# Engenharia de Requisitos de Sistemas IoT e Ciber-Físicos: Resultados Preliminares

Ernesto Fonseca Veiga and Renato F. Bulcão-Neto

Universidade Federal de Goiás, Goiás, Brasil
ernestoveiga,rbulcao@ufg.br

**Resumo** Internet of Things (IoT) e Cyber-Physical Systems (CPS) referem-se a um conjunto relacionado de tendências na integração de recursos digitais (conectividade de rede e capacidade computacional) com dispositivos físicos e sistemas, visando melhorar seu desempenho e funcionalidade. Esses paradigmas têm criado oportunidades de progresso e crescimento econômico em diversos setores, como indústria, energia e transportes. O desenvolvimento de IoT/CPS e as suas aplicações têm possibilitado a criação de sistemas cada vez mais complexos. Porém, os projetos destes sistemas, muitas vezes, se mostram desafiadores para o processo tradicional de Engenharia de Requisitos (ER), levando à adaptação de técnicas pré-existentes, ou mesmo à criação de novas abordagens de ER, no intuito de atender as características específicas desses sistemas. Neste contexto, o objetivo deste artigo é fornecer uma visão abrangente sobre o processo de ER para sistemas IoT/CPS. Para atingir esse objetivo, realizou-se um Mapeamento Sistemático em que foram encontrados, por meio de busca automática e critérios de seleção, 31 estudos primários de ER para IoT/CPS. Desses estudos, foram extraídos tipos e fontes de requisitos, atividades de ER, técnicas utilizadas e problemas tratados. Como resultado, a principal contribuição deste trabalho é um levantamento do estado da arte sobre ER para sistemas IoT/CPS.

**Keywords:** Engenharia de Requisitos · Internet das Coisas · IoT · Sistemas Ciber-Físicos · CPS · Mapeamento Sistemático · Estado da Arte

## 1 Introdução

A tendência crescente de integração de recursos digitais (incluindo conectividade de rede e capacidade computacional) com dispositivos e sistemas físicos, tem resultado na ampla disseminação da Internet das Coisas (IoT) e Sistemas Ciber-Físicos (CPS)[1], nas mais diversas áreas de aplicação [11]. As características específicas destes sistemas trazem novos desafios ao processo de Engenharia de Requisitos (ER), tais como: maior complexidade dos sistemas IoT/CPS, múltiplos *stakeholders* distribuídos (espacial e organizacionalmente) e o envolvimento de diferentes domínios com formalismos e modelos específicos [39].

[1] Trataremos os termos IoT e CPS como sinônimos, no contexto deste MSL, de modo a refletir as similaridades entre suas propostas como descrito em [11,13].

No intuito de identificar as tendências e desafios da Engenharia de Requisitos para IoT/CPS, este artigo realiza um estudo abrangente através de um Mapeamento Sistemático da Literatura (MSL), que analisa fontes e tipos de requisitos considerados em sistemas IoT/CPS, técnicas e ferramentas utilizadas, problemas de ER tratados, desafios e questões em aberto, domínios de aplicação e o nível de maturidade dos estudos selecionados. Os resultados apresentados neste trabalho são preliminares por se basearem em 31 artigos publicados entre 2020 e 2021, analisando o recorte mais recente da pesquisa nessa área.

O artigo está assim organizado: a Seção 2 apresenta trabalhos relacionados; a Seção 3 detalha o planejamento e a execução do protocolo do MSL; a Seção 4 reporta e discute os resultados obtidos; e a Seção 5 apresenta as considerações finais, ameaças à validade e trabalhos futuros.

## 2 Trabalhos Relacionados

Para identificar a necessidade e a validade de se conduzir este MSL foi realizada uma busca prévia por estudos secundários sobre o tema, a qual identificou dois estudos aqui descritos [20,25].

O trabalho de Kaleem et al. [20] compila práticas, técnicas e desafios de ER para aplicações IoT. A revisão de literatura dos autores é *ad hoc* e possui escopo de análise reduzido, o que dificulta o entendimento dos critérios aplicados na busca e inclusão dos estudos e a abrangência e o detalhamento dos resultados.

Já o trabalho de Lim et al. [25] inclui uma revisão sistemática da literatura (RSL) sobre técnicas de elicitação de requisitos de aplicações de IoT. O trabalho identifica as tendências de utilização de técnicas de elicitação, bem como os principais domínios e fontes de pesquisa.

Em comparação a esses dois trabalhos, o MSL descrito neste artigo possui maior escopo ao extrair um conjunto maior de informações sobre todo o processo de ER para IoT/CPS. Isto nos tem permitido uma compreensão e análise mais abrangente sobre o estado da arte dessa área de pesquisa. Além disso, este MSL possui um protocolo bem definido, executado e com ações para mitigação de ameaças à validade para permitir a sua reprodutibilidade por terceiros.

## 3 Métodos

O objetivo do MSL[2] é compreender o processo de ER para o desenvolvimento de sistemas IoT/CPS. Para isso, quatro questões de pesquisa foram definidas:

**QP1.** Quais as tendências identificadas no estado da arte em ER para sistemas IoT/CPS?
**QP2.** Como são aplicadas, na literatura, as práticas de ER em sistemas IoT/CPS?
**QP3.** Quais as principais contribuições dos estudos de ER para sistemas IoT/CPS?
**QP4.** Quais os principais desafios e questões em aberto evidenciados em ER para sistemas IoT/CPS?

[2] O protocolo completo do MSL encontra-se em: https://bit.ly/MSLProtocolo.

### 3.1 Estratégia e *String* de Busca

Adotou-se uma estratégia de busca automática[3], validada por um pesquisador de ER, nas bases digitais *ACM DL*, *Engineering Village*, *IEEE Xplore* e *Scopus*.

A *string* de busca, apresentada a seguir, foi definida após uma série de testes e ajustes para refinamento (conforme protocolo), com o auxílio de pesquisador experiente em ER e de outros estudos sistemáticos da área [20,24,25].

```
("requirements engineering"OR "requirements analysis"OR "requirements
  specification"OR "requirements model*"OR "requirements elicit*"OR
 "requirements management"OR "requirements gather*"OR "requirements
  validation"OR "requirements collect*"OR "requirements identif*"OR
     "requirements documentation"OR "requirements verification")
   AND ( "IoT"OR "internet of things"OR "cyber-physical systems")
```

As etapas do MSL foram apoiadas pela ferramenta *Parsif.al* e maiores detalhes encontram-se em https://bit.ly/MSLProtocolo.

### 3.2 Critérios de Inclusão e Exclusão

Como critério de inclusão (CI), definiu-se que "*o estudo deve relatar a utilização de abordagens ou práticas de ER no contexto de sistemas IoT/CPS*".

Caso não atenda ao CI, o estudo deve ser enquadrado em um dos critérios de exclusão (CE), a saber: o texto completo não se encontra disponível; não é um artigo publicado em conferência ou periódico; não é um estudo primário; o texto completo ou os metadados não estão em língua inglesa; e o artigo não relata abordagens ou práticas de ER ou não trata de aplicações ou sistemas IoT/CPS.

### 3.3 Seleção de Estudos e Extração de Dados

O período de análise do MSL inclui estudos publicados de 2016 a 2021. A estratégia de busca identificou 996 estudos, sendo 368 duplicados. Na etapa de seleção inicial, leram-se os metadados, a introdução e a conclusão de cada artigo, tendo como resultado 234 estudos para a fase de extração de dados.

Definido com base na literatura de ER e nos trabalhos relacionados, um Formulário de Extração de Dados direcionou a coleta das informações relevantes à análise e produção das respostas às QPs deste MSL.

Desses 234 estudos, 87 foram lidos e analisados na íntegra (para o escopo deste trabalho), correspondentes a 2021 e 2020, dos quais 31 foram incluídos. Portanto, este artigo apresenta resultados parciais do MSL, ao analisar uma parte do escopo total definido, ou seja, as 31 publicações incluídas de 2021 e 2020 referentes ao tema estudado.

A seguir, são listados os 31 estudos que compõem o corpo de conhecimento compilado nesta pesquisa. Cada estudo será referenciado ao longo do texto por meio de um código único de identificação.

[3] Realizada em todas as bases e finalizada em 7 de fevereiro de 2022.

**S1.** Model-based security requirements for cyber-physical systems in SysML [37]
**S2.** An integrated framework for traceability and impact analysis in requirements verification of cyber–physical systems [27]
**S3.** Security requirement management for cloud-assisted and internet of things: enabled smart city [36]
**S4.** Automatic generation of control flow from requirements for distributed smart grid automation control [41]
**S5.** The potential of industry 4.0 cyber physical system to improve quality assurance: An automotive case study for wash monitoring of returnable transit items [28]
**S6.** Safety requirements for symbiotic human–robot collaboration systems in smart factories: a pairwise comparison approach to explore requirements dependencies [8]
**S7.** SafeSec Tropos: Joint security and safety requirements elicitation [23]
**S8.** A preliminary evaluation of the SRE and SBPG components of the IoT-HarPSecA framework [33]
**S9.** Robust requirements gathering for ontologies in smart water systems [17]
**S10.** Supporting IoT-based applications to combat the Aedes aegypti mosquito: A case in Brazil [1]
**S11.** An improved RE framework for IoT-oriented smart applications using integrated approach [21]
**S12.** Cyber security in IoT communication (Internet of Things) on smart home [16]
**S13.** Signal-Based properties of cyber-physical systems: Taxonomy and logic-based characterization [4]
**S14.** The changing world and the adapting machine: How digital transformation changes requirements engineering in the embedded and cyberphysical systems industry [38]
**S15.** Shipping 4.0: Security requirements for the cyber-enabled ship [22]
**S16.** Automated formalization of structured natural language requirements [10]
**S17.** A Technology to support the building of requirements documents for IoT software systems [34]
**S18.** Formal requirements modeling for cyber-physical systems engineering: An integrated solution based on FORM-L and Modelica [6]
**S19.** Security & safety by model-based requirements engineering [19]
**S20.** Human-centric software engineering for next generation cloud- and edge-based smart living applications [12]
**S21.** Towards aspect based components integration framework for cyber-physical system [31]
**S22.** Eliciting timing requirements for cyber-physical systems: A multiform time based approach [42]
**S23.** Smart3E: Enabling end users to express their needs for smart homes [15]
**S24.** IoTsecM: A UML/SysML extension for internet of things security modeling [9]
**S25.** UCM4IoT: A use case modelling environment for IoT systems [7]
**S26.** Performance evaluation of the SRE and SBPG components of the IoT hardware platform security advisor framework [32]
**S27.** Non-Functional requirements elicitation based on domain knowledge graph for automatic code generation of industrial cyber-physical systems [43]
**S28.** Knowledge-assisted reasoning of model-augmented system requirements with event calculus and goal-directed answer set programming [14]
**S29.** An Extended meta-model of problem frames for enriching environmental descriptions [40]
**S30.** Enabling model-based requirements engineering in a complex industrial System of Systems environment [3]
**S31.** Investigating process algebra models to represent structured requirements for time-sensitive CPS [2]

## 4 Resultados e Discussão

Esta seção descreve as respostas a cada uma das questões de pesquisa deste MSL com base nos dados extraídos dos 31 estudos analisados. Ao final, sintetiza os achados do MSL apresentando os principais esforços de pesquisa e questões em aberto sobre ER de sistemas IoT/CPS.

### 4.1 Tendências no estado da arte em ER para sistemas IoT/CPS

Para responder à QP1 foram extraídas as seguintes informações de cada estudo: tipo de requisito tratado, fonte de requisito, atividades do processo de ER envolvidas, técnicas de ER aplicadas e problemas de ER endereçados. Neste contexto, um comportamento é considerado uma tendência quando ele se repete sistematicamente em um número significativo de estudos, dentro do conjunto de possibilidades analisadas, indicando a direção para a qual estão sendo conduzidos os esforços de pesquisa nesta área.

**Tipos de requisitos.** Quinze estudos investigaram requisitos funcionais (RF) e não-funcionais (RNF) para sistemas IoT/CPS. Dez estudos consideraram apenas RF, e outros seis, apenas RNF. Portanto, RF foi tratado em 25 estudos e diferentes tipos de RNF, em 21 estudos.

Os tipos de RNF considerados neste MSL são uma combinação das classificações descritas em [18,35]. Destacam-se os RNF de segurança, com 15 ocorrências (S1, S3, S5–S8, S12, S14, S15, S18–S21, S24 e S26), eficiência, com 8 ocorrências (S5, S6, S9, S17, S18, S21, S22 e S27) e confiabilidade, com 6 ocorrências (S6, S7, S14, S15, S26 e S27).

A partir destes dados, é possível afirmar que há uma preocupação com aspectos de qualidade no processo de ER para sistemas IoT/CPS. Isso se deve, em grande parte, à própria natureza do domínio em questão, que trata de sistemas complexos e que envolvem dados críticos (p.ex., sistemas de automação industrial, de aviação, marítimos, *smart-grid* e saúde), além de dados sensíveis de usuários, que precisam ter garantidos os aspectos de segurança e privacidade.

**Fontes de requisitos.** Os tipos de fontes foram definidas de acordo com classificações amplamente adotadas na literatura, apresentadas pelo IREB [30] e SWEBOK [5]. Além destas, foi incluída a fonte de requisitos "Dados Dinâmicos", objeto de estudo recente da abordagem de Engenharia de Requisitos Orientada a Dados [26], mudança de paradigma em que a ER se torna um esforço centrado em dados no apoio à evolução contínua de sistemas intensivos de software. Dessa forma, ao invés de executar o processo tradicional de ER, o processamento de dados gerados continuamente por usuários e sistemas leva aos requisitos. Esses dados podem ser fornecidos explicitamente por usuários ou implicitamente por meio de registros de uso e dados de monitoramento de sistemas.

"Stakeholders" foi a fonte de requisitos mais utilizada, presente em 25 estudos (S1–S11, S14, S15, S17–S21, S23–S27, S29 e S30), dos quais em 19 é combinada

com outros tipos. "Conhecimento de domínio" foi usado em conjunto com outras fontes em 12 estudos (S3, S4, S6, S9–S11, S18, S19, S22, S27, S29 e S30). Houve também a adoção de análise de documentos (11), sistemas legados (7), ambientes operacional (6) e organizacional (2), dentre outras. Ou seja, todas estas correspondem a fontes de requisitos tradicionais para sistemas de software.

O MSL permitiu identificar apenas 2 estudos que usam dados dinâmicos como fonte de requisitos (S14 e S24). Dado que a análise foi apenas de 2 anos, não se pode afirmar que seja uma tendência, embora a literatura [26] aponte que este tipo de dado estás e tornando uma importante fonte de requisito para sistemas intensivos de software, dentre eles, os sistemas IoT e Ciber-Físicos.

**Atividades do processo de ER.** A atividade de "elicitação" foi a mais investigada pelos estudos, com 27 ocorrências, seguida por "análise" (26), "especificação" (23), "validação" (20) e "gerenciamento" (7).

Em relação à completude do processo de ER, sete estudos realizaram todas as atividades do processo de ER (S2, S6, S9, S16, S17, S18 e S21), e outros nove não trataram apenas a atividade de gerenciamento de requisitos para sistemas IoT/CPS (S3, S5, S7, S10, S11, S19, S22, S25 e S29).

O fato de 16 dos 31 estudos realizarem ao menos quatro das cinco atividades do processo de ER demonstra uma tendência ao amadurecimento das pesquisas para o desenvolvimento de sistemas IoT/CPS. Além disso, apenas quatro estudos investigaram uma única atividade de ER (no caso, elicitação).

**Técnicas de ER.** Para classificação das técnicas de ER utilizadas pelos estudos, foi adotada como referência a taxonomia apresentada pelo SWEBOK.

O diagrama apresentado na Figura 1 relaciona cada técnica com a atividade de ER em que esta é utilizada, informando ainda o total de ocorrências de cada técnica e também a quantidade total de ocorrências de todas as técnicas relacionadas a uma mesma atividade de ER, nos estudos analisados.

As técnicas de ER mais utilizadas nos estudos foram "Especificação de Requisitos do Sistema", "Modelagem Conceitual" e "Validação de Modelo", com respectivamente 19, 16 e 15 ocorrências, sendo técnicas relativas às atividades de especificação, análise e validação, nesta ordem.

**Problemas de ER.** Os problemas de ER identificados à partir dos 31 estudos analisados foram classificados em quatro categorias, de acordo com as relações que apresentaram entre si. Foram definidas as categorias de problemas de ER de sistemas IoT/CPS: ambiguidade, segurança, processo de ER e rastreabilidade.

As categorias com maior ocorrência foram ambiguidade (S1, S4, S11, S13, S19, S21, S25, S27 e S31) e segurança (S3, S7, S8, S12, S15, S24, S26). Os trabalhos que tratam de questões relacionadas à ambiguidade de requisitos citam problemas referentes à natureza da especificação em linguagem natural (propensa a omissões, erros e ambiguidades) até a descrição inconsistente ou interpretação errônea de requisitos.

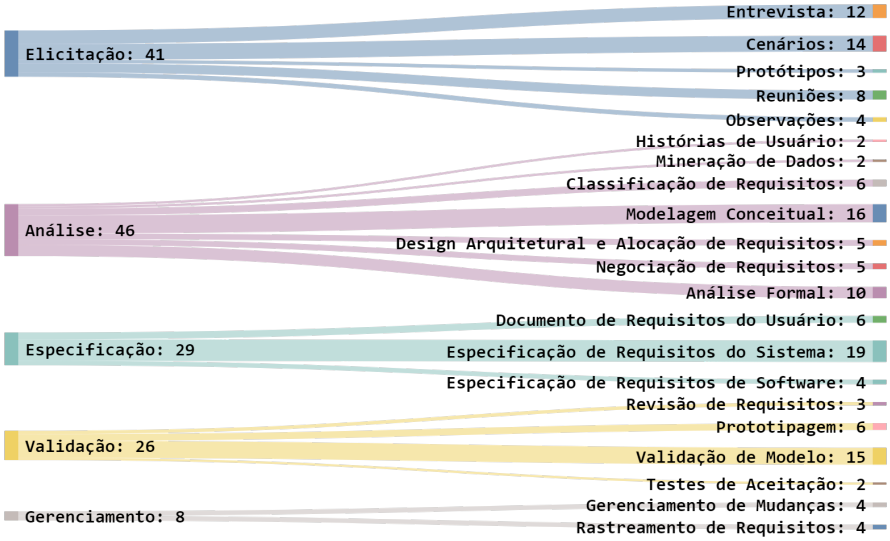


**Figura 1.** Técnicas realizadas em cada atividade do processo de ER.

Em relação à segurança, são citados desde a negligência quanto ao tratamento deste tipo de requisito até a realização do gerenciamento dos requisitos de segurança de forma inadequada. Alguns trabalhos tratam requisitos de privacidade como complementares aos requisitos de segurança.

Seguindo essa análise, seis estudos endereçaram problemas relacionados ao processo de ER, tratando desde a adaptação deste processo para as mudanças recentes no cenário de TIC, relacionadas principalmente a IoT e *smart cities*, até a inexistência de um processo de ER específico para os domínios de aplicação de sistemas IoT/CPS (S5, S9, S10, S14, S18 e S30). Ressalta-se como consenso dos estudos quanto a este tipo de problema, a preocupação em se atender às especificidades da construção de sistemas IoT/CPS, que possuem características particulares e maior complexidade em comparação com sistemas tradicionais.

A "rastreabilidade" foi identificada por quatro estudos como foco de problema no processo de ER, sendo muitas vezes realizada de forma inadequada (S2, S6, S11 e S17). Citam-se a necessidade de verificar a dependência entre tipos de requisitos diretamente relacionados e a descoberta e priorização desses requisitos.

### 4.2 Evidências de uso na prática de sistemas IoT/CPS

Foram extraídas informações relativas ao domínio geral do estudo (IoT, CPS, ou ambos – caso o estudo trate a relação entre os dois termos) e as informações do domínio de aplicação específico em que o estudo foi realizado. Além disso, baseado no trabalho de [29], foi feita a análise do nível de maturidade de pesquisa

dos 31 estudos, identificando o tipo de pesquisa realizado, os métodos aplicados e os participantes da pesquisa.

**Domínios de aplicação.** Treze estudos tratam de CPS e outros sete de sistemas IoT como domínio geral. Nesses 20 estudos não é apresentada relação explícita entre os dois termos. Porém, nos 11 estudos restantes, IoT e CPS são abordados com relação entre si: de equivalência (S3, S6, S9, S23 e S30), de sobreposição parcial (S5, S15, S17 e S26), CPS como um subconjunto de IoT (S14) e IoT como subconjunto de CPS (S21); conforme a classificação de Greer et al. [11].

Foi também analisada a relação entre os domínio geral e de aplicação específica em cada estudo. Os estudos que tratam os domínios de automação e indústria (S4, S5, S7, S13, S18 e S19) geralmente adotam a terminologia CPS. O termo IoT é usado em estudos cuja aplicação é ligada ao ser humano, como saúde, *smart home/living/cities* (S10, S11, S12, S17 e S20).

**Tipos e métodos de pesquisa.** Os tipos de pesquisa de maior ocorrência são: pesquisa de validação, realizada em 14 estudos (S1, S2, S4, S7, S8, S11, S12, S15, S17, S22, S25, S27, S29 e S30) e pesquisa de avaliação, em 13 estudos (S3, S5, S6, S9, S10, S13, S16, S18, S21, S24, S26, S28 e S31).

Esses resultados apontam para um crescente nível de maturidade nas pesquisas em ER para sistemas IoT/CPS, uma vez que 42% dos trabalhos foram avaliados junto a profissionais na indústria. Além disso, diversos estudos validados na academia apontam como trabalhos futuros a avaliação na indústria de software.

Quanto aos métodos empíricos de pesquisa, 16 aplicaram estudos de caso (S1, S4, S5, S7, S11, S12, S15, S21, S22, S24, S25, S26, S28, S29, S30 e S31). Há trabalhos que usaram mais de um método empírico, como estudo de caso e simulação (S13, S16, S18) e estudo de caso e *survey* (S3, S6 e S8). Apenas dois trabalhos não utilizaram nenhum método empírico, por se tratarem de artigos de opinião, relato de experiência e proposta de solução (S14 e S20).

### 4.3 Contribuições da ER para sistemas IoT/CPS

Os principais tipos de contribuição encontrados foram "Modelo" (S1, S4, S9, S13, S17, S22, S24, S25 S29), "Método" (S1, S4, S6, S7, S11, S12, S17, S19, S20 e S27) e "Processo" (S5, S6, S11, S14, S15, S16, S18, S22, S23 e S31). Por se tratarem de estudos sobre modelos, métodos e processos de ER, nestes casos não são propostas ferramentas ou aplicações, mas sim processos e métodos que podem ser utilizados independentemente do domínio de aplicação. Destaca-se ainda a proposta de "*Frameworks*" para suporte ao processo de ER em sistemas IoT/CPS (S2, S3, S8, S10, S16, S21 e S25).

### 4.4 Desafios e questões em aberto

Relatos de desafios e questões em aberto foram identificados, classificados e agrupados por similaridade em tópicos mais abrangentes, para que pudessem ser descritos como uma proposta de agenda de pesquisa.

Nota-se que alguns dos desafios de ER para IoT/CPS aqui destacados refletem dificuldades causadas por problemas relevantes e ainda não ultrapassados pela ER tradicional. Foram identificados cinco grupos de desafios e questões em aberto na literatura sobre ER para sistemas IoT/CPS, apresentados a seguir.

**Processo de ER específico.** Os estudos S11, S14, S17, S19, S20, S21, S24, S27, S28 e S30 apontam como *gap* a falta de abordagens abrangentes, genéricas e eficientes para ER de sistemas IoT/CPS. Os estudos S14 e S28 apontam a necessidade de mudanças no processo tradicional de ER para suporte efetivo ao desenvolvimento de sistemas complexos, como CPS, IoT e sistemas autoadaptativos. O estudo S14 destaca também a necessidade de tratamento da natureza dinâmica do contexto do mundo real, fator relevante para esses tipos de sistemas.

O estudo S17 sugere a adaptação das atividades de ER às especificidades de sistemas IoT e destaca que a falta de apoio metodológico para concepção e ideação de produtos para IoT traz como consequência um gargalo na identificação e na descrição das necessidades de *stakeholders* e de negócios. Ainda evidencia a falta de estudos para identificação de características e comportamentos de sistemas IoT, além de um gargalo em modelos de análise e protótipos para esse tipo de sistema. O estudo S19 cita a necessidade de tratamento da complexidade de CPS para evolução e melhorias no processo de ER. Por fim, S20 ressalta a importância do tratamento das questões centradas no ser humano no processo de desenvolvimento de sistemas IoT como parte do processo de ER.

**Modelagem formal de requisitos.** Em consonância com o problema de ambiguidade, identificado como um dos principais problemas do processo de ER para sistemas IoT/CPS, os estudos S4, S13, S16, S26, S29 e S31 identificam como desafio de pesquisa a modelagem formal de requisitos. O estudo S4 aponta a modelagem formal, não ambígua e interpretável por máquina como um dos principais desafios. Reforçando essa análise, S13 aponta uma ampla variação de expressividade em linguagens de especificação de requisitos de CPS, o que leva à falta de descrições precisas e problemas de ambiguidade. Neste mesmo sentido, o estudo S16 aponta a necessidade de formalização dos requisitos e melhorias no processo de definição de regras e fórmulas para essa finalidade.

**Tratamento de RNF de segurança.** Também refletindo outro problema de ER amplamente identificado, preocupações com RNF de segurança se estendem para desafios e questões em aberto em sistemas IoT/CPS, como descrevem os estudos S6, S7, S12, S15, S19 e S26. O estudo S6 aponta a necessidade de se avaliar a dependência entre requisitos e a realização de classificação de prioridades, uma vez que os requisitos de segurança geralmente possuem dependências com requisitos de outras categorias. Também neste sentido, S15 aponta como desafio a elicitação de requisitos de segurança e proteção de maneira conjunta, devido a interdependência entre eles.

O estudo S7 aponta a necessidade de padronização de requisitos de segurança e proteção para os domínios de CPS, bem como a definição de uma arquitetura

de proteção compatível com os requisitos identificados (e padronizados). Nesta mesma perspectiva, o estudo S12 aponta a necessidade de metodologias para definição de requisitos de segurança em sistemas IoT e o estudo S19 destaca o importante papel dos RNF de segurança e proteção no processo de ER de sistemas IoT/CPS, evidenciando a necessidade de tratamento desses requisitos.

**Gerenciamento de requisitos.** Este problema é evidenciado pelos dados extraídos neste MSL, que mostram a atividade de gerenciamento de requisitos como a menos explorada no processo de ER de sistemas IoT/CPS. Os estudos S2, S3 e S23 apontam os desafios de pesquisa para o avanço deste tópico. O estudo S2 evidencia um trabalho de rastreabilidade predominantemente manual, suscetível a erros, que se torna um entrave no processo de desenvolvimento. Também é discutido um gargalo quanto a ferramentas de visualização de padrões de rastreabilidade, bem como a necessidade de um gerenciamento integrado. Reforçando essas questões em aberto, o estudo S3 relata a baixa disponibilidade de técnicas de gerenciamento de requisitos de sistemas IoT como, por exemplo, requisitos de segurança, relacionando este problema ao citado anteriormente. Segundo os autores, não existem, na literatura, soluções abrangentes, multifuncionais e eficazes para gerenciamento de requisitos de segurança de sistemas IoT.

**Elicitação de requisitos.** Apesar de ser a atividade do processo de ER mais abordada pelos estudos analisados, algumas questões relacionadas à elicitação ainda são apontados como desafios de pesquisa. O estudo S1 relata as dificuldades na captura de requisitos com precisão e exatidão, em Sistemas Ciber-Físicos. Neste sentido, o estudo S10 cita como desafio a elicitação de requisitos não-funcionais em sistemas IoT/CPS, que muitas vezes não são comparados com sistemas existentes após sua especificação, podendo gerar problemas durante as etapas seguintes do processo de desenvolvimento destes sistemas.

### 4.5 Síntese dos resultados

A Tabela 1 apresenta uma síntese dos achados do MSL, sumarizando os resultados de pesquisa sobre ER de sistemas IoT/CPS – à partir dos resultados obtidos na extração de dados – para responder às questões de pesquisa.

A primeira coluna da tabela descreve os campos definidos no Formulário de Extração de Dados (tipos e fontes de requisitos, atividades, técnicas, etc.), que foram utilizados para responder as questões de pesquisa. Os principais resultados preliminares para cada uma das QPs são apresentados na segunda coluna, juntamente com quantidade de ocorrências nos estudos analisados (onde se aplica). Por fim, as colunas 3 a 6 referenciam a qual QP os resultados se referem.

A partir dessa tabela podem ser identificadas as principais relações entre os achados das QPs, principalmente no que diz respeito as tendências e práticas de ER em contraste com os desafios e questões em aberto. Os resultados relativos à QP4 podem ser considerados, neste contexto, uma prévia da agenda de pesquisa para ER em sistemas IoT/CPS, que será definida, posteriormente, com a conclusão desse mapeamento sistemático da literatura.

**Tabela 1.** Síntese dos resultados da pesquisa sobre ER de sistemas IoT/CPS.

| **Dados Extraídos** | **Achados do MSL** | **QP1** | **QP2** | **QP3** | **QP4** |
|---|---|---|---|---|---|
| Tipos de requisitos | Segurança (15), eficiência (8) e confiabilidade (6) | ✓ | | | |
| | Tratamento de RNF | | | | ✓ |
| Fontes de requisitos | Stakeholders (25), conhecimento de domínio (12) e documentos (11) | ✓ | | | |
| | Utilização de dados dinâmicos e regras de negócio | | | | ✓ |
| Atividades de ER | Elicitação (27), análise (26), especificação (23) e validação (20) | ✓ | | | |
| | Gerenciamento de requisitos | | | | ✓ |
| Técnicas de ER | Especificação de requisitos do sistema (19), modelagem conceitual (16) e validação de modelo (15) | ✓ | | | |
| | Técnicas para modelagem e formalização de requisitos | | | | ✓ |
| Problemas de ER | Ambiguidade (9), segurança (7), processo de ER para IoT/CPS (6) | ✓ | | | |
| | Esforços em gerenciamento, principalmente quanto à rastreabilidade | | | | ✓ |
| Domínios de aplicação | Automação e indústria (CPS); saúde, smart home/living/cities (IoT) | | ✓ | | |
| | Mudanças no processo de ER para atender à complexidade | | | | ✓ |
| Tipos e métodos de pesquisa | Tipos: validação (14) e avaliação (13); Métodos: estudo de caso (16) | | ✓ | | |
| | Amadurecimento das pesquisas | | | ✓ | |
| Contribuições | Método (10), processo (10) e modelo (9) | | | ✓ | |
| | Ferramentas e arcabouços em apoio ao processo de ER | | | | ✓ |

## 5 Considerações Finais

Como resultado deste MSL, a principal contribuição é um mapeamento dos esforços de pesquisa no tema, que podem servir de orientação para futuros estudos e avanço do estado da arte. Além disso, contribui-se com um protocolo de MSL no tema emergente de RE para sistemas IoT/CPS. Por fim, destaca-se que até a redação deste trabalho, havia apenas um estudo sistemático da literatura sobre ER para sistemas IoT [25]. No entanto, o trabalho citado limita-se à atividade de elicitação de requisitos, enquanto esta pesquisa estende o escopo, contemplando o processo completo de ER para sistemas IoT/CPS.

Para mitigar ameaças à validade do MSL, o protocolo foi elaborado por pesquisadores com experiência em ER e estudos sistemáticos da literatura [24]. Quanto à estratégia de busca, embora não tenha combinado múltiplas formas de

busca, a *string* elaborada passou por vários ciclos de testes, considerando a sensibilidade da mesma em relação aos resultados obtidos com a busca automática.

Dado que o escopo deste MSL abrange estudos de 2020 e 2021, como trabalho futuro, espera-se concluir a leitura, análise e síntese dos 157 estudos primários publicados de 2016 a 2019.

## Referências


1. de A. Silva, H., Adriano, E., Scatolini, D., Braga, R.T.V.: Supporting IoT-based applications to combat the Aedes aegypti mosquito: a case in Brazil. In: 2021 IEEE 34th International Symposium on Computer-Based Medical Systems (CBMS). pp. 330–335 (2021)
2. Arnaud, M., Bannour, B., Lapitre, A., Giraud, G.: Investigating process algebra models to represent structured requirements for time-sensitive CPS. In: SEKE 2021 - The 33rd International Conference Software Engineering & Knowledge Engineering (2021)
3. Binder, C., Polanec, K., Brankovic, B., Neureiter, C., Lastro, G., Lüder, A.: Enabling model-based requirements engineering in a complex industrial System of Systems environment. In: 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). pp. 1–6 (2021)
4. Boufaied, C., Jukss, M., Bianculli, D., Briand, L.C., Isasi Parache, Y.: Signal-Based Properties of Cyber-Physical Systems: Taxonomy and Logic-based Characterization. Journal of Systems and Software **174**, 110881 (2021)
5. Bourque, P., Fairley, R.E., Society, I.C.: Guide to the Software Engineering Body of Knowledge (SWEBOK): Version 3.0. IEEE Computer Society Press, Washington, DC, USA, 3rd edn. (2014)
6. Bouskela, D., Falcone, A., Garro, A., Jardin, A., Otter, M., Thuy, N., Tundis, A.: Formal requirements modeling for cyber-physical systems engineering: an integrated solution based on FORM-L and Modelica. Requirements Engineering pp. 1–30 (2021)
7. Boutot, P., Tabassum, M.R., Mustafiz, S.: UCM4IoT: A use case modelling environment for IoT systems. In: 2021 ACM/IEEE International Conference on Model Driven Engineering Languages and Systems Companion (MODELS-C). pp. 767–776 (2021)
8. Dede, G., Mitropoulou, P., Nikolaidou, M., Kamalakis, T., Michalakelis, C.: Safety requirements for symbiotic human–robot collaboration systems in smart factories: a pairwise comparison approach to explore requirements dependencies. Requirements Engineering **26**(1), 115–141 (2021)
9. Escamilla-Ambrosio, P.J., Robles-Ramírez, D.A., Tryfonas, T., Rodríguez-Mota, A., Gallegos-García, G., Salinas-Rosales, M.: Iotsecm: A UML/SysML extension for internet of things security modeling. IEEE Access **9**, 154112–154135 (2021)
10. Giannakopoulou, D., Pressburger, T., Mavridou, A., Schumann, J.: Automated formalization of structured natural language requirements. Information and Software Technology **137** (2021)
11. Greer, C., Burns, M., Wollman, D., Griffor, E., et al.: Cyber-physical Systems and Internet of Things (2019)
12. Grundy, J.: Human-centric software engineering for next generation cloud-and edge-based smart living applications. In: 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID). pp. 1–10. IEEE (2020)

13. Gunes, V., Peter, S., Givargis, T., Vahid, F.: A survey on concepts, applications, and challenges in cyber-physical systems. KSII Transactions on Internet and Information Systems (TIIS) **8**(12), 4242–4268 (2014)
14. Hall, B., Varanasi, S.C., Fiedor, J., Arias, J., Basu, K., Li, F., Bhatt, D., Driscoll, K., Salazar, E., Gupta, G.: Knowledge-assisted reasoning of model-augmented system requirements with event calculus and goal-directed answer set programming. arXiv preprint arXiv:2109.04634 (2021)
15. Han, B., Chen, X., Jin, Z., Liu, L.: Smart3E: Enabling end users to express their needs for smart homes. In: 2021 IEEE 29th International Requirements Engineering Conference (RE). pp. 422–423 (2021)
16. Heriadi, H., Pamuji, G.C.: Cyber security in IoT communication (Internet of Things) on smart home. IOP Conference Series: Materials Science and Engineering **879**, 012043 (aug 2020)
17. Howell, S., Beach, T., Rezgui, Y.: Robust requirements gathering for ontologies in smart water systems. Requirements Engineering **26**(1), 97–114 (2021)
18. ISO/IEC: ISO/IEC 25000:2014 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE. ISO/IEC 25000:2014 **2**, 1–27 (2014)
19. Japs, S.: Security & safety by model-based requirements engineering. In: 2020 IEEE 28th International Requirements Engineering Conference (RE). pp. 422–427 (2020)
20. Kaleem, S., Ahmad, S., Babar, M., Akre, V., Raian, A., Ullah, F.: A Review on Requirements Engineering for Internet of Things (IoT) Applications. In: 2019 Sixth HCT Information Technology Trends (ITT). pp. 269–275 (2019)
21. Kaleem, S., Ahmed, S., Ullah, F., Babar, M., Sheeraz, N., Hadi, F.: An improved re framewrok for IoT-oriented smart applications using inetgrated approach. In: 2019 International Conference on Advances in the Emerging Computing Technologies (AECT). pp. 1–6 (2020)
22. Kavallieratos, G., Diamantopoulou, V., Katsikas, S.K.: Shipping 4.0: Security requirements for the cyber-enabled ship. IEEE Transactions on Industrial Informatics **16**(10), 6617–6625 (2020)
23. Kavallieratos, G., Katsikas, S., Gkioulos, V.: SafeSec Tropos: Joint security and safety requirements elicitation. Computer Standards & Interfaces **70**, 103429 (2020)
24. Kudo, T.N., Bulcão Neto, R.F., Vincenzi, A.M.R.: Requirement patterns: A tertiary study and a research agenda. IET Software **14**(1), 18–26 (September 2020)
25. Lim, T.Y., Chua, F.F., Tajuddin, B.B.: Elicitation Techniques for Internet of Things Applications Requirements: A Systematic Review. In: Proceedings of the 2018 VII International Conference on Network, Communication and Computing. p. 182–188. ICNCC 2018, Association for Computing Machinery, New York, NY, USA (2018)
26. Maalej, W., Nayebi, M., Johann, T., Ruhe, G.: Toward data-driven requirements engineering. IEEE Software **33**(1), 48–54 (2016)
27. Mengist, A., Buffoni, L., Pop, A.: An integrated framework for traceability and impact analysis in requirements verification of cyber–physical systems. Electronics **10**(8) (2021)
28. Neal, A.D., Sharpe, R.G., van Lopik, K., Tribe, J., Goodall, P., Lugo, H., Segura-Velandia, D., Conway, P., Jackson, L.M., Jackson, T.W., West, A.A.: The potential of industry 4.0 Cyber Physical System to improve quality assurance: An automotive case study for wash monitoring of returnable transit items. CIRP Journal of Manufacturing Science and Technology **32**, 461–475 (2021)

29. Petersen, K., Vakkalanka, S., Kuzniarz, L.: Guidelines for conducting systematic mapping studies in software engineering: An Update. Information and Software Technology **64**, 1–18 (2015)
30. Pohl, K., Rupp, C.: Requirements Engineering Fundamentals - A Study Guide for the Certified Professional for Requirements Engineering Exam: Foundation Level - IREB compliant. rockynook (2011)
31. Saldivar, A.A.F., Li, Y., Chen, W.n., Zhan, Z.h., Zhang, J., Chen, L.Y.: Industry 4.0 with cyber-physical integration: A design and manufacture perspective. In: 2015 21st International Conference on Automation and Computing (ICAC). pp. 1–6 (2015)
32. Samaila, M.G., Lopes, C., Édi Aires, Sequeiros, J.B., Simões, T., Freire, M.M., Inácio, P.R.: Performance evaluation of the SRE and SBPG components of the IoT hardware platform security advisor framework. Computer Networks **199**, 108496 (2021)
33. Samaila, M.G., Lopes, C., Aires, E., Sequeiros, J.B.F., Simões, T., Freire, M.M., Inácio, P.R.M.: A Preliminary Evaluation of the SRE and SBPG Components of the IoT-HarPSecA Framework. In: 2020 Global Internet of Things Summit (GIoTS). pp. 1–7 (2020)
34. Silva, D.V.d., Gonçalves, T.G., Travassos, G.H.: A technology to support the building of requirements documents for IoT software systems. In: 19th Brazilian Symposium on Software Quality. SBQS'20, Association for Computing Machinery, New York, NY, USA (2020)
35. Sommerville, I.: Engenharia de Software. Pearson Prentice Hall (2011)
36. Tariq, M., Babar, M., Jan, M., Khattak, A., Alshehri, M., Yahya, A.: Security requirement management for cloud-assisted and internet of things enabled smart city. Computers, Materials and Continua **67**(1), 625–639 (2021)
37. Wach, P., Salado, A.: Model-based security requirements for cyber-physical systems in sysml. In: 2020 IEEE Systems Security Symposium (SSS). pp. 1–7 (2020)
38. Weyer, T., Daun, M., Tenbergen, B.: The changing world and the adapting machine: How digital transformation changes requirements engineering in the embedded and cyberphysical systems industry. IEEE Software **38**(5), 83–91 (2021)
39. Wiesner, S., Hauge, J.B., Thoben, K.D.: Challenges for Requirements Engineering of Cyber-Physical Systems in Distributed Environments. In: Umeda, S., Nakano, M., Mizuyama, H., Hibino, H., Kiritsis, D., von Cieminski, G. (eds.) Advances in Production Management Systems: Innovative Production Management Towards Sustainable Growth. pp. 49–58. Springer International Publishing (2015)
40. Xiao, H., Li, Z., Yang, Y., Deng, J., Wei, S.: An Extended Meta-Model of Problem Frames for Enriching Environmental Descriptions. In: 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW). pp. 428–434 (2021)
41. Yang, C.W., Dubinin, V., Vyatkin, V.: Automatic Generation of Control Flow From Requirements for Distributed Smart Grid Automation Control. IEEE Transactions on Industrial Informatics **16**(1), 403–413 (2020)
42. Yang, J., Chen, X., Yin, L.: Eliciting Timing Requirements for Cyber-Physical Systems: a Multiform Time based Approach. In: 2021 International Symposium on Theoretical Aspects of Software Engineering (TASE). pp. 199–206 (2021)
43. Zhang, Y., Kang, J., Dai, W.: Non-Functional Requirements Elicitation Based on Domain Knowledge Graph for Automatic Code Generation of Industrial Cyber-Physical Systems. In: IECON 2021 – 47th Annual Conference of the IEEE Industrial Electronics Society. pp. 1–6 (2021)