycle	Refers to publications whose main contribution is to the development phase and the development lifecycle
Testing and Quality assurance	Refers to publications whose main contribution is on the QA and testing incl. test strategies, concepts, implementation, automation, execution, design, etc.
Deployment	Refers to publications whose main contribution lays in the deployment of software in the context of the topic
Security	Refers to publications, whose main contribution area is the security

Table 11

Classification schema by Contribution type

Contribution type	Description
Open issue, Problem	Discusses issues, open points, problems, that need to be addressed in the topic field
Method	Refers to descriptions (both general or detailed ones) of how to solve particular problem in the topic area
Tool	Refers to any tool support presented in the publications as main type of contribution
Process	Refers to detailed descriptions how to ensure the overall quality of a system, platform and / or application
Demonstrator, PoC	Refers to a demonstrator or proof-of-concept (PoC) showing off how a QA approach in the topic area would work
Metric	Refers to any description how to measure quality in the topic area
Classification	Proposes a classification, clustering or taxonomy of particular subarea of the topic area

Table 12

Classification schema by Ecosystem domain

Ecosystem domain	Description
Ecosystem	Refers to publications where the domain of the ecosystem is not specified
Mobile ecosystem	Refers to publications in mobile or telecommunications domain
Industrial ecosystem	Refers to publications in the industrial domain
IoT ecosystem	Refers to publications in the IoT domain
Other types of ecosystems	Refers to publications addressing any other type of ecosystems than the ones mentioned above
Other	The publication does not refer to a software ecosystem

Table 13

Classification schema by Ecosystem aspect

Ecosystem aspect	Description
Platform	The publication refers to issues and solution approaches targeting a platform (an ecosystem one or any other)
Applications and libraries	The publication discusses on applications and libraries without to distinguish if these are provided by third parties or not
Native contributions	The publication is focused on applications and libraries which are provided by the platform provider
Third-party contributions	The publication addresses third-party applications and / or libraries
Other types of ecosystems	Refers to publications addressing other ecosystem aspects than the ones mentioned above
Other	Refers to any other system as a context of the publication

I. REPORTING

In the last step of the systematic mapping process the results of the study are summarized in a report. Depending on the stakeholders and the audience, the report could be a formal document following a certain template or a more informal presentation for example.

IV. RESULTS

This chapter provides an overview of the results of this systematic mapping study by presenting the pie and map charts created during the data extraction and visualization step of the systematic process. Every pie chart stands for the categorization of the relevant studies according to the facets specified by the classification schema. The map charts on the other hand provide a correlated overview of several facets. Thus, they offer more complete view on the research area and on the results of this study.

The actual mapping of the identified publications can be seen in Table 14 to Table 17 as given in the appendix.

A. PIE CHARTS

As evident by Figure 3 almost one third of the relevant publications in the research area propose a method for quality assurance. Nearly half of the publications are focused on a tool or a framework dealing with a specific problem. Significant part of the publications discusses about problems or open issues in the research area, whereas only 7% propose a process for quality assurance. There are only a few papers talking about a demonstrator or a proof of concept in the research area. Based on that information we can conclude that the majority of the publications deal rather with isolated quality-related issues and challenges than with holistic quality assurance approach.

The results of the categorization according to the “Publication type” facet visualized by Figure 4 provide insights about the maturity of the relevant papers. Almost one third of the studies were published in journals and thus, had undertaken more thorough review process. Two thirds of the publications were issued in conference proceedings and underwent a slightly easier review process than compared to those of the journals. 2% of the relevant studies were carried out as dissertation work and the remaining publications did not undergo a peer reviewed process.

The categorization based on the type of research depicted in Figure 5 provides valuable information about the type of the contributions. The proportion between publications proposing a solution to a concrete problem and those reporting about a validation research is equal and forms more than two thirds of the relevant studies. Only 8% of the publications discuss about evaluation research, i.e. solutions proven in practice. No opinion or philosophical papers contributing to the research question were identified during this study.

From the data in Figure 6 can be seen that the majority of the relevant publications have the focus of their contribution on quality assurance measures with respect to security. This witnesses the importance of the security topic on industrial ecosystems and industrial third-party applications. Every fourth publication deals with quality assurance activities carried out in the test phase of the software development. Significant part publication discusses how quality assurance in industrial ecosystems can be achieved during the design and architecture phase. The remaining part of the identified studies deals with quality assurance measures in the development and deployment phase.

The results of the categorization based on the “Domain” facet shown in Figure 7 are not very surprising considering the wide adoption of mobile ecosystems in the last decade and the maturity of mobile ecosystems compared to industrial ones. 72% of the publications are focused on ecosystems in the mobile domain. Less than every 10th publication identified in this study addresses industrial, IoT or Edge ecosystems, which were the main focus of this study. 15% of the relevant papers report about other types of ecosystems and other 4% does not refer to an ecosystem.

The data shown in Figure 8 provides information about which component of an ecosystem is addressed by the quality measures suggested in the relevant papers. Most papers discuss about third-party contributions and another 7% discuss about contributions without distinguishing between third-party

and native contributions. Thus, third-party applications and libraries are recognized in the research community as a major topic of interest with respect to quality assurance in software ecosystems. 11% of the papers are focused on apps in particular. Significant part of the considered studies, almost every fourth of them, talks about QA measures carried out on ecosystem platform site, which means that quality in software ecosystems cannot be achieved only during application development, but it requires actions by the ecosystem providers, too.

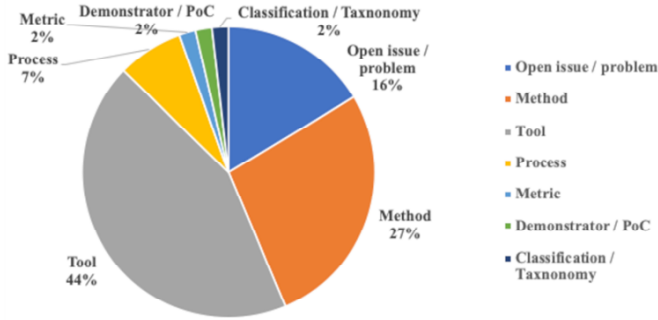


Fig. 3. Publications by Contribution type

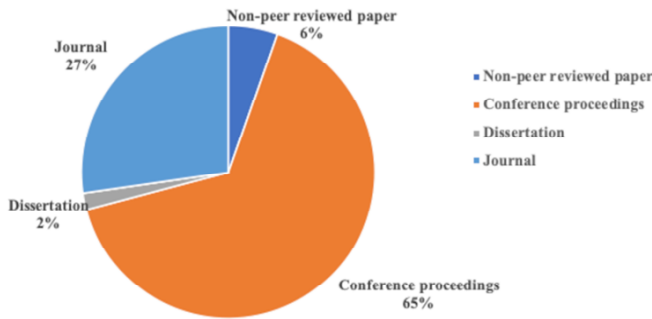


Fig. 4. Publications by Publication type

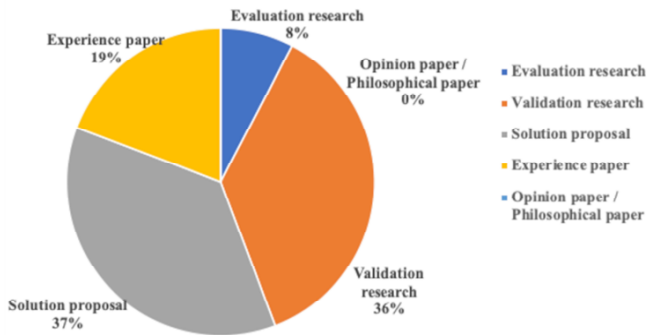


Fig. 5. Publications by Research type

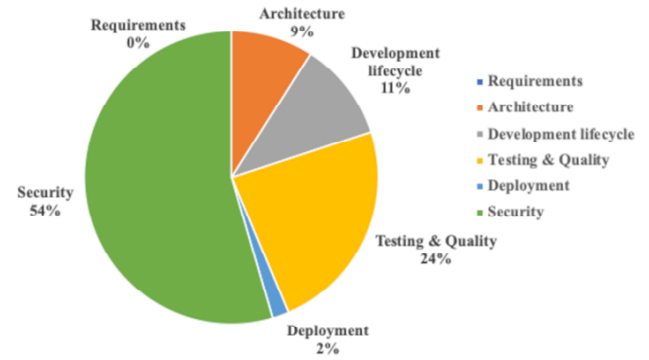


Fig. 6. Publications by Focus Area

The map chart shown in Figure 9 correlates the focus area of the relevant publications with their maturity based on the research and publication type of the studies. From this map chart is evident that Security is the most addressed topic by the identified publications and also the topic with the highest maturity level. The majority of the studies on this topic have high to medium maturity. On the other hand, Testing & Quality Assurance, is the second most targeted topic. Despite the fact that there are half as many studies discussing on quality assurance measures than on security, the maturity of the publications is rather high to medium. The percentual distribution of the papers focused on Testing & Quality Assurance in both facets is similar to the one of the Security-related papers.

Similar picture comes up, if we relate the focus of the publications and their contribution type as shown in Figure 10. Half of the publications focused on the Security topic have the focus of their contribution on a tool or a framework. Significant part of the remaining studies talks about methods ensuring the security of targeted object or about open issues and problem with respect to security. Similar is the distribution also for the publications focused on Testing & Quality Assurance. In both cases there are only a few publications proposing a process, reporting about a demonstrator or proof-of-concept (PoC) or introducing a classification or taxonomy.

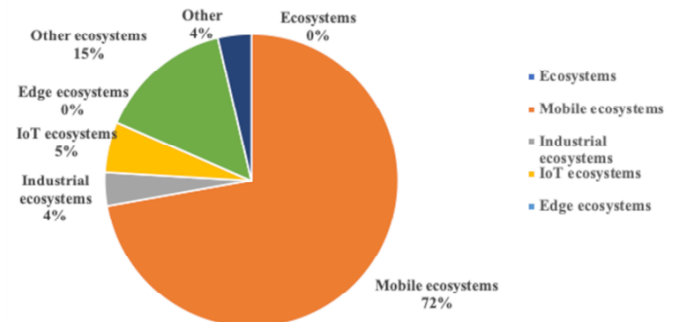


Fig. 7. Publications by Ecosystem domain

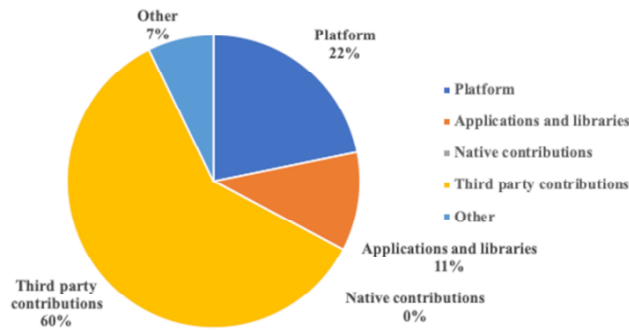


Fig. 8. Publications by Ecosystem aspect

B. MAP CHARTS

Fig. 11 provides insight information about the major topic of interest of this study. It shows a map chart of the publications from the industrial and IoT ecosystem domain. From the total number of 52 relevant publications, there are only 5 studies talking about industrial or IoT ecosystems or a combination of both. All remaining publications addressed the mobile ecosystem domain. The map chart below illustrates the aspects these papers aim to address based on their main focus. Only one single publication identified during this study targeted testing and quality assurance of apps in industrial or IoT ecosystem context. There were no papers identified, which explicitly targets the testing of third-party contributions.

The outcome of this study based on the information collected during the systematic process and on the charts visualizing the results will be presented in detail in the next chapter.

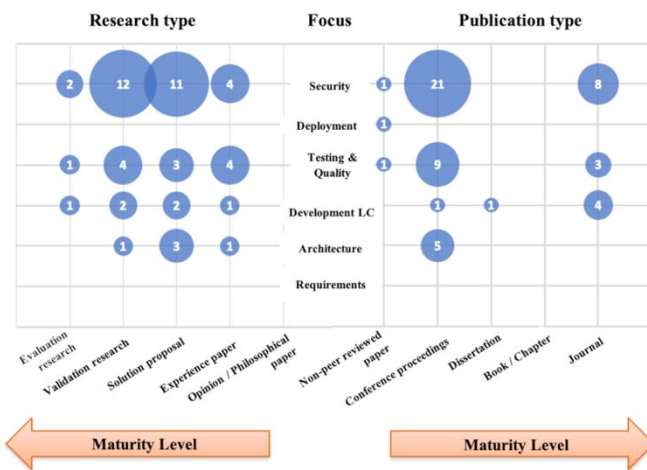


Fig. 9. Publications by Research type, Focus area and Publication type

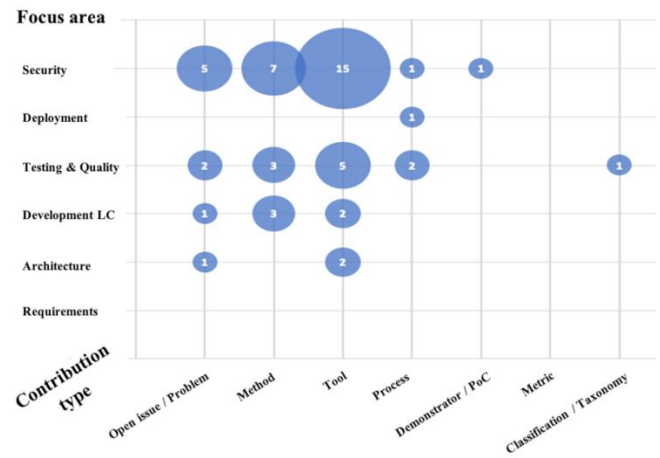


Fig. 10. Publications by Focus area and Contribution type

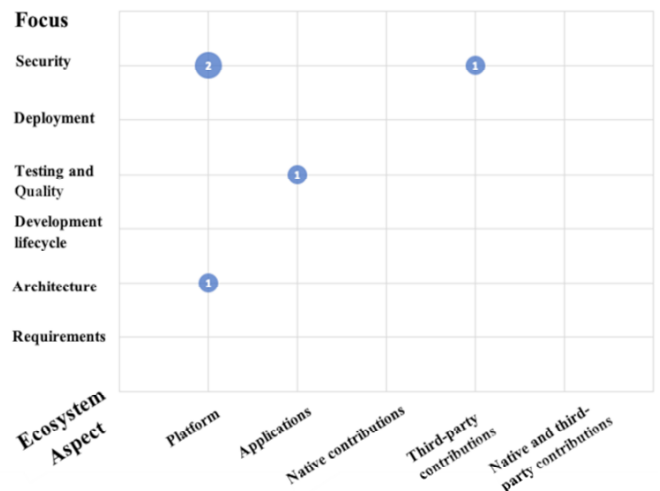


Fig. 11. Publications in the of industrial ecosystems by Focus area and Ecosystem aspect

V. MAIN FINDINGS AND TECHNICAL DIRECTIONS

The current chapter will provide a detailed summary of the major trends and findings identified during the study and will also point out the major technical directions of the relevant studies.

- Based on the number and the nature of the publications found in the research area, we can recognize the following trends with respect to the relevance and coverage of the research question:
- Number of publications is growing, which witnesses the relevance and importance of the research topic.
- Mobile ecosystems seem to be quite well-addressed, while industrial and edge ecosystems remain widely unexplored in the research community.
- Insufficient research in testing and quality of industrial applications
- Most scholars focus on security as main quality-related topic, while many other quality-oriented challenges lack of in-depth analysis or remain widely unaddressed.

Having all these trends in mind, it may be said that the verification and validation of industrial third party IoT applications is a growing topic, whose relevance from research point of view will increase in the next years. This assumption is proven by Figure 12, where the trendline depicted the growing number of relevant publications in recent years.

Furthermore, the results of the study indicate another set of trends and findings addressing the maturity of the proposed solutions:

- No (published) experience in verification and validation of industrial third-party applications
- There are many solution approaches addressing single challenges or issues, but there are no studies proposing a holistic approach for quality assurance in industrial software ecosystems with respect to third-party applications, neither are any best practices introduced.
- Lack of mature, standardized solutions suitable for industry domain

In summary, the results of the study show a need for industry-proven solutions in the research area. What's more, most of the relevant studies target concrete quality-related problems, but there is no alignment between them, so that they seem independent from each other. What's missing is a holistic approach, which proposes an orchestration of all measures necessary to ensure the quality in an industrial ecosystem with respect to third-party applications.

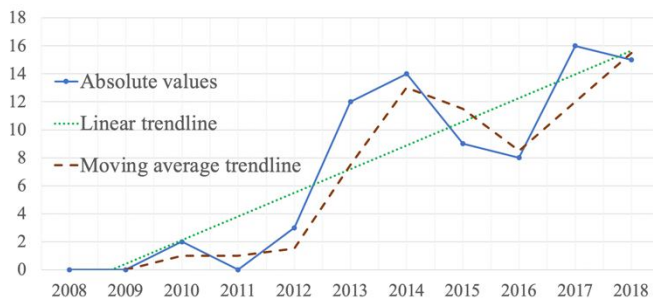


Fig. 12. Number of publications per year

VI. THREADS TO VALIDITY

The presented study is subject to threats with respect to research design, internal and conclusion validity. The results introduced in Chapter IV are valid only for the sample of publications considered in the study. It was essentially biased by a few criteria, which should be taken into account, when discussing the results of the study:

- As mentioned in Chapter III papers published before 1994 were not considered in the study. Since industrial software ecosystems, IoT and Industry 4.0 became popular terms in the last decade, I assume that the results will not be biased by considering publications published in the last 25 years. It is also noteworthy to say, that the screening for papers was carried out from November 2018 to April 2019. Publications published in research databases after that were not examined in this study.

- Books were excluded from during the screening for relevant studies, since the author of the study was not able to verify to what extend they underwent a thorough peer-review process. For the same reason invention disclosures were also not considered in this study. Nonetheless, patents and invention disclosures might help to bridge the gap between published and unpublished research and could be helpful to get more complete overview on the research area.
- During the screening for relevant publications, one has conducted systematic search in four digital libraries (s. Table 6) and in Google Scholar. Additionally, exploratory search was performed to find papers not published in scanned research databases. Despite this, it is still possible that relevant publications remained unidentified and thus, unconsidered by this study.
- The classification carried out during the systematic mapping process includes only publications, where the full text of the studies was available. The authors of publications with unavailable full text were contacted and were asked to provide, if possible, a full text copy of their work. However, not all authors were able due to legal or other reasons to provide full text copies of their papers. Thus, a subset of the papers identified during the screening were not considered during the classification step.

Threats to internal validity affect the data extraction conducted in the study. Since, there are no well-known best practices how to classify the relevant papers, neither there is an established taxonomy and terminology covering the research domain, it is possible that due to insufficient information or inaccurate presentation of the papers, some of them were not classified correctly.

The above-mentioned threats may have strong impact on the results of the study, which leads to threats to conclusion validity. Drawing conclusions based on the sample of publications considered and, on the classification, conducted in the study may be inaccurate, if one keeps in mind the treats to research design and internal validity.

VII. CONCLUSION AND FUTURE WORK

The research presented in this paper reports about a systematic mapping study conducted in the area of verification and validation of third-party IoT application in industrial software ecosystems. The main goal of the study was to provide a structured snapshot of the current state of research in the focus area, to identify potential gaps in the research area and to propose further research directions.

The study was conducted following a novel systematic research process combining two state of the art techniques in that area – the systematic mapping approach and the PICOC model for the definition of the research question. The process followed by this study work is the systematic definition of the search strings derived directly from the research question.

The results of my work revealed some interesting trends and findings in the research area. The number of publications in the targeted field is growing in the recent years, which

testifies the significance of the topic from research point of view. However, the majority of the identified papers focus mainly on mobile applications, leaving the industrial ones widely unaddressed. Another interesting takeaway is most scholars aim to solve security issues, while other quality-related aspects remain uncovered in depth. Based on the evaluation of the relevant papers identified by this study, I came to the conclusion that there is a lack of industry-proven solutions in the research area. Another gap I have identified is the absence of holistic approach addressing all challenges caused by third-party applications with respect to software quality in every corner of an industrial ecosystem.

In near future I aim to address these gaps by working on a holistic approach for quality assurance of industrial software ecosystems. It should consider all parties in the ecosystem, as well as the impact of third-party apps on the products involved in the ecosystem. Furthermore, I plan to work on concrete quality assurance measures to address the challenges raised by the use of third-party apps. I believe that the most challenging tasks are related to ensuring the testability of industrial third-party IoT apps, providing industrial-grade test environment for both simulation-based and hardware-based testing. The last step towards a state-of-the-art approach for quality assurance in an industrial ecosystem would be to provide testing as a service to the app developers in order to speed up the whole app development process.

APPENDIX

Table 16

Publication references in industrial and IoT ecosystem context by Focus area and Ecosystem aspect						
	References					
Security	[25], [48]–[51]	[28], [29], [40]–[42], [44], [45]	[23], [26], [37]–[39], [46], [47], [27], [30]–[36]	[28], [29], [40]–[42], [44], [45]	[24]	[43]
Deployment	-	-	-	[75]	-	-
Testing and Quality	[59], [62]	[55], [58], [77]	[52]–[54], [57], [60]	[56], [76]	-	[61]
Development lifecycle	[68]	[64], [66], [67]	[63], [65]	-	-	-
Architecture	[73]	[69], [72]	[70], [71]	-	-	-
Requirements	-	-	-	-	-	-
	Open issue / problem	Method	Tool	Process	Demonstr. / PoC	Classific. / Taxonomy

Table 17

Publication references by Focus area and Research type					
	References				
Security	[46], [48]	-	-	-	[47]
Deployment	-	-	-	-	-
Testing and Quality	-	[59]	-	-	-
Development lifecycle	-	-	-	-	-
Architecture	[69]	-	-	-	-
Requirements	-	-	-	-	-
	Platform	Applications and libraries	Native contributions	Third-party contributions	Other

Table 14

Publication references by Focus area and Research type					
	References				
Security	[23], [24],	[25]–[36]	[37]–[47]	[48]–[51]	-
Deployment	-	-	-	-	-
Testing and Quality	[51]	[52]–[55]	[56]–[58]	[59]–[61], [62]	-
Development lifecycle	[63]	[64], [65]	[66], [67]	[68]	-
Architecture	-	[69]	[70]–[72]	[73]	-
Requirements	-	-	-	-	-
	Evaluation research	Validation research	Solution proposal	Experience paper	Opinion paper / Philosophical paper

Table 15

Publication references by Focus area and Publication type					
	References				
Security	[74]	[23], [24], [26], [27]–[32], [34] [36], [38]–[42], [44], [47], [48], [50], [51],	-	[25], [33], [35], [37], [43], [45], [46], [49]	-
Deployment	[75]	-	-	-	-
Testing and Quality	[76]	[52]–[54], [57]–[59], [61], [62], [77]	-	[55], [56], [60]	-
Development lifecycle	-	[66]	[67]	[63]–[65], [68]	-
Architecture	-	[69]–[73]	-	-	-
Requirements	-	-	-	-	-
	Non-peer reviewed paper	Conference proceedings	Dissertation	Journal	

References

- [1] Federal Ministry for Economic Affairs and Energy, “What is Industry 4.0?,” 2019.
- [2] Fraunhofer, “Begriffsdefinitionen rund um Industrie 4.0,” Fraunhofer Institute, 2015.
- [3] “Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks,” ITU-T Y.2060, 2012.
- [4] D. Messerschmitt and C. A. Szyperki, Software Ecosystem: Understanding an Indispensable Technology and Industry. MIT Press, 2003.
- [5] J. Bosch; and P. Bosch-Sijsema, “Software Product Lines, Global Development and Ecosystems: Collaboration in Software Engineering,” in Collaborative Software Engineering, Springer Verlag, 2010.
- [6] S. Jansen, A. Finkelstein, and S. Brinkkemper, “A sense of community: A research agenda for software ecosystems,” 2009 31st Int. Conf. Softw. Eng. - Companion Vol. ICSE 2009, pp. 187–190, 2009.
- [7] K. Manikas and K. M. Hansen, “Software ecosystems-A systematic literature review,” J. Syst. Softw., vol. 86, no. 5, pp. 1294–1306, 2013.
- [8] S. Jansen, S. Brinkkemper, and A. Finkelstein, “Business network management as a survival strategy: A tale of two software ecosystems,” CEUR Workshop Proc., vol. 505, no. 2, pp. 34–48, 2009.
- [9] B. Kitchenham, “Guidelines for performing Systematic Literature Reviews in Software Engineering ppt,” 2001.
- [10] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, “Systematic Mapping Studies in Software Engineering,” in International Journal of Software Engineering & Knowledge Engineering, vol. 17, no. 1, pp. 33–55, 2008.
- [11] A. García-Holgado and F. J. García-Peñalvo, “Mapping the systematic literature studies about software ecosystems,” ACM Int. Conf. Proceeding Ser., 2018, pp. 910–918.

- [12] O. Barbosa and C. Alves, "A Systematic Mapping Study on Software Ecosystems through a Three-dimensional Perspective," in *Software Ecosystems: Analyzing and Managing Business Networks in the Software Industry*, Edward Elgar Publishing, 2013, pp. 59–81.
- [13] F. Fotrousi, S. A. Fricker, M. Fiedler, and F. Le-Gall, "KPIs for Software Ecosystems: A Systematic Mapping Study," in *Lecture Notes in Business Information Processing*, vol. 182 LNBIP, no. June, Springer, Cham, pp. 194–211, 2014.
- [14] A. Vegendla, A. N. Duc, S. Gao, and G. Sindre, "A Systematic Mapping Study on Requirements Engineering in Software Ecosystems," *J. Inf. Technol. Res.*, vol. 11, no. 1, pp. 49–69, 2018.
- [15] A. De Lima Fontao, R. P. Dos Santos, and A. C. Dias-Neto, "Mobile Software Ecosystem (MSECO): A Systematic Mapping Study," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 2, pp. 653–658, 2015.
- [16] A. (RWTH A. U. Wortmann and O. (Universite de R. Barais, "A Systematic Mapping Study on Modeling for Industry 4.0," in *2017 ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS)*, 2017.
- [17] S. Zein, N. Salleh, and J. Grundy, "A systematic mapping study of mobile application testing techniques," *J. Syst. Softw.*, vol. 117, no. Jul, pp. 334–356, 2016.
- [18] M. Petticrew and H. Roberts, "Systematic reviews – do they 'work' in informing decision-making around health inequalities?," *Heal. Econ. Policy Law*, vol. 3, no. 2, pp. 197–211, 2008.
- [19] M. Tsujimoto, Y. Kajikawa, J. Tomita, and Y. Matsumoto, "A review of the ecosystem concept — Towards coherent ecosystem design," *Technol. Forecast. Soc. Change*, vol. 136, no. December 2015, pp. 49–58, 2018.
- [20] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requir. Eng.*, vol. 11, no. 1, pp. 102–107, 2006.
- [21] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q. Manag. Inf. Syst.*, vol. 28, no. 1, pp. 75–105, 2004.
- [22] E. Engström and P. Runeson, "Software product line testing - A systematic mapping study," *Inf. Softw. Technol.*, vol. 53, no. 1, pp. 2–13, 2011.
- [23] A. Salman, I. H. Elhajj, A. Chehab, and A. Kayssi, "DAIDS: An architecture for modular mobile IDS," *Proc. - 2014 IEEE 28th Int. Conf. Adv. Inf. Netw. Appl. Work. IEEE WAINA 2014*, no. May, pp. 328–333, 2014.
- [24] A. Armando et al., "Mobile App Security Assessment with the MAVeriC Dynamic Analysis Module," no. January 2015, pp. 41–49, 2015.
- [25] D. Feng, W. Wang, J. Liu, X. Wang, X. Zhang, and Z. Han, "Exploring Permission-Induced Risk in Android Applications for Malicious Application Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 11, pp. 1869–1882, 2014.
- [26] G. Russello, A. B. Jimenez, H. Naderi, and W. van der Mark, "FireDroid," pp. 319–328, 2014.
- [27] R. Ando, Y. Takano, and S. Miwa, "An empirical study of third party APK's URL using scriptable API and fast identifier-specific filter," *2017 9th IEEE Int. Conf. Commun. Softw. Networks, ICCSN 2017*, vol. 2017-Janua, pp. 1501–1506, 2017.
- [28] A. Choliy, F. Li, and T. Gao, "Obfuscating function call topography to test structural malware detection against evasion attacks," *2017 Int. Conf. Comput. Netw. Commun. ICNC 2017*, pp. 808–813, 2017.
- [29] W. Li, J. Ge, and G. Dai, "Detecting Malware for Android Platform: An SVM-Based Approach," *Proc. - 2nd IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2015 - IEEE Int. Symp. Smart Cloud, IEEE SSC 2015*, no. January, pp. 464–469, 2016.
- [30] T.-H. Ho, D. Dean, X. Gu, and W. Enck, "PREC: Practical Root Exploit Containment for Android Devices," *Proc. 4th ACM Conf. Data Appl. Secur. Priv.*, pp. 187–198, 2014.
- [31] W. Yang, J. Li, Y. Zhang, Y. Li, J. Shu, and D. Gu, "APKLancet," no. June 2014, pp. 483–494, 2014.
- [32] W. Hu, D. Ocateau, P. D. McDaniel, and P. Liu, "Duet: Library Integrity Verification for Android Applications," *Proc. 2014 ACM Conf. Secur. Priv. Wirel. Mob. networks - WiSec '14*, pp. 141–152, 2014.
- [33] A. Martin, H. D. Menéndez, and D. Camacho, "MOCDroid: multi-objective evolutionary classifier for Android malware detection," *Soft Comput.*, vol. 21, no. 24, pp. 7405–7415, 2017.
- [34] S. Oberoi, W. Song, and A. M. Youssef, "AndroSAT: Security Analysis Tool for Android applications," *Secur. 2014 - 8th Int. Conf. Emerg. Secur. Information, Syst. Technol.*, no. c, pp. 124–131, 2014.
- [35] G. Bai et al., "Towards Model Checking Android Applications," *IEEE Trans. Softw. Eng.*, vol. 44, no. 6, pp. 595–612, 2018.
- [36] L. Onwuzurike, M. Almeida, E. Mariconti, J. Blackburn, G. Stringhini, and E. De Cristofaro, "A Family of Droids-Android Malware Detection via Behavioral Modeling: Static vs Dynamic Analysis," *2018 16th Annu. Conf. Privacy, Secur. Trust. PST 2018*, no. Pst, 2018.
- [37] L. Li et al., "On Locating Malicious Code in Piggybacked Android Apps," *J. Comput. Sci. Technol.*, vol. 32, no. 6, pp. 1108–1124, 2017.
- [38] G. Sarwar and O. Mehani, "On the Effectiveness of Dynamic Taint Analysis for Protecting against Private Information Leaks on Android-based Devices," no. July, pp. 461–468, 2013.
- [39] R. Johnson, Z. Wang, A. Stavrou, and J. Voas, "Exposing software security and availability risks for commercial mobile devices," *Proc. - Annu. Reliab. Maintainab. Symp.*, 2013.
- [40] M. Ghorbanzadeh, Y. Chen, Z. Ma, T. C. Clancy, and R. McGwier, "A neural network approach to category validation of Android applications," *2013 Int. Conf. Comput. Netw. Commun. ICNC 2013*, no. June 2015, pp. 740–744, 2013.
- [41] L. X. Min and Q. H. Cao, "Runtime-Based Behavior Dynamic Analysis System for Android Malware Detection," *Adv. Mater. Res.*, vol. 756–759, no. Iccia, pp. 2220–2225, 2013.
- [42] G.-H. Lai, Y.-H. Lee, T.-H. Chu, and T.-H. Cheng, "A Structure Similarity-based Approach to Malicious Android App Detection," *Pacis 2015 Proc.*, 2015.
- [43] Z. Han, Xinhui, Ding, Yijing; Wang, Dongqi; Li, Tonghin; Ye, "Android malicious AD threat analysis and detection techniques."
- [44] A. Hamed, H. Kaffel-Ben Ayed, and D. Machfar, "Assessment for Android apps permissions a proactive approach toward privacy risk," *2017 13th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2017*, no. October, pp. 1465–1470, 2017.
- [45] M. Li et al., "Large-scale Third-party Library Detection in Android Markets."
- [46] S. Siboni, V. Sachidananda, A. Shabtai, and Y. Elovici, "Security Testbed for the Internet of Things," 2016.
- [47] M. Nobakht, Y. Sui, A. Seneviratne, and W. Hu, "Permission Analysis of Health and Fitness Apps in IoT Programming Frameworks," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 533–538, 2018.
- [48] J. Hernández-Serrano et al., "On the road to secure and privacy-preserving IoT ecosystems," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10218 LNCS, pp. 107–122, 2017.

- [49] J. H. Jung, J. Y. Kim, H. C. Lee, and J. H. Yi, "Repackaging attack on android banking applications and its countermeasures," *Wirel. Pers. Commun.*, vol. 73, no. 4, pp. 1421–1437, 2013.
- [50] J. Cho, G. Cho, and H. Kim, "Keyboard or keylogger?: A security analysis of third-party keyboards on Android," 2015 13th Annu. Conf. Privacy, Secur. Trust. PST 2015, pp. 173–176, 2015.
- [51] E. Anthi and G. Theodorakopoulos, "Sensitive data in smartphone applications: Where does it go? Can it be intercepted?," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 239, pp. 301–319, 2018.
- [52] K. A. C. Faria, E. N. de A. Freitas, and A. M. R. Vincenzi, "Collaborative economy for testing cost reduction on Android ecosystem," no. December, pp. 11–18, 2017.
- [53] Y. Zhauniarovich, A. Philippov, O. Gadyatskaya, B. Crispo, and F. Massacci, "Towards black box testing of android apps," *Proc. - 10th Int. Conf. Availability, Reliab. Secur. ARES 2015*, no. November, pp. 501–510, 2015.
- [54] B. Deka, Z. Huang, C. Franzen, J. Nichols, Y. Li, and R. Kumar, "Zipt," pp. 727–736, 2017.
- [55] M. Arzetti, C. Ardagna, E. Damiani, and F. Gaudenzi, "A semi-automatic and trustworthy scheme for continuous cloud service certification," *IEEE Trans. Serv. Comput.*, vol. 1374, no. c, pp. 1–1, 2017.
- [56] A. Immonen, E. Ovaska, and T. Paaso, "Towards certified open data in digital service ecosystems," *Softw. Qual. J.*, vol. 26, no. 4, pp. 1257–1297, 2018.
- [57] Y. Falcone, S. Currea, and M. Jaber, "Runtime verification and enforcement for android applications with RV-droid," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7687 LNCS, pp. 88–95, 2013.
- [58] A. Avancini and M. Ceccato, "Security testing of the communication among Android applications," 2013 8th Int. Work. Autom. Softw. Test, AST 2013 - Proc., no. November 2017, pp. 57–63, 2013.
- [59] L. Antão, R. Pinto, J. Reis, and G. Gonçalves, "Requirements for testing and validating the industrial internet of things," *Proc. - 2018 IEEE 11th Int. Conf. Softw. Testing, Verif. Valid. Work. ICSTW 2018*, no. April, pp. 110–115, 2018.
- [60] A. F. Cattoni et al., "An end-to-end testing ecosystem for 5G the TRIANGLE testing house test bed," *J. Green Eng.*, vol. 6, no. 3, pp. 285–316, 2016.
- [61] L. Gazzola, L. Mariani, F. Pastore, and M. Pezze, "An Exploratory Study of Field Failures," *Proc. - Int. Symp. Softw. Reliab. Eng. ISSRE*, vol. 2017-Octob, pp. 67–77, 2017.
- [62] S. Thorve, C. Sreshtha, and N. Meng, "An empirical study of flaky tests in android apps," *Proc. - 2018 IEEE Int. Conf. Softw. Maint. Evol. ICSME 2018*, pp. 534–538, 2018.
- [63] S. Hyrynsalmi, M. Seppänen, and A. Suominen, "Sources of value in application ecosystems," *J. Syst. Softw.*, vol. 96, no. October, pp. 61–72, 2014.
- [64] A. Benlian, D. Hilkert, and T. Hess, "How open is this platform? The meaning and measurement of platform openness from the complementors' perspective," *J. Inf. Technol.*, vol. 30, no. 3, pp. 209–228, 2015.
- [65] L. O. Colombo-Mendoza, G. Alor-Hernández, A. Rodríguez-González, and R. Valencia-García, "MobiCloUP!: A PaaS for cloud services-based mobile applications," *Autom. Softw. Eng.*, vol. 21, no. 3, pp. 391–437, 2014.
- [66] C. Stritzke, C. Priesterjahn, and P. A. A. Gutiérrez, "Towards a Method for End-to-End SDN App Development," *Proc. - Eur. Work. Softw. Defin. Networks, EWSDN*, pp. 107–108, 2015.
- [67] M. Song, "Supporting Effective Reuse and Safe Evolution in Metadata-Driven Software Development," 2013.
- [68] N. Bidargaddi, Y. Van Kasteren, P. Musiat, and M. Kidd, "Developing a third-party analytics application using Australia's national personal health records system: Case study," *J. Med. Internet Res.*, vol. 20, no. 4, pp. 1–17, 2018.
- [69] I. Cabral, P. Espadinha-Cruz, A. Grilo, A. Gonçalves-Coelho, and A. Mourão, "A methodology for designing an interoperable industrial ecosystems, using the axiomatic design theory," *IEEE Int. Conf. Ind. Eng. Eng. Manag.*, 2014, pp. 1324–1328.
- [70] P. Arjunan, N. Batra, H. Choi, and A. Singh, "SensorAct: A Privacy and Security Aware Federated Middleware for Building Management", *Proc. in BuildSys*, 2012, pp. 80–87.
- [71] N. M. Tiwari, G. Upadhyaya, H. A. Nguyen and H. Rajan, "Candoia: A Platform for Building and Sharing Mining Software Repositories Tools as Apps," 2017 IEEE/ACM 14th International Conference on Mining Software Repositories (MSR), Buenos Aires, 2017, pp. 53–63, doi: 10.1109/MSR.2017.56.
- [72] Y. Yan Wang and Atanas Rountev, "Who changed you? obfuscator identification for Android," *Proc. in MOBILESoft*, 2017, pp. 154–164, doi:https://doi.org/10.1109/MOBILESoft.2017.18.
- [73] W. Ahmad, C. Kästner, J. Sunshine, and J. Aldrich, "Inter-app communication in Android," 2016, pp. 177–188.
- [74] Apple Inc., "iOS Security iOS 12," White Paper, no. September, 2018, p. 93.
- [75] "The Step-By-Step Guide to App Store Submission and Optimization," Clearbridge Mobile, 2015.
- [76] Apple, "iOS Lifecycle Management Contents," 2017, pp. 1–18.
- [77] J. Shimagaki, Y. Kamei, N. Ubayashi, and A. Hindle, "Automatic topic classification of test cases using text mining at an Android smartphone vendor," 2018, pp. 1–10.



Ivan Tritchkov received in 2011 from the Friedrich-Alexander University of Erlangen and Nuremberg in Germany a Ms.S. degree in information and communication technologies with focus on mobile communications and transmission technology.

He started his professional career in 2012 at Siemens Corporate Technology as test automation engineer and research scientist for software testing and quality. In the next years he worked on various projects in the rail automation domain. Since 2015 he has been working as test architect in industry domain. In 2018 he became portfolio manager at Siemens for research and innovations in the area of quality engineering. His current research interests and latest professional experience include software verification and validation of industrial-grade edge and IoT devices, quality assurance of industrial applications and third-party contributions, as well as quality engineering of industrial data. He is a certified test architect and certified iSTQB test manager. Mr. Tritchkov holds several patents in the software testing area.