



GUIA DE TESTE DE INTEROPERABILIDADE PARA APLICAÇÕES IoT

Autora: Karina da Silva Castelo Branco

Orientadora: Valéria Lelli Leitão Dantas

VERSÃO 1.0
JUNHO 2024

SUMÁRIO

| | |
|---|-----------|
| Introdução | 6 |
| 1. Definição da característica | |
| 2. Correlação das Características | 7 |
| 3. Desafios de Teste de Interoperabilidade | 10 |
| 4. Configuração do ambiente | 11 |
| 5. Semântica de dados | |
| Definição | 13 |
| Contextualização | 13 |
| Casos de Teste Abstratos | 16 |
| medidas | 12 |
| 6. Protocolo de comunicação | |
| Definição | 22 |
| Contextualização | 22 |
| Casos de Teste Abstratos | 23 |
| medidas | 20 |
| 7. Integração de sistema | |
| Definição | 30 |
| Contextualização | 30 |
| Casos de Teste Abstratos | 31 |
| medidas | 28 |
| 8. Protocolos de rede | |
| Definição | 38 |
| Contextualização | 38 |
| Casos de Teste Abstratos | 39 |
| medidas | 36 |
| 9. Impacto das Subcaracterísticas | 45 |
| 10. Custo benefício | 48 |
| 11. Sugestão de ferramentas | 49 |
| 12. Exemplo de uso do guia | 51 |
| 13. Referências | 54 |

Este guia tem como propósito oferecer assistência na realização de testes de Interoperabilidade em aplicações IoT. Ele está estruturado em 12 seções distintas, como: Definições de Interoperabilidade (Tópico 1), Correlação das Características (Tópico 2), Desafios do Teste Interoperabilidade (Tópico 3), Configuração do Ambiente de Teste (Tópico 4), Casos de Teste Abstratos (Tópico 4.c), medidas (Subtópico 4.d), Impacto da Subcaracterística (Tópico 8) e outros. Além de fornecer ao final um plano de teste que sirva como diretriz para os testadores durante a avaliação de interoperabilidade em aplicações de Internet das Coisas (IoT).

Este guia encontra sua base nas quatro subcaracterísticas de Interoperabilidade definidas na norma ISO/IEC 30141:2018, a saber: **Semântica dos Dados, Protocolos de Comunicação, Integração de Sistema e Protocolo de Rede**. Portanto, foi elaborado com o objetivo de abranger cenários de testes de Interoperabilidade para IoT com base nessas subcaracterísticas.

Para cada subcaracterística, o tópico 4 do guia oferece as definições pertinentes, contexto (propriedades), casos de teste abstratos e medidas. Além deste tópico, há outros sete tópicos destinados a abordar a avaliação das características de interoperabilidade como um todo. As 12 tópicos apresentam o seguinte:

- **Definição da Característica:** este tópico trata da característica que será objeto de teste.
- **Correlação das Características:** apresenta as correlações, tanto positivas quanto negativas, entre a característica alvo e outras características IoT.
- **Desafios do Teste de Interoperabilidade:** este tópico tem como objetivo apresentar os variados desafios relacionados à avaliação da característica de interoperabilidade em aplicações de IoT.
- **Configuração do Ambiente de Teste:** descreve o ambiente IoT necessário para realizar os testes da característica alvo, incluindo os tipos de dispositivos e o software ou hardware externo envolvidos.
- **Definição de Subcaracterística:** caso aplicável, este tópico descreve as subcaracterísticas associadas à característica alvo.
- **Contextualização:** Descreve as propriedades relacionadas à característica e, se aplicável, às subcaracterísticas.
- **Casos de Testes Abstratos:** fornece diretrizes gerais para conduzir os testes da característica alvo ou, quando aplicável, das subcaracterísticas.
- **Medidas:** apresenta as medidas utilizadas para avaliar a característica alvo e, se aplicável, as subcaracterísticas.
- **Impacto das Subcaracterísticas:** se necessário, este tópico aborda as relações entre as subcaracterísticas com base nas propriedades de contextualização.
- **Custo-Benefício:** apresenta uma análise da relação custo-benefício para a realização dos testes, com base nas correlações identificadas no tópico de Correlação de Características.
- **Sugestões de Ferramentas:** lista ferramentas que podem ser empregadas para automatizar a coleta de medidas relacionadas à característica alvo.
- **Exemplo de Uso do Guia:** fornecendo um cenário de aplicação prático, este tópico ilustra como utilizar o guia no contexto da característica alvo.

Esperamos que este guia seja valioso na execução eficiente de testes de Interoperabilidade em aplicações IoT e na compreensão abrangente das características e subcaracterísticas envolvidas.

Instruções para a Utilização do Guia

1. **Compreensão das Definições de Interoperabilidade:** inicialmente, é fundamental compreender as definições de Interoperabilidade apresentadas no tópico 1 deste guia, a qual foi concebida para alinhar o conhecimento em relação à característica abordada.
2. **Seleção de Características Relevantes:** com base na aplicação específica que pretende testar, recorra às definições e relações expostas na Correlação de Características (tópico 2) para identificar e listar as características de IoT relacionadas à interoperabilidade que assumem prioridade para a sua aplicação. Essas características podem abranger todas ou algumas, conforme ditado pelo contexto.
3. **Configuração do Ambiente de Teste:** assegure-se de que o ambiente destinado aos testes de interoperabilidade cumpra os requisitos delineados na tópico 4 (Configuração do Ambiente de Teste).
4. **Compreensão das Subcaracterísticas:** na etapa subsequente, dedique-se a compreender as definições e propriedades apresentadas nas tópico correspondentes a cada subcaracterística (tópico 5, 6 e 7). A partir dessa compreensão, selecione as propriedades das subcaracterísticas que serão submetidas a avaliação. Vale salientar que não é estritamente necessário avaliar todas as subcaracterísticas do guia; a decisão cabe ao usuário, levando em consideração as necessidades específicas da sua aplicação.
5. **Avaliação do Impacto das Subcaracterísticas:** Caso tenha optado por avaliar todas as propriedades no passo anterior, esta etapa pode ser ignorada. Utilizando a tópico 8 (Impacto das Subcaracterísticas) como referência, identifique quais propriedades selecionadas são influenciadas pelas outras propriedades. Certifique-se de que essas propriedades também sejam submetidas à avaliação.
6. **Seleção de medidas:** Selecione as medidas a serem empregadas na avaliação. Salientamos que não é aconselhável selecionar apenas uma medida; em vez disso, recomendamos a execução de todas as medidas relacionadas a subcaracterística selecionada.
7. **Cálculo do Custo-Benefício:** Após o planejamento completo, proceda ao cálculo do custo-benefício que os testes e medidas irão demandar. O tópico 9 (Custo-Benefício) explica detalhadamente este processo.
8. **Utilização de Ferramentas Sugeridas:** Se desejar utilizar alguma das ferramentas sugeridas neste guia, consulte a Tabela 2 para identificar quais ferramentas podem auxiliar na coleta das medidas selecionadas. No tópico 11, são fornecidas informações sobre as licenças dessas ferramentas e os sites para acessá-las.
9. **Execução dos Testes:** Após a conclusão de todo o planejamento, é o momento de executar os testes. Todos os testes abstratos selecionados devem ser transformados em casos de teste concretos, considerando o contexto da sua aplicação. Isso envolve a definição dos limites e dos valores aceitáveis para as medidas selecionadas, levando em conta as correlações identificadas no tópico 2. A Figura 8 no Apêndice A pode ser

utilizada como guia para acelerar esse processo. Caso surjam dúvidas quanto à implementação prática deste guia, o tópico 12 (Exemplo de Uso do Guia) fornece orientações adicionais.

Além disso, algumas informações adicionais importantes para a compreensão deste guia incluem:

- Todos os testes podem ser realizados localmente.
- As medidas podem ser coletadas por meio dos casos de teste.
- O custo-benefício pode ser usado como critério de priorização dos testes.
- As ferramentas sugeridas podem auxiliar nos testes e medidas, mas **não são obrigatórias**.
- O impacto das subcaracterísticas ajuda a identificar outras propriedades que podem ser relevantes para o teste.

Introdução

Este guia visa auxiliar na validação da característica de *Interoperabilidade* em aplicações Internet das Coisas (IoT), através de tópicos como Correlação das Características, Casos de testes abstratos, medidas, Impacto das subcaracterísticas, entre outras. Este guia foi construído baseado nas ISO/IEC 21823:2022 e ISO/IEC 30141:2018, estado atual da arte e nas subcaracterísticas de *Interoperabilidade* identificadas com base na literatura por meio de técnicas de um mapeamento sistemático.

O guia é construído deste modo para abranger o máximo de cenários de teste em *Interoperabilidade* de IoT. Para cada subcaracterística são apresentadas as definições, propriedades, casos de testes e medidas.

A norma ISO/IEC 21823:2022 apresenta as subcaracterísticas de Interoperabilidade em IoT. Essa norma foi publicada em 2022 e fornece diretrizes para a avaliação da Interoperabilidade em sistemas de IoT, incluindo definições de termos e requisitos de teste para as diferentes subcaracterísticas de *Interoperabilidade*. As subcaracterísticas incluem semântica dos dados, protocolos de comunicação, integração de sistema e protocolo de rede.

A norma ISO/IEC 30141:2018 estabelece um framework para a arquitetura de sistemas de Internet das Coisas (IoT). Ela define um conjunto de princípios e conceitos que orientam o desenvolvimento e a implementação de arquiteturas IoT, com o objetivo de garantir a interoperabilidade e a integração eficaz entre diferentes sistemas e dispositivos. A norma cobre aspectos fundamentais como a modelagem de sistemas IoT, a definição de interfaces e protocolos, e a gestão de dados.

Essas normas são importantes para organizações que trabalham em colaboração em processos de negócios, pois ajuda a garantir que a modelagem de processos de negócios seja consistente e compreensível para todos os envolvidos, o que pode levar a uma maior eficiência e eficácia na realização dos processos.

1. Definições da característica

A norma ISO/IEC 21823:2022 define *Interoperabilidade* como "*A interoperabilidade na IoT refere-se à capacidade dos dispositivos conectados (como sensores, dispositivos inteligentes, gateways etc.) de se comunicarem e interagirem de forma eficiente e transparente, independentemente de sua origem, fabricante ou protocolo de comunicação.*".

Essas definições destacam a importância de ter padrões comuns e especificações

técnicas para garantir que os sistemas possam trabalhar juntos de forma adequada e que a informação possa ser compartilhada e interpretada corretamente. A *Interoperabilidade* é fundamental para garantir a efetividade e eficiência dos processos de negócios colaborativos e para facilitar a comunicação entre as partes envolvidas. A Tabela 1 apresenta as principais definições de *Interoperabilidade*:

Tabela 1 - Definições de Interoperabilidade

| Definição | Autores |
|---|------------------------|
| A <i>Interoperabilidade</i> é a capacidade de dois ou mais sistemas ou componentes de trocar informações e usar as informações que foram trocadas. | Legner e Wander (2006) |
| A <i>Interoperabilidade</i> pode ser definida como um estado em que duas aplicações podem aceitar e compreender os dados do outro e realizar uma determinada tarefa de forma satisfatória sem intervenção humana. | (Gulla et al., 2006) |
| A capacidade de diferentes sistemas, dispositivos ou aplicativos se comunicarem e interagirem de forma eficiente e sem problemas. | Ferreira (2014) |
| A capacidade de um sistema para trocar dados e informações com outros sistemas sem perda ou corrupção de informações. | ISO/IEC 15926:2019 |
| A capacidade de diferentes sistemas e organizações para trabalhar juntos (troca de informações e ações) de forma eficaz e eficiente. | ISO/IEC 30141:2018 |
| A <i>Interoperabilidade</i> na IoT refere-se à capacidade dos dispositivos conectados (como sensores, dispositivos inteligentes, gateways etc.) de se comunicarem e interagirem de forma eficiente e transparente, independentemente de sua origem, fabricante ou protocolo de comunicação. | ISO/IEC 21823:2022 |

2. Correlação das características

Através de uma análise bibliográfica, foi possível estabelecer a relação de 14 características com a *Interoperabilidade* entre as 28 identificadas para IoT. Essas conexões podem ser úteis para detectar possíveis conflitos nos requisitos das aplicações e buscar maneiras de mitigá-los. A Figura 1 apresenta

as conexões classificadas em três tipos: os retângulos na cor vermelha indica características que exercem influência negativa sobre a *Interoperabilidade*, como o desempenho da aplicação; os retângulos de cor verde indica influência positiva, como a disponibilidade da aplicação, em que quanto maior os protocolos comuns exigida na aplicação, maiores benefícios terão os requisitos de *Interoperabilidade*; os retângulos nas cores amarelas são dependentes do contexto da aplicação, como a característica da eficiência, que podem exercer influência positiva ou negativa, por exemplo dependendo da disponibilidade ou não de servidores para atender à demanda de troca de mensagens entre dispositivos.

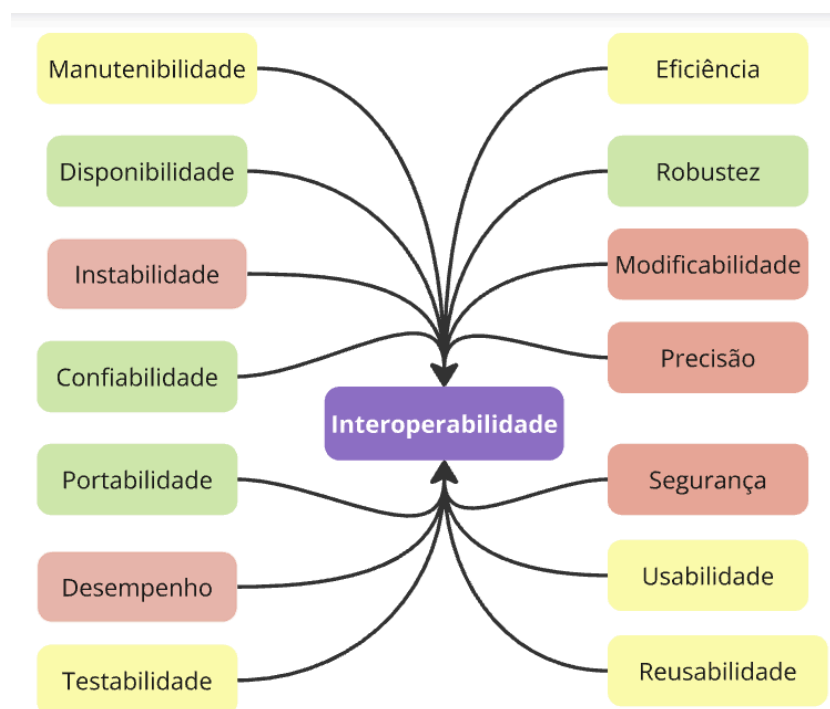


Figura 1 – Correlação das características da IoT com interoperabilidade

1. **Disponibilidade:** está associada à capacidade do sistema permanecer operacional e acessível quando necessário. Níveis elevados de disponibilidade favorecem a comunicação contínua entre dispositivos e serviços distribuídos, contribuindo para a efetiva troca de dados (Li et al., 2018; Chen et al., 2021; Noura et al., 2019).
2. **Instabilidade:** relaciona-se à ocorrência de falhas inesperadas e ao funcionamento inconsistente dos sistemas. Ambientes instáveis prejudicam a sincronização e a integração entre componentes heterogêneos, afetando negativamente a interoperabilidade (Xiong et al., 2018; Noubir et al., 2020).

3. **Desempenho:** refere-se à capacidade do sistema responder adequadamente às solicitações dentro de tempos aceitáveis. Atrasos excessivos na transmissão de dados podem comprometer a integração entre dispositivos e serviços IoT, especialmente em aplicações distribuídas (Li et al., 2018; Chen et al., 2021).
4. **Portabilidade:** diz respeito à facilidade de adaptação do sistema a diferentes plataformas e ambientes. Sistemas portáteis favorecem a interoperabilidade ao possibilitar sua execução em múltiplas infraestruturas e domínios de aplicação (Noura et al., 2019; Sivashanmugam et al., 2014).
5. **Confiabilidade:** está relacionada à execução correta e consistente das funções do sistema ao longo do tempo. Falhas recorrentes impactam diretamente a troca de informações entre sistemas heterogêneos, comprometendo o funcionamento conjunto esperado (Xiong et al., 2018; Chen et al., 2021).
6. **Robustez:** envolve a capacidade do sistema lidar com entradas inválidas ou condições adversas. Arquiteturas robustas permitem a continuidade da comunicação mesmo diante de falhas parciais de dispositivos, favorecendo a interoperabilidade (Noubir et al., 2020; Noura et al., 2019).
7. **Precisão:** está associada à correta interpretação e transmissão das informações trocadas entre dispositivos. Inconsistências na representação dos dados podem gerar erros de interpretação e comprometer a integração entre sistemas (Guinard et al., 2016; Sivashanmugam et al., 2014).
8. **Segurança:** refere-se à proteção dos dados e recursos contra acessos não autorizados. Embora seja essencial para garantir a confiabilidade da troca de informações, políticas excessivamente restritivas podem dificultar a integração entre sistemas interoperáveis (De Silva et al., 2017; Li et al., 2018; ISO 30141).
9. **Manutenibilidade:** relaciona-se à facilidade de realizar modificações e correções no sistema. Sistemas mais manuteníveis tendem a se adaptar melhor a novos requisitos de interoperabilidade, como mudanças em protocolos ou padrões de comunicação (Raza et al., 2017; Petrolo et al., 2018).

10. **Usabilidade:** influencia a configuração e a operação de sistemas interoperáveis, especialmente por usuários não especializados. Interfaces pouco intuitivas podem dificultar a correta parametrização das comunicações entre dispositivos (Alam et al., 2017; Tariq et al., 2018).
11. **Reusabilidade:** está associada ao uso de componentes padronizados e reaproveitáveis, favorecendo a integração com outros sistemas e plataformas (Guinard et al., 2016; Noura et al., 2019).
12. **Testabilidade:** refere-se à facilidade de verificar o funcionamento das interfaces e dos protocolos de comunicação. Maior testabilidade permite identificar falhas de interoperabilidade de forma antecipada, contribuindo para a confiabilidade do sistema (Winkler et al., 2019; Kovatsch et al., 2018; Alam et al., 2017).
13. **Modificabilidade:** diz respeito à facilidade de adaptação do sistema a novos padrões e requisitos. Sistemas pouco modificáveis enfrentam dificuldades em se manter compatíveis com a evolução tecnológica do ecossistema IoT (Xiong et al., 2018; Chen et al., 2021).
14. **Eficiência:** está relacionada ao uso otimizado de recursos computacionais. Sistemas eficientes favorecem a interoperabilidade ao evitar sobrecarga dos dispositivos; entretanto, otimizações excessivas podem comprometer o suporte a múltiplos protocolos e mecanismos de integração (Li et al., 2018; Noura et al., 2019; ISO 30141).

Ao estabelecer a correlação entre as características é possível identificar possíveis conflitos ou incompatibilidades entre os requisitos das aplicações. Por exemplo, a segurança pode exigir a criptografia dos dados trocados entre dispositivos, enquanto a portabilidade melhora ou afeta diretamente na facilidade com que um sistema pode ser transferido ou adaptado para diferentes ambientes ou plataformas. Nesse caso, é necessário encontrar formas de mitigar esses conflitos, a literatura sugere usar técnicas de tradução de dados ou protocolos de comunicação que permitam a criptografia e ainda assim possibilitem a interpretação dos dados.

Em resumo, a correlação das características de *Interoperabilidade* com base na ISO 30141:2018 pode ser uma ferramenta útil para a identificação de possíveis conflitos das aplicações IoT e para a busca de soluções que permitam atender a todos os requisitos de forma satisfatória.

3. Desafios do Teste de *Interoperabilidade*

A interoperabilidade, fundamentada em conceitos estruturais como contexto, perspectiva, propósito, nível de suporte fornecido e atributos do sistema, pode ser efetivamente medida, aprimorada e monitorada através de uma abordagem comportamental. Esta abordagem inclui métodos de avaliação específicos, identificação e superação de desafios, resolução de problemas e análise dos benefícios resultantes da interoperabilidade (MOTTA et al., 2019).

Avaliar a interoperabilidade em aplicações IoT envolve garantir que diversos dispositivos e sistemas possam se comunicar e operar conjuntamente de maneira eficiente e eficaz. A criação de um ambiente de teste que simula condições reais de operação, levando em consideração a diversidade de protocolos de comunicação, formatos de dados e requisitos de segurança, é essencial para validar a interoperabilidade, devido a essas complexidades, surgiram diversos desafios no teste de interoperabilidade (CRUZ et al., 2020). Foram identificados alguns desafios associados à avaliação da característica de *Interoperabilidade* em aplicações de IoT, conforme apresentado na Figura 2.

A adoção de padrões e tecnologias comuns emerge como um meio eficaz para assegurar que dispositivos e sistemas possam se comunicar e interagir de forma eficiente, estabelecendo, assim, um nível adequado de *Interoperabilidade* entre eles.

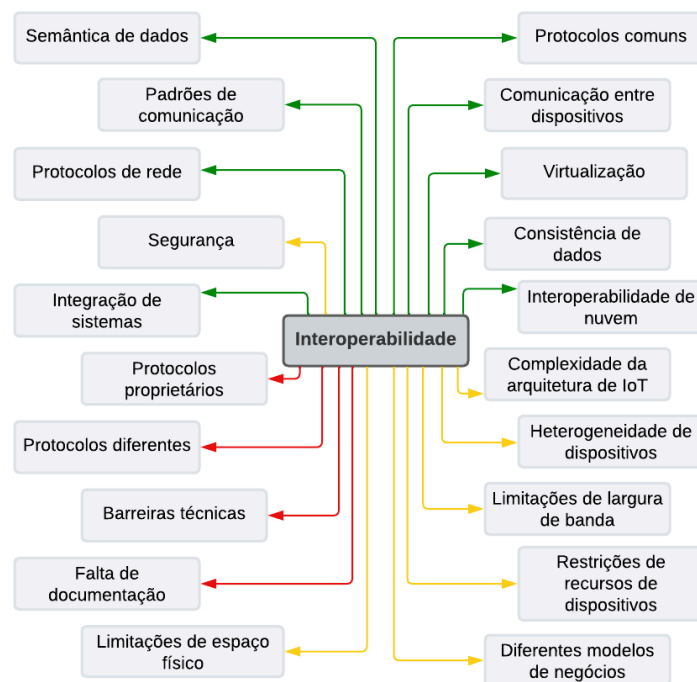


Figura 2 – Principais desafios nos testes de interoperabilidade

Nesse contexto, as setas vermelhas são utilizadas para indicar os desafios considerados mais críticos e frequentemente abordados na literatura. As setas verdes, por sua vez, são empregadas para destacar desafios que recebem maior ênfase em estudos de pesquisa, seja pela sua complexidade ou relevância. Já as conexões amarelas enfatizam os desafios que têm sido observados de forma significativa em aplicações práticas de IoT, indicando a sua importância na implementação e no funcionamento efetivo desses sistemas no mundo real. A seguir, apresentam-se as definições:

- **Protocolos de rede.** O desafio de testar a compatibilidade entre diferentes protocolos de rede (por exemplo, TCP/IP, UDP, HTTP e MQTT), abordando a diversidade de protocolos, a complexidade de integração e assegurando a comunicação eficaz entre dispositivos de diferentes fabricantes. O desafio é: "Como testar a compatibilidade entre diferentes protocolos de rede?" (Zanella et al., 2014).
- **Semântica de dados.** O desafio de garantir a consistência semântica dos dados trocados entre dispositivos IoT durante os testes, evitando ambiguidades e assegurando uma interpretação comum dos dados entre dispositivos e sistemas. O desafio é: "Como testar a consistência semântica dos dados trocados entre dispositivos IoT?" (Perera et al., 2014).

- **Segurança.** Os desafios relacionados à segurança envolvem testar a eficácia das medidas de proteção implementadas, garantir a integridade e confidencialidade dos dados sensíveis e assegurar que a Interoperabilidade não introduza vulnerabilidades. O desafio é: "Como testar a interoperabilidade sem comprometer a segurança dos dispositivos IoT?" (Sicari et al., 2015).
- **Padrões de comunicação.** O desafio de testar a adoção de padrões de comunicação diferentes (por exemplo, HTTP, CoAP, MQTT e AMQP) entre dispositivos IoT, lidando com a diversidade de padrões e assegurando a compatibilidade entre diferentes dispositivos para uma comunicação eficaz. O desafio é: "Como testar a adoção de diferentes padrões de comunicação entre dispositivos IoT?" (Atzori et al., 2010).
- **Integração de sistemas.** O principal desafio seria testar a integração de sistemas e dispositivos IoT, lidando com a complexidade da integração, a necessidade de coordenação entre sistemas e a compatibilidade entre diferentes tecnologias. O desafio é: "Como testar a integração de sistemas em dispositivos IoT?" (Bandyopadhyay et al., 2011).
- **Protocolos diferentes.** O desafio de testar a gestão da diversidade de protocolos de comunicação (por exemplo, Zigbee e Bluetooth), assegurando a compatibilidade e lidando com a complexidade das diferentes tecnologias empregadas. O desafio é: "Como testar a adoção de diferentes padrões de comunicação entre dispositivos IoT?" (Rayes et al., 2019).
- **Barreiras técnicas.** O desafio é testar considerando as barreiras técnicas que incluem limitações tecnológicas, como restrições de hardware (por exemplo, limitações de processamento em dispositivos de baixo custo) e software (como incompatibilidades entre diferentes sistemas operacionais e APIs), que podem impedir a comunicação eficaz entre dispositivos IoT. Isso abrange dificuldades como a incompatibilidade entre diferentes tecnologias (por exemplo, diferentes tipos de sensores e atuadores que utilizam protocolos distintos) e a necessidade de desenvolver soluções inovadoras para garantir a interoperabilidade. O desafio é: "Como testar os aspectos relacionados às barreiras técnicas para a interoperabilidade?" (Al-Fuqaha et al., 2015).
- **Falta de documentação.** O desafio de lidar com a falta de documentação clara e detalhada sobre dispositivos e protocolos (como APIs, formatos de dados e especificações de comunicação) durante os testes, enfrentando dificuldades de integração e a necessidade de desenvolver documentação própria para entender e conectar os dispositivos corretamente. O desafio é: "Como testar a interoperabilidade

de dispositivos e protocolos que não são claramente especificados e documentados?" (Vermesan et al., 2011).

- **Limitações de espaço físico.** O desafio de mitigar as limitações de espaço físico ao instalar e testar dispositivos IoT, enfrentando dificuldades relacionadas à instalação compacta e otimização do uso do espaço disponível para garantir que todos os dispositivos funcionem corretamente em um ambiente restrito. O desafio é: "Como testar a interoperabilidade de várias aplicações IoT considerando as limitações de espaço físico durante a instalação e operação?" (Khan et al., 2012).
- **Modelos de negócio diferentes.** O desafio de harmonizar diferentes modelos de negócios para promover a interoperabilidade durante os testes, lidando com a diversidade de abordagens e assegurando a compatibilidade entre soluções. O desafio é: "Como testar a harmonização de diferentes modelos de negócios para promover a interoperabilidade?" (Porter et al., 2014).
- **Restrições de recursos de dispositivos.** O desafio de testar a superação das restrições de recursos dos dispositivos IoT, incluindo limitações de energia, memória e capacidade de processamento, otimizando o desempenho e garantindo funcionalidade com recursos limitados. O desafio é: "Como testar as restrições de recursos dos dispositivos IoT?" (Caldas et al., 2023).
- **Limitações de largura de banda.** O desafio de testar a gestão das limitações de largura de banda em redes IoT (como redes LoRaWAN com baixa largura de banda ou redes 5G com alta largura de banda), otimizando a transmissão de dados e garantindo a comunicação eficiente entre dispositivos de diferentes fabricantes. Isso inclui avaliar como as restrições de largura de banda impactam a interoperabilidade e a eficiência da troca de informações entre sistemas distintos. O desafio é: "Como testar a interoperabilidade entre dispositivos IoT quando há limitações de largura de banda na rede, garantindo uma comunicação eficiente?" (Palattella et al., 2013).
- **Heterogeneidade de dispositivos.** O desafio de testar a compatibilidade e gerenciar a complexidade da integração de dispositivos com diferentes capacidades, protocolos e fabricantes. O desafio é: "Como testar a compatibilidade e gerenciar a heterogeneidade dos dispositivos IoT?" (Noura et al., 2019).
- **Complexidade da arquitetura IoT.** O desafio de simplificar a complexidade da arquitetura IoT para melhorar a interoperabilidade durante os testes, reduzindo a complexidade herdada pelos testes ao lidar com a coordenação entre múltiplas camadas e componentes do sistema. O desafio é: "Como lidar com a complexidade da

arquitetura IoT na condução dos testes de Interoperabilidade?" (Borgia et al., 2014).

- **Interoperabilidade na nuvem.** O desafio de testar a interoperabilidade entre diferentes serviços em nuvem, lidando com a diversidade de serviços, garantindo compatibilidade e integrando diferentes plataformas. O desafio é: "Como testar a interoperabilidade entre diferentes serviços em nuvem?" (Botta et al., 2016).
- **Consistência de dados.** O desafio de garantir a consistência dos dados entre dispositivos IoT durante os testes, lidando com a verificação e correção de dados inconsistentes e assegurando a precisão dos dados. O desafio é: "Como testar a consistência dos dados entre dispositivos IoT?" (Zaslavsky et al., 2013).
- **Protocolos proprietários.** O desafio de testar a interoperabilidade entre dispositivos IoT que utilizam protocolos proprietários (por exemplo, protocolos específicos de fabricantes para automação residencial), assegurando a comunicação e integração eficazes apesar das especificações e implementações fechadas. Isso inclui lidar com a falta de documentação aberta e a necessidade de adaptar ou desenvolver interfaces para compatibilizar dispositivos que utilizam protocolos exclusivos. O desafio é: "Como testar a interoperabilidade entre dispositivos IoT que utilizam protocolos proprietários?" (Noubir et al., 2020).
- **Virtualização.** O desafio de usar a virtualização para melhorar a interoperabilidade durante os testes, lidando com a implementação e gerenciamento de recursos virtualizados e assegurando compatibilidade. O desafio é: "Como testar a virtualização para melhorar a interoperabilidade?" (Kreutz et al., 2015).
- **Comunicação entre dispositivos.** O desafio de garantir uma comunicação eficaz entre dispositivos IoT durante os testes, padronizando os testes para atender tanto a aplicações que utilizam protocolos comuns quanto a aplicações que empregam protocolos diferentes. Isso inclui lidar com a diversidade de protocolos, assegurar a compatibilidade e gerenciar a comunicação entre dispositivos de diferentes fabricantes. O desafio é: "Como testar a comunicação eficaz entre dispositivos IoT de forma padronizada, considerando a diversidade de protocolos comuns e diferentes utilizados nas aplicações?" (Sicari et al., 2013).
- **Protocolos comuns.** O desafio de garantir a eficácia dos testes para aplicações IoT que utilizam protocolos diferentes, assegurando a compatibilidade e a comunicação eficiente entre dispositivos de diversos padrões. O desafio é: "Como padronizar os testes para garantir a interoperabilidade entre dispositivos IoT que utilizam diferentes protocolos?" (Shelby et al., 2016).

4. Configuração do ambiente

- Um ou mais dispositivo IoT;
- Infraestrutura de rede;
- Um ou mais atuadores;
- Aplicativo que tomará as decisões e enviará os comandos;

A presente exposição visa fornecer dados suplementares destinados a enriquecer a compreensão do leitor em relação à configuração do ambiente de teste em consideração. As informações a seguir foram dispostas com o propósito de aprimorar a clareza e abrangência do conhecimento acerca do contexto de estabelecimento do ambiente de teste.

Dispositivos de IoT: para testar a *Interoperabilidade* em IoT, é necessário ter dispositivos que possam se comunicar uns com os outros. Esses dispositivos podem incluir sensores, dispositivos de controle, dispositivos de rede e outros dispositivos que sejam compatíveis com o protocolo de comunicação escolhido.

Exemplos de dispositivos: Sensores de temperatura de fabricantes A, B e C; atuadores de iluminação de fabricantes X, Y e Z.

Infraestrutura de rede: a infraestrutura de rede deve ser configurada de forma a permitir a comunicação entre os dispositivos IoT, garantindo a sua disponibilidade e segurança. Isso pode envolver a configuração de redes sem fio (Wi-fi e Bluetooth), switches, roteadores e firewalls.

Exemplo: Testes realizados em redes Wi-Fi, redes celulares, redes LPWAN (Low Power Wide Area Network) para avaliar a *Interoperabilidade* em diferentes ambientes de rede.

Atuadores: Para testar a *Interoperabilidade* em IoT, é importante considerar também os atuadores, que são dispositivos capazes de executar ações com base em informações recebidas dos sensores ou comandos de sistemas externos.

Exemplos de atuadores em IoT: incluem atuadores para abrir e fechar cortinas, ajustar a temperatura do termostato, ligar ou desligar aparelhos eletrônicos, etc.

Aplicativo que tomará as decisões e enviará os comandos: Um aplicativo ou plataforma que toma decisões com base em informações dos dispositivos IoT e envia comandos para controlá-los. Esse aplicativo deve ser capaz de se comunicar com os dispositivos de diferentes fabricantes e protocolos.

Em resumo, para testar a *Interoperabilidade* em aplicações IoT, é essencial criar um ambiente diversificado que inclua dispositivos, protocolos, fabricantes e ambientes de rede variados. Isso garante que os dispositivos IoT possam funcionar harmoniosamente e se

comunicar eficazmente em cenários do mundo real, independentemente das diferenças técnicas entre eles.

A seguir, apresento informações complementares destinadas a aprimorar a compreensão do guia em questão, com enfoque na avaliação de *Interoperabilidade* no contexto da Internet das Coisas (IoT):

Realização de Testes Localmente: todos os procedimentos de teste abordados neste guia podem ser conduzidos em ambientes locais, proporcionando maior controle e facilidade na avaliação da *Interoperabilidade* entre dispositivos IoT.

Relevância dos Casos de Teste: é importante ressaltar que casos de teste que não se apliquem diretamente ao sistema específico em avaliação podem ser deixados de lado, a fim de concentrar os esforços nos aspectos de *Interoperabilidade* mais pertinentes e significativos para o contexto em questão.

Integração de Testes e medidas: a realização dos casos de teste propostos pode ser efetuada simultaneamente com as medidas, otimizando o processo de avaliação e proporcionando uma visão mais abrangente da eficácia da *interoperabilidade* entre os dispositivos IoT avaliados.

Priorização com Base no Custo-Benefício: a estratégia de priorização dos casos de teste pode ser embasada no princípio de custo-benefício, direcionando a atenção aos testes que oferecem maior *Interoperabilidade* e, ao mesmo tempo, são mais viáveis em termos de recursos e tempo.

Uso Opcional de Ferramentas: embora as ferramentas possam desempenhar um papel auxiliar durante os testes e medidas, é relevante observar que sua utilização não é obrigatória. A avaliação de *Interoperabilidade* pode ser efetuada com base em critérios próprios, sem depender exclusivamente das ferramentas disponíveis.

Consideração do Impacto das Subcaracterísticas: a análise do impacto das subcaracterísticas se mostra uma abordagem valiosa para identificar os casos de teste e as medidas que podem ser realizadas em conjunto. Essa consideração contribui para uma abordagem mais holística da avaliação de *Interoperabilidade*, permitindo uma compreensão mais profunda das relações entre os diferentes elementos do ecossistema IoT.

5. Semântica de dados

a. Definição

De acordo com a ISO 21823-4:2019 a semântica de dados se refere ao significado e contexto dos dados. É a capacidade de interpretar e compreender o significado dos dados, permitindo

que diferentes sistemas e dispositivos possam compartilhar e utilizar dados de maneira consistente e eficiente.

b. Contextualização

Semântica de dados é uma característica essencial de *Interoperabilidade* em IoT, uma vez que permite a integração e comunicação efetiva entre dispositivos e sistemas heterogêneos. A padronização e a utilização de modelos semânticos comuns são fundamentais para garantir que os dados sejam interpretados de forma correta e consistente.

No contexto de IoT, a semântica de dados se refere à capacidade de garantir que os dispositivos e sistemas de IoT possam compartilhar informações de maneira eficiente e precisa, mesmo que utilizem diferentes formatos de dados ou terminologias.

A semântica de dados em IoT é importante porque permite que dispositivos diferentes se comuniquem e troquem informações de maneira eficaz. Isso é particularmente importante em cenários em que diferentes dispositivos de IoT precisam trabalhar juntos para realizar uma tarefa específica. Por exemplo, imagine um sistema de iluminação inteligente que consiste em vários dispositivos, incluindo sensores de movimento, interruptores de luz e lâmpadas. Cada um desses dispositivos precisa entender as informações que estão sendo compartilhadas para garantir que as luzes sejam ligadas ou desligadas quando necessário. Para Semântica dos dados foram levantadas 8 propriedades importantes que incluem:

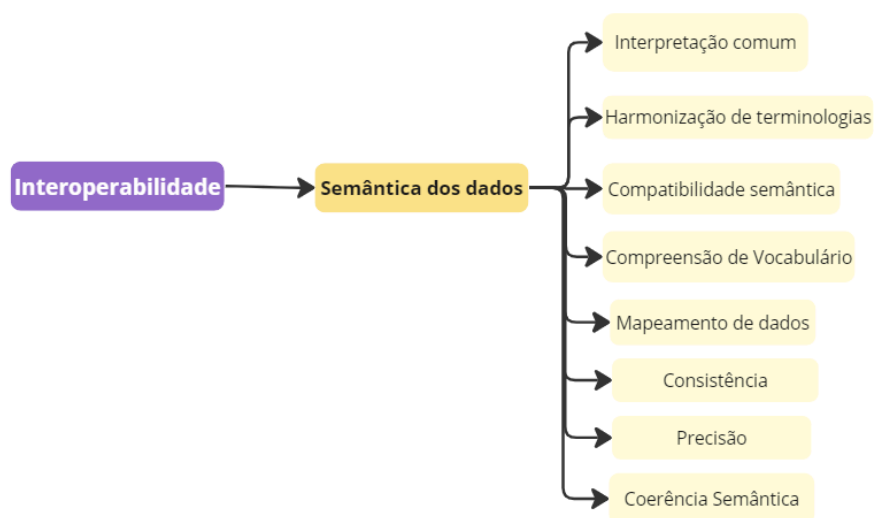


Figura 3 – Propriedades da semântica dos dados

- **P1- Interpretação comum:** a capacidade de garantir que diferentes sistemas possam entender e interpretar corretamente os dados que são compartilhados entre eles.

Exemplos do uso da propriedade Interpretação comum em aplicações IoT: Interoperabilidade de Aplicativos de Pagamento, aplicativos de pagamento móvel, como Apple Pay e Google Play, usam protocolos de comunicação que permitem que dispositivos móveis se comuniquem com terminais de pagamento compatíveis para garantir a correta interpretação dos dados da transação (GUINARD, 2016).

- **P2- Harmonização de terminologias:** a capacidade de garantir que os termos e conceitos utilizados para descrever os dados sejam consistentes entre diferentes sistemas, evitando ambiguidades e erros. Por exemplo, garantir que diferentes sensores utilizem a mesma terminologia para se referir a valores de localização, temperatura ou umidade (BANZI, 2015).
- **P3- Mapeamento de dados:** a capacidade de transformar os dados de um formato para outro, permitindo que diferentes sistemas possam compartilhar informações mesmo que usem diferentes padrões ou estruturas de dados. Por exemplo, converter dados de temperatura em Fahrenheit para Celsius e dados de km para latitude e longitude (SIVASHANMUGAM, 2014)
- **P4- Compatibilidade semântica:** a capacidade de garantir que os dados compartilhados entre diferentes sistemas possam ser facilmente combinados e usados em conjunto, mesmo que sejam originários de fontes diferentes. Por exemplo, garantir que diferentes sensores entendam que uma leitura de temperatura de 20 graus Celsius significa a mesma coisa em diferentes sistemas (Suryadevara et al. 2018).
- **P5- Consistência:** A consistência diz respeito à uniformidade dos dados ao longo do tempo e em diferentes sistemas. Dados consistentes garantem que as informações não sejam contraditórias e possam ser usadas de maneira confiável (Redman, 1998).
- **P6- Precisão:** A precisão se refere à capacidade de os dados representarem com exatidão o conceito que eles estão destinados a descrever. Em outras palavras, dados precisos são livres de erros e ambiguidades, garantindo uma representação fiel da informação (Welly e McGuinness, 2004)
- **P7- Compreensão de Vocabulário:** A necessidade de que os sistemas compartilhem um vocabulário comum ou ontologia para garantir a compreensão mútua dos termos utilizados na comunicação (Smith et al., 2004).

- **P8- Coerência Semântica:** A necessidade de que os dados mantenham consistência semântica em diferentes contextos e ao longo do tempo. Isso garante que os dados sejam compreendidos de maneira uniforme, independentemente das variações de contexto ou evoluções no sistema (Smith et al., 2004).

c. Casos de teste abstratos

| Caso de teste 1- CT01 | |
|------------------------------|--|
| Título: | Leitura de dados |
| Ambiente de Teste: | Uma rede de dispositivos IoT heterogêneos. |
| Pré-condição: | Dispositivos conectados à mesma rede Wi-Fi |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Iniciar o aplicativo móvel 2. Selecionar a leitura de um dado 3. Verificar o dado exibido na tela |
| Pós-condições: | O dado exibido na tela do dispositivo móvel deve corresponder ao mesmo dado solicitado pelo atuador |

| Caso de teste 2- CT02 | |
|------------------------------|---|
| Título: | Monitoramento de Tráfego por Latitude e Longitude |
| Ambiente de Teste: | Sistema de monitoramento de tráfego com informações de latitude e longitude |
| Pré-condição: | O sistema de monitoramento de tráfego está em operação e coletando dados de latitude e longitude |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Acessar o painel de controle do sistema de monitoramento de tráfego. 2. Selecionar a opção "Visualizar tráfego atual por Latitude e Longitude". |

| | |
|----------------|---|
| | 3. Verificar se os dados de tráfego exibidos no painel correspondem à localização especificada pelas coordenadas de latitude e longitude. |
| Pós-condições: | Os dados de tráfego exibidos no painel devem corresponder à área especificada pelas coordenadas de latitude e longitude fornecidas. |

| Caso de teste 3- CT03 | |
|-----------------------|---|
| Título: | Modelos semânticos comuns para interpretação de dados. |
| Ambiente de Teste: | Uma rede de dispositivos IoT heterogêneos. |
| Pré-condição: | Os dispositivos IoT estão configurados e operacionais. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Iniciar a plataforma de testes de interoperabilidade. 2. Conectar os dispositivos IoT à rede de teste. 3. Enviar dados de teste gerados por diferentes dispositivos IoT para o servidor central. 4. Verificar se os dados são interpretados corretamente pelos modelos semânticos comuns. 5. Executar operações de leitura e escrita nos dispositivos IoT por meio do servidor central. 6. Verificar se as operações são executadas corretamente e que os dispositivos respondem adequadamente. 7. Introduzir variações nos formatos de dados ou terminologias utilizadas pelos dispositivos IoT. 8. Confirmar que os modelos semânticos são capazes de interpretar os dados mesmo com variações. |
| Pós-condições: | A temperatura do forno deve ser alterada de acordo com o valor selecionado no painel de controle. |

| Caso de teste 4- CT04 | |
|------------------------------|---|
| Título: | Controle de iluminação |
| Ambiente de Teste: | Local com sistema de iluminação inteligente |
| Pré-condição: | Sistema de iluminação conectado e em funcionamento |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Iniciar o aplicativo móvel 2. Selecionar a opção "Iluminação" 3. Selecionar uma sala específica 4. Alterar a intensidade da luz |
| Pós-condições: | A intensidade da luz deve ser alterada na sala selecionada de acordo com o valor selecionado no aplicativo móvel. |

| Caso de teste 5- CT05 | |
|------------------------------|---|
| Título: | Monitoramento de temperatura e umidade |
| Ambiente de Teste: | Local com sensor de temperatura e umidade inteligentes |
| Pré-condição: | Sensores de temperatura e umidade conectados e em funcionamento |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Acessar o painel de controle do sistema de monitoramento de temperatura e umidade 2. Selecionar a opção "Visualizar temperatura e umidade atual" 3. Verificar os dados de temperatura e umidade exibidos no painel |
| Pós-condições: | Os dados de temperatura e umidade exibidos no painel devem corresponder aos dados coletados pelos sensores. |

| Caso de teste 6- CT06 | |
|-----------------------|---|
| Título: | Interpretação de Dados |
| Ambiente de Teste: | Dispositivos de diferentes fabricantes e protocolos de comunicação. |
| Pré-condição: | Dispositivos IoT estão fisicamente instalados e configurados no ambiente |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Envie uma mensagem contendo dados de temperatura em formato JSON de um dispositivo A. 2. Garanta que o dispositivo B interprete corretamente os dados recebidos. 3. Verifique se o dispositivo B acionou um atuador com base na interpretação correta dos dados. |
| Pós-condições: | Os dispositivos de diferentes fabricantes e protocolos de comunicação conseguiram interpretar e processar os dados corretamente, demonstrando a interoperabilidade em termos de semântica de dados. |

d. Medidas

| Capacidade de dispositivos - M01 | |
|----------------------------------|---|
| Propósito: | Avaliar a capacidade de diferentes dispositivos IoT interagirem uns com os outros de forma eficaz. |
| Método: | Realizar testes de interoperabilidade com diferentes combinações de dispositivos IoT e medir a taxa de sucesso das interações. |
| Medida: | <p>Taxa de sucesso de interações entre dispositivos IoT, medida como a proporção de interações bem-sucedidas em relação ao número total de interações realizadas.</p> <p>Taxa de Sucesso (%) = (Número de Interações Bem-Sucedidas / Número Total de Interações) x 100</p> |

| | |
|-------------|--|
| Explicação: | Essa fórmula calcula a taxa de sucesso em porcentagem, onde o número de interações bem-sucedidas é dividido pelo número total de interações realizadas e multiplicado por 100 para obter a representação em porcentagem. Essa fórmula permitirá que você quantifique a eficácia da interoperabilidade entre dispositivos IoT em seu teste. |
| Referência: | ISO 30141:2018 e Atzori et al. (2010) |

| Conformidade de protocolos - M02 | |
|----------------------------------|---|
| Propósito: | Avaliar a capacidade de dispositivos IoT interagirem entre si de acordo com protocolos estabelecidos. |
| Método: | Verificar se os dispositivos IoT seguem os protocolos estabelecidos para interação entre si, por meio de testes de compatibilidade e conformidade. |
| Medida: | <ol style="list-style-type: none"> Quantidade de protocolos suportados: número de protocolos que o dispositivo suporta Taxa de sucesso de interação: porcentagem de tentativas de interação que foram bem-sucedidas <p>MEDIDA = (Número de Protocolos Suportados / Número Total de Protocolos) * 100</p> |
| Explicação: | Essa fórmula calcula a taxa de sucesso de interação em termos de porcentagem, considerando a quantidade de protocolos suportados pelo dispositivo IoT em relação ao número total de protocolos testados. Isso proporciona uma medida quantitativa da conformidade de protocolos do dispositivo em relação aos padrões estabelecidos. |
| Referência: | ISO/IEC TR 30128:2018 e Sahni (2019) |

| Compatibilidade de plataformas - M03 | |
|--------------------------------------|--|
| Propósito: | Avaliar a capacidade de dispositivos IoT interagirem com diferentes plataformas. |
| Método: | Verificar se os dispositivos IoT são capazes de interagir com diferentes plataformas de IoT, por meio de testes de compatibilidade e conformidade. |

| | |
|-------------|---|
| Medida: | <ol style="list-style-type: none"> 1. Quantidade de plataformas suportadas: número de plataformas com as quais o dispositivo é compatível 2. Taxa de sucesso de interação: porcentagem de tentativas de interação que foram bem-sucedidas <p>Taxa de Sucesso (%) = (Número de Interações Bem-Sucedidas / Número Total de tentativas) x 100</p> |
| Explicação: | Essa fórmula calcula a porcentagem de tentativas de interação que foram bem-sucedidas em relação ao número total de tentativas realizadas durante os testes de compatibilidade de plataformas em dispositivos IoT. A medida resultante é expressa em porcentagem. |
| Referência: | ISO/IEC TR 30128:2018 e Sahni (2019) |

| Integração de dados - M04 | |
|---------------------------|--|
| Propósito: | Avaliar a capacidade de dispositivos IoT integrarem e compartilharem dados. |
| Método: | Verificar se os dispositivos IoT são capazes de integrar e compartilhar dados com outros dispositivos e sistemas, por meio de testes de compatibilidade e conformidade. |
| Medida: | X = Qtd de tipos de dados / Taxa de sucesso de integração de dados |
| Explicação: | Nesta fórmula, " <i>Quantidade de tipos de dados suportados</i> " representa o número de tipos de dados que o dispositivo é capaz de integrar e compartilhar, enquanto "Taxa de sucesso de integração de dados" é a porcentagem de tentativas de integração de dados que foram bem-sucedidas. O resultado dessa fórmula fornecerá uma medida que avalia a capacidade de dispositivos IoT em integrar e compartilhar dados, considerando tanto a diversidade de tipos de dados suportados quanto a eficácia da integração de dados. |
| Referência: | ISO/IEC TR 30128:2018 e Sahni (2019) |

6. Protocolo de comunicação

a. Definição

De acordo com a ISO 30141:2018 em um ambiente de IoT, é comum que dispositivos e sistemas sejam produzidos por diferentes fabricantes e possuam diferentes especificações

técnicas. Sem padrões de comunicação estabelecidos, pode ser difícil ou impossível para esses dispositivos se comunicarem e compartilharem dados. Portanto, a interoperabilidade em IoT depende da existência e adesão a padrões de comunicação bem definidos.

b. Contextualização

Protocolo de comunicação refere-se a um conjunto de especificações técnicas que definem as regras e os padrões de comunicação para permitir a *Interoperabilidade* entre dispositivos em um ambiente de IoT. Esses padrões ajudam a garantir que diferentes dispositivos e sistemas possam se comunicar e trocar informações de maneira eficiente e confiável. Para padrões de comunicação foram levantadas 7 propriedades importantes que incluem:

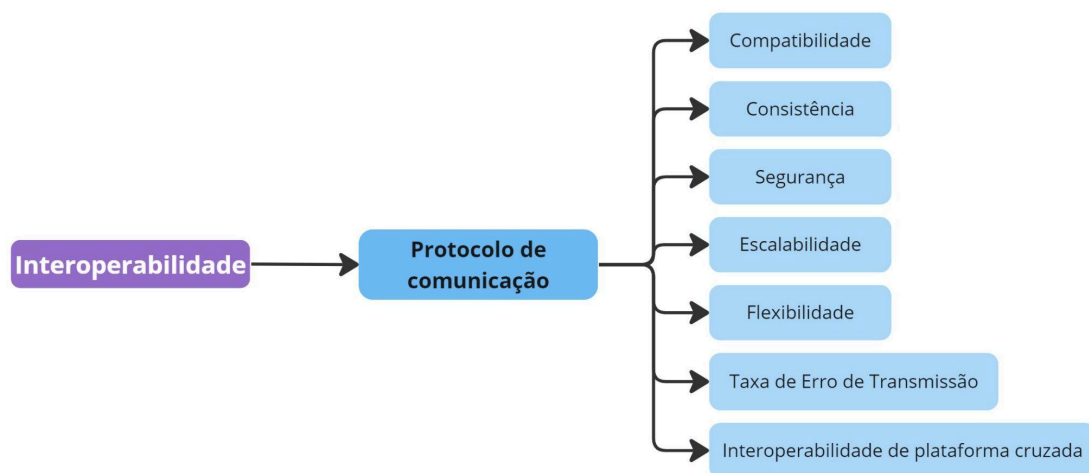


Figura 4 – Propriedades do protocolo de comunicação

- **P9- Compatibilidade:** Os padrões de comunicação devem ser compatíveis com uma ampla variedade de dispositivos e sistemas (SCHMIDT, 2015).
- **P10- Consistência:** As especificações técnicas devem ser claras e consistentes para garantir que todos os dispositivos e sistemas envolvidos possam se comunicar efetivamente (YAO et al., 2020).
- **P11- Segurança:** Os padrões de comunicação devem incluir protocolos de segurança robustos para proteger as informações transmitidas entre os dispositivos (DE SILVA et al., 2017).
- **P12- Escalabilidade:** protocolos como o MQTT são escaláveis e permitem que dispositivos IoT sejam adicionados ou removidos facilmente de uma rede sem comprometer a qualidade da comunicação (AL-FUQAHA et al., 2015).
- **P13- Flexibilidade:** Os padrões de comunicação devem ser flexíveis para permitir que diferentes tipos de dispositivos e sistemas sejam integrados à rede e para permitir que novas tecnologias sejam adicionadas à rede no futuro (PETROLO et al., 2018).

- **P14- Interoperabilidade de plataforma cruzada:** Os padrões de comunicação devem permitir que diferentes plataformas, como sistemas operacionais, se comuniquem de maneira eficaz, garantindo que as informações sejam compartilhadas de forma confiável entre dispositivos e sistemas que usam diferentes plataformas (CHENG et al., 2019).
- **P15- Taxa de Erro de Transmissão** - Mede a precisão na transmissão de mensagens, identificando a taxa de erros que podem afetar a interoperabilidade (Suryadevara et al. 2018).

c. Casos de teste abstratos

| Caso de teste 7- CT07 | |
|------------------------------|--|
| Título: | Teste de Padrões de Comunicação em Dispositivos IoT |
| Ambiente de Teste: | Dois dispositivos IoT de fabricantes diferentes (Dispositivo A e Dispositivo B). |
| Pré-condição: | Dispositivos conectados à mesma rede Wi-Fi |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Inicie a comunicação entre Dispositivo A e Dispositivo B por meio da plataforma IoT. 2. Envie um conjunto de dados de teste contendo leituras de dados a partir de Dispositivo A para Dispositivo B. 3. Verifique se o Dispositivo B interpreta corretamente os dados e compreende o significado das leituras. 4. Repita o processo, mas desta vez, envie os dados de teste de Dispositivo B para Dispositivo A. 5. Verifique se o Dispositivo A interpreta corretamente os dados recebidos de Dispositivo B. |
| Pós-condições: | Ambos os dispositivos (A e B) foram capazes de interpretar e compreender corretamente os dados enviados pelo outro. Confirmação de que a semântica de dados está sendo mantida na comunicação entre dispositivos de fabricantes diferentes, garantindo interoperabilidade eficaz em um ambiente IoT. |

| |
|-------------------------------|
| Caso de teste 8 - CT08 |
|-------------------------------|

| | |
|--------------------|--|
| Título: | Teste de Compatibilidade de Protocolos de Comunicação |
| Ambiente de Teste: | Ambiente de rede com dispositivos IoT que usam diferentes protocolos de comunicação |
| Pré-condição: | Os dispositivos IoT estão configurados para se comunicar uns com os outros, mas usam protocolos diferentes. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Os dispositivos IoT são ativados e conectados à rede. 2. Os dispositivos iniciam a comunicação uns com os outros usando seus respectivos protocolos de comunicação. 3. Os resultados da comunicação são registrados e analisados. |
| Pós-condições: | É verificado se os dispositivos IoT foram capazes de se comunicar uns com os outros com sucesso usando seus protocolos de comunicação diferentes. |

| Caso de teste 9- CT09 | |
|-----------------------|--|
| Título: | Teste de conexão de dispositivo com gateway |
| Ambiente de Teste: | Rede de IoT com dispositivo de gateway |
| Pré-condição: | O dispositivo e o gateway estão conectados na mesma rede de IoT. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. O dispositivo envia uma mensagem de conexão para o gateway. 2. O gateway recebe a mensagem e envia uma resposta de conexão para o dispositivo. 3. O dispositivo recebe a resposta e confirma a conexão com o gateway. |
| Pós-condições: | O dispositivo está conectado ao gateway e pronto para enviar e receber dados na rede de IoT |

| Caso de teste 10 - CT10 | |
|--------------------------------|--|
| Título: | Teste de comunicação entre dispositivos |
| Ambiente de Teste: | Rede de IoT com dois dispositivos conectados |
| Pré-condição: | Os dispositivos estão conectados na mesma rede de IoT |
| Passo a Passo: | <ol style="list-style-type: none"> 1. O dispositivo 1 envia uma mensagem para o dispositivo 2. 2. O dispositivo 2 recebe a mensagem e envia uma resposta para o dispositivo 1. 3. O dispositivo 1 recebe a resposta e confirma a comunicação entre os dispositivos. |
| Pós-condições: | Os dispositivos estão se comunicando corretamente na rede de IoT. |

| Caso de teste 11 - CT11 | |
|--------------------------------|--|
| Título: | Teste de integração com API externa |
| Ambiente de Teste: | Rede de IoT com dispositivo conectado a uma API externa |
| Pré-condição: | O dispositivo está conectado à API externa e tem as credenciais necessárias para acessá-la. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. O dispositivo envia uma solicitação para a API externa. 2. A API externa recebe a solicitação e envia uma resposta para o dispositivo. 3. O dispositivo recebe a resposta e confirma que os dados da API externa foram integrados corretamente. |
| Pós-condições: | Os dados da API externa foram integrados com sucesso no dispositivo da rede de IoT. |

| Caso de teste 12- CT12 | |
|-------------------------------|--|
| Título: | Teste de autenticação e segurança |
| Ambiente de Teste: | Rede de IoT com dispositivo e servidor de autenticação |
| Pré-condição: | O dispositivo está configurado para se autenticar com o servidor de autenticação. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. O dispositivo envia as credenciais de autenticação para o servidor. 2. O servidor recebe as credenciais e autentica o dispositivo. 3. O dispositivo recebe a confirmação de autenticação do servidor e pode acessar a rede de IoT |
| Pós-condições: | O dispositivo está autenticado e tem acesso seguro à rede de IoT. |

| Caso de teste 13 - CT13 | |
|--------------------------------|---|
| Título: | Teste de Segurança de Protocolos de Comunicação em Dispositivos IoT |
| Ambiente de Teste: | Laboratório de Testes IoT |
| Pré-condição: | Os dispositivos IoT devem estar conectados à rede e configurados para se comunicar usando o protocolo de comunicação especificado. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Tentar interceptar e decodificar a comunicação entre o dispositivo A e o dispositivo B. 2. Verificar se é possível obter acesso não autorizado aos dados transmitidos. 3. Tentar realizar um ataque de negação de serviço (DoS) nos dispositivos A e B. 4. Verificar se os dispositivos são capazes de lidar com o ataque e continuar a se comunicar. 5. Repetir os passos 1 a 4 para diferentes tipos de ataques e protocolos de comunicação. |

| | |
|----------------|--|
| Pós-condições: | Os dispositivos IoT devem ser capazes de se comunicar com segurança usando o protocolo de comunicação especificado e resistir a diferentes tipos de ataques. |
|----------------|--|

d. medidas

| Taxa de transferência de dados - M05 | |
|---|---|
| Propósito: | Avaliar a capacidade de comunicação entre dispositivos em uma rede de IoT. |
| Método: | Enviar uma quantidade definida de dados de um dispositivo para outro e medir o tempo necessário para a transferência completa. |
| Medida: | Medida: $X = D / T$ X = taxa de transferência de dados D = quantidade de dados transferidos T = tempo necessário para transferência completa |
| Explicação: | Essa fórmula é usada para calcular a taxa na qual os dados são transferidos entre dispositivos em uma rede de IoT com base na quantidade de dados transferidos e no tempo necessário para a transferência completa. É uma medida fundamental para avaliar o desempenho da comunicação em uma rede de IoT. |
| Referência: | ISO/IEC 29182-1:2017 |

| Número de falhas de comunicação - M06 | |
|--|--|
| Propósito: | Avaliar a confiabilidade da comunicação entre dispositivos em uma rede de IoT. |
| Método: | Realizar um conjunto de transferências de dados entre dispositivos em uma rede de IoT e contabilizar o número de falhas de comunicação ocorridas. |
| Medida: | $R = (N / (T * G))$ N é o número total de falhas de comunicação. T é o tempo total de observação (por exemplo, em horas). G é uma medida de gravidade das falhas (por exemplo, uma escala de 1 a 10, onde 1 representa falhas leves e 10 representa falhas graves). |

| | |
|-------------|---|
| Explicação: | Essa medida leva em consideração a frequência (número de falhas), a duração (tempo total de observação) e a gravidade das falhas para calcular a confiabilidade da comunicação em uma rede IoT. Quanto menor o valor de R, mais confiável é a comunicação |
| Referência: | ISO/IEC 29341-8-20:2016 |

| Latência de rede - M07 | |
|-------------------------------|---|
| Propósito: | Avaliar o tempo de resposta da rede de IoT. |
| Método: | Enviar uma mensagem de um dispositivo para outro e medir o tempo necessário para a recepção da mensagem. |
| Medida: | $X = t2 - t1$ X = latência de rede t1 = tempo do envio da mensagem t2 = tempo da recepção da mensagem |
| Explicação: | Essa fórmula calcula a diferença entre o tempo de recepção da mensagem (t2) e o tempo de envio da mensagem (t1) para determinar a latência da rede em uma aplicação de IoT. |
| Referência: | ISO/IEC 30141:2018 |

| Taxa de sucesso de conexão - M08 | |
|---|--|
| Propósito: | Avaliar a efetividade dos padrões de comunicação em estabelecer conexões entre dispositivos em uma rede de IoT. |
| Método: | Tentar estabelecer uma conexão entre dispositivos em uma rede de IoT e contabilizar o número de conexões bem-sucedidas. |
| Medida: | $X = \text{número de conexões bem-sucedidas} / \text{número total de tentativas de conexão}$ |
| Explicação: | Essa fórmula representa a proporção de conexões que foram estabelecidas com sucesso em relação ao número total de tentativas de conexão realizadas. É uma medida importante para avaliar a efetividade dos padrões de comunicação em uma rede de IoT em termos de estabelecimento de conexões bem-sucedidas. |
| Referência: | ISO/IEC 29341-8-20:2016 |

| Variação de latência de rede - M09 | |
|------------------------------------|---|
| Propósito: | Avaliar a estabilidade da rede de IoT em relação ao tempo de resposta. |
| Método: | Enviar uma mensagem de um dispositivo para outro em intervalos regulares e medir a variação da latência de rede ao longo do tempo. |
| Medida: | $X = (n / N) * 100,$ <p>X é a porcentagem de dados recebidos corretamente n é o número de dados recebidos corretamente N é o número total de dados enviados.</p> |
| Explicação: | Essa fórmula permite avaliar a estabilidade da rede de IoT em relação ao tempo de resposta, fornecendo uma medida da qualidade da comunicação entre os dispositivos na rede. Quanto maior a porcentagem X, melhor a estabilidade da rede em termos de latência de rede. |
| Referência: | ISO/IEC 29182-1:2017 |

8. Integração de sistema

a. Definição

A norma ISO 30141:2018 estabelece a integração de sistema como a habilidade dos sistemas em estabelecer conexões, realizar comunicações e interações com outros sistemas e serviços, com o propósito de prover informações e serviços de valor agregado. Essa capacidade desempenha um papel crucial na conquista da *Interoperabilidade* na Internet das Coisas, que é a capacidade dos dispositivos e sistemas provenientes de diferentes fornecedores de se comunicarem e interagirem de forma transparente entre si.

Essa norma reconhece a importância de estabelecer uma interconexão harmoniosa entre os sistemas e serviços, permitindo a troca de informações e a oferta de serviços de maior qualidade. Além disso, ao promover a *Interoperabilidade* a norma ISO 30141:2018 busca facilitar a integração de dispositivos e sistemas heterogêneos, assegurando uma comunicação fluida e uma interação eficiente entre eles.

b. Contextualização

A integração de sistemas é uma das facetas fundamentais da interoperabilidade, representando

um dos principais desafios enfrentados no contexto da IoT. A capacidade de integrar diferentes sistemas e dispositivos é crucial para garantir a comunicação eficaz e a interação entre componentes heterogêneos, permitindo a entrega de serviços integrados e valor agregado em um ambiente de IoT.

Um exemplo prático de integração de sistema pode ser observado em uma casa inteligente, onde vários dispositivos e sistemas, como iluminação, termostatos, câmeras de segurança e eletrodomésticos, colaboram para oferecer uma experiência de casa conectada. Para tornar isso possível, é crucial que esses sistemas sejam capazes de se conectar, comunicar e interagir de forma eficiente e confiável, independentemente do fornecedor ou da plataforma utilizada.

Assegurar a integração de sistema é essencial para possibilitar a troca de informações e o compartilhamento de recursos entre os dispositivos e sistemas envolvidos. Isso permite que os diferentes componentes da IoT trabalhem em conjunto de maneira harmoniosa, promovendo uma experiência aprimorada para os usuários finais e garantindo a viabilidade de soluções inovadoras no contexto da Internet das Coisas. Algumas propriedades da integração de sistema em IoT incluem (Chen et al., 2021):

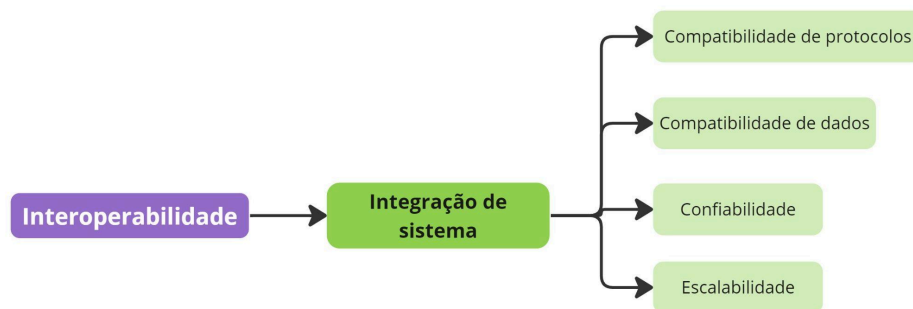


Figura 5 – Propriedades da integração de sistema

- **P16- Compatibilidade de protocolos:** diferentes dispositivos e sistemas devem ser capazes de se comunicar entre si, independentemente do protocolo utilizado.
- **P17- Compatibilidade de dados:** diferentes sistemas devem ser capazes de interpretar e utilizar os dados gerados por outros sistemas.
- **P18- Confiabilidade:** os sistemas integrados devem ser capazes de funcionar de forma confiável, apesar de falhas ou interrupções na rede ou nos dispositivos.
- **P19- Escalabilidade:** os sistemas integrados devem ser capazes de lidar com um grande número de dispositivos e usuários.
- **P20- Flexibilidade:** os sistemas integrados devem ser capazes de se adaptar a mudanças nas condições do ambiente ou nas necessidades dos usuários.

c. Casos de teste abstratos

| Caso de teste 14 - CT14 | |
|--------------------------------|---|
| Título: | Teste de interoperabilidade entre dispositivos |
| Ambiente de Teste: | Rede de dispositivos IoT |
| Pré-condição: | Todos os dispositivos da rede estão devidamente configurados e conectados. |
| Passo a Passo: | <ol style="list-style-type: none">1. Inicie o sistema de automação2. Envie um comando de ativação para um dispositivo A usando o protocolo X.3. Verifique se o dispositivo A responde corretamente e executa a ação esperada.4. Envie um comando de ativação para um dispositivo B usando o protocolo Y.5. Verifique se o dispositivo B responde corretamente e executa a ação esperada.6. Certifique-se de que não haja conflitos ou problemas de comunicação entre os dispositivos de diferentes protocolos. |
| Pós-condições: | Os dispositivos devem ser capazes de se comunicar e trocar informações de forma interoperável. |

| Caso de teste 15 - CT15 | |
|--------------------------------|---|
| Título: | teste de Confiabilidade em Ambiente Industrial |
| Ambiente de Teste: | Sistema de automação industrial |
| Pré-condição: | Vários dispositivos e sistemas de automação de diferentes fornecedores estão integrados para controlar o processo de fabricação. |
| Passo a Passo: | <ol style="list-style-type: none">1. Simular uma interrupção na rede que conecta os dispositivos e sistemas.2. Observar como os dispositivos e sistemas respondem à interrupção, se continuam funcionando ou entram em um estado |

| | |
|----------------|---|
| | <p>de falha.</p> <ol style="list-style-type: none"> 3. Restaurar a conexão de rede e verificar se os dispositivos e sistemas se recuperam e voltam a funcionar normalmente. 4. Repetir o processo, mas desta vez, simular uma falha em um dos dispositivos. 5. Registrar como a integração reage à falha do dispositivo e se a redundância ou sistemas de backup entram em ação. |
| Pós-condições: | Avaliar a confiabilidade do sistema de automação industrial em lidar com interrupções na rede e falhas de dispositivos, identificando áreas de melhoria na garantia de continuidade operacional. |

| Caso de teste 16 - CT16 | |
|-------------------------|--|
| Título: | Teste de Escalabilidade em Ambiente de Varejo |
| Ambiente de Teste: | Sistema de gerenciamento de estoque em uma rede de lojas de varejo. |
| Pré-condição: | O sistema de gerenciamento de estoque é usado em várias lojas e precisa lidar com um grande número de produtos e transações. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Aumentar gradualmente o número de lojas que utilizam o sistema de gerenciamento de estoque. 2. Realizar operações de entrada e saída de produtos em todas as lojas simultaneamente. 3. Monitorar o desempenho do sistema, incluindo tempo de resposta e capacidade de processamento. 4. Aumentar ainda mais o número de lojas e repetir as operações. 5. Registrar em que ponto o sistema começa a mostrar sinais de sobrecarga ou redução de desempenho. |
| Pós-condições: | Avaliar a escalabilidade do sistema de gerenciamento de estoque em lidar com um grande número de lojas e transações, identificando os limites de sua capacidade e necessidades de escalonamento. |

| Caso de teste 17 - CT17 | |
|--------------------------------|--|
| Título: | Teste de Compatibilidade de Protocolos |
| Ambiente de Teste: | Ambiente de uma cidade inteligente com vários dispositivos de fornecedores diferentes, incluindo sensores de tráfego, sistemas de iluminação pública e sistemas de monitoramento ambiental. |
| Pré-condição: | Todos os dispositivos estão funcionando corretamente e estão conectados à uma rede. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Selecionar dois dispositivos de fornecedores diferentes que usam protocolos de comunicação diferentes. 2. Configurar um cenário em que esses dispositivos precisam se comunicar para coordenar a gestão do tráfego em uma área da cidade. 3. Iniciar a comunicação entre os dispositivos e verificar se eles são capazes de trocar informações e coordenar suas ações. 4. Verificar se não há perda de dados ou erros de comunicação durante a interação. 5. Repetir o teste com diferentes dispositivos e protocolos para avaliar a capacidade geral de compatibilidade de protocolos. |
| Pós-condições: | Os dispositivos de fornecedores diferentes são capazes de se comunicar efetivamente e coordenar suas ações, demonstrando que a compatibilidade de protocolos está sendo atendida. |

| Caso de teste 18- CT18 | |
|-------------------------------|--|
| Título: | Teste de Escalabilidade e Flexibilidade |
| Ambiente de Teste: | Uma rede de dispositivos de monitoramento de tráfego em uma área metropolitana com um grande número de dispositivos e variações nas condições do tráfego. |
| Pré-condição: | A rede está funcionando com um número moderado de dispositivos e condições de tráfego normais. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Gradualmente aumentar o número de dispositivos na rede para verificar como ela lida com a escalabilidade. 2. Introduzir variações nas condições do tráfego, como |

| | |
|----------------|---|
| | <p>congestionamento repentino ou acidentes, para testar a flexibilidade da rede.</p> <p>3. Avaliar o desempenho da rede à medida que o número de dispositivos e a complexidade das condições de tráfego aumentam.</p> <p>4. Verificar se a rede é capaz de se adaptar às mudanças nas condições do ambiente de tráfego.</p> <p>5. Repetir o teste em diferentes escalas e com diferentes cenários de tráfego.</p> |
| Pós-condições: | A rede de dispositivos de monitoramento de tráfego demonstra escalabilidade e flexibilidade, atendendo aos requisitos estabelecidos. |

d. Medidas

| Taxa de sucesso na integração de sistema- M10 | |
|---|---|
| Propósito: | Avaliar a eficácia da interoperabilidade de serviços em um ambiente IoT. |
| Método: | Registrar o número de tentativas de interoperabilidade de serviços e o número de tentativas bem-sucedidas durante um período de tempo específico. |
| Medida: | $X = (n1 / n2) \times 100\%$ <p>X = taxa de sucesso na integração de sistemas n1 = número de tentativas bem-sucedidas durante o período avaliado n2 = número total de tentativas realizadas</p> |
| Explicação: | Essa medida calcula a eficácia da interoperabilidade de serviços em um ambiente IoT, representando a porcentagem de tentativas de interoperabilidade que foram bem-sucedidas em relação ao número total de tentativas realizadas. Quanto maior o valor de X, maior é a taxa de sucesso na integração de sistemas, indicando um melhor desempenho na interoperabilidade de serviços. |
| Referência: | ISO/IEC 30141:2018 |

| Tempo médio de integração de sistema- M11 | |
|--|---|
| Propósito: | Avaliar o tempo médio necessário para integrar sistemas em um ambiente IoT. |
| Método: | Registrar o tempo decorrido desde o início da interoperabilidade de serviços até sua conclusão bem-sucedida. |
| Medida: | $X = (\Sigma t) / n$ <p> x = tempo médio de integração de sistemas t = tempo necessário para a interoperabilidade de serviços bem-sucedida n = número total de tentativas de interoperabilidade de serviços durante o período avaliado </p> |
| Explicação: | Essa fórmula calcula a média dos tempos gastos em todas as tentativas de interoperabilidade de serviços durante um determinado período. Ela fornece uma medida quantitativa do tempo médio necessário para integrar sistemas em um ambiente IoT, com base nas tentativas realizadas e seus respectivos tempos de conclusão bem-sucedidos. Quanto menor for o valor de X, mais eficiente é o processo de integração de sistemas em relação ao tempo. |
| Referência: | ISO/IEC 30141:2018 |

| Nível de padronização de interfaces de integração - M12 | |
|--|--|
| Propósito: | Avaliar o grau de padronização das interfaces de interoperabilidade de serviços em um ambiente IoT. |
| Método: | Verificar se as interfaces de interoperabilidade de serviços estão em conformidade com os padrões definidos para o ambiente IoT. |
| Medida: | <p> X = nível de padronização de interfaces de integração n1 = número de interfaces de interoperabilidade de serviços em conformidade com os padrões definidos n2 = número total de interfaces de interoperabilidade de serviços avaliadas $X = (n1 / n2) \times 100\%$ </p> |
| Explicação: | Essa fórmula calcula a porcentagem de interfaces que estão em conformidade com os padrões definidos em relação ao número total de interfaces avaliadas. O resultado, X, representa o grau de padronização das interfaces de integração em um ambiente IoT, indicando o quão bem |

| | |
|-------------|--|
| | as interfaces estão alinhadas com os padrões estabelecidos pela norma ISO/IEC 30141:2018. Quanto maior o valor de X, maior o nível de padronização das interfaces. |
| Referência: | ISO/IEC 30141:2018 |

| Taxa de transferência de dados - M13 | |
|--------------------------------------|---|
| Propósito: | Avaliar a capacidade de comunicação entre sistemas interconectados na IoT. |
| Método: | Medir a quantidade de dados transmitidos entre os sistemas em um determinado período de tempo. |
| Medida: | $X = (T2 - T1) / S$ <p>X = taxa de transferência de dados T1 = tempo inicial da transferência de dados T2 = tempo final da transferência de dados S = quantidade de dados transmitidos</p> |
| Explicação: | Essa fórmula permite calcular a taxa de transferência de dados, que é uma medida fundamental para avaliar o desempenho da comunicação entre sistemas interconectados na IoT. Quanto maior a taxa de transferência, mais eficiente é a comunicação entre os sistemas, o que é essencial para garantir o funcionamento adequado da Internet das Coisas. |
| Referência: | ISO 30141:2018. |

| Tempo de integração - M14 | |
|---------------------------|--|
| Propósito: | Avaliar o tempo necessário para a integração de diferentes sistemas IoT. |
| Método: | Contabilizar o início do processo de integração e comparar com o tempo em que a integração esteja concluída. |
| Medida: | $X = t2 - t1$, onde X é o tempo de integração, t1 é o tempo de início do processo de integração e t2 é o tempo em que a integração esteja concluída. |
| Explicação: | Essa fórmula simples subtrai o tempo de início do tempo de conclusão para determinar o tempo necessário para realizar a integração dos sistemas IoT. O resultado X é o tempo de integração, que pode ser expresso na mesma |

| | |
|-------------|--|
| | unidade de tempo utilizada para t1 e t2 (por exemplo, segundos, minutos, horas, etc.). |
| Referência: | ISO/IEC 30141:2018. |

9. Protocolos de rede

a. Definição

A norma ISO/IEC 30141:2018 define protocolos de rede como um elemento essencial da *Interoperabilidade* em sistemas de IoT, que permite a comunicação entre dispositivos, serviços e aplicativos em uma rede. Um protocolo de rede define regras e padrões para troca de dados, sincronização e coordenação de operações entre dispositivos, permitindo a *Interoperabilidade* e integração de sistemas heterogêneos.

b. Contextualização

Com a crescente expansão da IoT e o aumento exponencial no número de dispositivos e sistemas conectados, a interoperabilidade tornou-se um requisito essencial para assegurar uma comunicação eficaz e a troca de informações entre eles. Os protocolos de rede são fundamentais para garantir essa interoperabilidade, permitindo que dispositivos e serviços de diferentes fabricantes e tecnologias possam se conectar e interagir de maneira eficiente. Para assegurar a eficácia desses protocolos, é importante considerar várias propriedades que definem sua capacidade de facilitar a comunicação entre sistemas distintos. Entre essas propriedades, destacam-se:

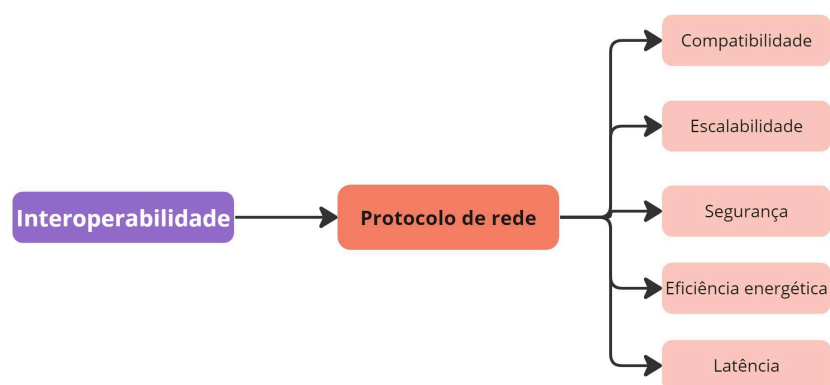


Figura 6 – Propriedades do protocolo de rede

- **P21- Compatibilidade:** os protocolos devem ser compatíveis com as especificações de hardware e software dos dispositivos conectados.
- **P22- Escalabilidade:** os protocolos devem permitir a expansão do sistema de IoT para

suportar um grande número de dispositivos e usuários.

- **P23- Segurança:** os protocolos devem garantir a segurança da comunicação entre dispositivos, incluindo autenticação, autorização e criptografia de dados.
- **P24- Eficiência energética:** os protocolos devem ser otimizados para reduzir o consumo de energia dos dispositivos conectados, maximizando a vida útil da bateria.
- **P25- Latência:** os protocolos devem garantir tempos de resposta rápidos o suficiente para permitir o controle em tempo real de dispositivos.

c. **Casos de teste abstratos**

| Caso de teste 19 - CT19 | |
|--------------------------------|---|
| Título: | Teste de Compatibilidade de Protocolo de Rede |
| Ambiente de Teste: | Sistema IoT com dispositivos de diferentes fornecedores conectados por meio de protocolos de rede distintos. |
| Pré-condição: | Os dispositivos estão configurados corretamente e conectados à rede |
| Passo a Passo: | <ol style="list-style-type: none">1. Verificar se todos os dispositivos estão conectados e funcionando corretamente.2. Enviar dados de um dispositivo para outro por meio do protocolo de rede.3. Verificar se os dados foram recebidos corretamente pelo dispositivo de destino. |
| Pós-condições: | Os dados foram transmitidos com sucesso e os dispositivos foram capazes de interoperar usando os protocolos de rede correspondentes. |

| Caso de teste 20 - CT20 | |
|--------------------------------|---|
| Título: | Teste de Escalabilidade de Protocolo de Rede |
| Ambiente de Teste: | Sistema de IoT com um grande número de dispositivos conectados por meio de um protocolo de rede específico. |
| Pré-condição: | O sistema está configurado corretamente e o protocolo de rede suporta o número de dispositivos conectados |

| | |
|----------------|---|
| Passo a Passo: | <ol style="list-style-type: none"> 1. Adicionar gradualmente dispositivos à rede até atingir o limite suportado pelo protocolo de rede. 2. Enviar dados entre os dispositivos conectados para verificar a integridade da comunicação. 3. Verificar se os dados foram recebidos corretamente pelos dispositivos de destino. |
| Pós-condições: | O protocolo de rede suportou o número de dispositivos conectados e os dados foram transmitidos com sucesso |

| Caso de teste 21- CT21 | |
|------------------------|--|
| Título: | Teste de Segurança de Protocolo de Rede |
| Ambiente de Teste: | Sistema de IoT com dispositivos conectados por meio de protocolos de rede que suportam recursos de segurança. |
| Pré-condição: | Os recursos de segurança dos protocolos de rede estão configurados corretamente. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Enviar dados entre dispositivos conectados por meio do protocolo de rede. 2. Verificar se os dados foram transmitidos com segurança, usando criptografia, autenticação e autorização de dados. 3. Tentar invadir o sistema de IoT por meio de vulnerabilidades de segurança conhecidas. |
| Pós-condições: | Os dados foram transmitidos com segurança e nenhuma vulnerabilidade de segurança foi explorada com sucesso. |

| Caso de teste 22- CT22 | |
|------------------------|---|
| Título: | Teste de Eficiência Energética de Protocolo de Rede |
| Ambiente de Teste: | Sistema IoT com dispositivos conectados por meio de protocolos de rede que suportam recursos de eficiência energética |

| | |
|----------------|---|
| Pré-condição: | Os recursos de eficiência energética dos protocolos de rede estão configurados corretamente. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Monitorar o consumo de energia dos dispositivos conectados. 2. Enviar dados entre dispositivos conectados por meio do protocolo de rede. 3. Verificar se o consumo de energia dos dispositivos foi otimizado pelo protocolo de rede. |
| Pós-condições: | O consumo de energia dos dispositivos foi otimizado e os dados foram transmitidos com sucesso pelo protocolo de rede. |

| Caso de teste 23 - CT23 | |
|-------------------------|--|
| Título: | Teste de Compatibilidade de Protocolos |
| Ambiente de Teste: | Uma rede de dispositivos IoT em uma cidade inteligente com diversos dispositivos de diferentes fabricantes. |
| Pré-condição: | Todos os dispositivos estão devidamente configurados e operacionais na rede. |
| Passo a Passo: | <p>Selecionar dois dispositivos IoT de fornecedores diferentes, cada um usando um protocolo de rede diferente.</p> <p>Configurar um cenário em que esses dispositivos precisam se comunicar e trocar informações para coordenar uma ação específica na cidade inteligente.</p> <p>Iniciar a comunicação entre os dispositivos e verificar se eles são capazes de trocar informações e coordenar suas ações.</p> <p>Garantir que não haja perda de dados ou erros de comunicação durante a interação.</p> <p>Repetir o teste com diferentes dispositivos e protocolos para avaliar a capacidade geral de compatibilidade de protocolos na rede IoT.</p> |
| Pós-condições: | Os dispositivos IoT de fornecedores diferentes são capazes de se comunicar eficazmente e coordenar suas ações, demonstrando que a |

| | |
|--|---|
| | compatibilidade de protocolos está sendo atendida na rede IoT |
|--|---|

| Caso de teste 24 - CT24 | |
|-------------------------|--|
| Título: | Teste de Compatibilidade de Protocolos para Rastreamento de Ativos IoT |
| Ambiente de Teste: | Ambiente de rastreamento de ativos IoT, com dispositivos de rastreamento de diferentes fabricantes e tecnologias, todos enviando dados de latitude e longitude. |
| Pré-condição: | Os dispositivos de rastreamento estão operando corretamente e enviando dados de latitude e longitude em diferentes protocolos |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Selecionar dois dispositivos de rastreamento de diferentes fornecedores que utilizam protocolos de comunicação diferentes. 2. Configurar um cenário em que esses dispositivos precisam compartilhar dados de latitude e longitude para rastreamento de ativos em tempo real. 3. Iniciar a comunicação entre os dispositivos e verificar se eles são capazes de trocar informações de latitude e longitude sem perda de dados. 4. Verificar se os dados são interpretados corretamente pelos dispositivos receptores. 5. Testar a capacidade de resposta em tempo real dos dispositivos, medindo a latência na transmissão e recepção dos dados de localização. 6. Repetir o teste com diferentes dispositivos e protocolos para avaliar a compatibilidade geral de protocolos para rastreamento de ativos IoT. |
| Pós-condições: | Os dispositivos de rastreamento de ativos IoT de diferentes fornecedores são capazes de trocar informações de latitude e longitude de forma eficaz e em tempo real, demonstrando a compatibilidade de protocolos para rastreamento de ativos IoT. |

| Caso de teste 25 - CT25 | |
|--------------------------------|---|
| Título: | Teste de segurança usando HTTPS |
| Ambiente de Teste: | Rede de IoT com dois ou mais dispositivos compatíveis com HTTPS |
| Pré-condição: | Os dispositivos devem estar conectados à mesma rede de IoT e configurados para usar o protocolo HTTPS. Cada dispositivo deve ser capaz de enviar e receber requisições HTTPS e deve ter certificados SSL/TLS válidos instalados. |
| Passo a Passo: | <ol style="list-style-type: none"> 1. Enviar uma requisição HTTPS para um dispositivo selecionado e verificar se a comunicação é estabelecida com sucesso. 2. Enviar uma requisição HTTPS para um dispositivo usando um certificado SSL/TLS inválido e verificar se a comunicação é bloqueada. 3. Tentar interceptar e decifrar o tráfego HTTPS usando uma ferramenta de interceptação de pacotes e verificar se a comunicação é bloqueada ou se os dados são ilegíveis. 4. Tentar enviar requisições falsas ou maliciosas para os dispositivos e verificar se as medidas de autenticação e autorização são aplicadas corretamente. |
| Pós-condições: | Todos os dispositivos devem ser capazes de estabelecer comunicação HTTPS segura, com autenticação e autorização aplicadas corretamente, garantindo a segurança da rede. |

c. medidas

| Latência de rede - M15 | |
|-------------------------------|--|
| Propósito: | Avaliar o tempo de resposta da rede durante a comunicação entre dispositivos. |
| Método: | Enviar um pacote de dados do dispositivo A para o dispositivo B e medir o tempo que leva para o dispositivo B receber o pacote e enviar uma resposta para o dispositivo A. |

| | |
|-------------|---|
| Medida: | $X = t_2 - t_1$ X= é a latência da rede, que é o tempo gasto para que um pacote de dados seja enviado do dispositivo A para o dispositivo B e para que a resposta seja enviada de volta do dispositivo B para o dispositivo A. t1= é o momento em que o dispositivo A enviou o pacote de dados. t2= é o momento em que o dispositivo B enviou a resposta. |
| Explicação: | Essa medida calcula a diferença de tempo entre o envio do pacote de dados pelo dispositivo A e o recebimento da resposta pelo dispositivo A, o que representa o tempo de latência da rede. Quanto menor for o valor de X, menor será a latência da rede, o que indica uma comunicação mais rápida e responsiva entre os dispositivos. A medida é expressa em unidades de tempo, como milissegundos (ms) ou microssegundos (µs), dependendo da precisão necessária para a avaliação da latência da rede. |
| Referência: | ISO/IEC 30141:2018 - Information technology -- Internet of Things (IoT) -- Part 4: Communication protocols. |

| Taxa de transferência de rede - M16 | |
|-------------------------------------|---|
| Propósito: | Avaliar a quantidade de dados que podem ser transmitidos entre dispositivos em um determinado período de tempo. |
| Método: | Enviar um conjunto de dados de tamanho conhecido do dispositivo A para o dispositivo B e medir o tempo necessário para a transmissão completa. |
| Medida: | $X = S / t$, onde X é a taxa de transferência da rede, S é o tamanho dos dados enviados e t é o tempo necessário para a transmissão completa. |
| Explicação: | Essa medida expressa quantos dados podem ser transmitidos de um dispositivo A para um dispositivo B em um determinado período de tempo, representando a eficiência da rede de comunicação em questão. Quanto maior o valor de X, mais rápida é a taxa de transferência da rede. Essa medida é útil para avaliar o desempenho e a capacidade de comunicação de dispositivos e sistemas, sendo uma medida importante em contextos como a Internet das Coisas (IoT). |
| Referência: | ISO/IEC 30141:2018 - Information technology -- Internet of Things (IoT) -- Part 4: Communication protocols. |
| Taxa de transmissão de dados - M17 | |

| | |
|-------------|---|
| Propósito: | Avaliar a capacidade do protocolo de rede para transmitir dados em uma determinada velocidade. |
| Método: | Enviar um conjunto de dados de tamanho conhecido do dispositivo A para o dispositivo B e medir a velocidade de transmissão dos dados. |
| Medida: | $X = S / t$, onde X é a taxa de transmissão de dados, S é o tamanho dos dados enviados e t é o tempo necessário para a transmissão completa. |
| Explicação: | Essa fórmula permite calcular a velocidade com que os dados são transmitidos da origem (dispositivo A) para o destino (dispositivo B). A taxa de transmissão de dados é uma medida crítica para avaliar a interoperabilidade de um protocolo de rede, pois indica a eficiência da transmissão em relação ao tamanho dos dados e ao tempo necessário para a entrega. Quanto maior a taxa de transmissão, mais rápida é a transferência de dados entre os dispositivos. Essa medida ajuda a determinar se um protocolo de rede é adequado para a aplicação específica em questão. |
| Referência: | ISO/IEC 30141:2018 - Information technology -- Internet of Things (IoT) -- Part 4: Communication protocols. |

| Confiabilidade da conexão - M18 | |
|--|---|
| Propósito: | Avaliar a capacidade do protocolo de rede para manter uma conexão estável e confiável entre os dispositivos. |
| Método: | Enviar um conjunto de dados do dispositivo A para o dispositivo B em uma conexão de rede instável e verificar se todos os dados foram recebidos corretamente. |
| Medida: | $X = (n / N) * 100$ <p>X é a porcentagem de dados recebidos corretamente. n é o número de dados recebidos corretamente. N é o número total de dados enviados.</p> |
| Explicação: | Essa fórmula calcula a porcentagem de dados que foram transmitidos com sucesso em relação ao número total de dados enviados. Quanto maior o valor de X, maior a confiabilidade da conexão, indicando que a conexão conseguiu manter a integridade dos dados enviados de forma mais eficaz. Isso é especialmente importante em ambientes de rede instável, onde a confiabilidade da conexão é fundamental para garantir que os dados sejam entregues com precisão. |
| Referência: | ISO/IEC 30141:2018 - Information technology -- Internet of Things (IoT) -- Part 4: Communication protocols. |

| Escalabilidade do sistema - M19 | |
|---------------------------------|---|
| Propósito: | Avaliar a capacidade do protocolo de rede para suportar um grande número de dispositivos conectados simultaneamente. |
| Método: | Adicionar um grande número de dispositivos ao sistema e verificar se o protocolo de rede é capaz de suportar o tráfego de dados gerado por todos os dispositivos. |
| Medida: | $X = N$, onde X é a escalabilidade do sistema e N é o número máximo de dispositivos conectados simultaneamente que o protocolo de rede pode suportar. |
| Explicação: | Essa medida é direta e simples, indicando o número máximo de dispositivos que o protocolo de rede é capaz de suportar simultaneamente antes de atingir seu limite de capacidade. Quanto maior o valor de N , maior a escalabilidade do sistema, indicando a capacidade do protocolo de rede de lidar com um grande número de dispositivos conectados sem degradação significativa no desempenho. Essa medida é útil para avaliar a capacidade do sistema em cenários de Internet das Coisas (IoT), onde muitos dispositivos podem estar conectados à rede ao mesmo tempo. |
| Referência: | ISO/IEC 30141:2018 - Information technology -- Internet of Things (IoT) -- Part 4: Communication protocols. |

10. Impacto das Subcaracterísticas

Os impactos dessas subcaracterísticas na *Interoperabilidade* em IoT podem ser significativos. A falta de *Interoperabilidade* pode resultar em sistemas incompatíveis que não podem se comunicar entre si, o que pode limitar a eficiência e a eficácia da IoT. Além disso, a falta de segurança pode levar a violações de privacidade e a vulnerabilidades, enquanto a falta de interpretação comum dos dados pode resultar em falha de comunicação. Em resumo, **a interoperabilidade é uma característica crítica da IoT** e as subcaracterísticas relacionadas devem ser gerenciadas adequadamente para garantir que os dispositivos IoT possam se comunicar e trabalhar juntos de forma eficiente e segura.

As subcaracterísticas de interoperabilidade estão interligadas de forma a impactar diretamente umas às outras, o que implica que a ausência de uma subcaracterística pode prejudicar o desempenho das demais. Dessa forma, é essencial adotar uma abordagem integral na validação da interoperabilidade, considerando o contexto da aplicação. Essa abordagem pode ser implementada por meio de testes que avaliem as subcaracterísticas em conjunto ou através da implementação de soluções que abordem as propriedades afetadas pelas diferentes subcaracterísticas de interoperabilidade.

Para estabelecer as interações entre as quatro subcaracterísticas de *Interoperabilidade*, é essencial analisar quais delas influenciam nas propriedades das outras subcaracterísticas. Será apresentado esses impactos com base nas propriedades das quatro subcaracterísticas. mostra as correlações da subcaracterística "Semântica de Dados" com as propriedades das outras três subcaracterísticas. As cores representam três categorias: (i) verde para representar "Integração de Sistemas"; (ii) azul denota "Protocolo de Comunicação"; e (iii) vermelho para representar o "Protocolo de Rede". A Figura 7 ilustra o impacto das propriedades da subcaracterística "Semântica de Dados". Quando se avalia uma propriedade específica, é necessário considerar a avaliação das propriedades relacionadas das outras subcaracterísticas. Por exemplo, ao avaliar "Interpretação Comum", deve-se levar em consideração a "Compatibilidade de Protocolo", "Compatibilidade de Dados", "Consistência" e "Compatibilidade". Da mesma forma, a avaliação da "Compatibilidade Semântica" implica considerar "Confiabilidade" e "Escalabilidade". Assim, a análise das propriedades de "Semântica de Dados" demanda uma abordagem integrada, onde as inter-relações entre as subcaracterísticas e suas respectivas propriedades são cuidadosamente examinadas para garantir uma avaliação abrangente e precisa.

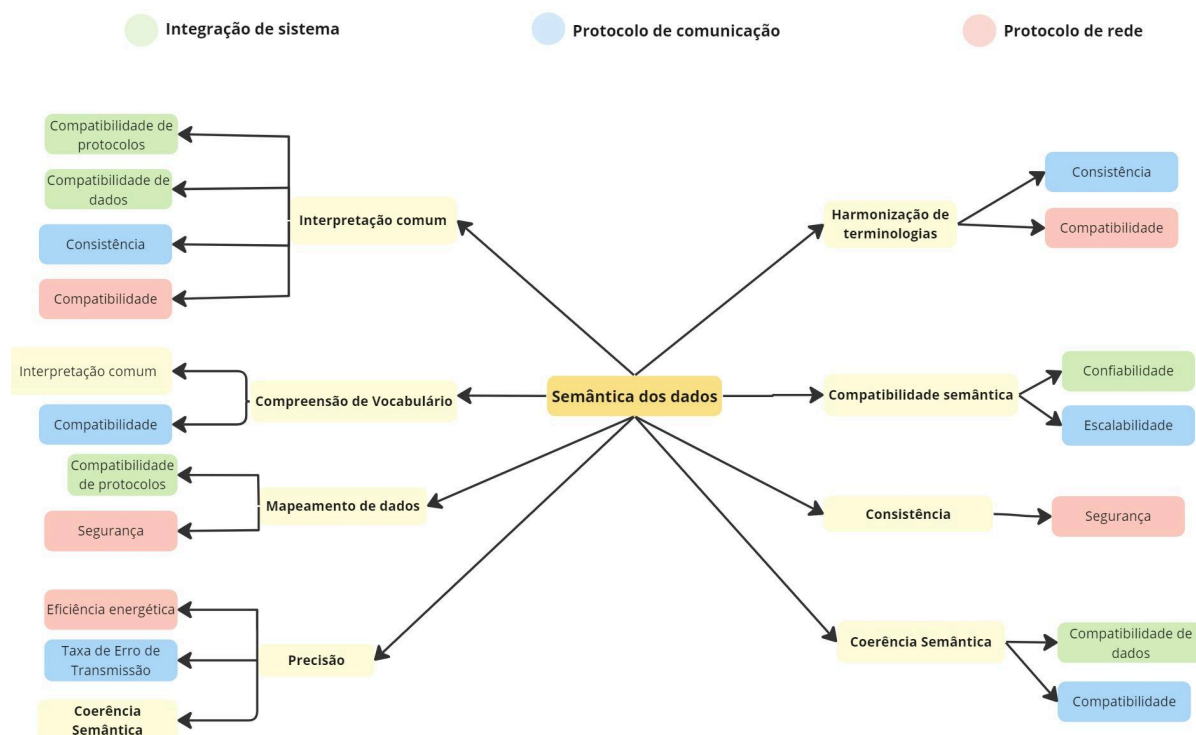


Figura 7 – Impacto da semântica dos dados com as propriedades das outras subcaracterísticas

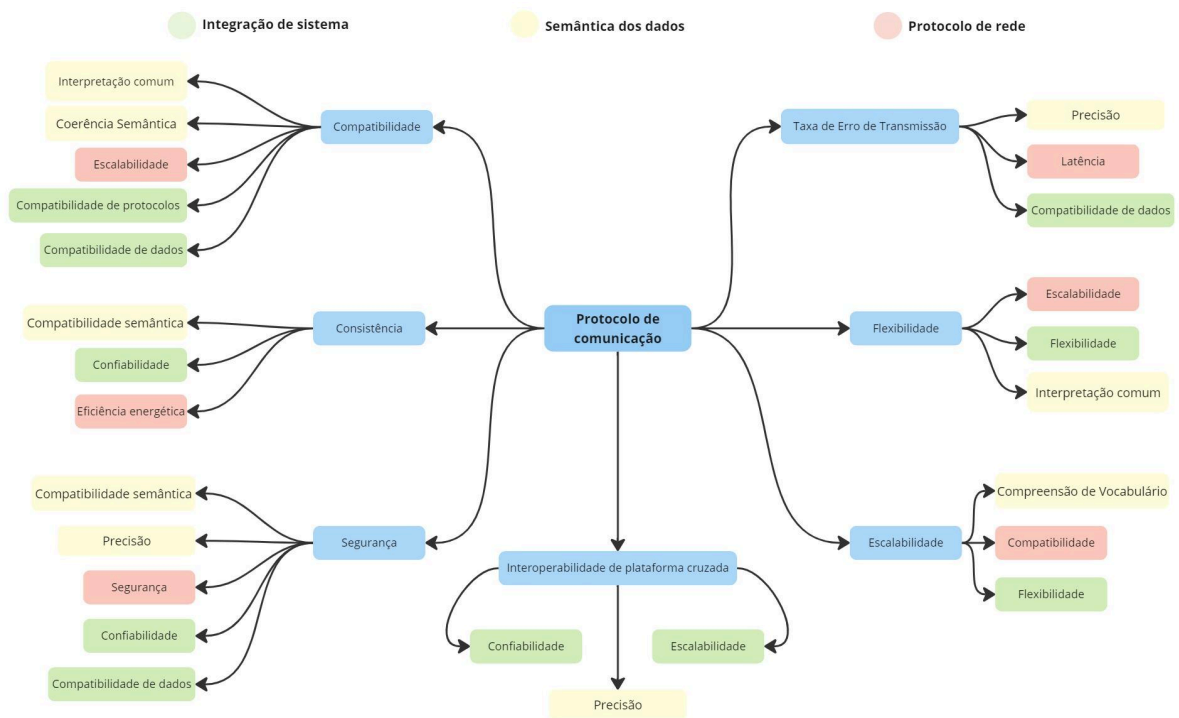


Figura 8 – Impacto de protocolo de comunicação com as propriedades das outras subcaracterísticas

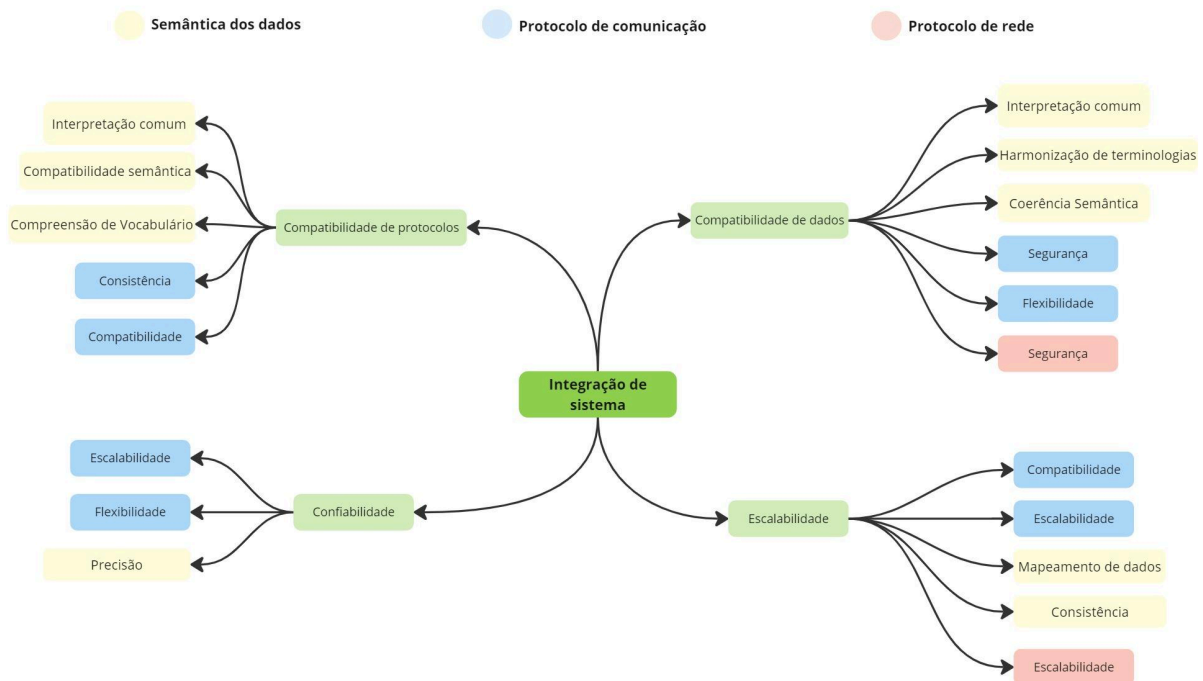


Figura 9 – Impacto de Integração de sistema com as propriedades das outras subcaracterísticas

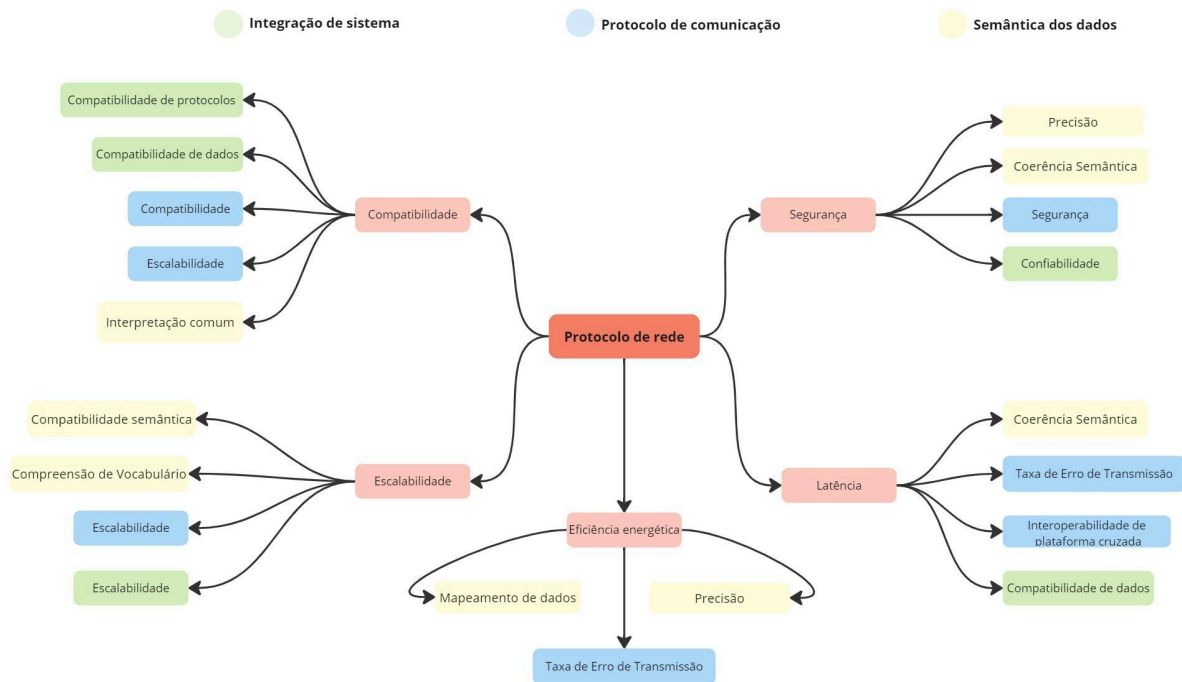


Figura 10– Impacto de protocolo de rede com as propriedades das outras subcaracterísticas

É importante notar que os impactos podem variar dependendo das implementações específicas e das circunstâncias, mas essas são algumas das tendências gerais que podem ser observadas com base nas propriedades apresentadas.

11. Custo benefício

Com base na correlação de uma característica com as outras, apresentada no tópico 2, é possível definir o impacto que uma característica tem sobre as aplicações. A interoperabilidade, por exemplo, é correlacionado a 14 características, mas nem todas as aplicações priorizaram todas as 14 características, então, dado que uma aplicação prioriza apenas 6 características de IoT que se correlacionam com o interoperabilidade, então o coeficiente de impacto (CI) é aproximadamente 0,43, ou seja:

$$CI = ORC/RC$$

Onde:

ORC: número de características correlacionadas à interoperabilidade priorizadas na aplicação.

RC: número total de características relacionadas à interoperabilidade.

Este impacto (CI) quando relacionado ao esforço na execução dos testes e métricas gera o custo benefício que pode ajudar na priorização dos testes. Para calcular este esforço as seguintes fórmulas

são aplicadas:

1º Calcula o custo estimado de cada caso de teste com base no tempo médio para o profissional responsável executar um teste e o valor do tempo do profissional responsável para executá-lo;

$$CT_i = TC_i * VHC_i$$

CT_i : Custo estimado para executar o caso de teste

TC_i : Tempo médio do profissional para executar um caso de teste

VHC_i : Valor do tempo do profissional que executará o caso de teste

2. Após a conclusão de todos os CTs, o valor máximo encontrado é obtido;

$$MCT = \max(CT)$$

MCT: custo mais alto para realização do caso de teste

CT: todas as estimativas de custo

3. Normaliza os custos médios dos casos de teste;

$$CCT = (\sum_{i=1}^n CT_i / MCT) / n$$

CCT: custo médio de casos de teste normalizados

CT_i / MCT: valor estimado do custo do caso de teste i normalizado para o custo mais alto

n: número de casos de teste

4. Repita o processo para as medições e assim obtenha o CMD;

CMD: custo médio das medidas padronizadas;

5. Assim, o Esforço (ESF) é definido por:

$$ESF = (CCT + CMD) / 2$$

Com o Impacto (CI) e o Esforço (ESF), o custo benefício é possível definir em qual quadrante de priorização está a realização dos testes de interoperabilidade da aplicação. O eixo x mostra o Impacto

(CI), e o eixo y mostra o Esforço (ESF). Um Esforço acima de 0,5 é considerado alto, o mesmo para Impacto. Portanto, em uma aplicação onde o coeficiente de impacto (CI) para interoperabilidade é 0,68 a característica de interoperabilidade é considerada uma característica que exerce alto impacto para aquela aplicação IoT em questão. Os grupos representam:

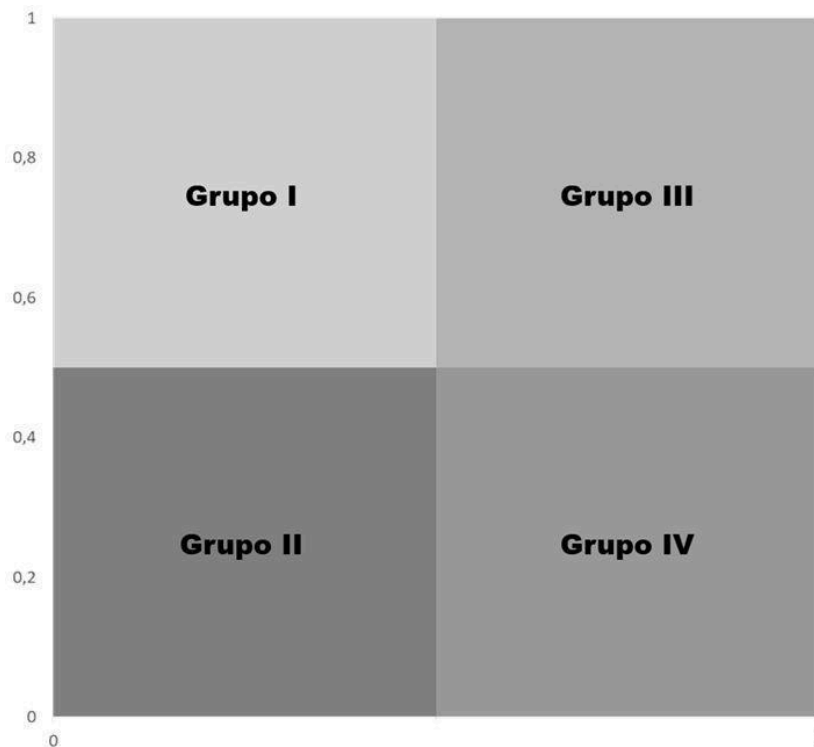


Figura 11- Relação de Custo-Benefício

Grupo I: Alto esforço e baixo impacto. Alto custo e baixo benefício = baixa prioridade - o esforço para executar os testes é muito alto e a não execução impacta algumas características correlacionadas, deve ser avaliado se as poucas características que são impactadas são essenciais para o sistema, se sim mesmo com o alto esforço deve ser priorizado para conduzir os testes e fazer uso das ferramentas e das tabelas de relacionamentos para reduzir o esforço durante a execução, se as características impactadas não são essenciais para o sistema não há necessidade de execução imediata dos testes.

Grupo II: Baixo esforço e baixo impacto. Baixo custo e baixo benefício = prioridade média - o esforço para executar os testes é baixo e não executá-los impacta algumas características correlacionadas, deve-se avaliar se as poucas características que são impactadas são essenciais para o sistema, se sim, elas devem ser priorizadas para conduzir os testes, caso contrário, não há necessidade de execução imediata dos testes, mas como para a execução dos testes é necessário um baixo esforço, em tempo hábil esses testes podem ser realizados facilmente e mais completamente usando a seção Impacto das Subcaracterísticas, adicionando ainda mais propriedades a serem avaliadas.

Grupo III: Alto esforço e alto impacto. Alto custo, mas alto benefício = alta prioridade - o esforço para executar os testes é muito alto e não executá-los impacta muitas características correlacionadas, os testes devem ser conduzidos e devem usar as estratégias do guia, como ferramentas e tabelas de relacionamento para diminuir o esforço na execução dos testes.

Grupo IV: Baixo esforço e alto impacto. Baixo custo e alto benefício = prioridade muito alta - alta prioridade - o esforço para executar os testes é baixo e não executá-los tem um impacto em muitas características correlacionadas, os testes devem ser conduzidos e porque envolvem baixo esforço, ainda mais propriedades podem ser adicionadas para serem avaliadas através da seção Impacto das subcaracterísticas, e se nem todos os casos de teste abstratos estiverem sendo usados, sugere-se que todos sejam adicionados.

12. Sugestão de ferramentas

A partir dos resultados dos estudos lidos na literatura foi possível elencar 8 ferramentas para testar a *Interoperabilidade* em aplicações IoT, cada uma com suas próprias funcionalidades e limitações. Para cada ferramenta identificada foram definidos: descrição, método de teste, ambiente de teste, execução do teste, licença e o acesso a ferramenta, esses resultados são apresentados na tabela 2.

Tabela 2 - Sugestão de ferramentas

| Ferramenta | Descrição | Método de teste | Ambiente de teste | Execução do teste | Licença | Acesso |
|-------------|--|-----------------|-------------------|---------------------|------------|---|
| Eclipse IoT | Conjunto de ferramentas para desenvolvimento e teste de aplicações IoT | Caixa Preta | Remoto | Plataforma | OpenSource | https://iot.eclipse.org/tstware/ |
| IoTIFY | Simulador de dispositivos IoT para teste de interoperabilidade | Caixa Preta | Remoto | Simulador | Fechada | https://iotify.io/ |
| CoAPthon | Biblioteca para desenvolvimento e teste de aplicações IoT baseadas no protocolo CoAP | Caixa Preta | Local | Software instalável | OpenSource | https://github.com/Tanganelli/CoAPthon3 |
| FreeRTOS | Sistema operacional em tempo real para dispositivos IoT | Caixa branca | Remoto | Plataforma | OpenSource | |

| | | | | | | |
|----------------|---|--------------|---------------|---------------------|------------|---|
| Tasmota | Firmware de código aberto para dispositivos IoT baseados em ESP8266 e ESP32 | Caixa branca | Remoto | Software instalável | OpenSource | https://tasmota.github.io/docs/ |
| Wireshark | Analizador de protocolos de rede para monitoramento e depuração de tráfego IoT | Caixa cinza | Local | Software instalável | OpenSource | https://www.wireshark.org/ |
| OpenIoT | Plataforma de interoperabilidade e integração para IoT. Possui um conjunto de ferramentas para testar a interoperabilidade entre dispositivos IoT e suas interfaces de programação de aplicativos (APIs). | Caixa cinza | Local e Nuvem | Plataforma | OpenSource | https://github.com/OpenIoTOrg/openiot |
| Home Assistant | Software de automação residencial de código aberto, com suporte a uma grande variedade de dispositivos IoT. Possui uma ferramenta de teste de integração que verifica a compatibilidade de dispositivos específicos com a plataforma. | Caixa Preta | Local | Software instalável | OpenSource | https://www.home-assistant.io/integrations/pytest_home_assistant/ |

Essas são apenas algumas sugestões de ferramentas gratuitas disponíveis para testar a *Interoperabilidade* em aplicações IoT. É importante lembrar que a escolha da ferramenta dependerá das necessidades específicas de cada aplicação testada.

13. Exemplo de uso do guia

Um exemplo de uso para um **GUIA DE TESTE DE INTEROPERABILIDADE PARA APLICAÇÕES IoT** seria em um aplicativo web, que envolve diversos dispositivos IoT de diferentes fabricantes. O guia de teste de *Interoperabilidade* pode ser usado para testar a *Interoperabilidade* entre esses dispositivos e a aplicação que os gerencia.

***Cenário:** O aplicativo web Rottas_UFC, desenvolvido para melhorar a mobilidade dos alunos da Universidade Federal do Ceará (UFC), fornece informações detalhadas sobre o transporte público no campus universitário. O aplicativo visa aprimorar a experiência dos alunos ao planejar suas viagens e reduzir o tempo de espera nas paradas de ônibus. Para garantir a eficácia da Interoperabilidade, são considerados vários cenários de teste que abordam diferentes aspectos do aplicativo.*

A partir dessas informações, seguimos os passos para a realização dos testes de *Interoperabilidade* no aplicativo Rottas_UFC. Passos para a realização dos testes de *Interoperabilidade*:

1. **Leitura do guia:** deve ser realizada a leitura do guia completo para entender os conceitos e aplicação. Neste ponto, as medidas podem ser vinculadas aos casos de teste, para que quando os testes forem feitos, os dois sejam feitos juntos. Além disso, é necessário entender as subcaracterísticas para auxiliar na execução dos testes.

Preparação: envolve a preparação dos dispositivos e da aplicação para testes. Isso pode incluir a configuração dos dispositivos e da rede, a instalação de ferramentas de teste e a criação de cenários de teste.

2. **Identificação de interfaces:** devem ser identificadas as interfaces de comunicação entre os dispositivos e a aplicação. Isso inclui as interfaces de rede, protocolos de comunicação e formatos de dados.

Com base nas definições e correlações apresentadas, as características de Interoperabilidade correlacionadas tomadas como prioridades na aplicação Rottas UFC foram: disponibilidade, desempenho, segurança, portabilidade e integração de sistemas. Essas características são fundamentais para garantir que essa aplicação funcione de maneira eficaz em um ambiente que envolve informações de transporte, horários, localizações e atualizações em tempo real.

3. **Ambiente de Teste:** consiste em configurar o ambiente de teste de acordo com os requisitos da aplicação. Por exemplo, a aplicação Rottas UFC, foi necessário um dispositivo inteligente, um atuador e um aplicativo externo que toma as decisões e envia os comandos de localização

em tempo real.

As propriedades de interoperabilidade que são avaliadas incluem:

- Tempo de resposta nas solicitações de informações de transporte;
- Capacidade de se adaptar a diferentes sistemas de transporte;
- Segurança na troca de informações sensíveis;
- Facilidade de integração com sistemas de terceiros; e
- Portabilidade entre diferentes plataformas de dispositivos.

4. medidas selecionadas: seleção das medidas para avaliar as propriedades de interoperabilidade. No caso da aplicação Rottas UFC, as medidas selecionadas são:

- Tempo médio de resposta nas solicitações de informações;
- Taxa de sucesso na integração com sistemas de transporte;
- Nível de conformidade com protocolos de comunicação;
- Tempo necessário para adaptar o aplicativo a novos sistemas de transporte; e
- Nível de segurança das transações de dados.

5. Cálculo do Custo-Benefício (com valores fictícios): para calcular o custo-benefício, são apresentados valores fictícios no cenário. O resultado do custo-benefício deve se enquadrar nos quadrantes do plano cartesiano apresentado o resultado do cálculo feito pelos valores fictícios não fiquem negativos, indicando que investir nos testes de interoperabilidade valerá a pena. No exemplo do aplicativo Rottas UFC é vantajoso realizar os testes de interoperabilidade.

$CDI = 0,68$, sendo assim de alto impacto

Sabendo que o valor $CCT = 0,4$ e o $CMD = 0,38$

O custo seria de $Custo = 0,39$, sendo assim de baixo esforço

Estando portanto no quadrante 4 apresentado na Figura 11, ou seja, uma altíssima prioridade na realização da validação para interoperabilidade da aplicação em questão, visto o seu baixo custo e alto benefício.

Gerar plano de teste: ao usar o guia no final é gerado um plano de teste, incluindo os problemas encontrados e as recomendações de correção. Esse plano de teste pode ser utilizado para aprimorar a *Interoperabilidade* dos dispositivos e da aplicação, garantindo que eles possam trabalhar juntos de maneira eficiente e confiável.

Este exemplo demonstra como usar o guia de *Interoperabilidade* em um cenário específico, considerando as características prioritárias e medidas relevantes, além de calcular o custo-benefício com valores fictícios. Em adição às tópicos e subtópicos previamente delineadas, o guia incorpora todas as fontes de referência que foram consultadas durante o processo de sua composição.

Referências

- ISO/IEC. ISO/IEC 30141:2018 - Tecnologias de informação - Arquitetura IoT - Parte 4: Protocolo de comunicação de ponta a ponta seguro para IoT. Genebra: ISO/IEC, 2019. Disponível em: <https://www.iso.org/standard/72832.htm>. Acesso em: 28 mar. 2023.
- ISO/IEC. ISO/IEC 21823:2019 - Tecnologias de informação - Arquitetura IoT. Genebra: ISO/IEC, 2020. Disponível em: <https://www.iso.org/standard/74820.html>. Acesso em: 28 mar. 2023.
- ISO. ISO 15926 - Industrial automation systems and integration - Integration of life-cycle data for process plants including oil and gas production facilities. Genebra: ISO, 2011. Disponível em: <https://www.iso.org/standard/50694.html>. Acesso em: 28 mar. 2023.
- LEGNER, C. WENDE, K. Towards na Excellence Framework for Business Interoperability, 19thBled e Conference e Values. Bled, Slovenia, 2006.
- GULLA, J.; TOMASSEN, S.; STRASUNSKAS, D. (2006) Semantic interoperability in the norwegian petroleum industry. In: Karagiannis, D., Mayer, H.C. (eds.): 5th International Conference on Information Systems Technology and its Applications. ISTA, 2006.
- FERREIRA, Hiro Gabriel Cerqueira. Arquitetura de Middleware para Internet das Coisas. 2014. 125 f. Dissertação (Mestrado em Engenharia Elétrica) – Universidade de Brasília, Brasília, 2014
- Winkler, T. et al. (2019). Interoperability Testing of Internet of Things Devices. In IEEE 5th World Forum on Internet of Things (WF-IoT).
- Kovatsch, M. et al. (2018). Evaluating IoT Platforms for Interoperability: The Need for a Standardized Testing Infrastructure. In IEEE Internet Computing.
- Li, X. et al. (2018). A Comprehensive Study of IoT Interoperability Challenges and Opportunities. In IEEE Communications Surveys & Tutorials.
- H. Kouakou, F. Ouedraogo, A. Sawadogo, M. M. Sanou, and B. J. Somé, “An IoT Based Smart Home System: Design and Implementation,” in 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC), 2019, pp. 132–137.
- D. Guinard and V. Trifa, “Towards the Web of Things: Web Mashups for Embedded Devices,” in Proceedings of the 1st International Workshop on Mashups of Things and APIs (MoTA 2010), 2010, pp. 1–6.
- Smith, M., Welty, C., & McGuinness, D. L. (2004). OWL Web Ontology Language Guide. W3C Recommendation, World Wide Web Consortium (W3C). Disponível em: <https://www.w3.org/TR/owl-guide/>
- S. Qaisar, A. Awais, M. Anwar, and S. A. Madani, “IoT Communication Protocols: A Comprehensive Study,” Journal of Sensor and Actuator Networks, vol. 7, no. 3, p. 38, 2018.
- F. Tariq, M. A. Khan, M. Alnuem, and M. A. Imran, “IoT Simulation Tools and Applications: A Survey,” in Proceedings of the 8th International Conference on the Internet of Things, 2018, pp. 1–8.
- M. N. Alam, J. Misra, and S. M. Hasan, “An Overview of IoT Testing: Challenges, Tools, and Techniques,” in Proceedings of the 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 2017, pp. 1–7.

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1), 49-69.

GUINARD, D. et al. A Semantic Web-based Approach for Interoperability of Smart Home Systems. *Journal of Universal Computer Science*, v. 22, n. 1, p. 78-101, 2016.

BANZI, M. MQTT: A Technical Overview. IBM Developer, 2015. Disponível em: <https://developer.ibm.com/articles/iot-mqtt-why-good-for-iot/>. Acesso em: 29 mar. 2023.

SIVASHANMUGAM, K. et al. Semantic Interoperability in the Internet of Things: A Survey. *IEEE Communications Surveys & Tutorials*, v. 16, n. 3, p. 1513-1530, 2014.

N. K. Suryadevara et al. "Interoperability in Internet of Things: Taxonomies and Open Challenges", in *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1973-1994, thirdquarter 2018.

AL-FUQAHA, A., et al. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, v. 17, n. 4, p. 2347-2376, 2015.

CHENG, B., et al. An effective big data processing method for internet of things. *Wireless Communications and Mobile Computing*, v. 2019, 2019.

DE SILVA, L., et al. Survey of security in internet of things. *Journal of Computer and System Sciences*, v. 88, p. 122-147, 2017.

PETROLO, R., et al. Towards a flexible and scalable IoT communication architecture based on dynamic grouping of devices. *Journal of Network and Computer Applications*, v. 118, p. 97-108, 2018.

SCHMIDT, D. C. Guest editor's introduction: modeling and simulation of complex software systems. *IEEE Transactions on Software Engineering*, v. 41, n. 12, p. 1187-1190, 2015.

YAO, J., et al. Consistency verification of large-scale internet of things data streams based on functional dependencies. *IEEE Transactions on Industrial Informatics*, v. 16, n. 7, p. 4668-4677, 2020.

ISO 30141:2018 - Information technology — Internet of Things (IoT) — Interoperability for IoT systems — Part 4: Network protocols.

NOUBIR, G.; KHOKHAR, A. Interoperability in iot systems: Challenges and solutions. *IEEE Internet of Things Journal*, IEEE, v. 7, n. 10, p. 9712–9725, 2020.

NOURA, M.; ATIQUZZAMAN, M.; GAEDKE, M. Interoperability in internet of things: Taxonomies and open challenges. *Mobile networks and applications*, Springer, v. 24, p. 796–809, 2019.

NUNES, P. R. d. A. F. Validação de padrões de web services transacionais. Tese (Doutorado) – Universidade de São Paulo, 2011.

OLIVEIRA, R.; KAMIENSKI, C. A. Iot redirector: um redirecionador para gerenciamento da heterogeneidade de dados em aplicações iot. In: SBC. *Anais do VI Workshop de Computação Urbana*. [S. l.], 2022. p. 15–28.

Raza, S., & Wolter, K. (2017). Middleware for Internet of Things: A Survey. *IEEE Internet of Things Journal*, 4(5), 1202-1221.

Shrestha, B., Bhattarai, S., & Mahmood, A. N. (2020). IoT Network Protocols: A Survey. *IEEE Access*, 8, 73470-73489.

Xiong, N., Ma, J., Chen, X., & Liu, S. (2018). IoT interoperability: a review. *Journal of Sensors*, 2018

Chen, X., Huang, Y., Zhang, Z., & Liu, Y. (2021). A survey of IoT interoperability: From the perspective of standardization and technology. *Journal of Network and Computer Applications*, 173, 102943

APÊNDICE A

A Figura 8 refere-se aos relacionamentos entre medidas, casos de testes abstratos e ferramentas e busca auxiliar no processo de execução de testes. Por exemplo, C01 quando executado pode auxiliar na coleta de 12 medidas. A figura também mostra as ferramentas que podem ajudar a automatizar a coleta das medidas, como a ferramenta Eclipse IoT que pode ajudar a coletar as medidas M01, M06 e M21.

| medidas | | M 01 | M 02 | M 03 | M 04 | M 05 | M 06 | M 07 | M 08 | M 09 | M 10 | M 11 | M 12 | M 13 | M 14 | M 15 | M 16 | M 17 | M 18 | M 19 |
|---------|-----|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| | C01 | | | | | | | | | | | | | | | | | | | |
| | C02 | | | | | | | | | | | | | | | | | | | |
| | C03 | | | | | | | | | | | | | | | | | | | |
| | C04 | | | | | | | | | | | | | | | | | | | |
| | C05 | | | | | | | | | | | | | | | | | | | |
| | C06 | | | | | | | | | | | | | | | | | | | |
| | C07 | | | | | | | | | | | | | | | | | | | |
| | C08 | | | | | | | | | | | | | | | | | | | |
| | C09 | | | | | | | | | | | | | | | | | | | |
| | C10 | | | | | | | | | | | | | | | | | | | |
| | C11 | | | | | | | | | | | | | | | | | | | |
| | C12 | | | | | | | | | | | | | | | | | | | |
| | C13 | | | | | | | | | | | | | | | | | | | |
| | C14 | | | | | | | | | | | | | | | | | | | |
| | C15 | | | | | | | | | | | | | | | | | | | |
| | C16 | | | | | | | | | | | | | | | | | | | |
| | C17 | | | | | | | | | | | | | | | | | | | |
| | C18 | | | | | | | | | | | | | | | | | | | |
| | C19 | | | | | | | | | | | | | | | | | | | |

Casos de teste

[illegible]

Figura 8 - Relacionamento medidas X Casos de Teste Abstratos X Ferramentas