



**UNIVERSIDADE FEDERAL DO CEARÁ**  
**CAMPUS DE RUSSAS**  
**CURSO DE GRADUAÇÃO EM ENGENHARIA DE SOFTWARE**

**LIANA MARA CARVALHO DE MENEZES**

**UM MAPEAMENTO SISTEMÁTICO SOBRE TESTES EM APLICAÇÕES IOT**

**RUSSAS**  
**2018**

LIANA MARA CARVALHO DE MENEZES

UM MAPEAMENTO SISTEMÁTICO SOBRE TESTES EM APLICAÇÕES IOT

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Software.

Orientadora: Profa. Dra. Valéria Lelli Leitão Dantas.

RUSSAS  
2018

Dados Internacionais de Catalogação na Publicação  
Universidade Federal do Ceará  
Biblioteca Universitária

Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

---

M511m Menezes, Liana Mara Carvalho de.  
Um Mapeamento Sistemático de Testes para Aplicações IoT / Liana Mara Carvalho de Menezes. – 2018.  
83 f. : il. color.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Russas,  
Curso de Engenharia de Software, Russas, 2018.  
Orientação: Profª. Dra. Valéria Lelli Leitão Dantas.

1. Internet das Coisas. 2. Testes. 3. Sistemas de Sistemas. 4. Mapeamento Sistemático. I. Título.  
CDD 005.1

---

LIANA MARA CARVALHO DE MENEZES

UM MAPEAMENTO SISTEMÁTICO DE TESTES PARA APLICAÇÕES IOT

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Engenharia de Software do Campus de Russas da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Engenharia de Software.

Aprovada em:

BANCA EXAMINADORA

---

Profa. Dra. Valéria Lelli Leitão Dantas (Orientadora)  
Universidade Federal do Ceará (UFC)

---

Profa. Dra. Anna Beatriz dos Santos Marques  
Universidade Federal do Ceará (UFC)

---

Profa. Dra. Marília Soares Mendes  
Universidade Federal do Ceará (UFC)

À minha mãe que nunca mediu esforços na  
realização dos meus sonhos, sua força me deu  
coragem para seguir.

## **AGRADECIMENTOS**

À Deus pela Sua presença constante em minha vida, por conduzir-me sempre aos melhores caminhos e por suas orientações e incentivos. A Ele meus eternos agradecimentos.

À minha família, principalmente, a minha mãe, Silvia Carvalho e ao meu pai, Washington de Menezes, que sempre se fizeram presentes nessa trajetória, auxiliando-me em todos os momentos. Amo vocês.

À minha orientadora Valéria Lelli, por todo incentivo, esforço e empenho dedicado a este trabalho, muito obrigada.

Aos amigos que o âmbito acadêmico me proporcionou, Lavínia Matoso e Alex Felipe, obrigada por me fornecerem, diariamente, ânimo nesta caminhada.

Agradeço a todos os professores da Universidade Federal do Ceará (UFC) - Campus Russas, por fazerem destes anos uma experiência incrível de muito aprendizado, obrigada por me proporcionarem mais que um ambiente de estudo, mas um ambiente de companheirismo e troca de conhecimento, vocês são completamente responsáveis por esta conquista.

E ao Laboratório Interdisciplinar de Ciência da Computação e Engenharia de Software (LINCE) por fornecer as ferramentas para os primeiros passos na pesquisa, muito obrigada.

“Digo e repito: Seja forte e corajoso! Nada de desânimo! Não fique com medo! Lembre-se bem: o Senhor seu Deus está com você, esteja onde estiver!”

(Josué 1:9, Bíblia Viva)

## RESUMO

A internet das coisas (IoT) está se difundindo rapidamente devido ao fácil acesso à internet e aos grandes desafios que estão sendo levantados pela comunidade de pesquisa. As aplicações IoT possuem diversas peculiaridades em sua construção, são objetos inteligentes (*smart objects*) que se conectam por diferentes canais com o ser humano ou com eles mesmos, possuem diferentes arquiteturas, diferentes interfaces, diferentes funções, estão inseridos em contextos diferentes, podem tomar suas próprias decisões de forma autônoma e fornecer diferentes serviços. Visto que os sistemas IoT possuem diversas peculiaridades, testar essas aplicações se torna algo complexo, são necessárias abordagens, metodologias específicas para a realização dos testes. Deste modo, este trabalho propõe caracterizar o estado da arte dos testes em aplicações IoT por meio de um mapeamento sistemático. Este mapeamento tem por objetivo levantar as abordagens usadas nos testes de aplicações IoT e os principais desafios encontrados nesses testes. Foram levantados 25 estudos que abordam as questões de pesquisas definidas neste trabalho. Dentre esses estudos foram encontradas abordagens que tinham mais foco em testes baseados em modelos, construção de plataformas e ferramentas para o auxílio dos testes. Dentre os principais desafios encontrados, o teste de segurança de aplicações IoT e o tratamento da interoperabilidade presentes nessas aplicações foram os mais abordados na literatura. Através deste mapeamento também se observou esforços, principalmente, nesses últimos anos, em propor abordagens para testar aplicações IoT, porém, ainda não há consenso na comunidade sobre os melhores processos, metodologias, ferramentas a serem adotados.

**Palavras-chave:** Internet das Coisas. Testes. Sistemas de Sistemas. Mapeamento Sistemático.



## ABSTRACT

The Internet of Things (IoT) is spreading rapidly due to easy access to the internet and the major challenges being raised by the research community. IoT applications have many peculiarities in their construction, they are smart objects that connect through different channels with humans or with themselves, they have different architectures, different interfaces, different functions, they are inserted in different contexts, they can make their own decisions autonomously and provide different services. Because the IoT systems have several peculiarities, testing these applications becomes complex, specific approaches and methodologies are necessary to perform the tests. Therefore, this work proposes to characterize the state of the art of the tests in IoT applications through a systematic mapping. This mapping aims to find the approaches used in the IoT application tests and the main challenges encountered in these tests. Twenty-five papers that address the research questions defined in this paper were selected. Among these papers, we found for aiding testing that had more focus on model-based testing, construction of platforms and tools for the aid of the tests. Among the main challenges for the IoT applications testing, the security and the interoperability are the most discussed in the literature. Through this mapping, we have also observed efforts in the last few years to propose approaches for testing IoT applications, but there is still no consensus in the community about the best processes, methodologies and tools to be adopted.

**Keywords:** Internet of Things. Software Testing. Systems of Systems. Systematic Mapping.

## LISTA DE FIGURAS

<b>Figura 1</b> - Internet das Coisas	<b>22</b>
<b>Figura 2</b> – Processo de Mapeamento Sistemático	<b>28</b>
<b>Figura 3</b> - Processo de seleção dos estudos	<b>34</b>
<b>Figura 4</b> - Autores por Países	<b>48</b>
<b>Figura 5</b> - Nuvem de Palavras	<b>49</b>

## LISTA DE TABELAS

<b>Tabela 1</b> - Semelhanças e Diferenças com os Trabalhos Relacionados	<b>18</b>
<b>Tabela 2</b> - Estudos de Controle	<b>29</b>
<b>Tabela 3</b> - Estudos totais de acordo com a base	<b>35</b>
<b>Tabela 4</b> - Estudos Finais	<b>35</b>
<b>Tabela 5</b> - Abordagens para testes de IoT	<b>41</b>
<b>Tabela 6</b> - Estudos que continha Estudos de Casos e Experimentos	<b>42</b>
<b>Tabela 7</b> - Desafios na área de IoT	<b>42</b>
<b>Tabela 8</b> - Relação entre Características IoT e os Desafios levantados	<b>44</b>
<b>Tabela 9</b> - Características IoT críticas para o processo de teste	<b>45</b>

## **LISTA DE GRÁFICOS**

<b>Gráfico 1</b> - Estudos selecionados distribuídos por base de dados	<b>46</b>
<b>Gráfico 2</b> - Estudos publicados por ano	<b>46</b>
<b>Gráfico 3</b> - Estudos que apresentaram estudos de caso	<b>47</b>
<b>Gráfico 4</b> - Estudos que apresentaram experimentos	<b>48</b>

## LISTA DE ABREVIATURAS E SIGLAS

<b><i>BLE</i></b>	<i>Bluetooth Low Energy</i>
<b><i>DDoS</i></b>	<i>Distributed denial-of-service attack</i>
<b><i>ES</i></b>	<i>Engenharia de Software</i>
<b><i>IoT</i></b>	<i>Internet of Things</i>
<b><i>LINCE</i></b>	<i>Laboratório Interdisciplinar de Ciência da Computação e Engenharia de Software</i>
<b><i>MS</i></b>	<i>Mapeamento Sistemático</i>
<b><i>RS</i></b>	<i>Revisão Sistemática</i>
<b><i>SoS</i></b>	<i>Systems of Systems</i>
<b><i>TBM</i></b>	<i>Teste Baseado em Modelos</i>
<b><i>UFC</i></b>	<i>Universidade Federal do Ceará</i>
<b><i>V&amp;V</i></b>	<i>Verificação e Validação</i>

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>15</b>
<b>2</b>	<b>TRABALHOS RELACIONADOS</b>	<b>17</b>
<b>3</b>	<b>OBJETIVOS</b>	<b>20</b>
3.1	Objetivo geral	20
3.2	Objetivos específicos	20
<b>4</b>	<b>FUNDAMENTAÇÃO TEÓRICA</b>	<b>21</b>
4.1	Internet das Coisas (IoT)	21
4.2	Testes de Software	23
4.3	Mapeamento Sistemático	25
<b>5</b>	<b>METODOLOGIA</b>	<b>28</b>
5.1	Planejamento	28
5.2	Condução	33
5.3	Resultados	39
<b>6</b>	<b>RESULTADOS E ANÁLISE DO MAPEAMENTO</b>	<b>40</b>
6.1	Estudos por base de dados	45
6.2	Estudos publicados por Ano	46
6.3	Tipos de publicações e avaliações	47
6.4	Autores por País	48
6.5	Nuvem de Palavras	49
6.6	Ameaças à validade do mapeamento	49
<b>7</b>	<b>CONCLUSÃO</b>	<b>51</b>
	<b>REFERÊNCIAS</b>	<b>54</b>
	<b>APÊNDICE A</b>	<b>62</b>
	<b>APÊNDICE B</b>	<b>64</b>
	<b>APÊNDICE C</b>	<b>65</b>
	<b>APÊNDICE D</b>	<b>81</b>

## 1 - INTRODUÇÃO

Com a ascensão da Internet, novas aplicações estão sendo criadas, parte desse avanço se dá pelo favorecimento proporcionado pela evolução da banda larga, que está se tornando mais rápida e de fácil acesso como afirma Razzaque et al. (2016). Todo esse crescimento fomenta a indústria na criação de novos dispositivos que se conectam mais facilmente à rede, com isso passou-se a ouvir, a partir, de 1999, o termo Internet das Coisas (IoT). De acordo com L. Patel e M. Patel (2016) a Internet das Coisas é um paradigma onde diversos dispositivos são conectados à internet e impulsionados a fornecer serviços.

A conectividade de diversos dispositivos por meio da internet já é vista atualmente através de computadores, videogames, *smartphones* etc., porém, através do paradigma IoT é possível elevar essa conectividade não apenas a dispositivos que já usam comumente a internet, mas sim a outros, por exemplo, eletrodomésticos como geladeiras em que poderiam possuir um painel em sua porta onde informaria os alimentos que estão em falta e até mesmo apresentar os preços desses produtos.

O Instituto SENAI de Inovação para Tecnologias da Informação e Comunicação (ISI-TICs) apresentou em seu trabalho *A Internet das Coisas na Indústria: A criação de novos modelos de negócios a partir da transformação da interação entre consumidor, produto e indústria* (2018) que em 2017, 19% das empresas brasileiras abordadas na pesquisa estavam interessadas em implantar algum projeto na área de IoT, em 2018 esse percentual atingiu 23%.

Atualmente, existem várias iniciativas tanto nacionais quanto internacionais voltadas para a inteligência urbana. O Grupo *Planet Idea* (*Planet Idea*, 2018) desde 2015 iniciou o projeto da construção da primeira cidade inteligente (*smart city*) do Ceará e no início do ano de 2018 iniciaram as vendas das primeiras casas. A cidade seria (*Smart City Laguna*, 2018) toda gerenciada por meio de um aplicativo (*Planet App*) onde o morador poderá controlar seus gastos e habilitar, quando necessário, a função SOS<sup>1</sup>, código universal de socorro criado em 1906 (Moreno, 2007), configurando telefones para casos emergenciais. Por exemplo, ao gravar mensagens de ajuda no telefone, o aplicativo automaticamente localizaria o usuário e enviaria essa informação para que um amigo pudesse ajudá-lo. Além disso, funcionaria como um aplicativo de interação entre todos os moradores da *smart city*. Dessa forma é possível vislumbrar as diversas aplicações e assim o crescimento do paradigma IoT incitando um maior domínio sobre tais assuntos para destinar esforços aos reais desafios presentes na área.

---

<sup>1</sup> Código universal de socorro criado em 1906 quando as comunicações eram feitas principalmente em código morse

A construção de uma aplicação IoT adota processos comumente utilizados na concepção de um software tradicional. Considerando as fases típicas do ciclo de vida de um software e suas atividades, alguns trabalhos na área de IoT como o trabalho de Maia et al. (2014) e Razzaque et al. (2016) exploram problemas enfrentados na fase de desenvolvimento e na arquitetura, respectivamente. Por outro lado, outros trabalhos como o trabalho de Marwah, Mateen e Sirshar (2015) dão ênfase na qualidade do produto. Alguns estudos são mais gerais como o trabalho de Reetz et al. (2013) e Rosenkranz et al. (2015) que abordam os diversos desafios encontrados no desenvolvimento de aplicações IoT. Dentre os desafios, os autores destacam a problemática em testar aplicações IoT.

Embora IoT esteja sendo bastante explorada tanto na academia como na indústria, não há estudos que identifiquem e avaliem quais abordagens são, por exemplo, utilizadas para testar aplicações IoT. Dessa forma, observando as oportunidades e desafios enfrentados no desenvolvimento de aplicações IoT torna-se fundamental uma visão sobre o estado da arte com o intuito de que pesquisas possam ser direcionadas de maneira mais efetiva.

Nesse contexto, o processo de mapeamento sistemático visa reunir estudos sobre uma área específica para fornecer uma visão geral sobre a mesma (Kitchenham e Charters, 2007). Tendo em vista que a etapa de teste é essencial na construção de um software de qualidade e que esta pode ser crítica para aplicações IoT, este trabalho propõe um mapeamento sistemático que busca encontrar os desafios no teste de aplicações IoT bem como as abordagens de testes usadas nessas aplicações. Este trabalho tem por objetivo responder às seguintes questões de pesquisa:

- Q1: Quais as abordagens utilizadas para testar aplicações IoT?
- Q2: Quais são os desafios encontrados nos testes de aplicações IoT?
- Q3: Quais são as características de aplicações IOT mais críticas para o processo de teste?

A estrutura deste trabalho consistirá da seguinte forma: na seção de Trabalhos Relacionados serão apresentados estudos que de algum forma se relacionaram com o trabalho em questão, na seção de Objetivos é apresentada o objetivo principal e específicos deste trabalho, na seção de Fundamentação Teórica são apresentados os principais termos usados para a compreensão deste trabalho, na seção de Metodologia é apresentada a execução do mapeamento sistemático, na seção de Resultados e Análises do Mapeamento são apresentados dados relevantes que foram levantados no decorrer do mapeamento inclusive as respostas às questões de pesquisa deste trabalho e então a seção de Conclusão.



## **2 - TRABALHOS RELACIONADOS**

Os trabalhos apresentados nessa Seção estão relacionados a IoT, mapeamento sistemático, testes e Sistemas de Sistemas (SoS). SoS compreendem um conjunto generalizados de sistemas que podem ser fundamentados sobre paradigma IoT (Maia et al., 2014), caso haja a relação entre ambos então as características presentes em aplicações IoT também serão características de SoS, como interconectividade, heterogeneidade, grandes escalas entre outras (L. Patel e M. Patel, 2016). Neste trabalho, também serão considerados os estudos que apresentem SoS fundamentados no paradigma IoT.

### **2.1 - Desafios no teste de SoS**

Dahmann, Lane e Rebovich (2010) apresentam algumas características que dificultam a realização de testes em Sistemas de Sistemas, além de apresentar os desafios presentes nessa área e sugerir estratégias. O trabalho trata diretamente de Sistemas de Sistemas e não oferece um mapeamento sistemático como metodologia, mas sim a partir de um estudo bibliográfico simples são levantados os desafios encontrados. Apesar do mesmo referir-se a Sistemas de Sistemas (SoS) e relacioná-lo a o paradigma IoT, não é dado uma maior ênfase ao paradigma. Além disso, por não se tratar de um estudo aprofundado da literatura, como uma revisão sistemática ou um mapeamento, os desafios encontrados em testar tais aplicações são apresentados de maneira superficial, sem haver um detalhamento que um mapeamento sistemático se propõe a realizar.

### **2.2 - Estado da Arte de SoS**

Nakagawa et al. (2013) apresentam o estado da arte de Sistemas de Sistemas voltado para a arquitetura do software. No trabalho é dada a perspectiva dos desafios que se encontra na área da arquitetura de Sistemas de Sistemas assim como são apresentadas as arquiteturas existentes. A semelhança encontrada neste trabalho está voltada para a apresentação do estado da arte de Sistemas de Sistemas, porém, esse estado se volta para a arquitetura. Assim como foi relatado acima, conceitualmente Sistemas de Sistemas (SoS) tem uma proximidade com aplicações IoT, porém, não é possível tomar os mesmos desafios existentes na área de SoS para a área de IoT. Além disso, o trabalho não apresenta uma metodologia baseada em um mapeamento sistemático o que difere do trabalho que está sendo proposto.

### 2.3 - Desenvolvimento de aplicações IoT

Maia et al. (2014) apresentam a proposta de um mapeamento sistemático para o desenvolvimento de Sistemas de Sistemas baseados em um paradigma IoT. O estudo se desenvolve a partir de aplicações que foram construídas por meio da Internet das Coisas. Os autores definem um protocolo de mapeamento sistemático, onde através do mesmo é possível obter o resultado de aplicações SoS que foram construídas nos últimos anos, tais resultados são categorizados de acordo com as características propostas pelos autores e deste modo é possível ter uma visão do estado da arte no desenvolvimento de aplicações SoS baseados em IoT. Apesar da proximidade entre aplicações SoS e aplicações IoT ainda assim o enfoque do trabalho não trata exclusivamente de aplicações IoT, além de não relatar sobre processos de teste que são realizados na construção de tais aplicações, frisando apenas a etapa de desenvolvimento.

### 2.4 - IoT de código aberto

Tang et al. (2017) apresentam os desafios existentes para testes de sistemas de código aberto de aplicações IoT. Os autores não realizam um estudo de mapeamento sistemático para apresentação do trabalho, apenas é feito um estudo simples da literatura onde são levantados alguns trabalhos que apresentam os desafios nos testes de aplicações IoT em softwares de código aberto, logo o estado da arte apresentado no trabalho relaciona-se aos resultados obtidos em seus estudos bibliográficos. Apesar de tratar de testes, o trabalho destina-se apenas a aplicações de código aberto, além do mais como foi dito acima, não é adotado uma metodologia de mapeamento sistemático, impossibilitando assim uma visão mais ampla do estado da arte.

### 2.5 - Comparativo

Abaixo é apresentado uma Tabela 1 de semelhança e diferenças entre os trabalhos relacionados e este trabalho.

**Tabela 1** - Semelhanças e Diferenças com os Trabalhos Relacionados

ID	Título	Autor	Semelhanças	Diferenças
1	<i>Systems of systems test and evaluation challenges</i>	Dr. Judith Dahmann, Dr. Jo Ann Lane, George Rebovich, Ralph Lowry	O trabalho apresenta abordagem de testes para SoS	Não é seguido uma metodologia que possa ser replicada por outro pesquisador, além disso não é

				tratado de sistemas IoT
2	<i>The state of the art and future perspectives in systems of systems software architectures</i>	Elisa Y. Nakagawa , Marcelo Gonçalves, Milena Guessi, Lucas B. R. Oliveira , Flavio Oquendo	São levantados desafios em arquitetura de SoS, inclusive nos testes das arquiteturas desses sistemas.	São apresentados apenas desafios voltados a SoS.
3	<i>On the development of systems-of-systems based on the Internet of Things</i>	Maia,P., Cavalcante, E., Gomes, P., Batista, T., Delicato, F.C., Pires, P.F.	Um mapeamento sistemático sobre aplicações IoT e SoS	Tem um maior foco na etapa de desenvolvimento dessas aplicações
4	<i>Quantifying Cloud Elasticity with Container-Based Autoscaling</i>	X. Tang, F. Zhang, X. Li, S. U. Khan and Z. Li	Apresenta os desafios existentes nos testes de sistemas IoT de código aberto.	Restringe apenas a sistemas IoT de código aberto, além de não ser seguida uma metodologia que possa ser replicada por outro pesquisador.

**Fonte:** a autora.

Diferentemente dos trabalhos apresentados na Tabela 1, este trabalho tem foco em apresentar os desafios existentes nos testes de aplicações IoT e de SoS que estão pautados no paradigma IoT, para o levantamento desses desafios é usado um mapeamento sistemático, metodologia esta que permite replicação por outros pesquisadores.

### **3 - OBJETIVOS**

Este trabalho visa auxiliar o crescimento na área de testes em aplicações IoT abrindo novas perspectivas para a atuação dos pesquisadores da área. Nas próximas subseções são apresentados o objetivo geral e específicos.

#### **3.1 - Objetivo geral**

Identificar os desafios existentes na área de testes de aplicações IoT por meio de um mapeamento sistemático.

#### **3.2 - Objetivos específicos**

- Identificar as abordagens/técnicas utilizadas em testes de aplicações IoT;
- Identificar os desafios encontrados nos testes de aplicações IoT e relacioná-los com as características inerentes dessas aplicações;
- Identificar as características de aplicações IoT mais críticas no processo de teste.

## 4 - FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta os termos que são necessários para uma melhor compreensão do trabalho apresentado. Na Seção 4.1 são apresentados os principais conceitos relacionados ao paradigma Internet das Coisas. Na Seção 4.2 são abordadas as principais técnicas de testes de software e na Seção 4.3 são apresentados o vocabulário comum e o processo de mapeamento sistemático.

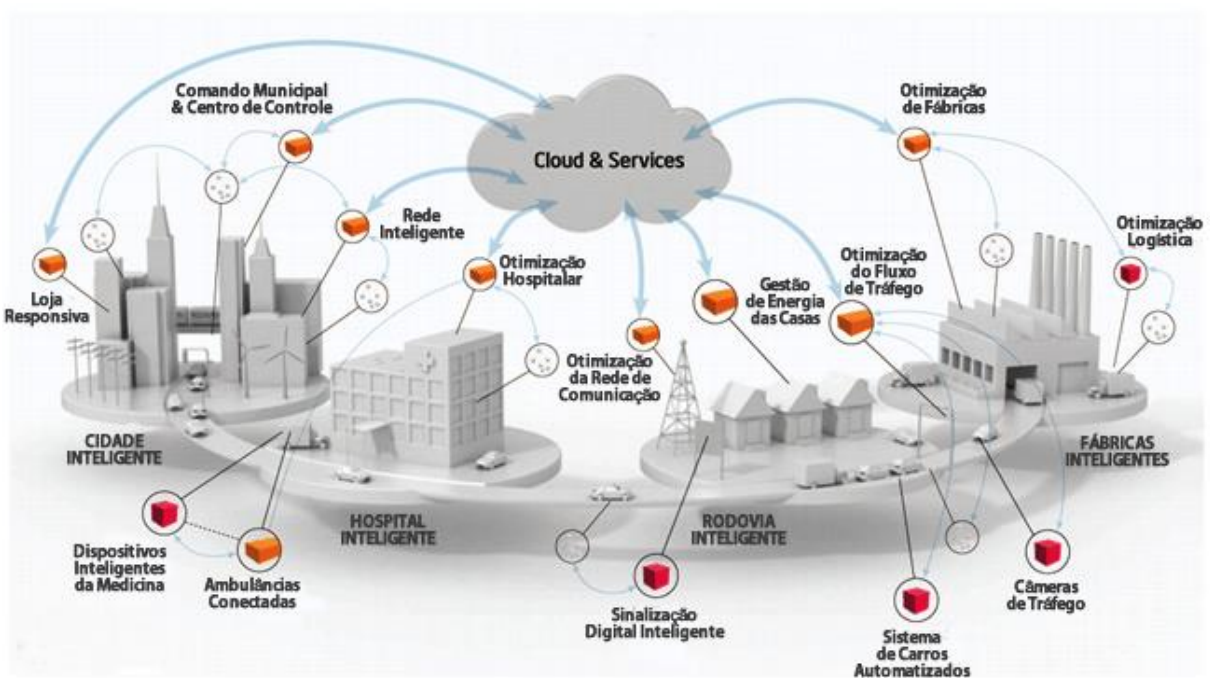
### 4.1 - Internet das Coisas (IoT)

O termo *Internet of Things* foi definido inicialmente em 1999 por Ashton (2009), tal conceito definia objetos, coisas, que a partir da conexão com a internet conseguem comunicar-se a fim de realizar um objetivo comum. Giusto et al. (2010) apresentou a Internet das Coisas como um paradigma em que as coisas inteligentes trocam informações entre si ou com outras coisas físicas e virtuais na rede, essas coisas podem ser desde *smartphones*, computadores ou até mesmo outros sistemas mais complexos conectados através da rede quando tais sistemas obedecem às mesmas características presentes no paradigma IoT são caracterizados os Sistemas de Sistemas (SoS) (Maia et al., 2014).

Para Atzori et al. (2010) IoT tem a ideia centralizada na presença da pervasiva de diversas “coisas” (*smartphones*, sensores, computadores) conectadas com endereçamento único, e tais “coisas” interajam entre si para o fornecimento de um serviço. Maia et al. (2014) afirma que em um futuro bem próximo grande parte de objetos comuns como: eletrodomésticos, veículos, aparelhos médicos, poderão ser endereçados, monitoradas e controladas através da Internet. A Figura 1 ilustra a Internet das Coisas como sendo um conjunto de sensores e dispositivos, destacados em vermelho, atuando em conjunto com aplicações, destacados em laranja, que armazena dados em nuvem e fornecem serviço e recebe serviços também através da nuvem.

Dentre diversas características existentes em aplicações IoT estão a ubiquidade e pervasividade citadas por Friedewald e Raabe (2011) e Anzelmo et al. (2011). A ubiquidade é a onipresença das aplicações IoT, onde diversos microprocessadores em variados ambientes se comunicam a fim de gerarem um serviço único (Friedewald e Raabe, 2011). Já a pervasividade citada por Anzelmo et al. (2011) faz referência a rápida propagação das informações atingida pelas aplicações IoT.

**Figura 1 - Internet das Coisas**



Fonte: (CREA-RJ, 2017)

L. Patel e M. Patel (2016) afirmam que existe pelo menos três interações distintas de IoT: (1) Pessoas para Pessoas, (2) Pessoas para Coisas; e (3) Coisas para Coisas, essas interações são sustentadas pela Internet. Além das características citadas por Friedewald e Raabe (2011) e Anzelmo et al. (2011), L. Patel e M. Patel (2016) apresentam outras características presentes em aplicações IoT, tais como:

- **Interconectividade:** relaciona-se a ideia de tudo está conectado a informação global, cada parte da infraestrutura para criação da rede pode se comunicar;
- **Serviços:** através de aplicações IoT é possível fornecer serviços que estejam relacionados a aplicação em questão, tais serviços são possíveis graças à implementação da tecnologia IoT nessas coisas;
- **Heterogeneidade:** cada dispositivo IoT pode por muitas vezes ser baseado em diferentes estruturas de rede e hardware e ao menos tempo interagir com diferentes dispositivos em outras redes;
- **Alterações dinâmicas:** O estado do dispositivo pode muitas vezes sofrer alterações como: Ligado/Desligado ou Conectado/Desconectado, além de sofrer mudanças na quantidade de dispositivos conectados;
- **Grandes escalas:** A quantidade de dispositivos conectados geralmente é de uma escala de grande magnitude, o que leva a um gerenciamento crítico dos dados em questão;

- **Segurança:** com o crescimento de diversos dispositivos de redes conectados é necessária uma segurança no tratamento dos dados que serão gerados a partir dessas conexões;
- **Conectividade:** relaciona-se à acessibilidade e compatibilidade, a acessibilidade relaciona-se a poder acessar e permanecer acessando a rede e a compatibilidade é fornecer esse acesso de forma comum, sem distinção de dispositivo ou plataforma.

Friedewald e Raabe (2011) e Anzelmo et al. (2011) defendem as infinitudes de mudanças positivas que podem ser geradas por aplicações IoT. Pode-se esperar a facilidade em atividades de vários setores, por exemplo, na medicina onde é possível, através de dispositivos conectados à internet medir batimentos cardíacos e direcionar os resultados desses exames rapidamente para sistemas que gerenciam esses resultados agilizando assim o processo de entrega e análise. Porém, para que tais benefícios possam ser usufruídos de maneira total são necessários a superar alguns desafios presentes na área de IoT. Bandyopadhyay e Sem (2011) trata a Segurança das Informações como um dos principais desafios a serem enfrentados na área de IoT, pois para que o paradigma possa ser prontamente utilizado é necessário a garantia que as informações que estarão trafegando na rede não sejam de alguma maneira alteradas ou até mesmo que haja ataques maliciosos, *Distributed denial-of-service attack* (DDoS). Tal desafio deve ser considerado, principalmente, ao tratar-se de áreas que exigem uma maior segurança de dados, tais como: aplicações bancárias, redes sociais, sistemas governamentais etc.

Outro desafio citado por Bandyopadhyay e Sem (2011) é o gerenciamento de dados, a quantidade de dados gerados a partir dessas aplicações são enormes e tais dados precisam ser armazenados e minerados para que possam ser fornecidos serviços úteis. L. Patel e M. Patel (2016) também relatam os mesmos desafios citados por Bandyopadhyay e Sem (2011) e adicionam o de custo como mais um desafio justificando que para haver o crescimento na adoção do paradigma IoT é necessário que os custos dos componentes, como sensores e controladores, sejam barateados nos próximos anos.

## 4.2 - Testes de Software

De acordo com Myers (1979), testar é analisar um programa com a intenção de descobrir erros e defeitos. O tipo de teste a ser aplicado durante a de construção de software depende da fase do ciclo de vida em que o software se encontra, pois não há como, por exemplo, realizar testes na interface se o sistema se encontra no início do processo de codificação, é necessário

um planejamento na realização do teste de software. Neste contexto, o processo de Verificação e Validação (V&V) auxilia o planejamento e execução dos testes de software, através dessas atividades é possível não só testar o produto, mas avaliar também a sua qualidade.

De acordo com Sommerville (2011), teste é a principal técnica no processo de Verificação e Validação de uma aplicação. Na Verificação, o objetivo é atingir os requisitos funcionais e não-funcionais propostos, enquanto na Validação é analisado o produto na perspectiva do cliente, ou seja, se o mesmo se adequa ao que cliente espera.

Os testes de software podem caracterizados em duas abordagens principais: testes de caixa branca e testes de caixa preta (Myers, 1979). A primeira concentra-se no código-fonte da aplicação, trata da parte interna do software, é tratado como um teste estrutural, pois testa componentes específicos permitindo uma verificação mais precisa do comportamento estrutural da aplicação. Na segunda abordagem por sua vez não há conhecimento sobre o código-fonte e a parte interna do software, o foco dos testes do tipo caixa preta é na parte funcional da aplicação, por isso se trata de um teste que se baseia, principalmente, nos requisitos funcionais da aplicação. Na realização das abordagens de testes apresentadas por Myers (1979) é possível integrar o uso de um *software* como meio de controlar a execução dos testes e comparar os resultados esperados com os resultados reais, caracterizando assim o teste automatizado.

As estratégias que serão utilizadas para o teste de software dependem, por exemplo, do domínio da aplicação, dos atributos de qualidade, dentre outros. Sommerville (2011) apresenta três estágios de testes: Teste de Desenvolvimento ou Teste de Unidade, Teste de Sistema e Teste de Aceitação. O Teste de Desenvolvimento é feito pelo o próprio desenvolvedor do componente. Uma vez que os componentes são testados individualmente, estes devem ser integrados para a criação do sistema, nesse caso, o Teste de Sistema valida os sistemas e seus subsistemas. No Teste de Aceitação são avaliadas as funcionalidades do pelo cliente e/ou usuários.

Dentre os tipos de testes, pode-se destacar os testes que se concentram nos atributos de qualidade, tais como testes de desempenho que buscam avaliar o produto de acordo com a agilidade e tempo de resposta; testes de interface que analisam a adequação da interface do software baseado em critérios estabelecidos e requisitos do cliente; e testes de segurança onde é avaliado se dados estão criptografados, se não há meios de invasão ou acesso não autorizado a dados, entre outros.

Os sistemas IoT possuem peculiaridades que os fazem necessitar de maior atenção na realização de testes. Aplicações IoT são compostas por objetos heterogêneos, que estão



distribuídos e essas “coisas” interagem com o ser humano e entre si, podem-se conectar por diversos meios, esses objetos inteligentes podem tomar decisões de maneira autônoma, realizar auto-reparação, são implantados em diversas plataformas com interfaces diferentes e composto por diferentes componentes, por essas peculiaridades que testar essas aplicações não é algo trivial, requer um maior esforço, através de processos e abordagens específicas.

No que diz respeito às abordagens de teste para aplicações IoT, Lee. I. e Lee. K, (2015) apresentam em seu trabalho uma abordagem de teste em nuvem para aplicações IoT, avaliando consumo de memória bem como o desempenho da aplicação. Na análise dos resultados foi possível observar que o elevado volume de dados gerado pela aplicação acabava por elevar o consumo de memória e diminuir o desempenho na aplicação gerando assim resultados de testes não satisfatórios.

Para a realização de testes de sistemas IoT são requeridos recursos sofisticados Reetz et al. (2013), como por exemplo, a avaliação do funcionamento de uma “aplicação crítica” em seu ambiente de atuação como sistemas de controle de tráfego, requer todo um aparato tecnológico para que os testes possam ser feitos sem que pessoas sejam prejudicadas com os testes, enquanto em aplicações tradicionais a criticidade, muitas vezes, não é alta.

Rosenkranz et al. em seu trabalho intitulado: *A Distributed Test System Architecture for Open-source IoT Software* de 2015, apresentam as principais dificuldades encontradas no teste de aplicações IoT. Apresentando como principal o fato dos casos de testes serem executados diretamente na rede e não na aplicação, isso acarreta em alguns casos a necessidade de emuladores. Outro desafio apresentado é o acoplamento entre o software e o hardware, pois determinadas aplicações, em sua execução, necessitam de uma estrutura específica de rede, por exemplo.

### **4.3 - Mapeamento Sistemático**

De acordo com Petersen et al. (2008) mapeamento sistemático tem como função primordial fornecer uma visão sobre uma determinada área de estudo, através da identificação dos trabalhos relacionados, resultados já existentes, além de reunir publicações já realizadas no decorrer do tempo para que se possa compreender o estado da arte do estudo em questão.

Mapeamento sistemático por muitas vezes é confundido com uma revisão sistemática, porém, existem distinções entre os mesmos. Kitchenham e Charters (2007) afirmam que a revisão sistemática é proposta a partir de um assunto específico, ou seja, dada uma área amplamente difundida é possível explorar algo específico que ainda não há muitos trabalhos

realizados, mas que é visto com interesse. Por outro lado, o mapeamento sistemático parte de um assunto mais geral, onde há pouca exploração da área, o mapeamento sistemático pode fornecer os assuntos específicos para que posteriormente possa ser realizado uma revisão sistemática. Ao final ambos os estudos fornecerão uma visão sobre o estado da arte, porém, o mapeamento sistemático fornecerá uma visão mais abrangente do aspecto pesquisado tratando-o de uma maneira ampla. O mapeamento sistemático normalmente deve ser considerado quando há interesse em se conhecer os desafios presentes em uma determinada área, de um modo que haja uma compilação desses trabalhos facilitando o acesso aos mesmos.

O principal objetivo de se realizar um mapeamento sistemático é identificar, avaliar e interpretar todas as pesquisas que são relevantes para o tema abordado e com isso resumir as evidências existentes sobre o tratamento ou tecnologia (Kitchenham, 2004). Além disso a autora afirma que a razão de resumir todas as informações sobre um fenômeno, de interesse de pesquisadores, de forma detalhada e de maneira imparcial são motivos suficientes para a realização de um mapeamento sistemático.

Kitchenham (2004) apresenta o mapeamento sistemático dividido em 3 fases: Planejamento, Condução e Resultados. No Planejamento é identificada a necessidade do mapeamento sistemático, após define-se o protocolo. Segundo a autora, o protocolo é um artefato importante presente no mapeamento sistemático, o mesmo possibilita que outros pesquisadores da área possam ter uma maior facilidade na replicação do trabalho, além de facilitar a compreensão sobre o estudo. Tal artefato apresenta diversos aspectos úteis para construção do mapeamento como as questões de pesquisa que serão abordadas no estudo, os critérios de exclusão e inclusão que são as cláusulas responsáveis por selecionar os documentos que serão aceitos e rejeitados, além da *string* de busca que é utilizada nas bases de dados para a obtenção dos resultados. As bases de dados são os mecanismos de busca, no qual a *string* será executada, cada base de dados possui particularidades que devem ser tratadas para que os trabalhos sejam retornados de forma correta.

Na fase de Condução é propriamente realizado o mapeamento sistemático, nesta fase são feitas as seleções dos estudos, os mesmos são analisados como forma de garantir a qualidade. Após a seleção, é feita a extração dos dados e sua síntese onde são levantadas as respostas para as questões de pesquisa e apresentados os dados obtidos no estudo.

Na fase dos Resultados são descritas a metodologia para realização, resultados do mapeamento sistemático e uma discussão sobre eles. Também são abordadas as ameaças de validade do mapeamento sistemático e apresentados possíveis trabalhos futuros.

Felizardo (2017) define o processo de mapeamento baseado nas mesmas fases que Kitchenham (2004), porém, algumas atividades realizadas em cada etapa são diferentes, por exemplo, a fase de Planejamento assemelha-se a Kitchenham (2004). Na fase de Condução são feitas apenas a seleção dos estudos e extração dos dados, e apenas na última fase, Resultados, são apresentados dados e respostas às questões de pesquisa.

Petersen et al. (2008) não realizam a divisão em fases, ao invés disso, define as próprias atividades anteriormente citadas como fases gerais do mapeamento sistemático como, por exemplo, definições de questões de pesquisa, definição dos critérios de seleção, seleção dos estudos primários, extração de dados em sua metodologia são todas definidas como fases e não atividades.

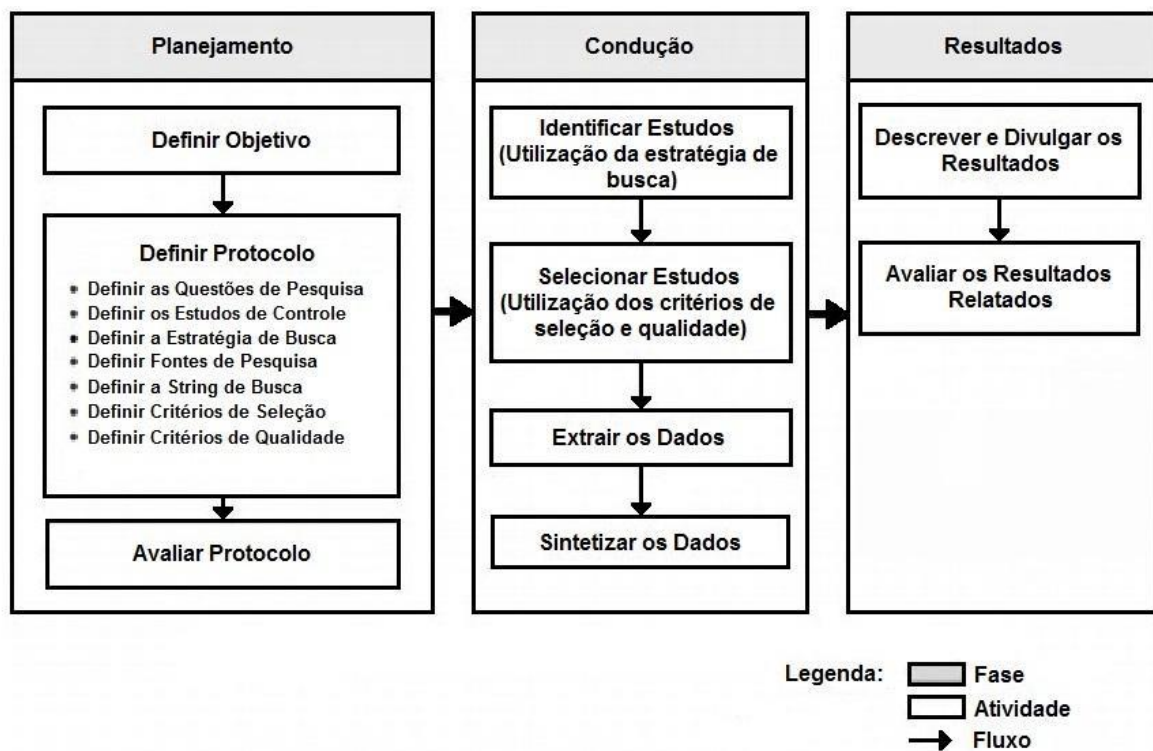
Considerando-se os objetivos e os benefícios de se realizar um mapeamento sistemático, este trabalho se propõe a realizar um mapeamento sistemático com o intuito de identificar as abordagens utilizadas nos testes de aplicações IoT, bem como apresentar os desafios enfrentados nessa área. Para este mapeamento será utilizada a metodologia apresentada em Kitchenham (2004).

## 5 - METODOLOGIA

Para a pesquisa descrita neste trabalho optou-se por um mapeamento sistemático por mostrar-se satisfatório para o resultado que se pretende alcançar, além disso, é possível uma posterior revisão sistemática obtendo os estudos primários a partir deste mapeamento.

A metodologia para a realização do mapeamento baseia-se na metodologia proposta por Kitchenham (2004). Ela é dividida em três fases Planejamento, Condução e Resultados (ver subseção 4.3). A Figura 2 apresenta as fases, suas atividades e como elas estão relacionadas.

**Figura 2** – Processo de Mapeamento Sistemático



Fonte: Processo baseado em Kitchenham (2004). Figura adaptada de Sampaio (2015).

Nas próximas subseções são apresentadas as fases da metodologia, detalhando as atividades que ocorrerão em cada fase e os artefatos já gerados neste estudo.

### 5.1 - Planejamento

A fase de planejamento busca avaliar a viabilidade e objetivos para a realização do mapeamento sistemático. Para o desenvolvimento deste trabalho, primeiramente avaliou-se a relevância do tema para a comunidade científica. Em seguida, foi feito um levantamento

bibliográfico para embasamento teórico e obter estudos relacionados. Após essa pesquisa inicial, foi elaborado o protocolo (ver Apêndice A) para o mapeamento sistemático.

Dentre as atividades presentes na construção do protocolo (ver Apêndice A) está a atividade de **definição das questões de pesquisa**, na qual devem ser elaboradas, a partir de uma avaliação do tema do trabalho. As questões de pesquisas investigadas neste trabalho são:

**Q1** - Quais as abordagens utilizadas para testar aplicações IoT?

**Q2** - Quais são os desafios encontrados nos testes de aplicações IoT?

**Q3** - Quais são as características de aplicações IoT mais críticas para o processo de teste?

Após definir as questões de pesquisa, são levantados os **estudos de controle**. Através de um levantamento na literatura feito pela especialista, também orientadora deste trabalho, foram selecionados trabalhos publicados na área de testes e IoT. Todos os trabalhos encontrados foram lidos de maneira completa, tais trabalhos serviram como garantia para a qualidade da busca que será realizada, pois os mesmos devem ser retornados na execução da *string* de busca definida no protocolo (ver Apêndice A). Foram lidos cerca de 15 artigos e selecionados 7 desses. Os trabalhos que foram descartados (8 artigos) abordavam testes e IoT de maneira separadas, seja por não fornecer nenhuma abordagem de testes para aplicações IoT ou por não se tratar de aplicações IoT. A Tabela 2 apresenta os trabalhos selecionados como estudos de controle.

**Tabela 2** - Estudos de Controle

<b>ID</b>	<b>Título</b>	<b>Autor</b>	<b>Ano</b>	<b>Motivação</b>
<b>1</b>	<i>Power-aware testing in the Era of IoT</i>	P. Girard	2018	Apresenta os desafios em testar aplicações IoT no aspecto elétrico
<b>2</b>	<i>Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective</i>	D. Pal; S. Funilkul; N. Charoenkitkarn; P. Kanthamanon	2018	Apresenta um modelo IoT para construção de casas inteligentes para idosos e aborda testes que seriam realizados neste modelo

3	<i>IoT-TaaS: Towards a Prospective IoT Testing Framework</i>	H. Kim; A. Ahmad; J. Hwang; H. Baqa; F. Le Gall; M. A. Reina Ortega; J. Song	2018	Fornece uma nova abordagem de teste estrutural para aplicações IoT
4	<i>IoT challenge: older test machines modernization in an automotive plant</i>	Juraj Pancí e Vladimír Benes	2017	Descreve o projeto para elaboração de um sistema baseado no paradigma IoT, tratam sobre os desafios para a realização de testes.
5	<i>Towards Quality-Assured Data Delivery in Cloud-Based IoT Platforms for Smart Cities</i>	S. S. Samant; M. B. Chhetri; Q. B. Vo; R. Kowalczyk; S. Nepal	2017	Propõe uma abordagem de teste baseado em computação em nuvem para plataformas IoT
6	<i>IoT testing - The big challenge why, what and how</i>	Benny Sand	2016	Apresenta os desafios para testar aplicações IoT relacionado a quantidade de dados gerados pelas aplicações.
7	<i>A Ubiquitous Model for Wireless Sensor Networks Monitoring</i>	A. G. F. Elias; J. J. P. C. Rodrigues; L. M. L. Oliveira; B. B. Zarpelão	2012	Apresenta uma abordagem de teste sensores de redes baseado em computação ubíqua.

Fonte: a autora.

Para a definição da **estratégia de busca** devem ser considerados: (1) método de busca; (2) fontes de pesquisa; (3) *string* de busca; (4) critérios de seleção; e (5) o processo de seleção dos estudos. Para Wohlin et al. (2013) o escopo de um mapeamento sistemático normalmente é mais amplo e a análise e síntese mais superficiais do que em uma revisão sistemática. Deste modo, a estratégia de busca deve ser menos restritiva, de modo permitir recuperar mais estudos (Kitchenham, Brereton e Budgen, 2011)

Jalali e Wohlin (2012) apresentam pelo menos três **métodos de busca** como possíveis métodos de busca para estudos para mapeamento ou revisão sistemática, são eles: bola de neve (*snowballing*), a busca manual e a busca automática em bases de dados digitais. O primeiro método é mais destinado a revisões sistemáticas por basear-se em estudos primários como forma de obter estudos secundários mais relevantes. A busca manual normalmente é aplicada quando se sabe que existem periódicos ou eventos que não são contemplados pelas bases de dados digitais ou até mesmo para seleção de poucos estudos sem grandes restrições como, por exemplo, na escolha de estudos de controle. A busca automática em bases de dados digitais é aplicada neste trabalho, para esse tipo de busca são construídas *strings* de buscas que ao serem executadas nas bases de dados digitais resultam em estudos que possuem as palavras-chaves descritas nas *strings*. Optou-se por essa busca, pois para um mapeamento convém uma visão mais ampla oferecendo diversos estudos na área e de maneira rápida.

Para a seleção das **fontes de pesquisa** é necessário fazer a distinção entre bibliotecas digitais de editores e as bases indexadoras. Normalmente as bibliotecas apresentam apenas estudos que tenham sido publicados por ela, já as bases indexam estudos de diversas bibliotecas digitais. Para este trabalho optou-se inicialmente por fazer uso das bibliotecas digitais IEEE (*IEEE Xplore*) e ACM (*ACM Digital Library*), por já ter uma quantidade suficiente de estudos para geração de dados.

Para a execução da busca nas bases de dados é utilizado um artefato de entrada: a **string de busca**, ela é elaborada através da união de termos que devem ou não conter nos resultados pretendidos pelo mapeamento. Essa união é feita por meio de operadores lógicos como: AND, OR, NOT etc. A *string* de busca definida para este trabalho é apresentada abaixo. Ela é baseada nas questões de pesquisa Q1, Q2 e Q3, em seus termos-chave e derivações.

*("internet of things" OR "IoT" OR "system of system" OR "systems of systems")*

*AND*

*(test OR testing)*

*AND*

*(approach OR process OR method OR procedure OR technique OR methodology OR model  
OR framework OR tool OR architecture)*

Os **critérios de seleção** definem os trabalhos que serão tomados como relevantes para a pesquisa (critérios de inclusão) e quais serão descartados (critérios de exclusão). Inicialmente, será feita uma seleção baseada na leitura dos títulos, palavras-chaves e resumos. Após essa

seleção, será feito outro refinamento com a leitura completa dos estudos e, assim gerados os resultados. Baseado nos critérios de seleção para mapeamento sistemático definidos por Sampaio (2015), os critérios de seleção (inclusão e exclusão) utilizados para o mapeamento deste trabalho são:

- **Critérios de Inclusão:**

**Critério 1 - Todos os estudos devem conter resumos:** Serão selecionados aqueles estudos que contiverem pelo menos um resumo inicial, para que possa ser executado a primeira fase da seleção.

**Critério 2 - Estudos que tratam de testes para aplicações IoT:** Trabalhos que tratam de sistemas IoT, que apresente a etapa de teste em seu contexto serão selecionados.

**Critério 3 - Estudos escritos em inglês:** Por inglês tratar-se de um idioma abrangente para a comunidade científica e para facilitar a reprodução do mapeamento e o uso dos resultados, optou-se por considerar apenas trabalhos neste idioma.

- **Critérios de Exclusão:**

**Critério 1 - O estudo é apenas um resumo:** Em muitos casos o estudo publicado é apenas um resumo, como uma apresentação de pôster em evento, por esse critério tais estudos serão descartados. Não confundir com artigos curtos (*short papers*), por mais que sejam curtos, duas ou três páginas, são apresentados resumos. Um estudo que se trata apenas de resumos não apresenta corpos.

**Critério 2 - O estudo é uma versão reduzida de outro:** Às vezes há publicações que são feitas em diferentes veículos de publicações e são lançadas em versões mais curtas, desse modo serão considerados apenas os estudos na versão completa para que se pode obter todas as informações relevantes para o estudo.

**Critério 3 - Não é possível ter acesso ao estudo:** Para a segunda etapa de seleção será considerado o estudo por inteiro, caso não seja possível o acesso completo ao estudo, o mesmo será desconsiderado.

A Figura 3 apresenta as etapas utilizadas para o **processo de seleção dos estudos**. Na primeira etapa é feita a remoção de artigos duplicados. Após essa etapa, é dado início a etapa 2 que na Figura 3 é representado por um subprocesso, pois nessa etapa são realizadas duas atividades, a primeira é a seleção dos estudos a partir da leitura do título, resumo e palavras-chave, onde cada estudo é categorizado em: “selecionados”, “rejeitados” ou “em dúvida”, essa



categorização se dá pela adequação aos critérios de seleção. A segunda atividade que ocorre em paralelo a primeira é a realização da análise da especialista sobre os artigos que são postos como “em dúvida”, para que assim possam ser definidos como selecionados ou rejeitados, após finalizadas essas atividades são gerados os artigos selecionados da segunda etapa. Na etapa 3, também representado por um subprocesso na Figura 3, é realizada a leitura completa dos artigos selecionados na etapa anterior, enquanto isso, em paralelo, a especialista realiza esse mesmo processo de leitura para  $\frac{1}{3}$  dos estudos, a fim de que ao final seja verificada a equivalência entre os dois resultados, caso houvesse uma grande divergência, mais de 4 estudos, uma análise dos resultados seria feita a fim de entender as razões na diferença dos resultados, para que os conflitos fossem devidamente resolvidos. Ainda foi levantada a possibilidade de calcular o *Alfa de Cronbach*<sup>2</sup>, porém, é uma técnica indicada quando há um maior número maior de especialistas, por razão do aumento na probabilidade de divergência, contudo achou-se suficiente basear-se nos resultados da amostra como forma de validação da seleção. Finalizada as etapas os estudos finais são gerados e caracterizados no formulário (ver apêndice B) na fase 2 da metodologia.

De acordo com Petersen et al. (2008) a principal diferença entre a revisão sistemática e o mapeamento é avaliação de qualidade, pois se tratando de uma revisão sistemática após a leitura completa dos artigos selecionados é feita uma detalhada avaliação de qualidade. Petersen et al. (2015) apresentam em seu trabalho que de 52 mapeamentos sistemáticos analisados apenas 14 deles, cerca de 27%, apresentaram algum estudo de qualidade. Dessa forma, para este trabalho foram definidos **critérios de qualidade** através do desenvolvimento de uma pequena lista de verificação, incluída no formulário de extração de dados (ver apêndice B), esta lista será usada apenas para caracterizar os estudos selecionados após etapa 3 do processo de seleção (ver Figura 3).

## 5.2 - Condução

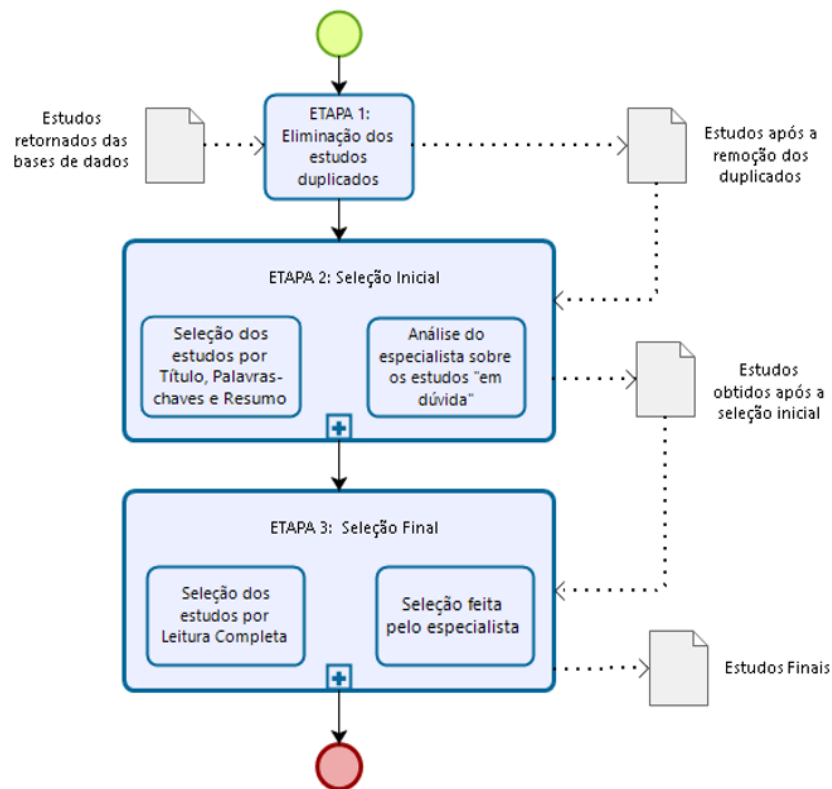
Nesta fase é realizado o mapeamento sistemático propriamente dito baseado na estratégia de busca definida na fase de Planejamento. O mapeamento foi conduzido por uma aluna de graduação em Engenharia de Software e uma especialista, doutora na área de ES com experiência em Verificação e Validação para aplicações móveis e também orientadora deste trabalho. A etapa de Condução ocorreu entre março de 2018 e outubro de 2018.

---

<sup>2</sup> Forma de estimar a confiabilidade de uma pesquisa, normalmente usada em questionários.

Na execução da *string* foram identificados 293 artigos na *ACM Digital library* e na *IEEE Xplore 1904*, tais estudos passaram pelo o processo de seleção (ver Figura 3), onde na etapa 1 foram retirados 40 estudos duplicados, restando 2157. A ferramenta *StArt3* foi útil principalmente na etapa de condução como forma de auxílio para as seleções dos estudos. Os 2157 estudos foram passados para a etapa 2, onde com a leitura do título, resumo e palavras-chaves foi feita a seleção baseada nos critérios apresentados na Seção 4.1 deste trabalho. Quando havia dúvida em selecionar ou não um estudo, a especialista era consultada a fim de definir pelo descarte ou seleção do estudo. Dos 2157 selecionados, 67 passaram para etapa 3. Na Tabela 3 é apresentada a quantidade de trabalhos retornados de cada base de dados e a porcentagem desses valores.

**Figura 3** - Processo de seleção dos estudos



**Fonte:** Processo baseado em Kitchenham (2011). Figura adaptada de Sampaio (2015).

Na etapa 3, os 67 estudos passaram por uma nova etapa de seleção, onde foram aplicados novamente os critérios de seleção. Nessa etapa foi feita a leitura completa dos 67 estudos e, em paralelo, o especialista selecionou, de forma aleatória,  $\frac{1}{3}$  desses estudos, 22, e também realizou a leitura completa. Nessa análise, a especialista constatou 8 artigos

<sup>3</sup> Ferramenta de auxílio na aplicação MS e RS.

selecionados, enquanto o aluno selecionou 9, comparando quais estudos foram aceitos apenas 1 divergiu, deste modo achou-se suficiente a análise amostral como validação dos resultados.

**Tabela 3** - Estudos totais de acordo com a base

Base de Dados	Quantidade	Selecionados	% Selecionados
<i>ACM Library</i>	293	40	55,5%
<i>IEEE Xplore</i>	1904	32	44,5%

Fonte: a autora.

Após finalizada a etapa 3 restaram 25 estudos dos 67 selecionados inicialmente. Os 25 estudos estão listados na Tabela 4 com título, ano, autores e um id que referenciam cada estudo no decorrer do texto, se necessário.

**Tabela 4** - Estudos Finais

ID	Título	Autores	Ano
P1	<i>Do We Need New Strategies for Testing Systems-of-systems?</i>	Vânia de Oliveira Neves, Antonia Bertolino, Guglielmo De Angelis e Lina Garcés	2018
P2	<i>Automation Testing and Monitoring Lab on the Cloud for IOT Smart Fleet System (ATML e SFS)</i>	Ruba Mohammad; Haj Hamad (Hamad, R. M. H., 2018)	2018
P3	<i>Architectures and Experiences in Testing IoT Communications</i>	Teemu Kanstren, Jukka Mäkelä, Pekka Karhula (Kanstren, T. et al., 2018)	2018
P4	<i>IoT-TaaS: Towards a Prospective IoT Testing Framework</i>	Hiun Kim, Abbas Ahmad, Jaeyoung Hwang, Hamza Baqa, Franck Le Gall, Miguel Angel Reina Ortega, and Jaeseung Song (Kim, H. et al., 2018)	2018

P5	<i>Test-based risk assessment and security certification proposal for the Internet of Things</i>	Sara N. Matheu García, Jose L. Hernández-Ramos, Antonio F. Skarmeta (García, S. N. M. et al., 2018)	2018
P6	<i>IoT security assessment through the interfaces P-SCAN test bench platform</i>	Thomas Maurin, Laurent-Frédéric Ducreux, George Caraiman, Philippe Sissoko (Maurin, T. et al., 2018)	2018
P7	<i>Tiny TTCN-Inspired Testing Tools for Experimenting with Hybrid IoT Systems</i>	Krzysztof M. Brzezinski (K. M. Brzezinski, 2018)	2018
P8	<i>PlaTIBART: A Platform for Transactive IoT Blockchain Applications with Repeatable Testing</i>	Michael A. Walker, Abhishek Dubey, Aron Laszka, and Douglas C. Schmidt (Walker, M. A. et al., 2017)	2017
P9	<i>Let the Cat Out of the Bag: A Holistic Approach Towards Security Analysis of the Internet of Things</i>	Vinay Sachidananda, Shachar Siboni, Asaf Shabtai, Jinghui Toh, Suhas Bhairav, Yuval Elovici (Sachidananda, V. et al., 2017)	2017
P10	<i>Service Virtualisation of Internet-of-things Devices: Techniques and Challenges</i>	Zeinab Farahmandpour, Steve Versteeg, Jun Han, Anand Kameswaran (Farahmandpour, Z. et al., 2017)	2015
P11	<i>Autonomous real-time software &amp; systems testing</i>	Thomas Fehlmann, Eberhard Kranich (Fehlmann, T.; Kranich, E., 2017)	2017

P12	<i>Towards a Thing-In-the-Loop Approach for the Verification and Validation of IoT Systems</i>	Domenico Amalfitano, Vincenzo De Simone, Vincenzo Riccio, Fasolino Anna Rita (Amalfitano, D. et al., 2017)	2017
P13	<i>Fault Injection in the Internet of Things Applications</i>	Mohammad Amin Alipour (Alipour, M. A., 2017)	2018
P14	<i>Towards an open framework of online interoperability and performance tests for the Internet of Things</i>	Sebastien Ziegler, Eunsook Eunah Kim (Ziegler, S.; Kim, E. E, 2017)	2017
P15	<i>Reverberation chambers for flexible over-the-air testing of internet-ofthings devices</i>	Mats Kristoffersen, Christian Patané Lötbäck, Derek Skousen (Kristoffersen, M. et al., 2017)	2017
P16	<i>Towards an emulated IoT test environment for anomaly detection using NEMU</i>	Shane Brady, Adriana Hava, Philip Perry, John Murphy, Damien Magoniy, and A. Omar PortilloDominguez (Brady, S. et al., 2017)	2017
P17	<i>PENTOS: Penetration testing tool for Internet of Thing devices</i>	Vasaka Visoottiviseth, Phuripat Akarasiriwong, Siravitch Chaiyasart, Siravit Chotivatunyu (Visoottiviseth, V et al., 2017)	2017

P18	<i>IoT-Testware - An Eclipse Project</i>	Ina Schieferdecker, Sascha Kretzschmann, Axel Rennoch, Michael Wagner (Schieferdecker, I. et al., 2017)	2017
P19	<i>Modelling an IoT testbed in context with the security vulnerabilities of South Africa</i>	Kishor Krishnan Nair, Erick Dube, Samuel Lefophane (Nair, K. K. et al., 2017)	2017
P20	<i>A Distributed Test System Architecture for Open-source IoT Software</i>	Philipp Rosenkranz, Matthias Wählisch (Rosenkranz, P. et al., 2015) Omar Portillo-Dominguez	2015
P21	<i>How to Test IoT-based Services before Deploying them into Real World</i>	Eike Steffen Reetz, Daniel Kuemper, Klaus Moessner, Ralf Tonjes (Reetz, E. S. et al., 2013)	2013
P22	<i>Testing Highly Complex System of Systems: An Industrial Case Study</i>	Nauman Bin Ali, Kai Petersen, Mika V. Mäntylä (Ali, N. B. et al., 2012)	2012
P23	<i>Systems of systems test and evaluation challenges</i>	Dr. Judith Dahmann, Dr. Jo Ann Lane, George Rebovich, Ralph Lowry (Dahmann, J. et al., 2010)	2010
P24	<i>Data-flow Integration Testing Adapted to Runtime Evolution in Component-based Systems</i>	Éric Piel, Alberto GonzalezSanchez (Piel, É.; GonzalezSanchez, A., 2009)	2009

P25	<i>Randomization for testing systems of systems</i>	<i>Qianhui Liang, Stuart H. Rubin (Liang, Q.; Rubin, S. H., 2009)</i>	2009
-----	---	---	------

Fonte: a autora.

### 5.3 - Resultados

Nesta fase os dados extraídos e sintetizados serão discutidos baseado nas questões de pesquisa definidas no protocolo (ver Apêndice A) do mapeamento. Após a finalização da etapa 3, foram aplicados o formulário de extração de dados (ver Apêndice C) para cada um dos 25 estudos selecionados, a fim de obter as informações relevantes para responder às questões de pesquisa. Os resultados do mapeamento serão apresentados na seção 6.

## 6 – RESULTADOS E ANÁLISE DO MAPEAMENTO

Nessa seção serão apresentadas as respostas às questões de pesquisa deste mapeamento e alguns outros dados que foram considerados relevantes. Os dados serão apresentados por meio de gráficos e tabelas.

### Q1 - Quais as abordagens utilizadas para testar aplicações IoT?

Analisando as dificuldades no teste de aplicações IoT, o principal objetivo dessa questão de pesquisa é visualizar que diferentes abordagens para testar aplicações IoT estão sendo usadas atualmente. Na Tabela 5 são apresentadas as abordagens encontradas e a porcentagem baseadas na quantidade de estudos que fizeram uso das mesmas.

A abordagem mais encontrada foi a de “Teste Baseado em Modelos” (TBM), nessa abordagem são levantados modelos, que podem ser retirados dos requisitos, casos de usos entre outros, a fim de que baseados nesses modelos possam ser escritos casos de testes para a execução dos testes. Nos estudos encontrados grande parte dos modelos foram baseados nos requisitos, nessa abordagem pode-se destacar o estudo P25 onde através de um modelo de teste randômicos é feita uma busca para selecionar casos de testes de forma aleatória para *SoS*, fornecendo uma possível baixa nos custos da geração desses casos. Outra abordagem foi a criação de “Ferramentas ou Plataformas”, nessa abordagem 4 estudos apresentaram o desenvolvimento de ferramentas ou plataformas que auxiliem a execução dos testes, como a apresentada no estudo P17, que é detalhado em parágrafos seguintes. A terceira abordagem mais encontrada foi a de “Teste Automatizado” onde a partir do conhecimento do sistema são definidos os casos de teste automatizados, a fim de agilizar o processo de testes, nos estudos levantados nessa abordagem foi usado o *Selenium* como linguagem de automatização desses testes. Outra abordagem foi o “*Testbed*”, na qual é realizado o teste por componentes do sistema, essa abordagem fornece um esqueleto que funcionaria como padrão para os testes de diversos componentes de um sistema, nos estudos levantados não são detalhados como funciona o padrão de *testbed* usado, é apenas citado a abordagem como meio usado para chegar aos resultados dos trabalhos. “Emuladores” também foi uma abordagem levantada, se baseia na construção de um ambiente que se assemelha ao ambiente em que a aplicação irá executar, a partir disso são executados uma bateria de testes a fim de garantir ao máximo a validade da aplicação. Outra abordagem apresentada nos estudos é a “Injeção de Falhas” presente no estudo P13, onde através da inserção de falhas no código-fonte o estudo busca ajudar na visualização de problemas relacionados à segurança no sistema antes que o mesmo esteja em seu ambiente



final, além de ajudar ao programador a reconhecer falhas e atuar sobre elas. Por último é apresentado “*Service-oriented architecture*” (SOA), onde a partir da arquitetura de cada dispositivo são estabelecidos padrões de testes a fim de que seja facilitada a comunicação entre eles.

**Tabela 5** - Abordagens para testes de IoT

ABORDAGEM	ESTUDOS	PORCENTAGEM
Baseado em Modelos	P8, P12, P24, P25, P4, P5, P15, P17	32%
Plataformas/Ferramentas	P20, P6, P14, P7	16%
Teste Automatizado	P10, P11, P2	12%
Testbed	P9, P16, P19	12%
Sem abordagem definida	P22, P3, P23	12%
Emuladores	P18, P21	8%
Injeção de Falhas	P13	4%
SOA	P1	4%

Fonte: a autora.

Na Tabela 6 é possível observar que dos 25 estudos selecionados, 22 deles realizam estudos de caso, por exemplo, no estudo P22 é apresentado um estudo de caso onde é avaliado um site de desenvolvimento de uma grande empresa de Telecomunicação que utiliza *SoSs*, a abordagem que não é detalhada no estudo, visa testar sistemas industriais e levantar os desafios em testá-los como principais desafios foram levantadas as dificuldades em manter o escopo dos casos de testes desses sistemas, pois com as alterações dinâmicas das aplicações IoT esse processo se torna custoso.

**Tabela 6** - Estudos que continha Estudos de Casos e Experimentos

Estudos que contém Estudo de Caso	Estudos que contém Experimento
P1, P2, P3, P4, P5, P7, P8, P9, P10, P11, P12, P13, P14, P17, P18, P19, P20, P21, P22, P23, P24, P25	P2, P4, P6, P7, P11, P14, P18, P20, P21, P22
<b>Total: 88%</b>	<b>Total: 40%</b>

Fonte: a autora.

Entre os 25 estudos, 10 deles apresentaram algum experimento para validar a abordagem proposta (ver Tabela 6), dentre esses experimentos pode-se destacar o P17, onde é proposta uma ferramenta para testar a segurança de aplicações IoT através de testes de penetração<sup>4</sup>, ao final do estudo é apresentado o experimento que foi feito com Raspberry Pi<sup>5</sup>, onde foi implantado em um sistema que sofreu diferentes ataques de segurança simulados. Antes da realização desses ataques a ferramenta Pentos, proposta no estudo, realizou testes de penetração a fim de validar a segurança do sistema que após a análise dos resultados mostrou-se satisfatória nos testes de segurança de IoT

## Q2 - Quais são os desafios encontrados nos testes de aplicações IoT?

Nessa questão de pesquisa foram levantados a partir dos 25 estudos os principais desafios encontrados para testar aplicações IoT. O principal objetivo dessa questão é apresentar os desafios, que atualmente estão sendo mais investigados no teste de aplicações IoT, a fim de vislumbrar onde poderão ser investidos esforços na área. No total foram levantados 10 desafios, apresentados na Tabela 7, que estão separados de acordo com os respectivos estudos onde foram encontrados.

**Tabela 7** - Desafios na área de IoT

DESAFIOS	ESTUDOS	PORCENTAGENS
Segurança	P8, P22, P9, P13, P3, P4, P6, P14, P15, P17, P19	44%
Interoperabilidade	P1, P12, P13, P20, P5, P18	24%

<sup>4</sup> Método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa

<sup>5</sup> Uma série de computadores de placa única do tamanho reduzido, que se conecta a um monitor de computador ou TV

Desempenho	P12, P2, P23, P7, P18, P19	24%
Integração	P12, P20, P24, P5	16%
Manutenibilidade	P22, P18, P2	12%
Altos custos	P13, P25, P4, P16	12%
Heterogeneidade	P10, P1	8%
Fluxo de Dados	P10, P14	8%
Escalabilidade	P13, P6	8%
Flexibilidade	P1, P23	8%

Fonte: a autora.

“Segurança”, “Interoperabilidade” e “Desempenho” foram os desafios mais abordados, dentre dos 25 estudos 18 deles trataram de algum desses desafios. A segurança é vista como um grande desafio na área devido à necessidade das aplicações IoT de lidar com diversas informações pessoais do usuário, a fim de fornecer um ambiente mais vestível possível, para isso é preciso garantir que tais informações permanecerão inalteradas e anônimas, porém, essa garantia nem sempre é simples quando se trata em transição de dados dentro de uma rede em que a diversas aplicações com diferentes arquiteturas, assim se apresenta a dificuldade é testar a segurança quando a tantos dispositivos diferentes conversando entre si. Nos estudos que levantam a “Interoperabilidade” como desafio, apontam a dificuldade em testar de forma “igual” dispositivos com funções diferentes, ou seja, que operam de formas diferentes, mas que interagem entre si, de forma a garantir a transparência. Os estudos que apontam o “Desempenho” como desafio tratam principalmente do mínimo de gasto de energia que essas aplicações precisam ter e com isso a minimização de valores de hardware, como memória, dificultando assim a criação de ambientes de testes que se adequem especificamente a essas circunstâncias. O estudo P6 levantou o desafio “Segurança” em seu escopo apresentando a plataforma *P-SCAN*, que fornece uma biblioteca de conjuntos de testes para auxiliar na automatização dos testes, no quesito segurança, tais testes abordam diversos aspectos comuns de segurança em sistemas IoT, como transição dos dados, criptografia entre outros. Desse

modo, o estudo buscou fornecer uma plataforma que contribuísse na diminuição da vulnerabilidade do sistema antes de executado no ambiente final.

### **Q3 - Quais são as características de aplicações IoT mais críticas para o processo de teste?**

Essa questão de pesquisa leva em consideração os desafios encontrados na Q2 e os relaciona com as definições das características de aplicações IoT definidas por L. Patel e M. Patel (2016) (ver Seção 4.1). As criações dessas relações podem ser exemplificadas através do estudo P19, onde é apresentado uma abordagem para a realização de testes em aplicações IoT com foco na flexibilidade desses sistemas, a justificativa principal para construção do trabalho se dá pela dificuldade em testar as constantes mudanças que ocorrem em sistemas IoT, como adições de novos sensores, rápidas mudanças no contexto ou até mudanças arquiteturais. Desse modo, o desafio de flexibilidade levantado neste estudo foi relacionado diretamente com a definição da característica de “Alterações Dinâmicas” apresentada por L. Patel e M. Patel (2016), visto que ambas, flexibilidade e “Alterações Dinâmicas” tratam das mudanças contínuas existentes nessas aplicações. Esse processo seguiu para todos os demais desafios a fim de construir a relação que é apresentada na Tabela 8, alguns desafios estão relacionados a mais de uma característica devido às peculiaridades de cada estudo.

**Tabela 8** - Relação entre Características IoT e os Desafios levantados

<b>Características</b>	<b>Desafios</b>
Interconectividade	Interoperabilidade
Heterogeneidade	Heterogeneidade
Segurança	Segurança
Alterações Dinâmicas	Interoperabilidade, Flexibilidade e Desempenho
Grandes Escalas	Fluxo de Dados e Escalabilidade
Conectividade	Manutenibilidade e Integração
Serviços	Altos Custos

**Fonte:** Adaptada de L. Patel e M. Patel (2016).

A relevância dessa questão se dá por levantar as características de aplicações IoT mais críticas no âmbito de testes, entende-se por crítica neste trabalho aquelas características onde há um maior investimento de esforços a fim de testá-las. Na Tabela 9 são apresentadas as características das aplicações IoT relacionadas com seus respectivos estudos.

**Tabela 9** - Características IoT críticas para o processo de teste

CARACTERÍSTICA	ESTUDO	PORCENTAGEM
Segurança	P3, P4, P6, P8, P9, P13, P14, P15, P17, P19, P22	44%
Alterações Dinâmicas	P1, P2, P12, P18, P19, P22, P23	28%
Conectividade	P5, P12, P18, P20, P21, P22, P24	28%
Interconectividade	P1, P5, P12, P13, P18, P20	24%
Grandes Escalas	P10, P13, P14, P16	16%
Heterogeneidade	P10, P11	8%
Serviços	P4, P25	8%

Fonte: a autora.

Dado que os maiores desafios são na área de Segurança de aplicações IoT é comum que esta também seja a característica levantada como a mais crítica devido a quantidade de estudos que a abordam, representando assim um maior esforço em seus testes.

### 6.1 - Estudos por base de dados

Os 25 estudos selecionados ficaram divididos entre as duas bases da *ACM library* e *IEEE Xplore*, é importante visualizar no Gráfico 1 para definir os impactos de cada base. Deste modo de acordo com o Gráfico 1 fica claro que a *IEEE Xplore* teve um maior número de estudos selecionados, 14, enquanto a *ACM Library* com uma porcentagem de 44%, teve 11 estudos selecionados.

**Gráfico 1** - Estudos selecionados distribuídos por base de dados

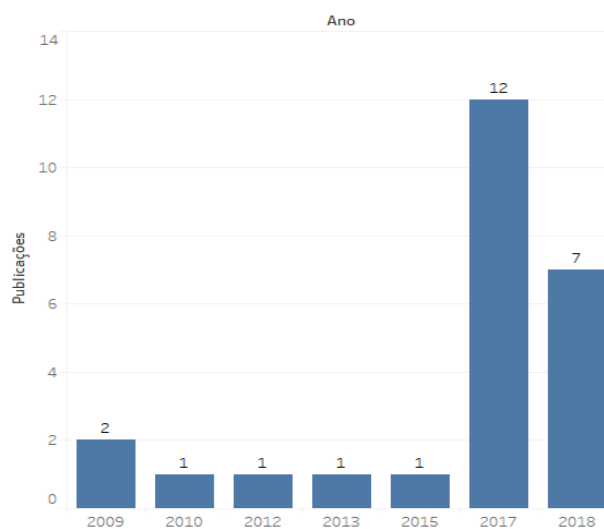


Fonte: a autora.

## 6.2 - Estudos publicados por Ano

No Gráfico 2 é apresentada a quantidade de publicações retornadas de acordo com ano de cada um deles, a publicação mais recente é de março de 2018. Avaliar essa quantidade de estudos por ano ajuda a identificar o crescimento ou não da área. É importante ressaltar que a pesquisa em IoT avança mais fortemente a partir de 2014, nesse mesmo período a tecnologia *Bluetooth Low Energy* (BLE) se difundiu no mercado (Collotta, M.; Pau, G., 2015), barateado assim seu custo, isso unido as construções de sistemas IoT, fomentou a área de pesquisa de testes dessas aplicações, e essa fomentação é vista no Gráfico 2 com o crescimento significativo em 2017 e 2018 das pesquisas na área de testes. Os estudos de 2009 são todos voltados diretamente para SoSs.

**Gráfico 2** - Estudos publicados por ano



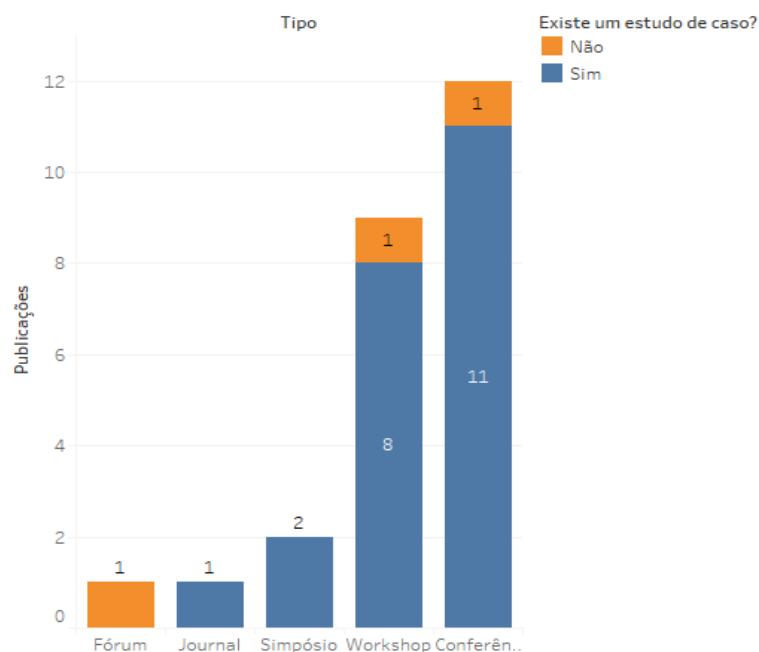
Fonte: a autora.

### 6.3 - Tipos de publicações e avaliações

Os 25 estudos selecionados foram divididos em seus respectivos tipos de publicações e se apresentavam estudos de caso ou experimentos. A definição usada para estudos de casos e experimentos foi baseada em Per Runeson e Martin Höst (2008), onde a principal distinção está em estudos de caso são estudos realizados nos ambientes reais da execução do sistema e experimento são realizados em ambientes simulados.

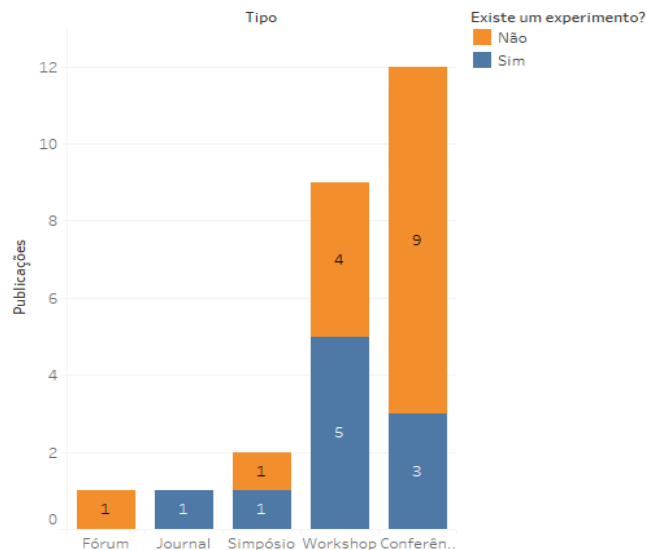
Os 25 estudos selecionados foram divididos em seus respectivos tipos de publicações e se apresentavam estudos de caso ou experimentos, o Gráfico 3 ajuda a visualizar a relação dos veículos de publicação com os trabalhos que apresentaram Estudos de Caso. Os tipos de publicações foram baseados nos nomes dos eventos em que foram publicados, por exemplo, uma publicação no *Proceedings of the First International Workshop on Software Engineering for Systems-of-Systems* foi considerada como *Workshop*.

**Gráfico 3** - Estudos que apresentaram estudos de caso



Fonte: a autora.

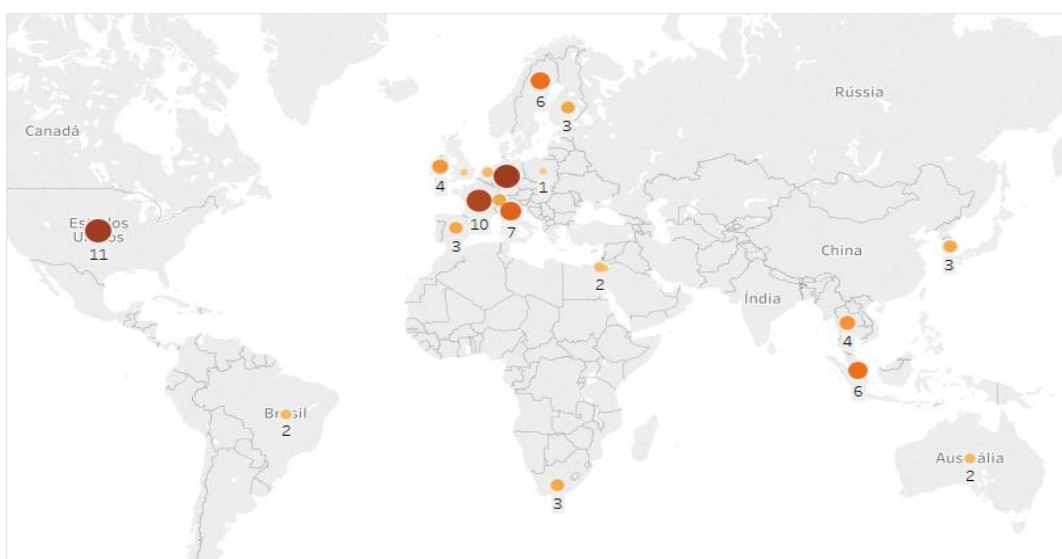
O Gráfico 4 ajuda a visualizar a relação dos veículos de publicação com os trabalhos que apresentaram Experimentos. É importante observar que um trabalho pode apresentar as duas avaliações, como foi o caso de 9 estudos ou nenhuma delas, onde apenas dois estudos não apresentaram nenhuma avaliação.

**Gráfico 4 - Estudos que apresentaram experimentos**

Fonte: a autora.

#### 6.4 - Autores por País

Dos 25 estudos selecionados foram contabilizados 85 pesquisadores (ver Apêndice D) no total. A Figura 4 apresenta as marcações desses autores de acordo com seu país. Essa visualização é importante para verificar em quais países há um maior movimento de pesquisa na área. É possível observar que a Europa possui o maior número de pesquisadores envolvidos. Os países com o maior número de envolvidos são a Alemanha que apresenta 11 pesquisadores de igual modo os Estados Unidos, seguidos pela França com 10. O Brasil é representado por dois autores no estudo P1 (ver Apêndice D).

**Figura 4 - Autores por Países**

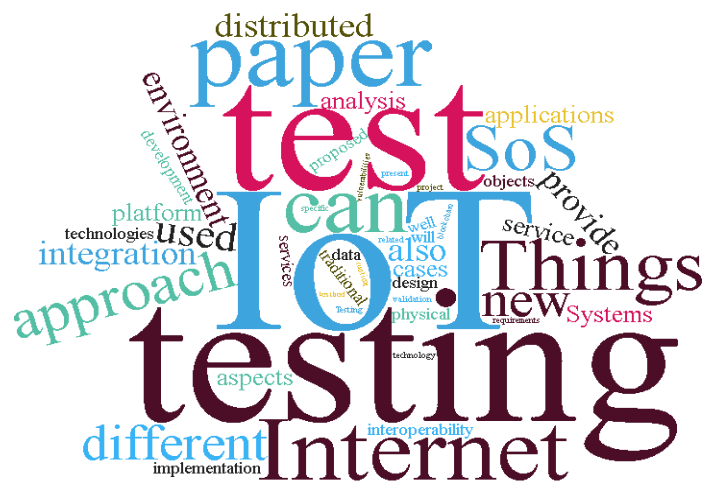
Fonte: a autora.



## 6.5 - Nuvem de Palavras

A partir dos 25 estudos foram levantadas as palavras que surgiram com maior frequência nos textos, pode-se observar na Figura 9, que as palavras mais comuns foram: *test*, *IoT*, *SoS*, são as palavras presentes na *string* de busca, confirmando a relação dos estudos selecionados com as questões de pesquisa.

**Figura 5** - Nuvem de Palavras



Fonte: a autora.

## 6.6 - Ameaças à validade do mapeamento

No decorrer das construções do mapeamento foram verificadas algumas possíveis ameaças que invalidaria o mapeamento, abaixo elas são apresentadas.

- Trabalhos relevantes podem ter sido rejeitados: a quantidade de trabalhos retornados na execução da *string*, tornou o processo do mapeamento árduo e cansativo, como medida de minimização desse problema foram definidos os estudos de controle (ver subseção 5.1) apresentados no início do trabalho que ajudaram a validar os resultados da busca.
- Poucos Revisores: este mapeamento foi produzido por uma aluna da graduação de ES e uma especialista em ES. A quantidade pequena de revisores pode ter interferido no resultado do mapeamento, quando se diz respeito a dúvidas em selecionar ou não estudos, pois não havia outros revisores para estabelecer uma decisão comum. Porém, o fato de ter poucos revisores foi minimizado pelo fato da especialista ter conhecimento

no domínio abordado neste mapeamento. Dessa forma, em caso de divergências, a especialista tomava a decisão.

- *String* de busca: a elaboração da *string* pode levar a perdas de estudos relevantes para a pesquisa, a falta de um termo na *string* ou o excesso de termos, podem manipular os resultados e tornar o mapeamento inválido, porém, esse problema foi minimizado com a definição da *string* de busca baseada nos termos chaves das questões de pesquisa que foram previamente revisadas pela especialista.
- Detalhamento dos estudos: Por muitas vezes os estudos não ofereciam o detalhamento necessário para o preenchimento do formulário a fim de responder às questões de pesquisa, mas, nesse caso, os estudos eram descartados ou discutidos com a especialista sobre a importância em sua seleção.

## 7 - CONCLUSÃO

Este trabalho apresentou um mapeamento sistemático de testes para aplicações IoT com o intuito de levantar as principais abordagens que estão sendo usadas nesses testes e os principais desafios. De 2157 de estudos obtidos restaram apenas 25, o que é um número pequeno considerando a relevância do tema abordado. No Gráfico 2 da Seção 4.2, a área está em crescimento, o esperado é que nos próximos anos mais estudos estejam sendo publicados, visto que é de extrema importância pesquisar sobre esse assunto, pois quando há a intenção de promover um ambiente de IoT, ou seja, diversos objetos inteligentes que conversam entre si, testes precisam ser aplicados nesses ambientes a fim de garantir essa interação, caso contrário não há garantia de que as características de IoT estejam presentes na aplicação.

Esse mapeamento teve como base o modelo de processo proposto por Kitchenham e Charters. A metodologia apresentada consistiu em três fases: Planejamento, Condução e Resultados. No Planejamento foram identificadas as necessidades do mapeamento e definido o protocolo (ver Apêndice A). O protocolo é o documento responsável por conduzir o Mapeamento, nele foram definidas as questões de pesquisa, que foram respondidas na etapa de Resultados, os critérios de exclusão e inclusão, a *string* de busca que foi utilizada nas bases de dados, *ACM Library* e *IEEE Xplore*, para a obtenção dos resultados. Na fase de Condução foram feitas as seleções dos estudos, que se dividiu em três etapas. Após a execução da *string* nas bases, o resultado passou para a primeira etapa onde foi feita a retirada dos estudos duplicados, após isso, na etapa 2 foi executada a seleção dos estudos com base no Título, Resumo e Palavras-Chaves e então os 67 estudos selecionados passaram para etapa 3 onde foram analisados o texto completo e assim gerado os 25 estudos finais. Vale ressaltar que as etapas 2 e 3 eram realizadas em paralelo, uma análise da especialista quanto aos estudos. Na fase dos Resultados foram respondidas as questões de pesquisa, apresentados graficamente os dados gerados e discutida a validade do mapeamento.

Dos 25 estudos levantados no mapeamento foram verificadas 7 abordagens onde a mais usada foi o “Teste Baseado em Modelos”, 8 estudos utilizaram essa abordagem, a construção de “Plataformas ou Ferramentas” foram usados em 4 estudos, três estudos apresentaram o “Teste Automatizado” como abordagem utilizadas, o “*Testbed*” também foi apresentado em três estudos, “Emuladores” de ambientes foram apresentados em 2 estudos, 1 estudo levantou a abordagem de “Injeção de Falhas” e outro usou a abordagem “SOA”, três estudos não destacaram nenhuma abordagem. É possível verificar uma quantidade relativamente alta de abordagens comparando a quantidade de estudos avaliados, de 25 estudos foram levantadas 7

abordagens, com isso, pode-se constatar que há um esforço de estudos na área, porém, não há comparativo entre as abordagens de testes utilizadas, indicando, por exemplo, qual seria mais adequada. Acreditamos que isso ocorra pelo fato de ser uma área de pesquisa mais recente e, portanto, menos explorada.

A contribuição do estudo de qualidade se deu na averiguação validade do conteúdo dos estudos, como por exemplo, se tinha feito experimentos ou não ou se tinha realizado uma discussão sobre os resultados obtidos, a partir disso é possível avaliar a credibilidade do trabalho. No levantamento dos resultados foram avaliados os que continham Estudos de Caso ou Experimentos que os avaliassem, dentro dos 25 estudos, 22 deles possuíam estudos de caso e 10 deles apresentaram algum experimento. A partir desses dados é possível verificar a relevância dos estudos, os que apresentam algo já validado oferecem um maior respaldo à pesquisa.

Além das abordagens de teste, foram levantados os principais desafios encontrados nos testes das aplicações IoT, através desses desafios é possível evidenciar as peculiaridades dos testes dessas aplicações. Nos 25 estudos selecionados foram encontrados 10 desafios, os destaques principais são de Segurança, Interoperabilidade e Desempenho, o primeiro devido a dificuldade em garantir a confidencialidade dos dados em diferentes aplicações, o segundo por construir testes que possam ser usados para diferentes contextos e que abarque diferentes arquiteturas e o último trata principalmente da dificuldade definir um ambiente de teste que garanta um alto desempenho, porém, com um baixo custo de energia.

Em conjunto ao levantamento dos desafios foi feita a relação com as possíveis características mais críticas de serem testadas das aplicações IoT. Segurança, Alterações Dinâmicas e Conectividade foram definidas, pelos estudos, como a mais crítica, com isso é possível vislumbrar onde os esforços de pesquisa devem ser mais fortemente concentrados, a fim de buscar soluções para os problemas que estão sendo mais desafiadores.

Além disso, também foram apresentados os possíveis problemas que poderiam invalidar esse mapeamento, tais como: trabalhos que poderiam ser importantes que devido à quantidade de estudos retornados, possam ter sido descartados. Outro problema seria a *string* de busca que poderia não contemplar algum termo ou conter em excesso os termos alterando assim o resultado.

Porém, mesmo com essas possibilidades, foi possível levantar estudos que, em sua grande maioria, apresentavam estudos de casos ou experimentos que validassem suas abordagens e também com resultados obtidos no mapeamento vislumbrou-se um crescimento

grande na pesquisa a partir de 2017, ou seja, a área está em ascensão, possivelmente diversos estudos deverão surgir nos próximos anos.

Com esse mapeamento concluiu-se que a área de teste de aplicações IoT está em crescimento, esforços estão sendo, mais fortemente, investidos nos últimos anos, até porque a Internet das Coisas é um assunto ainda recente, porém, existe uma necessidade de maior aprofundamento, definições de padrões, metodologias, processos que sejam validados como auxílios significativos nos testes de IoT.

Como perspectiva futura deste trabalho, os próximos passos são o aprofundamento em algum dos desafios encontrados nos testes dessas aplicações, esse aprofundamento pode ser feito com a realização de uma Revisão Sistemática, através dos resultados poderia ser fornecido auxílio na realização dos testes no contexto IoT escolhido.

## REFERÊNCIAS

ALI, N. B.; PETERSEN, K.; MANTYLA, M. V. Testing Highly Complex System of Systems: an Industrial case study. In: PROCEEDINGS OF THE ACM-IEEE INTERNATIONAL SYMPOSIUM ON EMPIRICAL SOFTWARE ENGINEERING AND MEASUREMENT, 2012, Lund - Suécia. **Proceedings**[...]. IEEE, 2012. p. 211–220.

ALIPOUR, M. A. Fault Injection in the Internet of Things Applications. In: PROCEEDINGS OF THE 1ST ACM SIGSOFT INTERNATIONAL WORKSHOP ON TESTING EMBEDDED AND CYBER-PHYSICAL SYSTEMS, 2017, Santa Barbara, CA – USA, **Proceedings**[...]. ACM, 2017. p 9-11.

AMALFTANO, D.; SIMONE, V. D.; RICCIO, V.; RITA, F. A. Towards a Thing-In-the-Loop Approach for the Verification and Validation of IoT Systems. In: PROCEEDINGS OF THE 1ST ACM WORKSHOP ON THE INTERNET OF SAFE THINGS, 2017, Delft - Holanda, **Proceedings**[...]. ACM, 2017. p. 57–63

Anzelmo, E.; Bassi, A.; Caprio, D.; Dodson, S.; Kranenburg, R.; Ratto, M. Internet of Things. Institute for Internet and Society, Berlin, 2011.

ASHTON, K. That ‘Internet of Things’ Thing. **RFID Journal**, 22 jun. 2009. Disponível em: <<http://www.rfidjournal.com/articles/view?4986>>. Acesso em: 28 maio 2018.

Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: a survey. **Computer Networks**, [S. l.], v. 54, p. 2787-2805, 28 out. 2010.

Bandyopadhyay, D.; Sen, J. Internet of things: Applications and challenges in technology and standardization. **Wireless Personal Communication**, [S. l.], v. 58, n. 1, p. 49–69, mai. 2011.

BRADY, S.; HAVA, A.; PERRY, P., A.; MAGONIY, D.; PORTILLO-DOMINGUEZ, A. O. Towards an emulated IoT test environment for anomaly detection using NEMU. In: PROCEEDINGS OF THE 2017 GLOBAL INTERNET OF THINGS SUMMIT (GIOTS), 2017, Geneva - Suíça. **Proceedings**[...]. IEEE, 2017.

Collotta, M.; Pau, G. A Solution Based on Bluetooth Low Energy for Smart Home Energy Management. **Energies**, [S. l.], v. 8, p. 11916–11938, out. 2015.

WORKSHOP DE INOVAÇÃO (INTERNET DAS COISAS, DRONES, CIDADES INTELIGENTES, ENTRE OUTRAS) CREA-RJ, 2017, Rio de Janeiro: INOVPLAN, 2017. Disponível em: <[http://www.sympla.com.br/workshop-de-inovacao-internet-das-coisas-drones-cidades-inteligentes-entre-outras-crea-rj\\_\\_109767](http://www.sympla.com.br/workshop-de-inovacao-internet-das-coisas-drones-cidades-inteligentes-entre-outras-crea-rj__109767)>. Acesso em: 01 jun. 2018.

DAHMANN, J.; G. REBOVICH, J; LANE; LOWRY, R. Systems of systems test and evaluation challenges. In: PROCEEDINGS OF INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS SYSTEMS OF SYSTEMS ENGINEERING CONFERENCE, 2010, Loughborough -Reino Unido. **Proceedings**[...]. IEEE, 2010. p. 1-6.

ELIAS, A. G. F.; RODRIGUES, J. J. P. C.; OLIVEIRA, L. M. L.; ZARPELÃO, B. B. A ubiquitous model for wireless sensor networks monitoring. In: PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON INNOVATIVE MOBILE AND INTERNET SERVICES IN UBIQUITOUS COMPUTING (IMIS '12), 2012, Palermo - Itália. **Proceedings**[...]. IEEE, 2012. p. 835-839.

FARAHMANDPOUR, Z.; VERSTEEG, S.; HAN, J.; KAMESWARAN, A. Service Virtualisation of Internet-of-things Devices: techniques and Challenges. In: PROCEEDINGS OF THE 3RD INTERNATIONAL WORKSHOP ON RAPID CONTINUOUS SOFTWARE ENGINEERING, 2017, Buenos Aires - Argentina. **Proceedings**[...]. IEEE, 2017. p. 32–35.

FEHLMANN, T.; KRANICH, E. Autonomous Real-time Software & Systems Testing. In: PROCEEDINGS OF THE 27TH INTERNATIONAL WORKSHOP ON SOFTWARE MEASUREMENT AND 12TH INTERNATIONAL CONFERENCE ON SOFTWARE PROCESS AND PRODUCT MEASUREMENT, 2017, Gothenburg - Suécia. **Proceedings**[...]. ACM, 2017. p. 54–63.

Felizardo, K.R.; Nakagawa, E.Y.; Fabri, S.C.P.F; Ferrari, F.C. **Revisão Sistemática da Literatura em Engenharia de Software**: teoria e prática. [S. l.]: Elsevier. 2017.

Friedewald, M.; Raabe, O. Ubiquitous computing: An overview of technology impacts. **Telematics and Informatics**, [S. l.], v. 28, p. 55-65, mai. 2011.

GARCÍA, S. N. M.; GARCÍA, M.; HERNÁNDEZ-RAMOS, J. L.; SKARMETA, A. F. Test-based risk assessment and security certification proposal for the Internet of Things. In: PROCEEDINGS OF THE 2018 IEEE 4TH WORLD FORUM ON INTERNET OF THINGS (WF-IoT), 2018, Singapore - Singapore. **Proceedings[...]**. IEEE, 2018. p. 641-646.

GIRARD, P. Power-aware testing in the Era of IoT. In: PROCEEDINGS OF THE 2018 19TH INTERNATIONAL SYMPOSIUM ON QUALITY ELECTRONIC DESIGN (ISQED), 2018, Santa Clara, CA - USA. **Proceedings[...]**. IEEE, 2018. p. 17–20.

Giusto, D.; Iera, A.; Morabito, G.; Atzori, L. **The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications**. New York:Springer, 2010.

HAMAD, R. M. H. Automation Testing and Monitoring Lab on the Cloud for IOT Smart Fleet System (ATML SFS). In: PROCEEDINGS OF THE FOURTH INTERNATIONAL CONFERENCE ON ENGINEERING MIS 2018, 2018, Istanbul - Turquia. **Proceedings[...]**. ACM, 2018. p. 42:1--42:7.

A INTERNET das Coisas na Indústria: a criação de novos modelos de negócios a partir da transformação da interação entre consumidor, produto e indústria. Recife: Instituto SENAI de Inovação para Tecnologias da Informação e Comunicação, 2018.

JURAJ P. VLADIMÍR B. Iot challenge: older test machines modernization in an automotive plant. n Michal Balog, Lucia Knapcikova, Jakub Soviar, Peter Dorcak, Frantisek Pollak, Dagmar Caganova, Peppino Fazio and Kadir Aydin. SmartCity360 2016, 2016.

K. M. BRZEZINSKI. Tiny TTCN-Inspired Testing Tools for Experimenting with Hybrid IoT Systems. In: PROCEEDINGS OF THE 2018 11TH INTERNATIONAL CONFERENCE ON HUMAN SYSTEM INTERACTION (HSI), 2018, Gdansk - Polônia. **Proceedings[...]**. IEEE, 2018, p. 261-267.



KANSTREN, T.; MÄKELÄ, J.; KARHULA, P. Architectures and Experiences in Testing IoT Communications. In: PROCEEDINGS OF THE 2018 IEEE INTERNATIONAL CONFERENCE ON SOFTWARE TESTING, VERIFICATION AND VALIDATION WORKSHOPS (ICSTW), 2018, Vasteras - Suécia. **Proceedings**[...]. IEEE, 2018, p. 98-103.

Kim, H.; Ahmad, A.; Hwang, J.; Baqa, H.; Le Gall, F.; Reina Ortega, M. A.; Song, J. Iot-taas: Towards a prospective iot testing framework. **IEEE Access**, [S. l.], v. 6, p. 15480–15493, fev. 2018.

KITCHENHAM, B. Procedures for performing systematic reviews. Disponível em: <http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf>. Acesso em: 01 de maio de 2018.

Kitchenham, B.; Charters, S. Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, 2007.

Kitchenham, B.A.; Brereton, O.P.; Budgen, D. Using Mapping Studies as the Basis for Further Research – A Participant-Observer Case Study. **Information and Software Technology**, ACM, v. 53, p. 638–651, jun. 2011.

KRISTOFFERSEN, M.; LÖTBÄCK, C. P.; SKOUSEN, D. Reverberation chambers for flexible over-the-air testing of internet-of-things devices. In: PROCEEDINGS OF THE 2017 IEEE INTERNATIONAL SYMPOSIUM ON ANTENNAS AND PROPAGATION USNC/URSI NATIONAL RADIO SCIENCE MEETING, 2017, San Diego, CA - USA. **Proceedings**[...]. IEEE, 2017. p. 1937-1938.

Lee, I.; Lee, K. The IoT (IoT): applications, investments, and challenges for enterprises. **Business Horizons**, v. 58, p. 431-440, abr. 2015.

LIANG, Q.; RUBIN, S. H. Randomization for testing systems of systems. In: PROCEEDINGS OF THE 2009 IEEE INTERNATIONAL CONFERENCE ON INFORMATION REUSE INTEGRATION, 2009, Las Vegas, NV - USA. **Proceedings**[...]. IEEE, 2009. p. 110-114.

MAIA, P.; CAVALCANTE, E.; GOMES, P.; BATISTA, T.; DELICATO, F.C.; PIRES, P.F. On the development of systems-of-systems based on the Internet of Things. In:

PROCEEDINGS OF THE 2014 EUROPEAN CONFERENCE ON SOFTWARE ARCHITECTURE WORKSHOPS, 2014, Viena - Áustria. **Proceedings**[...], ACM, 2014. p. 23:1–23:8

Marwah, Q.; Mateen; Sirshar, M. Software Quality Assurance in Internet of Things. **International Journal of Computer Applications**, v. 109, p. 16–24, jan. 2015.

MAURIN, T.; DUCREUX, L. F.; CARAIMAN, G.; SISSOKO, P. Iot security assessment through the interfaces p-scan test bench platform. In: PROCEEDINGS OF THE 2018 DESIGN, AUTOMATION TEST IN EUROPE CONFERENCE EXHIBITION (DATE), 2018, Dresden - Alemanha. **Proceedings**[...], IEEE, 2018. p.1007-1008.

MYERS, G. J. **The Art of Software Testing**. Hoboken, NJ: Wiley, 1979.

Nair, K. K.; Dube, E.; Lefophane, S. Modelling an IoT testbed in context with the security vulnerabilities of South Africa. In: INTERNATIONAL CONFERENCE ON COMPUTER AND COMMUNICATIONS, 3., 2017, Chengdu, China. IEEE [...]. [S. l.]: **IEEE**, 2017.

NAKAGAWA, E. Y.; GONÇALVES, M.; GUESSI, M.; OLIVEIRA, L. B. R.; OQUENDO, F. The state of the art and future perspectives in systems of systems software architectures. In: PROCEEDINGS OF THE FIRST INTERNATIONAL WORKSHOP ON SOFTWARE ENGINEERING FOR SYSTEMS-OF-SYSTEMS, 2013, Montpellier - França. **Proceedings**[...], ACM, 2013. p. 13–20.

NEVES, V. O.; BERTOLINO, A.; ANGELIS, G.; GARCÉS, L. Do We Need New Strategies for Testing Systems-of-systems? In: PROCEEDINGS OF THE 6TH INTERNATIONAL WORKSHOP ON SOFTWARE ENGINEERING FOR SYSTEMS-OF-SYSTEMS, 2018, Gothenburg - Suécia. **Proceedings**[...], ACM, 2018. p. 29–32,

Pal, D.; Funilkul, S.; Charoenkitkarn, N.; Kanthamanon, P. Internet-of-Things and Smart Homes for Elderly Healthcare: An End User Perspective. **IEEE Access**, IEEE, v. 6, p. 10483–10496, fev. 2018.

Patel, K. L.; Patel, S. M. Internet of Things-IOT: Definition Characteristics Architecture Enabling Technologies Application Future Challenges. **International Journal of Engineering Science and Computing**, [S. l.], v. 6, p. 6122–6131, 2016.

PETERSEN, K.; FELDT, R.; MUJTABA, S.; MATTSSON, M. Systematic mapping studies in software engineering. In: PROCEEDINGS OF THE 12TH INTERNATIONAL CONFERENCE ON EVALUATION AND ASSESSMENT IN SOFTWARE ENGINEERING, 2008, Itália. **Proceedings**[...], ACM, 2008. p. 68–77.

PIEL, É.; GONZALEZ-SANCHEZ, A. Data-flow Integration Testing Adapted to Runtime Evolution in component-based systems. In: PROCEEDINGS OF THE 2009 ESEC/FSE WORKSHOP ON SOFTWARE INTEGRATION AND EVOLUTION, 2009, Amsterdam - Holanda. **Proceedings**[...], [S. l.], 2009. p. 3–10.

PLANET Idea Smart Enginner. Disponível em: <<http://www.planetidea.it/>> . Acesso em: 01 jun. 2018.

Razzaque, M. A.; Milojevic-Jevric, M.; Palade, A.; Clarke, S. Middleware for Internet of Things: A survey. **IEEE Internet Things J**, IEEE, v. 3, n. 1, p. 70–95, fev. 2016.

REETZ, E. S.; KUEMPER, D.; MOESSNER, K.; TOENJES, R. Test derivation for semantically described IoT services. In: FUTURE NETWORK AND MOBILE SUMMIT (FutureNetworkSummit), 2013, Guildford - Reino Unido. **Proceedings**[...], IEEE, 2013. p. 1–10.

REETZ, E. S.; KUEMPER, D.; MOESSNER, K.; TOENJES, R. How to Test IoT-based Services before Deploying them into Real World. In: PROCEEDINGS OF THE EUROPEAN WIRELESS 2013; 19TH EUROPEAN WIRELESS CONFERENCE, 2013, Guildford - Reino Unido. **Proceedings**[...], IEEE, 2013. p. 1–6.

ROSENKRANZ, P.; WÄHLISCH, M.; BACCELLI, E.; ORTMANN, L. A Distributed Test System Architecture for Open-source IoT Software. In: PROCEEDINGS OF THE ACM

MOBISYS WORKSHOP ON IOT CHALLENGES IN MOBILE AND INDUSTRIAL SYSTEMS, 2015, Florence - Itália. **Proceedings**[...], ACM, 2015. p. 43--48.

Runeson, P. & Höst, M. M. *Empir Software Eng* [US] Springer. 2008

SACHIDANANDA, V.; SIBONI, S.; SHABTAI, A.; TOH, J.; BHAIKAV, S.; ELOVICI, Y. Let the Cat Out of the Bag: A Holistic Approach Towards Security Analysis of the Internet of Things. In: PROCEEDINGS OF THE 3RD ACM INTERNATIONAL WORKSHOP ON IOT PRIVACY, TRUST, AND SECURITY, 2017, Abu Dhabi - Emirados Árabes Unidos. **Proceedings**[...], ACM, 2017. p. 3--10.

SAMANT, S. S.; CHHETRI, M. B.; VO, Q. B., K.; NEPAL, S. Towards Quality-Assured Data Delivery in Cloud-Based IoT Platforms for Smart Cities. In: PROCEEDINGS OF THE 2017 IEEE 3RD INTERNATIONAL CONFERENCE ON COLLABORATION AND INTERNET COMPUTING, 2017, San Jose, CA - USA. **Proceedings**[...], IEEE, 2017. p. 291--298.

Sampaio, A. Improving systematic mapping reviews. **SIGSOFT Softw. Eng.** ACM, v. 40, p. 1--8, nov. 2015.

Sand B. IoT Testing - The Big Challenge Why, What and How. **Springer**, Cham, v. 170, p. 70--76, 2016.

SCHIEFERDECKER, I.; KRETZSCHMANN, S.; RENNOCH, A.; WAGNER, M. IoT-Testware - An Eclipse Project. In: PROCEEDINGS OF THE 2017 IEEE INTERNATIONAL CONFERENCE ON SOFTWARE QUALITY, RELIABILITY AND SECURITY, 2017, Prague, República Tcheca. **Proceedings**[...], IEEE, 2017. p. 1--8.

SMART City Laguna Empreendimento. Disponível em: <<http://smartcitylaguna.com.br/empreendimento/>> . Acesso em: 01 jun. 2018.

Sommerville, I. *Engenharia de Software*. 9. ed. [S.l.]: Pearson Education, 2011.

TANG, X.; ZHANG, F.; LI, X.; KHAN, S. U.; LI, Z. Quantifying Cloud Elasticity with Container-based Autoscaling. In: PROCEEDINGS OF THE 2017 IEEE 15TH INTL CONF ON DEPENDABLE, AUTONOMIC AND SECURE COMPUTING, 15TH INTL CONF ON PERVASIVE INTELLIGENCE AND COMPUTING, 3RD INTL CONF ON BIG DATA INTELLIGENCE AND COMPUTING AND CYBER SCIENCE AND TECHNOLOGY CONGRESS(DASC/PICOM/DATACOM/CYBERSCITECH), 2017, Orlando, FL - USA. **Proceedings**[...], IEEE, 2017. p. 853–860.

VISOOTTIVISETH, V; AKARASIRIWONG, P.; CHAIYASART, P.; CHOTIVATUNYU, S. PENTOS: Penetration testing tool for Internet of Thing devices. In: PROCEEDINGS OF TENCON 2017 - 2017 IEEE REGION 10 CONFERENCE, 2017, Penang - Malásia, 2017. **Proceedings**[...], IEEE, 2017. p. 2279-2284.

WALKER, M. A.; DUBEY, A.; LASZKA, A.; SCHMIDT, D. C. PlaTIBART: A Platform for Transactive IoT Blockchain Applications with Repeatable Testing. In: PROCEEDINGS OF THE 4TH WORKSHOP ON MIDDLEWARE AND APPLICATIONS FOR THE INTERNET OF THINGS, 2017, Las Vegas, Nevada - USA. **Proceedings**[...], ACM, 2017. p. 17–22.

Wohlin, C.; Runeson, P.; Silveira Neto; P.A.M.; Engstrom, E.; Machado, I.C.; Almeida, E.A. On the Reliability of Mapping Studies in Software Engineering. **Journal of Systems and Software**, [S. l.], v. 86, n. 10, p. 2594–2610, out. 2013.

ZIEGLER, S.; KIM, E. E. Towards an open framework of online interoperability and performance tests for the Internet of Things. In: PROCEEDINGS OF THE 2017 GLOBAL INTERNET OF THINGS SUMMIT (GIoTS), 2017, Geneva - Suíça. **Proceedings**[...], IEEE, 2017. p. 1–6.

## APÊNDICE A

### Um Mapeamento Sistemático de Testes para Aplicações IoT

Liana M. C. Menezes; Valéria L.L Dantas  
Universidade Federal do Ceará, Russas, Brasil  
*valerialelli@ufc.br; lianacdemenezes@gmail.com*

#### Protocolo de Mapeamento Sistemático

##### Objetivo:

Caracterizar o estado da arte dos testes em aplicações IoT por meio de um mapeamento sistemático. Deste modo o objetivo é levantar as abordagens usadas nos testes de aplicações IoT e os principais desafios encontrados nesses testes.

##### Questões de Pesquisa:

- Q1: Quais as abordagens utilizadas para testar aplicações IoT?
- Q2: Quais são os desafios encontrados nos testes de aplicações IOT?
- Q3: Quais são as características de aplicações IOT mais críticas para o processo de teste?

##### Palavras-chaves:

test, approach, internet of things, systems of systems

##### Critérios PICO:

- População: À todos que tenham interesse em visualizar o estado da arte no âmbito de testes em aplicações IoT
- Intervenção: Abordagens utilizadas nos testes de aplicações IoT
- Comparação: Não se aplica
- Resultados: O estado da arte em testes de aplicações IoT, no que diz respeito às abordagens usadas, desafios encontrados e características IoT mais críticas a serem testadas

##### Seleção das Fontes:

- Critério de definição da seleção das fontes: Busca na internet de bases, que possivelmente, mais teriam estudos relacionados à área em questão
- Língua dos Estudos: Inglês
- Fontes de Pesquisa: IEEE Xplore e ACM Digital Library
- *String* de Busca:

*("internet of things"OR "IoT" OR "system of system" OR "systems of systems")*

AND

(*test OR testing*)

AND

(*approach OR process OR method OR procedure OR technique OR methodology OR model OR framework OR tool OR architecture*)

### Seleção dos Estudos:

- **Critérios de Inclusão:**

**Critério 1 - Todos os estudos devem conter resumos:** Serão selecionados aqueles estudos que contiverem pelo menos um resumo inicial, para que possa ser executado a primeira fase da seleção.

**Critério 2 - Estudos que tratam de testes para aplicações IoT:** Trabalhos que tratam de sistemas IoT, que apresente a etapa de teste em seu contexto serão selecionados.

**Critério 3 - Estudos escritos em inglês:** Por inglês tratar-se de um idioma abrangente para a comunidade científica e para facilitar a produção do mapeamento e o uso dos resultados, optou-se por considerar apenas trabalhos neste idioma.

- **Critérios de Exclusão:**

**Critério 1 - O estudo é apenas um resumo:** Em muitos casos o estudo publicado é apenas um resumo, como uma apresentação de pôster em evento, por esse critério tais estudos serão descartados. Não confundir com artigos curtos (*short papers*), por mais que sejam curtos, duas ou três páginas, são apresentados resumos. Um estudo que se trata apenas de resumos não apresenta corpos.

**Critério 2 - O estudo é uma versão reduzida de outro:** Às vezes há publicações que são feitas em diferentes veículos de publicações e são lançadas em versões mais curtas, desse modo serão considerados apenas os estudos na versão completa para que se pode obter todas as informações relevantes para o estudo.

**Critério 3 - Não é possível ter acesso ao estudo:** Para a segunda etapa de seleção será considerado o estudo por inteiro, caso não seja possível o acesso completo ao estudo, o mesmo será desconsiderado.

## APÊNDICE B

## Formulário de Extração dos Dados

<b>Item</b>	<b>Valor</b>	<b>Comentário</b>
<b>Ano</b>		
<b>Autor</b>		
<b>Título</b>		
<b>Base de Dados</b>		
<b>São de autores brasileiros? (Sim/Não)</b>		
<b>Palavras-Chaves</b>		
<b>Que tipos de trabalhos de referência?</b>		
<b>Onde foi publicado</b>		
<b>Objetivo do Estudo</b>		
<b>Tipo de iniciativa</b>		
<b>Descrição da Iniciativa</b>		
<b>Descrição da importância da iniciativa</b>		
<b>Resultados do trabalho</b>		
<b>Trabalhos futuros</b>		
<b>Estudo da Qualidade</b>		
<b>Existe um estudo de caso? (Sim/Não)</b>		
<b>Existe um experimento? (Sim/Não)</b>		
<b>Os objetivos do estudo estão claramente definidos? (Sim / Não)</b>		
<b>Existe alguma discussão sobre os resultados do estudo? (Sim / Não / Parcialmente)</b>		



## APÊNDICE C

### Formulário de Extração dos Dados – Estudo P1

Item	Valor
<b>Ano</b>	2018
<b>Autor</b>	Vânia de Oliveira Neves, Antonia Bertolino, Guglielmo De Angelis e Lina Garcés
<b>Título</b>	<i>Do We Need New Strategies for Testing Systems-of-systems?</i>
<b>Base de Dados</b>	ACM
<b>São de autores brasileiros? (Sim/Não)</b>	Sim, dois deles
<b>Palavras-Chaves</b>	systems-of-systems, testing, validation
<b>Que tipos de trabalhos referência?</b>	Workshop
<b>Onde foi publicado</b>	SESoS '18 Proceedings of the 6th International Workshop on Software Engineering for Systems-of-Systems Pages 29-32
<b>Objetivo do Estudo</b>	Apresentar abordagens existentes de VV & T podem ser usadas para SoS
<b>Tipo de iniciativa</b>	Estudo exploratório
<b>Descrição da Iniciativa</b>	Analisar as principais características dos Sistemas de Sistemas (SoS) que podem afetar sua verificação, validação e teste (VV & T). Com isso apresentar abordagens existentes de VV & T podem ser usadas para SoS.
<b>Descrição da importância da iniciativa</b>	Ajuda a visualizar como possíveis SoS podem ser testados e assim quem sabe estender até aplicações IoT
<b>Resultados do trabalho</b>	Foram apresentadas 4 abordagens que poderiam ser usadas para testar SoS's: Baseado em Componentes, SOA, Teste adaptativo e Testes Concorrentes.
<b>Trabalhos futuros</b>	Não é dito
<b>Existe um estudo de caso? (Sim/Não)</b>	Sim
<b>Existe um experimento? (Sim/Não)</b>	Não
<b>Os objetivos do estudo estão claramente definidos?</b>	Sim
<b>Existe alguma discussão sobre os resultados do estudo?</b>	Sim

### Formulário de Extração dos Dados – Estudo P2

Item	Valor
<b>Ano</b>	2018
<b>Autor</b>	Ruba Mohammad; Haj Hamad (Hamad, R. M. H., 2018)
<b>Título</b>	<i>Automation Testing and Monitoring Lab on the Cloud for IOT Smart Fleet System (ATML e SFS)</i>
<b>Base de Dados</b>	ACM
<b>São de autores brasileiros? (Sim/Não)</b>	Não
<b>Palavras-Chaves</b>	Compatibility Testing, IOT Testing, Mobile Testing, Performance Testing, Security Testing, Smart Fleet System, Testing Lab on the Cloud
<b>Que tipos de trabalhos referência?</b>	Conferência
<b>Onde foi publicado</b>	ICEMIS '18 Proceedings of the Fourth International Conference on Engineering & MIS 2018 Article No. 42
<b>Objetivo do Estudo</b>	Apresentar um Laboratório de Testes e Monitoramento de Automação (ATML) na nuvem para testar e monitorar sistemas IoT em todos os níveis relacionados e um protótipo para Smart Fleet Systems (SFS) da IoT para ajudar as empresas de comércio eletrônico a gerenciar as operações da frota com eficiência
<b>Tipo de iniciativa</b>	Arquitetura de uma ferramenta
<b>Descrição da Iniciativa</b>	Promover um ATML na nuvem que será conectada a um sistema IoT para executar scripts de testes de automação e aumento da qualidade. Este ATML ser instalado e configurado na nuvem.

<b>Descrição da importância da iniciativa</b>	<i>Contribuir para testar tecnologias integradas e aumentar o nível de qualidade delas.</i>
<b>Resultados do trabalho</b>	<i>É apresentado o ATML que é um grupo de ferramentas integradas de teste automatizado e monitoramento mecanismos para acelerar a fase de testes e apoiar QTEs para alcançar um alto nível de qualidade com menor custo, tempo e esforço. Em segundo lugar, o Smart Fleet System (SFS) pode gerenciar, controlar e monitorar as operações da frota de empresas de comércio eletrônico todos os bens, pacotes e encomendas durante a jornada de entrega e cumprir os embarques para seus clientes.</i>
<b>Trabalhos futuros</b>	<i>Não é dito</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

### Formulário de Extração dos Dados – Estudo P3

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2018</i>
<b>Autor</b>	<i>Teemu Kanstren, Jukka Mäkelä, Pekka Karhula (Kanstren, T. et al., 2018)</i>
<b>Título</b>	<i>Architectures and Experiences in Testing IoT Communications</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>embedded systems; Internet of Things ;program testing; software architecture; software reliability; sensor nodes; end-user services; dynamic communication;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)</i>
<b>Objetivo do Estudo</b>	<i>Apresentar as experiências com diferentes aspectos do teste de comunicações de IoT e arquiteturas de teste relacionadas.</i>
<b>Tipo de iniciativa</b>	<i>Estudo de caso</i>
<b>Descrição da Iniciativa</b>	<i>Foram construídos vários sistemas de IoT e testados em ambientes para vários tipos em diferentes domínios, como saúde, sistemas industriais e esportes. Isso inclui o sensores para coletar os dados, os gateways para agregar e gerenciar os dados na borda da rede e os serviços a processar os dados. Incluiu a concepção dos sistemas e ambientes de teste relacionados, para os próprios sistemas e os de nossos parceiros. E então apresentado a experiência desses testes.</i>
<b>Descrição da importância da iniciativa</b>	<i>Apresenta os problemas comuns no teste de aplicações IoT independente do domínio.</i>
<b>Resultados do trabalho</b>	<i>A experiência, em comparação com testes de software mais gerais, o elemento mais específico em testes de IoT é a comunicação altamente distribuída e dinâmica de nós de IoT, como sensores. Outros desafios para o teste de confiabilidade da IoT são os elementos arquiteturais dos gateways IoT que conectam os dispositivos às redes e as próprias redes que podem hospedar todos os outros tipos de tráfego ao mesmo tempo.</i>
<b>Trabalhos futuros</b>	<i>Não é dito</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

### Formulário de Extração dos Dados – Estudo P4

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2018</i>

<b>Autor</b>	<i>Hiun Kim, Abbas Ahmad, Jaeyoung Hwang, Hamza Baqa, Franck Le Gall, Miguel Angel Reina Ortega, and Jaeseung Song (Kim, H. et al., 2018)</i>
<b>Título</b>	<i>IoT-TaaS: Towards a Prospective IoT Testing Framework</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>conformance testing; Internet of Things; open systems; program testing; Web services; scalable automated conformance testing; testing components; prospective IoT Testing framework; distributed decentralized form;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Journal</i>
<b>Onde foi publicado</b>	<i>IEEE Access ( Volume: 6 )</i>
<b>Objetivo do Estudo</b>	<i>Apresentar uma abordagem baseada em serviços para uma estrutura de testes de IoT automatizada</i>
<b>Tipo de iniciativa</b>	<i>Abordagem</i>
<b>Descrição da Iniciativa</b>	<i>IoT Testing funciona como um Service-IoT-TaaS, uma nova abordagem baseada em serviços para uma estrutura de testes de IoT automatizada com o objetivo de resolver restrições relacionadas a coordenação, custos e escalabilidade de testes de software tradicionais no contexto de padrões desenvolvimento baseado em dispositivos de IoT e explorar seu design e implementação.</i>
<b>Descrição da importância da iniciativa</b>	<i>Como a escalabilidade dos testes de software tradicionais, e a heterogeneidade dos dispositivos de IoT aumenta os custos, a ideia é através do IoT Testing diminuir a complexidade da coordenação de testes.</i>
<b>Resultados do trabalho</b>	<i>Foi apresentado conceitos de teste de interoperabilidade, juntamente com validação semântica para testar vários dispositivos e plataformas de IoT. Como esses conceitos são agora implementado e adotado como uma ferramenta para certificações de IoT, e esses conceitos terão papéis fundamentais uma moderna estrutura de testes de IoT.</i>
<b>Trabalhos futuros</b>	<i>Trabalhar com novas IoT técnicas de teste, uma vez que fornecem conceitos fundamentais e aprimora o IoT-TaaS.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

#### Formulário de Extração dos Dados – Estudo P5

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2018</i>
<b>Autor</b>	<i>Sara N. Matheu García, Jose L. Hernández-Ramos, Antonio F. Skarmeta (García, S. N. M. et al., 2018)</i>
<b>Título</b>	<i>Test-based risk assessment and security certification proposal for the Internet of Things</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>certification; Internet of Things; risk management ;security of data; security certification proposal; certification methodology; risk assessment phase; security solutions; large-scale</i>
<b>Que tipos de trabalhos referência?</b>	<i>Fórum</i>
<b>Onde foi publicado</b>	<i>2018 IEEE 4th World Forum on Internet of Things (WF-IoT)</i>
<b>Objetivo do Estudo</b>	<i>Propor uma metodologia de certificação para IoT</i>
<b>Tipo de iniciativa</b>	<i>Metodologia</i>
<b>Descrição da Iniciativa</b>	<i>Propõem o projeto de uma metodologia de certificação para IoT, prestando atenção à fase de avaliação de risco baseada em teste para capacitar os testadores com a capacidade de avaliar soluções de segurança para implantações de IoT em larga escala.</i>
<b>Descrição da importância da iniciativa</b>	<i>Ajudar aos testadores a exergarem melhor as possíveis falhas de segurança dentro de aplicações IoT.</i>

<b>Resultados do trabalho</b>	<i>A metodologia Armor foi apresentada com todas as suas fases, baseada na proposta do ETSI, centrando-se no risco avaliação.</i>
<b>Trabalhos futuros</b>	<i>Geração automática de testes de segurança também como a automação dos resultados por meio do MBT, CertifyIT e TITAN.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Não</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

**Formulário de Extração dos Dados – Estudo P6**

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2018</i>
<b>Autor</b>	<i>Thomas Maurin, Laurent-Frédéric Ducreux, George Caraiman, Philippe Sissoko (Maurin, T. et al., 2018)</i>
<b>Título</b>	<i>IoT security assessment through the interfaces P-SCAN test bench platform</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>Internet of Things; security of data; IoT security assessment; P-SCAN test bench platform; interconnected networks; cyber-attacks; mainstream industrial devices; IoT products; P-SCAN test platform;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2018 Design, Automation &amp; Test in Europe Conference &amp; Exhibition (DATE)</i>
<b>Objetivo do Estudo</b>	<i>Apresentar a plataforma P-SCAN, como forma de democratizar a avaliação de segurança de objetos conectados.</i>
<b>Tipo de iniciativa</b>	<i>Estudo de Caso/Avaliação</i>
<b>Descrição da Iniciativa</b>	<i>Estudo de Caso/Avaliação</i>
<b>Descrição da importância da iniciativa</b>	<i>A plataforma de teste P-SCAN é projetada como uma solução conveniente para democratizar a avaliação de segurança de objetos conectados. Associada a diretrizes que facilitam a definição de um destino de segurança de dispositivo, a plataforma fornece uma biblioteca de conjuntos de testes que permite automatizar o processo de teste de recursos de segurança nas interfaces de comunicação do dispositivo.</i>
<b>Resultados do trabalho</b>	<i>Foi descrito alguns aspectos relacionados ao segurança cibernética para IoT. E apresentado o P-SCAN, contribuindo na melhoria desses desafios.</i>
<b>Trabalhos futuros</b>	<i>Não foi dito</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Não</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

**Formulário de Extração dos Dados – Estudo P7**

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2018</i>
<b>Autor</b>	<i>Krzysztof M. Brzezinski (K. M. Brzezinski, 2018)</i>
<b>Título</b>	<i>Tiny TTCN-Inspired Testing Tools for Experimenting with Hybrid IoT Systems</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>Internet of Things; program testing; specification languages; hybrid IoT systems; Tiny TTCN-inspired Testing Tool; IoT-class distributed systems; virtually zero-cost on-line passive testing technology;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2018 11th International Conference on Human System Interaction (HSI)</i>

<b>Objetivo do Estudo</b>	<i>Realmente constatou-se as "técnicas de desconto, custando menos, mas, no entanto, o custo do trabalho a ser medido em termos de quanto esforço é necessário para aprender ainda é alto. Mostrou que é tecnicamente possível realizar a metas definidas usando os recursos extremamente limitados do Plataforma Arduino, embora o espaço não permita um exemplo de um programa de testes completo a ser testado.</i>
<b>Tipo de iniciativa</b>	<i>Ferramenta</i>
<b>Descrição da Iniciativa</b>	<i>Um testador é construído em torno de um microcontrolador de classe Arduino e é programado em uma linguagem de teste que recria a semântica básica e a aparência da linguagem de teste padronizada TTCN-3 (Testing and Test Control Notation). Destina-se à prototipagem rápida e como uma plataforma de desenvolvimento única para a validação de sistemas distribuídos de classe IoT envolvendo humanos em loop, especialmente para supervisão discreta a longo prazo de experimentos de mudança de comportamento em estado selvagem em um casa instrumentada / instalação de trabalho.</i>
<b>Descrição da importância da iniciativa</b>	<i>Minimiza os custos na realização de teste em aplicações IoT</i>
<b>Resultados do trabalho</b>	<i>Realmente constatou-se as "técnicas de desconto, custando menos mas, no entanto, o custo do trabalho a ser medido em termos de quanto esforço é necessário para aprender ainda é alto. Mostrou que é tecnicamente possível realizar a metas definidas usando os recursos extremamente limitados do Plataforma Arduino, embora o espaço não permita um exemplo de um programa de testes completo a ser testado.</i>
<b>Trabalhos futuros</b>	<i>Não é dito</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

#### Formulário de Extração dos Dados – Estudo P8

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Michael A. Walker, Abhishek Dubey, Aron Laszka, and Douglas C. Schmidt (Walker, M. A. et al., 2017)</i>
<b>Título</b>	<i>PlaTIBART: A Platform for Transactive IoT Blockchain Applications with Repeatable Testing</i>
<b>Base de Dados</b>	<i>ACM</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>blockchain, design patterns, internet of things, testing</i>
<b>Que tipos de trabalhos referência?</b>	<i>Workshop</i>
<b>Onde foi publicado</b>	<i>M4IoT '17 Proceedings of the 4th Workshop on Middleware and Applications for the Internet of Things</i>
<b>Objetivo do Estudo</b>	<i>Oferecer uma plataforma de teste reatíveis para aplicações IoT com blockchain</i>
<b>Tipo de iniciativa</b>	<i>Plataforma</i>
<b>Descrição da Iniciativa</b>	<i>PlaTIBART é uma plataforma para aplicações blockchain de IoT com testes repetíveis que combinam o padrão Actor (que é um modelo comumente usados de computação em IoT) junto com uma linguagem específica de domínio (DSL) e ferramentas de gerenciamento de rede de teste.</i>
<b>Descrição da importância da iniciativa</b>	<i>Plataforma para desenvolver, testar e analisar aplicativos blockchain IoT tolerantes a falhas.</i>
<b>Resultados do trabalho</b>	<i>Os resultados dos experimentos apresentaram que a plataforma tem alta consistência nos dados de teste ao serem comparados, levando a ser viável a construção de testes repetitivos.</i>
<b>Trabalhos futuros</b>	<i>Tentar diminuir as restrições que a plataforma tem em administrar as configurações dos arquivos DSL que são usados como entrada na aplicação.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>

Os objetivos do estudo estão claramente definidos?	<i>Sim</i>
Existe alguma discussão sobre os resultados do estudo?	<i>Sim</i>

**Formulário de Extração dos Dados – Estudo P9**

Item	Valor
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Vinay Sachidananda, Shachar Siboni, Asaf Shabtai, Jinghui Toh, Suhas Bhairav, Yuval Elovici (Sachidananda, V. et al., 2017)</i>
<b>Título</b>	<i>Let the Cat Out of the Bag: A Holistic Approach Towards Security Analysis of the Internet of Things</i>
<b>Base de Dados</b>	<i>ACM</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>internet of things (IoT), privacy, security, testbed framework</i>
<b>Que tipos de trabalhos referência?</b>	<i>Workshop</i>
<b>Onde foi publicado</b>	<i>IoTPTS '17 Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security</i>
<b>Objetivo do Estudo</b>	<i>Realizar uma análise na segurança de aplicações IoT através de testes de penetração (escaneamento de porta, impressão digital, enumeração de processo e verificação de vulnerabilidades)</i>
<b>Tipo de iniciativa</b>	<i>Estudo de caso</i>
<b>Descrição da Iniciativa</b>	<i>Realização de uma análise de segurança para dispositivos de IoT e introduzido com testbed de IoT para realizar essas análises.</i>
<b>Descrição da importância da iniciativa</b>	<i>É trivial executar a análise de segurança para dispositivos IoT para entender os buracos de loop e a própria natureza dos dispositivos.</i>
<b>Resultados do trabalho</b>	<i>A análise de segurança foi conduzido com dispositivos IoT de última geração e os relatórios apresentados mostram que esses dispositivos são vulneráveis, através dos resultados apresentados no trabalho é possível ver isso.</i>
<b>Trabalhos futuros</b>	<i>Desenvolver ainda mais a arquitetura da proposta sistema de análise de segurança, a fim de tornar a arquitetura mais adaptável e sintonizável. Isso permitirá testar dispositivos IoT mais facilmente com qualquer protocolo e capacidades de comunicação.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

**Formulário de Extração dos Dados – Estudo P10**

Item	Valor
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Zeinab Farahmandpour, Steve Versteeg, Jun Han, Anand Kameswaran (Farahmandpour, Z. et al., 2017)</i>
<b>Título</b>	<i>Service Virtualisation of Internet-of-things Devices: Techniques and Challenges</i>
<b>Base de Dados</b>	<i>ACM</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>continuous delivery, internet-of-things, service virtualisation</i>
<b>Que tipos de trabalhos referência?</b>	<i>Workshop</i>
<b>Onde foi publicado</b>	<i>RCoSE '17 Proceedings of the 3rd International Workshop on Rapid Continuous Software Engineering Pages 32-35</i>
<b>Objetivo do Estudo</b>	<i>Identificar os principais desafios técnicos que precisam ser abordados para implementar virtualização de serviços em ambientes de IoT.</i>
<b>Tipo de iniciativa</b>	<i>Estudo Exploratório</i>
<b>Descrição da Iniciativa</b>	<i>Examinar as diferenças estruturais entre vários protocolos IoT e protocolos corporativos e assim entender os desafios existentes para virtualizar serviços em ambientes IoT, a fim de usar esses ambientes virtualizados para testar automaticamente os serviços corporativos em condições de produção.</i>

<b>Descrição da importância da iniciativa</b>	<i>A virtualização pode acelerar o desenvolvimento de aplicativos IoT, ativando testes automatizados sem exigir uma conexão contínua com os dispositivos físicos.</i>
<b>Resultados do trabalho</b>	<i>Foram e identificados protocolos principais em IoT e levantados os desafios em virtualizar o serviços da mesma como principais desafio levantaram o de heterogeneidade e sincronização de comunicação.</i>
<b>Trabalhos futuros</b>	<i>Para abordar a heterogeneidade, é planejado implementar uma extensão da Opaque Service Virtualization. Em particular, uma fase explícita de modelagem de dados a ser incluído na abordagem. Isso permitirá a criação de ambientes de IoT sem exigir conhecimento prévio dos protocolos IoT. Isso ajudará muito aos desenvolvedores de IoT testem continuamente suas aplicações de forma automatizada sem exigir acesso aos dispositivos físicos.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

#### Formulário de Extração dos Dados – Estudo P11

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Thomas Fehlmann, Eberhard Kranich (Fehlmann, T.; Kranich, E., 2017)</i>
<b>Título</b>	<i>Autonomous real-time software &amp; systems testing</i>
<b>Base de Dados</b>	<i>ACM</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>automated testing, defects density, headcombinatory logic, legal compliance, metrics for software testing, real-time testing, six sigma for software, testing the internet of things (iot)</i>
<b>Que tipos de trabalhos referência?</b>	<i>Workshop</i>
<b>Onde foi publicado</b>	<i>IWSM Mensura '17 Proceedings of the 27th International Workshop on Software Measurement and 12th International Conference on Software Process and Product Measurement Pages 54-63</i>
<b>Objetivo do Estudo</b>	<i>Apresentar uma abordagem para a realização de testes em tempo real</i>
<b>Tipo de iniciativa</b>	<i>Abordagem</i>
<b>Descrição da Iniciativa</b>	<i>Descreve a abordagem de implementação como uma estrutura para testes em tempo real autônomos de um sistema baseado em software em tempo de execução, com um exemplo da IoT.</i>
<b>Descrição da importância da iniciativa</b>	<i>Para segurança no setor automotivo ou para proteção de dados, seja legalmente compatível, é necessário testar o impacto de quaisquer ações antes de permitir que elas ocorram. No entanto, os limites do sistema mudam no tempo de execução. Ao adicionar um novo dispositivo anteriormente desconhecido a um contexto IoT, o sistema base original se expande e precisa ser testado antes de poder tomar decisões com o potencial de afetar os seres humanos.</i>
<b>Resultados do trabalho</b>	<i>Para testes a IoT, essa abordagem oferece uma economia significativa; No entanto, o pleno potencial da lógica combinatória na organização do conhecimento é significativamente maior.</i>
<b>Trabalhos futuros</b>	<i>Adicionar mais "coisas" a esse sistema requer testes que provam segurança e proteção, outras qualidades e funcionalidades do sistema expandido.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Não</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

#### Formulário de Extração dos Dados – Estudo P12

<b>Item</b>	<b>Valor</b>
-------------	--------------

<b>Ano</b>	2017
<b>Autor</b>	Domenico Amalfitano, Vincenzo De Simone, Vincenzo Riccio, Fasolino Anna Rita (Amalfitano, D. et al., 2017)
<b>Título</b>	<i>Towards a Thing-In-the-Loop Approach for the Verification and Validation of IoT Systems</i>
<b>Base de Dados</b>	ACM
<b>São de autores brasileiros? (Sim/Não)</b>	Não
<b>Palavras-Chaves</b>	<i>Internet of Things, Model-driven engineering, Thing-In-the-loop, verification and validation</i>
<b>Que tipos de trabalhos referência?</b>	Workshop
<b>Onde foi publicado</b>	<i>SafeThings'17 Proceedings of the 1st ACM Workshop on the Internet of Safe Things Pages 57-63</i>
<b>Objetivo do Estudo</b>	<i>Abordagem de verificação e validação Thing-In-the-Loop baseada em modelos que transfere as melhores práticas adotadas em diferentes domínios do sistema embarcado para o mundo da IoT.</i>
<b>Tipo de iniciativa</b>	Abordagem
<b>Descrição da Iniciativa</b>	<i>Geração de casos de teste apropriados que são executados de acordo com o modelo Thing-In-the-Loop.</i>
<b>Descrição da importância da iniciativa</b>	<i>Ajudar no fornecimento de soluções valiosas e eficazes para apoiar a verificação e validação de sistemas IoT.</i>
<b>Resultados do trabalho</b>	<i>A abordagem permitiu testar as coisas, mesmo quando a parte principal do sistema não está disponível, desde que um modelo do Contexto seja definido. Além disso, não requer manualmente definir Casos de Teste específicos para cada plataforma na qual a Coisa é vai ser implantado.</i>
<b>Trabalhos futuros</b>	<i>Estender a abordagem para suportar: integração, interoperabilidade, desempenho e testes de segurança de Sistemas de IoT.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	Sim
<b>Existe um experimento? (Sim/Não)</b>	Sim
<b>Os objetivos do estudo estão claramente definidos?</b>	Sim
<b>Existe alguma discussão sobre os resultados do estudo?</b>	Sim

#### Formulário de Extração dos Dados – Estudo P13

Item	Valor
<b>Ano</b>	2017
<b>Autor</b>	Mohammad Amin Alipour (Alipour, M. A., 2017)
<b>Título</b>	<i>Fault Injection in the Internet of Things Applications</i>
<b>Base de Dados</b>	ACM
<b>São de autores brasileiros? (Sim/Não)</b>	Não
<b>Palavras-Chaves</b>	<i>Fault Injection, Internet of Things, Smart Home</i>
<b>Que tipos de trabalhos referência?</b>	Workshop
<b>Onde foi publicado</b>	<i>TECPS 2017 Proceedings of the 1st ACM SIGSOFT International Workshop on Testing Embedded and Cyber-Physical Systems Pages 9-11</i>
<b>Objetivo do Estudo</b>	<i>Aumentar a conscientização dos programadores sobre as situações que podem surgir na natureza das falhas de sistemas através da injeção de falhas.</i>
<b>Tipo de iniciativa</b>	Abordagem
<b>Descrição da Iniciativa</b>	<i>É proposto um conjunto preliminar de falhas para injeção de falhas na Internet das Coisas baseada em eventos, a fim de investigar o teste de aplicativos da Internet of Things</i>
<b>Descrição da importância da iniciativa</b>	<i>Com a inserção de falhas no sistema ajudará os testes em aplicações IoT assim como os programadores a lidar com essas falhas</i>
<b>Resultados do trabalho</b>	<i>A injeção de falhas pode ser cara em sistemas com muitos eventos possíveis. Desse modo foi usado a injeção de falhas como um meio entender e modelar falhas na programação para eventos baseados em eventos.. Essa técnica pode não ser bem dimensionada para grandes sistemas cyber-físicos em rede com diversos tipos de dispositivos, mas pelo menos ajuda a fornecer uma maior compreensão. Um problema com esta abordagem é a relação entre o comportamento da simulação e o comportamento do real sistema. Quando os</i>



	<i>desenvolvedores criam simulações, eles estão abstraindo e simplificando o comportamento dos dispositivos.</i>
<b>Trabalhos futuros</b>	<i>Automatizar a geração de testes para Smart- Sistemas de coisas.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

#### Formulário de Extração dos Dados – Estudo P14

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Sebastien Ziegler, Eunsook Eunah Kim (Ziegler, S.; Kim, E. E, 2017)</i>
<b>Título</b>	<i>Towards an open framework of online interoperability and performance tests for the Internet of Things</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>Internet of Things; open systems; open framework; online interoperability; Internet of Things; F-Interop European research project; online platform; IoT interoperability testing; IoT solutions;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2017 Global Internet of Things Summit (GIoTS)</i>
<b>Objetivo do Estudo</b>	<i>Apresentar um conjunto inicial de resultados do projeto de pesquisa europeu F-Interop que pesquisa plataforma online para testes de interoperabilidade e desempenho para a Internet das Coisas</i>
<b>Tipo de iniciativa</b>	<i>Estudo de Caso</i>
<b>Descrição da Iniciativa</b>	<i>O teste de interoperabilidade da IoT é um passo importante para as soluções de IoT, mas os testes atuais face-a-face são ineficientes em termos de custos e exigem mão-de-obra intensiva. A F-Interop tem como objetivo fornecer interoperabilidade on-line, conformidade e ferramentas de teste de desempenho, permitindo testes remotos.</i>
<b>Descrição da importância da iniciativa</b>	<i>Fornecer uma extensa plataforma experimental para testes on-line.</i>
<b>Resultados do trabalho</b>	<i>A plataforma F-Interop ainda está em fase de desenvolvimento, mas já lançou uma chamada aberta com financiamento dedicado para apoiar colaborações com terceiros interessados em desenvolver ferramentas de testes complementares, abordar padrões e / ou organizar a interoperabilidade baseada em F-Interop testes em processos de padronização.</i>
<b>Trabalhos futuros</b>	<i>A F-Interop pretende fornecer um progresso além do estado de a arte em termos de experiência do usuário também.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

#### Formulário de Extração dos Dados – Estudo P15

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Mats Kristoffersen, Christian Patané Lötbäck, Derek Skousen (Kristoffersen, M. et al., 2017)</i>
<b>Título</b>	<i>Reverberation chambers for flexible over-the-air testing of internet-of-things devices</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>Bluetooth; Internet of Things; reverberation chambers; over-the-air testing ;internet-of-things devices; wireless devices; test volume; total isotropic sensitivity; Bluetooth devices; reverberation chamber setups;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Simpósio</i>

<b>Onde foi publicado</b>	<i>2017 IEEE International Symposium on Antennas and Propagation &amp; USNC/URSI National Radio Science Meeting</i>
<b>Objetivo do Estudo</b>	<i>Propor a realização de testes flexíveis em câmara de reverberação para testar dispositivos IoT</i>
<b>Tipo de iniciativa</b>	<i>Estudo de Caso</i>
<b>Descrição da Iniciativa</b>	<i>É analisada a potência total irradiada e a sensibilidade isotrópica total para três modelos de dispositivos Bluetooth. As medições são repetidas em três configurações diferentes de câmaras de reverberação com tamanhos muito diferentes, com o objetivo de investigar se os resultados alinhados podem ser obtidos.</i>
<b>Descrição da importância da iniciativa</b>	<i>Apresentar outra possível abordagem que possa ajudar a testar a flexibilidade de dados nos dispositivos IoT</i>
<b>Resultados do trabalho</b>	<i>Os resultados mostram que uma clara a classificação do desempenho pode ser obtida, com muito boa repetibilidade inter e intra-câmara. Em todos os casos, os resultados para cada dispositivo estava dentro de 0,6 dB, independentemente do tamanho da câmara.</i>
<b>Trabalhos futuros</b>	<i>Não é dito</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

#### Formulário de Extração dos Dados – Estudo P16

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Shane Brady, Adriana Hava, Philip Perry, John Murphy, Damien Magoniy, and A. Omar Portillo Domínguez (Brady, S. et al., 2017)</i>
<b>Título</b>	<i>Towards an emulated IoT test environment for anomaly detection using NEMU</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>cyber-physical systems; Internet of Things ;performance evaluation; power aware computing; ubiquitous computing; emulated IoT test environment; anomaly detection; NEMU; Internet of Things; ubiquitous connected devices; smart objects ;cyber-physical systems;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2017 Global Internet of Things Summit (GIoTS)</i>
<b>Objetivo do Estudo</b>	<i>Apresentar um ambiente para emular testes de IoT, mais barato.</i>
<b>Tipo de iniciativa</b>	<i>Ferramenta</i>
<b>Descrição da Iniciativa</b>	<i>Propõem um método para emular um ambiente de IoT usando o Network Emulator for Mobile Universes (NEMU), construído sobre o popular emulador de sistema QEMU, a fim de construir um testbed de dispositivos Raspberry Pi emulados interconectados</i>
<b>Descrição da importância da iniciativa</b>	<i>Facilita a replicação por outros pesquisadores e assim facilita o teste dessas aplicações.</i>
<b>Resultados do trabalho</b>	<i>O resultados experimentais mostraram como tal emulador se assemelha a um ambiente real da IoT, já que ambos tipos de ambientes produziram resultados semelhantes quando usados Aplicativos IoT. No entanto, os resultados também mostraram que o processamento e aplicações intensivas de memória não devem ser avaliadas na emulação, pois as performances ainda são muito diferentes de um sistema real. Os profissionais devem, portanto, verificar se a IoT aplicação sob teste não está estressando os dispositivos em termos de processamento, memória ou largura de banda de rede, caso contrário o testbed emulado será incorreto.</i>
<b>Trabalhos futuros</b>	<i>concentrará no fortalecimento do experimento de validação da abordagem.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>

Os objetivos do estudo estão claramente definidos?	<i>Sim</i>
Existe alguma discussão sobre os resultados do estudo?	<i>Sim</i>

#### Formulário de Extração dos Dados – Estudo P17

Item	Valor
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Vasaka Visoottiviseth, Phuripat Akarasiriwong, Siravitch Chaiyasart, Siravit Chotivatunyu (Visoottiviseth, V et al., 2017)</i>
<b>Título</b>	<i>PENTOS: Penetration testing tool for Internet of Thing devices</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>computer crime; computer network security; graphical user interfaces; Internet of Things; Linux; PENTOS system; IoT vulnerabilities; security guidance; Web attack; Internet of Things technology; wireless attack; password attack;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>TENCON 2017 - 2017 IEEE Region 10 Conference</i>
<b>Objetivo do Estudo</b>	<i>Apresentar um sistema de teste de penetração para dispositivos IoT chamado PENTOS</i>
<b>Tipo de iniciativa</b>	<i>Ferramenta</i>
<b>Descrição da Iniciativa</b>	<i>PENTOS reúne automaticamente as informações do dispositivo IoT de destino por meio da comunicação sem fio, que é WiFi e Bluetooth. O sistema permite que os usuários executem vários tipos de testes de penetração em seus dispositivos de IoT, como ataque de senha, ataque na Web, e ataque sem fio, a fim de obter o privilégio de acesso por vários algoritmos.</i>
<b>Descrição da importância da iniciativa</b>	<i>umentar a conscientização de segurança do usuário</i>
<b>Resultados do trabalho</b>	<i>Foi apresentado os testes realizados no PENTOS e ele se mostrou uma ferramenta apropriada para testes em penetração.</i>
<b>Trabalhos futuros</b>	<i>adicionar um função para realizar testes de penetração para protocolos de IoT</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

#### Formulário de Extração dos Dados – Estudo P18

Item	Valor
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Ina Schieferdecker, Sascha Kretzschmann, Axel Rennoch, Michael Wagner (Schieferdecker, I. et al., 2017)</i>
<b>Título</b>	<i>IoT-Testware - An Eclipse Project</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>Internet of Things; program testing; public domain software; IoT-testware; Eclipse project; TTCN-3 test suites; protocols; CoAP; MQTT; ETSI ES 201873;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)</i>
<b>Objetivo do Estudo</b>	<i>Apresentar a ferramenta IoT-Testware que tem por intuito fornecer um conjunto avançado de suítes de testes TTCN-3 e casos de teste para tecnologias IoT</i>
<b>Tipo de iniciativa</b>	<i>Ferramenta</i>
<b>Descrição da Iniciativa</b>	<i>Inicialmente, o IoT-Testware se concentrará em protocolos como CoAP e MQTT. Para garantir a independência da tecnologia de teste e implementação, os conjuntos de testes serão realizados no TTCN-3 e implementados com o Titan. O TTCN-3 foi definido e padronizado pelo</i>

	<i>European Telecommunication Standards Institute no ETSI ES 201873 e pacotes de extensão relacionados. Ele é implementado e suportado no Eclipse IoT pelo projeto Titan.</i>
<b>Descrição da importância da iniciativa</b>	<i>Permite que os desenvolvedores criem um ambiente de teste abrangente, se necessário, desde o início de um projeto.</i>
<b>Resultados do trabalho</b>	<i>Fornecimento de um conjunto de testes aberto para os sistemas IoT e soluções é uma maneira possível de atender a qualidade exigida de tais implementações. ETSI, por exemplo, fornece conjuntos de testes padronizados disponíveis publicamente (conformidade, interoperabilidade, benchmarking de desempenho, etc.) implementado com TTCN-3 para quase todos os seus padrões protocolo de comunicação ou especificação de serviço em todo o domínio fronteiras.</i>
<b>Trabalhos futuros</b>	<i>TTCN-3 VIRTUALIZADO</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

#### Formulário de Extração dos Dados – Estudo P19

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2017</i>
<b>Autor</b>	<i>Kishor Krishnan Nair, Erick Dube, Samuel Lefophane (Nair, K. K. et al., 2017)</i>
<b>Título</b>	<i>Modelling an IoT testbed in context with the security vulnerabilities of South Africa</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>cloud computing; Internet; Internet of Things; security of data; South Africa; transformative approach; heterogeneous devices; potential threats; possible attacks; IoT devices;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2017 3rd IEEE International Conference on Computer and Communications (ICCC)</i>
<b>Objetivo do Estudo</b>	<i>Apresentar a implementação de um testbed de IoT centrado no usuário e automatizado</i>
<b>Tipo de iniciativa</b>	<i>Ferramenta</i>
<b>Descrição da Iniciativa</b>	<i>Implementação de um testbed de IoT centrado no usuário e automatizado, em um contexto próximo ao ambiente sul-africano do mundo real para lidar com as vulnerabilidades específicas do IoT no país.</i>
<b>Descrição da importância da iniciativa</b>	<i>Contribuição para preencher a lacuna que falta na área de vulnerabilidades de segurança de IoT, mas também contribuirá para uma melhor compreensão do assunto e aceitação de a tecnologia IoT.</i>
<b>Resultados do trabalho</b>	<i>O testbed opera e gerencia dentro de um tangível ambiente de segurança no qual os testes automatizados de IoT ser executado. Isso aumentará as chances de atender às objetivos e metas esperados do projeto. O testbed precisa coletar dados durante a execução do teste de segurança, usado para realizar análise forense de segurança e relatórios. Além disso, os resultados dos testes eo relatório produzido contém o tipo de configuração do dispositivo de ponto de extremidade IoT, conectividade, protocolos de comunicação suportados e casos de teste de segurança executados e seu status (sucesso ou falha).</i>
<b>Trabalhos futuros</b>	<i>Implementar as ideias propostas no trabalho</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

## Formulário de Extração dos Dados – Estudo P20

Item	Valor
Ano	2015
Autor	Philipp Rosenkranz, Matthias Wählisch (Rosenkranz, P. et al., 2015) Omar Portillo-Dominguez
Título	A Distributed Test System Architecture for Open-source IoT Software
Base de Dados	ACM
São de autores brasileiros? (Sim/Não)	Não
Palavras-Chaves	interoperability, open-source iot, test system architecture
Que tipos de trabalhos referência?	Workshop
Onde foi publicado	IoT-Sys '15 Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems Pages 43-48
Objetivo do Estudo	Discutir os desafios específicos do teste de sistemas de software de IoT abertos.
Tipo de iniciativa	Arquitetura
Descrição da Iniciativa	Propor uma estrutura de teste que (a) suporta técnicas de integração contínua, (b) permite a integração dos colaboradores do projeto de voluntariado recursos de hardware e software para o sistema de teste, e (c) pode funcionar como um plugtest distribuídos permanente para testes de interoperabilidade da rede .
Descrição da importância da iniciativa	A arquitetura introduz grupos de testes, permitindo que praticamente qualquer pessoa contribuir com plataformas de teste para este sistema. Essas plataformas distribuídas de teste permitem acesso compartilhado a dispositivos IoT únicos ou testbeds IoT de pleno direito. Além disso, o sistema permite casos de teste em diferentes plataformas de teste, devido ao uso de uma camada de abstração de plataforma. A mesma camada de abstração também simplifica as funcionalidades funcionais e de interopera- testes.
Resultados do trabalho	A arquitetura pode ser usado para testes de interoperabilidade de rede por encaminhamento o tráfego de comunicação de um sistema em teste para outros, independentemente da sua localização física, criando assim plug-in distribuído permanente.
Trabalhos futuros	null
Existe um estudo de caso? (Sim/Não)	Sim
Existe um experimento? (Sim/Não)	Não
Os objetivos do estudo estão claramente definidos?	Sim
Existe alguma discussão sobre os resultados do estudo?	Sim

## Formulário de Extração dos Dados – Estudo P21

Item	Valor
Ano	2013
Autor	Eike Steffen Reetz, Daniel Kuemper, Klaus Moessner, Ralf Tonjes (Reetz, E. S. et al., 2013)
Título	How to Test IoT-based Services before Deploying them into Real World
Base de Dados	IEEE Explorer
São de autores brasileiros? (Sim/Não)	Não
Palavras-Chaves	functional testing; model-based testing; stream X-Machine; semantic test derivation
Que tipos de trabalhos referência?	Conferência
Onde foi publicado	European Wireless 2013; 19th European Wireless Conference
Objetivo do Estudo	Propor uma abordagem para testar a criação de serviços baseada em IoT em uma metodologia de inserção de código
Tipo de iniciativa	Abordagem
Descrição da Iniciativa	Uma nova abordagem para testar a criação de serviços baseada em IoT em uma metodologia de inserção de código, que pode ser derivada da descrição semântica do serviço baseado em IoT. A interface de

	<i>emulação de recursos IoT proposta é descrita da perspectiva semântica, arquitetural e de implementação.</i>
<b>Descrição da importância da iniciativa</b>	<i>Oferecer uma solução de teste de aplicações sem exijam muita capacidade de tempo e recursos.</i>
<b>Resultados do trabalho</b>	<i>A solução proposta de uma emulação de recursos interface, diretamente controlada pela estrutura de teste, tem potencial para simplificar e acelerar o processo de teste devido a questões de tempo das soluções concorrentes.</i>
<b>Trabalhos futuros</b>	<i>Investigar se o modelo de emulação pode ser estendido tanto por medições físicas de recursos de IoT (por exemplo, atrasos típicos de resposta) ou descrições semânticas do recurso IoT.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

#### Formulário de Extração dos Dados – Estudo P22

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2012</i>
<b>Autor</b>	<i>Nauman Bin Ali, Kai Petersen, Mika V. Mäntylä (Ali, N. B. et al., 2012)</i>
<b>Título</b>	<i>Testing Highly Complex System of Systems: An Industrial Case Study</i>
<b>Base de Dados</b>	<i>ACM</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>case study, software test, system of systems</i>
<b>Que tipos de trabalhos referência?</b>	<i>Simpósio</i>
<b>Onde foi publicado</b>	<i>ESEM '12 Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement Pages 211-220</i>
<b>Objetivo do Estudo</b>	<i>Apresentar os desafios em testes de SoS para a indústria</i>
<b>Tipo de iniciativa</b>	<i>Estudo de Caso</i>
<b>Descrição da Iniciativa</b>	<i>Muitas das características do SoS (como independência operacional e gerencial, a integração de sistema de sistemas, SoS composto de complexo sistemas) tornam seu desenvolvimento e teste desafiadores. Com isso é importante que essas desafios sejam levantados para possíveis investimentos no futuro.</i>
<b>Descrição da importância da iniciativa</b>	<i>Fornece uma compreensão de Teste de SoS em configurações de indústria em larga escala com relação a desafios e como abordá-los</i>
<b>Resultados do trabalho</b>	<i>Foram identificados os desafios relacionados ao SoS com com relação a falhas, teste de tempo de reversão e teste manutenção.</i>
<b>Trabalhos futuros</b>	<i>Não é abordado</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Sim</i>

#### Formulário de Extração dos Dados – Estudo P23

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2010</i>
<b>Autor</b>	<i>Dr. Judith Dahmann, Dr. Jo Ann Lane, George Rebovich, Ralph Lowry (Dahmann, J. et al., 2010)</i>
<b>Título</b>	<i>Systems of systems test and evaluation challenges</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>automatic test equipment; military computing; systems-of-systems test; military capabilities ;system-of-system approach; system-of-system engineering; System testing;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2010 5th International Conference on System of Systems Engineering</i>

<b>Objetivo do Estudo</b>	<i>Apresentar os principais desafios nos teste de SoS</i>
<b>Tipo de iniciativa</b>	<i>Estudo de Caso</i>
<b>Descrição da Iniciativa</b>	<i>Os sistemas de sistemas diferem dos sistemas tradicionais de maneiras que exigem a adaptação de processos de engenharia de sistemas para fornecer com êxito suas capacidades. Este artigo descreve as características distintas de sistemas de sistemas que afetam seus testes e avaliações, discute seus desafios únicos e sugere estratégias para gerenciá-los.</i>
<b>Descrição da importância da iniciativa</b>	<i>Ajudar a trabalhos futuros visualizar os principais desafios encontrados nessa área e assim abordá-los</i>
<b>Resultados do trabalho</b>	<i>Descreve várias estratégias de nível superior que as equipes do SoS SE estão empregando para alcançar e testes eficazes no nível do SoS. Estes focam no SoS SE estabelecendo uma estrutura para SoS T &amp; E, baseada em evidências abordagens, avaliação do SoS ao longo do tempo e estendendo os testes para incluir processos contínuos de feedback.</i>
<b>Trabalhos futuros</b>	<i>Não é dito</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>

#### Formulário de Extração dos Dados – Estudo P24

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2009</i>
<b>Autor</b>	<i>Éric Piel, Alberto GonzalezSanchez (Piel, É.; GonzalezSanchez, A., 2009)</i>
<b>Título</b>	<i>Data-flow Integration Testing Adapted to Runtime Evolution in Component-based Systems</i>
<b>Base de Dados</b>	<i>ACM</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>component-based, data-flow, evolution, integration testing</i>
<b>Que tipos de trabalhos referência?</b>	<i>Workshop</i>
<b>Onde foi publicado</b>	<i>SINTER '09 Proceedings of the 2009 ESEC/FSE workshop on Software integration and evolution @ runtime Pages 3-10</i>
<b>Objetivo do Estudo</b>	<i>Apresentado o conceito de componentes virtuais, uma maneira de definir unidades de comportamento de fluxo de dados que simplifica muito a definição e manutenção de testes de integração quando o sistema evolui em tempo de execução.</i>
<b>Tipo de iniciativa</b>	<i>Abordagem</i>
<b>Descrição da Iniciativa</b>	<i>As técnicas já existentes para integração e teste de tempo de execução são geralmente focadas em sistemas baseados em componentes que seguem o paradigma cliente-servidor e não são adequados para sistemas de fluxo de dados. É proposto uma abordagem que visa adequar o teste de integração ao tempo de execução.</i>
<b>Descrição da importância da iniciativa</b>	<i>Facilita o teste de integração de sistemas componentes organizados em um estilo de fluxo de dados.</i>
<b>Resultados do trabalho</b>	<i>O primeiro teste, TestWarning, verifica que os avisos são corretamente gerados em caso de inconsistência nas mensagens recebidas pelo núcleo do sistema. UMA seqüência de mensagens AIS é enviada em alta frequência (o que não está autorizado no protocolo AIS) e o caso de teste Seies que o aviso correto é gerado. O segundo teste, TestDuplicate, verifica que apenas um aviso é gerado mesmo que uma mensagem contendo inconsistências seja recebida várias vezes (o que é frequentemente o caso, como a cobertura de muitos estações locais se sobrepõem)</i>
<b>Trabalhos futuros</b>	<i>Ver como a técnica pode ser aplicado a estruturas de publicação / assinatura, onde os componentes nents não são explicitamente vinculados a outros, mas somente subscrever um tipo de dados.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Sim</i>

Os objetivos do estudo estão claramente definidos?	<i>Não</i>
Existe alguma discussão sobre os resultados do estudo?	<i>Não</i>

**Formulário de Extração dos Dados – Estudo P25**

<b>Item</b>	<b>Valor</b>
<b>Ano</b>	<i>2009</i>
<b>Autor</b>	<i>Qianhui Liang, Stuart H. Rubin (Liang, Q.; Rubin, S. H., 2009)</i>
<b>Título</b>	<i>Randomization for testing systems of systems</i>
<b>Base de Dados</b>	<i>IEEE Explorer</i>
<b>São de autores brasileiros? (Sim/Não)</b>	<i>Não</i>
<b>Palavras-Chaves</b>	<i>program testing; programming languages; software architecture; testing componentized systems of systems; randomization theory; software test cases; software systems;</i>
<b>Que tipos de trabalhos referência?</b>	<i>Conferência</i>
<b>Onde foi publicado</b>	<i>2009 IEEE International Conference on Information Reuse &amp; Integration</i>
<b>Objetivo do Estudo</b>	<i>Aplicar a teoria da randomização ao problema de selecionar casos de teste de software para sistemas e aplicativos de software, a fim de superar o obstáculo do alto custo no teste de sistemas de sistemas de componentes (SoS)</i>
<b>Tipo de iniciativa</b>	<i>Abordagem</i>
<b>Descrição da Iniciativa</b>	<i>Através do uso de uma semântica de ponto de canto, que pode aproximar uma prova de correção - denominada uma pseudo-prova de correção, é buscado randomizar o problema de selecionar casos de testes para SoS.</i>
<b>Descrição da importância da iniciativa</b>	<i>A contribuição de uma possível baixa nos custos de realizar a seleção dos casos de testes dessas aplicações.</i>
<b>Resultados do trabalho</b>	<i>A possibilidade de visualizar as vantagens da randomização no algoritmo, linguagem de programação, integração e design de fluxo de trabalho</i>
<b>Trabalhos futuros</b>	<i>Provar as vantagens de randomização em outros domínios.</i>
<b>Existe um estudo de caso? (Sim/Não)</b>	<i>Sim</i>
<b>Existe um experimento? (Sim/Não)</b>	<i>Não</i>
<b>Os objetivos do estudo estão claramente definidos?</b>	<i>Sim</i>
<b>Existe alguma discussão sobre os resultados do estudo?</b>	<i>Não</i>



## APÊNDICE D

### LISTA DE AUTORES, PAÍSES E UNIVESIDADES DOS ESTUDOS SELECIONADOS

<b>Autor</b>	<b>País</b>	<b>Universidade</b>
A. Omar Portillo-Dominguez	Irlanda	Universidade College Dublin
Abbas Ahmad	França	Mercado Global Fácil
Abhishek Dubey	Estados Unidos	Universidade de Vanderbilt
Adriana Hava	Irlanda	Universidade College Dublin
Alberto Gonzalez-Sanchez	Países Baixos	Universidade de Tecnologia de Delft
Anand Kameswaran	Estados Unidos	CA Technologies - Plano
Antonia Bertolino	Itália	Consiglio Nazionale delle Ricerche
Antonio F. Skarmeta	Espanha	Soluções Odin
Aron Laszka	Estados Unidos	Universidade de Vanderbilt
Asaf Shabtai	Israel	Universidade Ben-Gurion do Negev
Axel Rennoch	Alemanha	Fraunhofer FOKUS
Christian Patané Lötbäck	Suécia	Bluetest AB
Damien Magoni	França	Universidade de Bordeaux
Daniel Kuemper	Alemanha	Universidade de Ciências Aplicadas de Osnabruck
Derek Skousen	Suécia	Bluetest AB
Domenico Amalfitano	Itália	Universidade de Nápoles Federico II
Douglas C. Schmidt	Estados Unidos	Universidade de Vanderbilt
Eberhard Kranich	Alemanha	Escritório do Projeto Euro
Eike Steffen Reetz	Alemanha	Universidade de Ciências Aplicadas de Osnabruck
Emmanuel Baccelli	França	INRIA
Éric Piel	Países Baixos	Universidade de Tecnologia de Delft
Erick Dube	África do Sul	Modelagem e Ciência Digital (MDS)
Eunsook Eunah Kim	Suíça	Gateway de dispositivo
Fasolino Anna Rita	Itália	Universidade de Nápoles Federico II
Franck Le Gall	França	Mercado Global Fácil
George Caraiman	França	LCIE Bureau Veritas
George Rebovich	Estados Unidos	Universidade do Sul da California

Guglielmo De Angelis	Itália	Consiglio Nazionale delle Ricerche
Hamza Baqa	França	Mercado Global Fácil
Hiun Kim	Coreia do Sul	Universidade de Sejong
Ina Schieferdecker	Alemanha	TU Berlin e Fraunhofer FOKUS
Jaeseung Song	Coreia do Sul	Universidade de Sejong
Jaeyoung Hwang	Coreia do Sul	Universidade de Sejong
Jinghui Toh	Cingapura	Universidade de Tecnologia e Design de Cingapura
Jo Ann Lane	Estados Unidos	MITRA
John Murphy	Irlanda	Universidade College Dublin
Josá L. Hernández-Ramos	Espanha	Universidade de Múrcia
Judith Dahmann	Estados Unidos	MITRA
Jukka Makela	Finlândia	Centro de Pesquisa Técnica da Finlândia
Jun Han	Austrália	Universidade de Tecnologia de Swinburne
Kai Petersen	Suécia	Blekinge Institute of Technology
Kishor Krishnan Nair	África do Sul	Modelagem e Ciência Digital (MDS)
Klaus Moessner	Reino Unido	Universidade de Surrey
Krzysztof M. Brzezinski	Polónia	Universidade de Tecnologia de Varsóvia
Laurent-Frédéric Ducreux	França	Univ. Grenoble Alpes
Lina Garcés	Brasil	Universidade Federal de São Paulo
Ludwig Ortmann	Alemanha	Freie Universität Berlin
Mats Kristoffersen	Suécia	Bluetest AB
Matthias Wählich	Alemanha	Freie Universität Berlin
Michael A. Walker	Estados Unidos	Universidade de Vanderbilt
Michael Wagner	Alemanha	Fraunhofer FOKUS
Miguel Angel Reina Ortega	França	Instituto Europeu de Normas de Telecomunicações
Mika V. Mäntylä	Suécia	Universidade de Lund
Mohammad Amin Alipour	Estados Unidos	Universidade de Houston
Nauman Bin Ali	Suécia	Blekinge Institute of Technology
Nicola Amatucci	Itália	Universidade de Nápoles Federico II
Pekka Karhula	Finlândia	Centro de Pesquisa Técnica da Finlândia
Philipp Rosenkranz	Alemanha	Freie Universität Berlin
Philippe Sissoko	França	LCIE Bureau Veritas
Phuripat Akarasiriwong	Tailândia	Faculdade de Tecnologia da Informação e

		Comunicação
Qianhui Liang	Cingapura	Universidade de Administração de Cingapura
Ralf Tonjes	Alemanha	Universidade de Ciências Aplicadas de Osnabruck
Ralph Lowry	Estados Unidos	Soluções Tecnológicas Modernas
Ruba Mohammad Haj Hamad	Jordânia	Universidade Princesa Sumaya para Tecnologia
Samuel Lefophane	África do Sul	Modelagem e Ciência Digital (MDS)
Sara N. Matheu García	Espanha	Universidade de Múrcia
Sascha Kretzschmann	Alemanha	Fraunhofer FOKUS
Sebastien Ziegler	Suíça	Mandat International
Shachar Siboni	Israel	Universidade Ben-Gurion do Negev
Shane Brady	Irlanda	Universidade College Dublin
Siravit Chotivatunyu	Tailândia	Faculdade de Tecnologia da Informação e Comunicação
Siravitch Chaiyasart	Tailândia	Faculdade de Tecnologia da Informação e Comunicação
Steve Versteeg	Estados Unidos	CA Technologies - Melbourne
Stuart H. Rubin	Cingapura	Centro de Sistemas SPAWAR (SSC)
Suhas Bhairav	Cingapura	Universidade de Tecnologia e Design de Cingapura
Teemu Kanstren	Finlândia	Centro de Pesquisa Técnica da Finlândia
Thomas Fehlmann	Suíça	Euro Project Office AG
Thomas Maurin	França	Univ. Grenoble Alpes
Vânia de Oliveira Neves	Brasil	Universidade Federal de Juiz de Fora
Vasaka Visoottiviseth	Tailândia	Faculdade de Tecnologia da Informação e Comunicação
Vinay Sachidananda	Cingapura	Universidade de Tecnologia e Design de Cingapura
Vincenzo De Simone	Itália	Universidade de Nápoles Federico II
Vincenzo Riccio	Itália	Universidade de Nápoles Federico II
Yuval Elovici	Cingapura	Universidade de Tecnologia e Design de Cingapura
Zeinab Farahmandpour	Austrália	Universidade de Tecnologia de Swinburne

Fonte: a autora.