Casos de Garantia de Segurança aplicados a sistemas robóticos: revisão sistemática da literatura

Mozart de Melo Alves Júnior[1], Maria Lencastre [1],
Lucas Florêncio de Brito[2] , Jaelson Castro[2 1], Moniky Ribeiro [2]
Escola Politécnica de Pernambuco - POLI – Universidade de Pernambuco - UPE
[2]Centro de informática – CIN – Universidade Federal de Pernambuco – UFPE
[1]{mmaj, mlpm}@ecomp.poli.br, [2]{lfb, jbc, smsr}@cin.ufpe.br

Resumo: Contexto: A segurança dos sistemas robóticos é de extrema importância, pois falhas ou acidentes relacionados a eles podem resultar em perdas irreparáveis. Estes sistemas precisam ser certificados por entidades reguladoras que exijam evidências de sua segurança em termos de Casos de Garantia de Segurança. **Objetivo**: Analisar abordagens, conceitos, ferramentas, normas e métodos relacionados à garantia da segurança em robôs e descobrir o estado da arte em relação ao uso e aplicação dos Casos de Garantia de Segurança em Sistemas Robóticos. **Método**: Condução de uma revisão sistemática da literatura (RSL) para identificar e analisar as abordagens aplicadas aos sistemas robóticos com base em Casos de Garantia de Segurança. **Resultados**: Foram identificados 21 estudos de um conjunto de 857 trabalhos publicados. Os resultados indicam que os Casos de Garantia de Segurança podem assumir um papel importante na gerência das especificações dos requisitos de segurança. **Conclusão**: A análise realizada pode auxiliar os profissionais a compreender melhor a área em trabalhos porvir. Foram relatadas as descobertas mais relevantes e suas implicações, também foi proposta uma agenda de pesquisa para a comunidade de engenharia de requisitos, especificamente para os sistemas robóticos, que será abordado em trabalhos futuros.

Palavras-chaves: caso de garantia, caso de garantia de segurança, garantia de segurança, caso de segurança, certificação de segurança, robótica.

1 Introdução

Uma estreita interação entre humanos e robôs acontece desde a introdução dos robôs industriais no início do ano 1950, quando os robôs se tornaram uma parte natural de vários processos de manufatura [10]. Avanços nos campos da eletrônica, ciência da computação e mecatrônica tornaram essas ferramentas inteligentes, abundantes e robustas. Espera-se que com esses avanços tecnológicos, a robótica contribua cada vez mais com suas contrapartes humanas para o desempenho eficiente e eficaz de todos os tipos de tarefas [4]; mas, essa relação humano-robôs precisa ser prudente e planejada, uma vez que os sistemas robóticos também são Sistemas Críticos de Segurança (SCS). Portanto, caso ocorram falhas ou se comportem de maneira inesperada, os robôs podem levar a acidentes, resultando em danos as pessoas ou propriedades, em grandes prejuízos financeiros, ambientais ou até mesmo perda de vidas [11].

É fundamental que o desenvolvimento de sistema robóticos seja de acordo com os padrões e normas técnicas relevantes. Por exemplo, no caso de Robôs para Cuidados Pessoais há o padrão de segurança ISO 13482 [1] que especifica requisitos e diretrizes

para o projeto inerentemente seguro, medidas de proteção e informações para alguns tipos de robôs de cuidados pessoais.

Apesar da evolução constante das normas e dos processos de certificação, pesquisas científicas e de organizações internacionais relatam dificuldade em garantir, de forma eficaz e eficiente, as exigências das normas de segurança nos sistemas críticos de software [12]. Um dos problemas relatado, presente na maioria das normas, é como os objetivos das mesmas podem ser descritos de uma forma clara e rastreável.

Novas abordagens, métodos e ferramentas têm sido sugeridos, dentre elas destaca-se os Casos de Garantia de Segurança (*Safety Assurance Cases*) [3], que visam a construção de argumentos claros, abrangentes e defensáveis em relação às propriedades de segurança e proteção dos sistemas [5]. Para auxiliar sistematicamente na construção desses argumentos, deve-se utilizar as normas existentes que tratam especificamente da construção dos Casos de Garantia de Segurança, tais como a ISO15026-1 [37] e a ISO15026-2 [21].

Os Casos de Garantia de Segurança frequentemente são utilizados para atestar a segurança de vários tipos de sistemas críticos. Neste artigo estamos interessados em investigar como eles têm sido utilizados na área da robótica.

Até onde os autores pesquisaram, não há nenhuma Revisão Sistemática da Literatura (RSL) que envolva Casos de Garantia de Segurança, robótica e normas de certificação. Deste modo, conduzimos uma RSL, com o objetivo de descobrir o estado da arte em relação ao uso e aplicação dos Casos de Garantia de Segurança em Sistemas Robóticos. Primeiro, identificamos as técnicas e ferramentas utilizadas bem como os artefatos gerados. Depois, descrevemos os tipos de trabalhos publicados na literatura. Em seguida, apresentamos as normas de certificação que são usadas, identificamos os benefícios do uso de Caso de Garantia de Segurança no processo de certificação. Por último, relatamos os desafios e problemas identificados.

Este artigo está organizado da seguinte forma: a seção 2 apresenta o referencial teórico; a seção 3 detalha a metodologia de pesquisa adotada para conduzir o RSL; já a seção 4 mostra os resultados e análises relacionados às nossas questões de pesquisa; por fim, a seção 5 resume as conclusões e trabalhos futuros.

2 Referencial Teórico

Desde o conto de ficção científica "Eu, Robô"[53], escrito por Isaac Asimov em 1942, onde foram definidas as três regras relativas ao comportamento dos robôs e à interação com os seres humanos, já se reivindicavam que os robôs fossem seguros, projetados e operados para cumprir as leis, direitos e liberdades fundamentais já existentes para os humanos.

Diferentes significados para os robôs ainda persistem e mudam de acordo com a aplicação e o domínio. De acordo com [54], o IEEE afirma que um robô é uma máquina construída como um conjunto de elos unidos para que possam ser articulados, em posições desejadas, por um controlador programável e atuadores de precisão para executar uma variedade de tarefas. De maneira geral, podemos afirmar que um robô é uma máquina autônoma capaz de detectar seu ambiente, executar ações no mundo real e que pode através da inteligência artificial evoluir encontrando soluções melhores para tomada de decisões.

Todos os robôs são controlados por sistemas complexos que combinam *hardware* e *software* e são fortemente dependentes e influenciados por interações com o ambiente. Com a evolução dos sistemas robóticos e sua integração dentro da indústria, onde realizam diversas tarefas, torna-se imprescindível e crítico garantir os requisitos de segurança pois, quaisquer operações de *software* ou *hardware* que não sejam executadas, ou aconteçam fora da sequência ou incorretamente, podem resultar em funções de controle inadequadas. Tais problemas podem causar direta ou indiretamente a existência de condições perigosas, que podem afetar os humanos que estão trabalhando lado a lado com as máquinas [6].

Diante de cenários onde robôs estão presentes no convívio direto com humanos, é essencial que as autoridades certificadoras de segurança exijam, da indústria e dos fornecedores de soluções, documentações convincentes que demonstrem que o sistema pode ser considerado seguro. Uma forma que vem se mostrando adequada para documentação de segurança é fornecer argumentos com base em elaboração de evidências através de Casos de Garantia.

Segundo a ISO15026-2, um Caso de Garantia deve incluir uma alegação de alto nível para uma propriedade de um sistema ou produto, uma argumentação sistemática sobre essa alegação e as evidências e suposições explícitas subjacentes a esta argumentação [37]. Os Casos de Garantia são geralmente desenvolvidos para apoiar reivindicações em áreas confiabilidade, manutenção, fatores humanos, e operabilidade [21].

Para atestar aspectos de segurança e outras propriedades críticas de sistemas complexos, tem sido proposta a elaboração de Casos de Garantia de Segurança. Eles fornecem argumentos de segurança que justifiquem uma reivindicação sobre o sistema, com base em evidências sobre seu projeto, desenvolvimento e comportamento testado [8].

Avaliar e garantir a segurança de um sistema depende da construção de confiança suficiente na execução segura do sistema em seu contexto operacional. Essa confiança é frequentemente desenvolvida ao se satisfazer os objetivos que reduzem os riscos potenciais que um sistema pode representar durante seu ciclo de vida. Os objetivos de segurança são geralmente estabelecidos por um conjunto de critérios aceitos pela indústria, normalmente disponíveis como padrões [9].

O processo para garantir segurança em sistemas robóticos é caro e sujeito a erros, pois envolve exigências maiores do que a tradicional verificação e validação de sistemas. Várias perspectivas de segurança devem ser levadas em consideração, uma vez que falhas ou acidentes podem resultar em perdas irreparáveis.

Portanto, é oportuno realizar uma revisão da literatura para identificar no domínio de sistemas robóticos como os Casos de Garantia voltados para Segurança vêm sendo aplicados.

3 Metodologia da Pesquisa

Segundo [6], uma Revisão Sistemática da Literatura é um tipo de estudo secundário que usa uma metodologia definida e confiável para identificar e analisar os estudos primários que estejam disponíveis e que sejam relevantes a uma questão de pesquisa. Estudos secundários têm como finalidade revisar estudos primários relativos a determinadas questões de pesquisa, com o objetivo de integrar e sintetizar evidências relacionadas a essas questões. De maneira geral, o objetivo de um estudo secundário é prover a pesquisadores uma visão geral de uma área de pesquisa [7].

Este artigo relata uma RSL conduzida com o objetivo de investigar se existem trabalhos na literatura que abordem e utilizem Casos de Garantia de Segurança aplicados a sistemas robóticos. O protocolo, que norteou a RSL, foi aprovado por quatro pesquisadores, sendo dois doutores especialistas em engenharia de software e três doutorandos que atuam na área de engenharia de software e engenharia de segurança.

A RSL procurou responder a uma questão de pesquisa principal (QP) e a 5 questões de pesquisa específicas (QE) descritas na Tabela 1.

Tabela 1. Questões de Pesquisa

QP: *Como os Casos de Garantia de Segurança estão sendo estudados e aplicados em sistemas robóticos?* O objetivo é identificar como os Casos de Garantia de Segurança vêm sendo empregados de forma a garantir a eficiência, a adequação e a rastreabilidade dos requisitos de segurança, no domínio específico de sistemas robóticos.
QP1: *Quais técnicas, ferramentas e artefatos foram utilizados em Casos de Garantia de Segurança para sistemas robóticos?* Essa questão é subdividida em três perguntas, que visam melhorar o seu entendimento. A primeira, QP1.1, procura identificar as técnicas/métodos (modelo, processo, procedimento) pelas quais tarefas são realizadas; a segunda, QP1.2, busca mapear as ferramentas CASE (C*omputer-Aided Software Engineering)* usadas nas abordagens que integram casos de garantia e engenharia de segurança na análise das especificações de requisitos de segurança de sistemas robóticos. Já a terceira, QP1.3, busca identificar os artefatos gerados pelos engenheiros de requisitos para realizar tarefas de garantia de segurança em sistemas robóticos.
QP2: *O trabalho relatado sobre Casos de Garantia de Segurança para sistemas robóticos é teórico ou aplicado?* Esta questão busca identificar a natureza do trabalho realizado.
QP3. *Quais as normas de certificação de segurança foram utilizadas em sistemas robóticos?* O objetivo é identificar quais são as normas vigentes que estão relacionadas a certificação de sistemas robóticos.
QP4: *Quais os benefícios relacionados à segurança com o uso de Casos de Garantia?* Esta questão busca identificar os benefícios à segurança ao utilizar casos de garantia nos sistemas robóticos.
QP5: *Quais os desafios e/ou problemas, relacionados a Casos de Garantia de segurança em sistemas robóticos, foram identificados pelas pesquisas?* O objetivo é identificar problemas e lacunas relacionados ao uso de Casos de Garantia de Segurança nos sistemas robóticos visando identificar seus desafios e possíveis oportunidades de pesquisa da área.

3.1 Estratégias de Busca e Seleção

Para o processo de busca e seleção dos estudos primários, fontes automáticas de buscas de dados digitais foram utilizadas como estratégia para a seleção destes estudos. Este processo foi executado a partir da definição de uma *string* de busca, derivada de palavras-chave com relação às questões de pesquisa, juntamente com sinônimos ou palavras provenientes, nos quais são concatenados por meio dos operadores booleanos OR e AND. Desta forma, a *string* de busca automática foi definida com os termos relacionados "casos de garantia" e "robótica", bem como seus respectivos sinônimos.

((“safety assurance” OR “assurance case” OR “safety case”) AND (“robotic”))

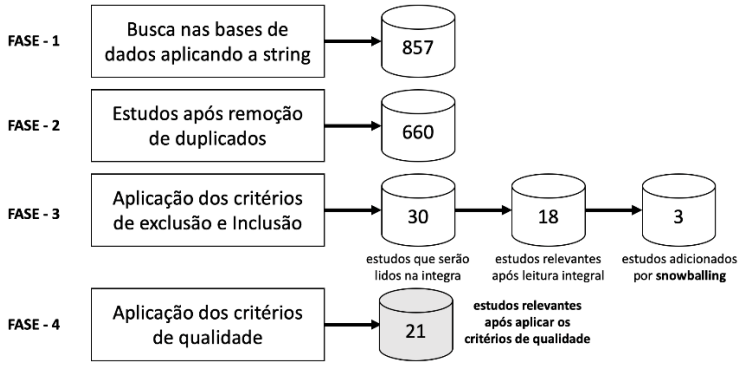
A busca dos estudos primários foi executada de forma automática e eletrônica, realizadas nos títulos, resumo e palavra chaves, utilizando 7 (sete) bases de dados

especializadas e de renome científico-acadêmico (*IEEE Explore, ACM Digital Library, SCOPUS, Science Direct, Springer, Web of Science e El Compendex*); estas foram selecionadas devido à sua abrangência e por possuírem estudos primários relevantes na área da pesquisa coberta nesta RSL.

3.2 Processo de Condução e Seleção dos Estudos

O processo de seleção dos estudos primários englobou quatro fases, como mostra a Figura 1. Cada uma destas é detalhada a seguir.

Figura 1. Processo de condução da Revisão Sistemática da Literatura.



Fase-1: Busca nas bibliotecas digitais: Foi feita a busca nas 7 bibliotecas digitais tomando como base a *string* definida; ao final, 857 estudos iniciais foram retornados.

Fase-2: Remoção de estudos duplicados: Foram removidos os estudos duplicados; assim restaram 660 trabalhos.

Fase-3: Análise dos trabalhos e aplicação de critérios de inclusão e exclusão: Cada trabalho foi analisado através da leitura do título, do resumo, das palavras-chave e da introdução (quando necessário), sendo aplicados os critérios de inclusão (CI) e exclusão (CE), ver Tabela 2. A aplicação destes critérios visou garantir a identificação de estudos primários relevantes e coerentes, com a área e o objetivo da pesquisa. Ao final, 30 estudos foram retornados e lidos de modo integral. Após leitura, 12 artigos foram retirados pois atendiam ao critério de exclusão CE-6. Através da estratégia *backward snowbolling*, mais 3 artigos foram adicionados.

Fase-4: Aplicação de Critérios de Qualidade: Os 21 artigos selecionados foram analisados aplicando-se critérios de qualidade, tratando-os com maior rigor sobre o tema desta pesquisa. Isto resultou num novo conjunto de artigos selecionados, que posteriormente foi classificado e sobre o qual foi feita a sua avaliação de qualidade. Os 12 Critérios de Qualidade (CQ), estabelecidos para esta RSL, foram adaptados de [14,15,16,17,18,19]. As avaliações dos critérios de qualidade, juntamente com as referências completas de cada estudo utilizado nesta revisão sistemática, estão disponíveis em *http://bit.ly/WER24-2021*.

Tabela 2. Critérios de Inclusão (CI) e Critérios de Exclusão (CE)

CI-1: Estudos primários que apresentem os casos de garantia aplicados na certificação de sistemas robóticos
CI-2: Estudos primários que incluam tipos de métodos relacionados aos casos de garantia
CI-3: Estudos primários que possuam ferramentas, técnicas e métodos utilizados em casos de garantia
CE-1: Estudos primários que não estejam escritos na língua inglesa
CE-2: Estudos duplicados
CE-3: Estudos secundários ou terciários
CE-4: Estudos com falta de relevância científica comprovada e que não possuam citações
CE-5: Estudos que não estejam disponíveis de modo integral e *online*
CE-6: Estudos que não estão claramente relacionados com as questões de pesquisa
CE-7: Artigo curto (igual ou inferior a quatro páginas)
CE-8: Literatura cinzenta

Verificou-se através da fórmula (nota da menor avaliação/número de CQ)*100, que todos os estudos desta RSL possuem qualidade superior a 54,16% com uma pontuação média geral de 80,55%, o que é aceitável dentro de um padrão de avaliação geral. A avaliação da qualidade ajudou a aumentar a confiabilidade das conclusões obtidas, além de verificar a credibilidade e síntese coerente dos resultados [22].

3.3 Ameaças à validade

Foram analisadas quatro categorias de ameaças apresentadas por [20], por ser amplamente utilizada pelas RSL que envolve Engenharia de Software, elas incluem:

- Validade de construção – Para mitigar o tipo de ameaça seguimos as orientações fornecidas em [13], para desenvolver um protocolo de pesquisa confiável e auditável; o protocolo foi validado empregando inspeção e comparação entre protocolos RSL já publicados. Dada a terminologia variável em Engenharia de Software, a *string* de pesquisa de um RSL foi avaliada várias vezes para evitar o risco de omissão de estudos relevantes.
- Validade interna - Durante a extração de dados, decisões subjetivas podem ter ocorrido, uma vez que alguns artigos não forneceram uma descrição clara ou objetivos e resultados adequados. Conduzimos o processo RSL de modo gradual, para tentar mitigar as probabilidades, devido ao viés pessoal, na compreensão do estudo.
- Validade externa - Para mitigar ameaças externas, a pesquisa foi definida apenas após várias pesquisas de ensaio e validada com o consenso de todos os autores.
- Validade de conclusão: A metodologia escolhida em [6] já considera que nem todos os estudos primários relevantes existentes podem ser identificados. Assim, possível que alguns estudos excluídos nesta revisão tenham sido incluídos. Para mitigar essa ameaça, o processo de seleção e os critérios de inclusão e exclusão foram cuidadosamente elaborados e discutidos pelos autores para minimizar o risco de exclusão de estudos relevantes.

4 Resultados da RSL e Discussões

A leitura completa dos estudos selecionados (21 estudos primários) permitiu responder às questões de pesquisa, visando identificar como os Casos de Garantia de Segurança estão sendo estudados e aplicados em sistemas robóticos. Os estudos analisados foram

publicados entre 1985 até janeiro de 2021, sendo o ano de 2020 aquele com o maior número de publicações (6 artigos, 28%). Observa-se uma prevalência de estudos entre 2018 e 2021, totalizado 57% das publicações desta RSL, o que faz acreditar que este tema é uma tendência. A seguir, são relatadas as respostas às questões de pesquisa.

QP1: Quais técnicas, ferramentas e artefatos foram utilizados em Casos de Garantia de Segurança para certificação de sistemas robóticos?

Devido à complexidade dos sistemas robóticos, é necessário buscar as técnicas, métodos e ferramentas que são usados neste domínio, independentemente de em qual área da robótica são aplicados. Para melhor esclarecimento e compilação dos dados, esta questão foi dividida em outras três sub questões QP1.1, QP1.2 e QP1.3.

QP1.1. Quais são as técnicas/métodos que estão sendo utilizadas pelos engenheiros de requisitos e de segurança durante a análise de Casos de Garantia de Segurança em sistemas robóticos?

Nas 21 publicações houve prevalência da utilização de técnicas de modelagem, estando em 10 artigos (43%) [S01-S03, S05, S09-S1, S15, S19, S20]. Em 4 artigos (17%) não foi apresentado nenhum tipo de técnica/método [S04, S07, S13, S14]. Algumas publicações, 3 artigos (13%) utilizaram técnicas de segurança [S01, S08, S19], métodos formais [S12, S15, S17], para descrição dos Casos de Garantia de Segurança. Também foram relatadas, todas com 1 artigo (4%), a técnica de gerenciamento de risco [S06], a técnica orientada por consenso [S05], e a técnica de aprendizado por demonstração [S05], onde as técnicas são discutidas em [27, 28, 54].

QP1.2. Quais são as ferramentas utilizadas pelos engenheiros de requisitos durante a análise de Casos de Garantia de Segurança em sistemas robóticos?

Como resultado, 21% dos artigos não relataram uso de ferramenta (5 artigos) [S04, S07, S08, S13, S18]; na sequência, tivemos ferramentas não nomeadas, que foram utilizadas com a finalidade de construir modelos (5 artigos, 21%) [S01, S03, S09, S10, S21]. Em 2 artigos foi utilizada ferramentas existentes para criar os diagramas de fluxograma [S01, S14], modelo SYSML [26] em outros 2 artigos [S09, S10] e modelos UML [25] em mais 2 artigos [S11, S20] (8%). Os demais artigos trabalharam com ferramentas distintas, algumas desenvolvidas pelos próprios autores GSN-DRAW [S02], ParReEx [S06], SaftyMet [S21] e outras ferramentas já existentes como: GSN [S02], jenkins.io [S05], MATLAB [S06], RoboTool [S15] e Simulador Jack [S19], todas com 1 artigo, equivalente a 4%.

QP1.3. Quais são os artefatos gerados pelos engenheiros de requisitos para a análise de Casos de Garantia de Segurança em sistemas robóticos?

A maioria das publicações (8 artigos, 28%) refere-se à criação de modelos ou metamodelos, todos com a finalidade de servir de base para descrever um processo de desenvolvimento de *software* que garante a segurança em diversas áreas [S01-S03, S11, S15, S17, S20, S21]. Em seguida, temos 5 artigos (17%) relacionados a orientações de fundamentação teórica [S07, S12-S14, S18]. Já a criação de algoritmos/códigos está em 14% dos trabalhos (4 artigos) [S06, S15-S17]. A documentação de requisitos funcional, não funcional e principalmente de segurança têm representação de 10% [S01, S08, S19]; a criação de protótipo em 3 artigos (10%) [S09, S10, S16].

Também foram encontrados, com 1 artigo, artefatos como modelo GSN [S02], vocabulário [S04] e *framework* [S05], representando 3% dos artigos.

QP2: O trabalho relatado sobre Casos de Garantia de Segurança para sistemas robóticos é teórico ou aplicado?
Destaca-se nos trabalhos desta RSL as seguintes categorias:

- **Teórico**, com dois artigos (9,52%). Um trata técnicas formais para fornecer evidências para certificação [S12], já o outro, busca garantir que a terminologia seja consistente em todos os padrões técnicos relevantes para robôs industriais e de serviço [S04], vale salientar que este artigo também se encontra na categoria aplicado.
- **Aplicado**, com 20 artigos correspondente a 95,24% [S01-S11, S13-S21], temos a maioria das pesquisas sendo realizada para atender a automação industrial. Concentra boa parte das publicações, sistemas robóticos para serem aplicados na área automotiva principalmente em veículos autônomos (9 artigos, 33%) [S02, S03, S08-S11, S16, S20, S21]; temos também, os robôs colaborativos, *cobots* [23], destinados à interação direta com um trabalhador humano na indústria (4 artigos, 15%) [S01, S14, S15, S18,]; sistemas robóticos para uso na construção civil [S01, S05, S15, S18] (4 artigos, 15%); sistemas robóticos usados para transporte ferroviário [S11, S20, S21] e aeronáutico [S11, S20, S21] (3 artigos, 12%); robótica social (2 artigos, 8%) [S13, S19]; completa a lista, a área médica com um sistema de reabilitação de paciente (1 artigo, 4%) [S06].

QP3. Quais as normas de certificação de segurança foram usadas em sistemas robóticos.

As normas, associadas por área e por quantidade de publicação, são detalhadas na Tabela 3. Percebe-se uma prevalência das normas que tratam das diretivas de segurança que regulam a indústria, sendo citadas por 34% dos artigos. Em seguida, estão as normas que tratam de segurança em sistemas de veículos automatizados, aeronáutica, ferroviário, normas que especificam requisitos e diretrizes para os projetos inerentemente seguros para uso de robôs de cuidados pessoais e normas de vocabulário utilizadas como referência para certificação. Vale salientar também, que em 11% dos artigos não houve referência a nenhuma das normas.

QP4: Quais são os benefícios obtidos relacionados à segurança com o uso de Casos de Garantia?

Os principais benefícios são apresentados na Tabela 4. O benefício mais recorrente é B1- Facilitar o entendimento da especificação de requisitos de segurança, sendo citado por 62% das publicações. De fato, é crucial especificar de forma compreensível e objetiva os requisitos de segurança de sistemas que utilizam robôs [1, 24, 45], evitando requisitos dúbios que podem ocasionar perigos levando a acidentes. Os Casos de Garantia de Segurança ajudam a entender a especificação.
Em segundo lugar está o benefício B2-Gerenciar a identificação de perigos e falhas, com 52%. Este benefício trata especificamente de como organizar os perigos detectados em decorrência de falhas de segurança de sistemas.
Outros três benefícios são listados com 43% de incidência nos artigos, são eles B3, B4 e B5. Onde benefício B3-Garantir que as metas e requisitos de segurança sejam

Tabela 3. Normas de certificação de segurança utilizadas em sistemas robóticos

Descrição Normas	Norma	Referência	Nº artigos	%
Normas que tratam da certificação de segurança em industrias	CE 2006/42 [33]	[S14, S17]	13	34%
	IEC 61508 [34]	[S05, S09-S11, S17, S20, S21]		
	ISO 10218 [24]]	[S04, S07, S13, S14]		
	ISO 11161 [35]	[S14]		
	ISO 15066 [36]	[S07, S14, S18]		
	ISO 12100 [51]	[S06, S14],		
Normas de segurança de sistemas de veículos automatizados	ISO 21448 [38]	[S03, S08]	8	21%
	ISO 26262 [39]	[S03, S05, S08-S11, S20, S21]		
	SAE J3016 [40] , SAE J3088 [41], SAEJ3131 [42]	[S03]		
Artigos que não citam qualquer norma de segurança	não informada	[S02, S12, S15, S16].	4	11%
Normas de segurança da aeronáutica.	DO-178B [47],	[S11, S20]	4	11%
	DO-178C [48]	[S05, S11, S20, S21]		
Normas de segurança relacionadas aos meios de transporte ferroviário	EN 50126 [42]	[S11, S20]	3	8%
	EN 50128 [43]	[S11, S20, S21]		
	EN 50129 [44]	[S11, S20, S21]		
Norma de requisitos e diretrizes de segurança para uso de robôs de cuidados pessoais.	ISO 13482 [45]	[S11, S18, S20]	3	8%
Normas utilizadas como referencia para certificação	ISO/IEC 15026-1 [52],	[S04]	2	5%
	JIS B0134[53], JIS B0185[54], JIS B0186[55], JIS B0187[56]	[S14]		

Tabela 4. Benefícios relacionados a Casos de Garantia de Segurança em sistemas robóticos

#	BENEFICIOS	ESTUDOS
B1	Facilitar o entendimento da especificação de requisitos de segurança.	[S02, S03, S05, S06, S08, S09, S10, S11, S13, S14, S16, S17, S20]
B2	Gerenciar identificação de perigos e falha.	[S01, S02, S03, S05, S06, S07, S09, S10, S13, S16, S19]
B3	Garantir que as metas e requisitos de segurança sejam completa e corretamente declarados.	[S02, S03, S06, S11, S14, S16, S18, S20, S21]
B4	Maximizar a utilidade das técnicas existentes.	[S01, S02, S09, S10, S12, S15, S17, S18, S19]
B5	Criar processo/modelo de avaliação de risco	[S02, S06, S09, S10, S11, S15, S18, S20, S21]
B6	Criar e gerenciar as evidências.	[S02, S05, S08, S11, S12, S16]
B7	Facilita a validação dos Argumentos.	[S02, S05, S09, S10, S19]
B8	Reduzir do esforço de certificação.	[S05, S11, S12, S17, S21]
B9	Atualizar e padronizar o vocabulário utilizado pela robotica.	[S04, S11, S21]
B10	Colaboração multidisciplinar focada nos aspectos de segurança da robótica.	[S18]

completa e corretamente declarados indica que as metas e requisitos utilizados nos casos de garantia devem ser construídos detalhadamente, para que não haja ambiguidade e incompletude; outra vantagem é B4-Maximizar a utilidade da técnica existente. Percebeu-se que alguns artigos, com o uso de casos de garantia, conseguiram potencializar algumas técnicas de segurança no que tange a requisitos de segurança. Finalizando, as cinco vantagens mais citadas temos B5-Criar processo/modelo de avaliação de risco.

Como ficou evidente na QP1.3 boa parte das publicações utilizavam os requisitos de segurança como base para criação de modelos ou meta-modelos, ou na definição de novos processos.

Complementam a lista de benefícios, B6-Criar e gerenciar as evidências; B7-Facilitar a validação dos argumentos; B8-Reduzir o esforço de certificação; B9-Atualizar e padronizar o vocabulário utilizado pela robótica. Por último, B10-Ter colaboração multidisciplinar focada nos aspectos de segurança robótica, essa vantagem produz artefatos para orientações de pesquisas acadêmicas relatada na questão QP1.3.

QP5: Quais desafios e/ou problemas, relacionados a Casos de Garantia de Segurança utilizadas em sistemas robóticos, foram identificados pelas pesquisas?

A Tabela 5 mostra os problemas identificados relacionados a Casos de Garantia de Segurança em sistemas robóticos; a seguir são descritos aqueles que tiveram mais relatos.

O problema P8- Especificação de requisitos de segurança foi citado por 52% dos artigos como sendo o problema mais reincidente; esta dificuldade, impacta diretamente no segundo maior problema, com 43%, que é P3-Garantir os aspectos relacionados à segurança de um sistema, uma vez que só se consegue garantir aquilo que foi bem especificado. Por exemplo, incompletude na especificação de requisitos de segurança afetará diretamente na descrição dos casos de garantia.

Tabela 5. Problemas relacionados a Casos de Garantia de Segurança em sistemas robóticos

#	PROBLEMAS	ESTUDOS
P1	Garantia de segurança no ambiente médico	[S06]
P2	Projetar robôs inteligentes eticamente correto	[S13]
P3	Garantir os aspectos relacionados à segurança de um sistema.	[S01, S03, S07, S08, S11, S13, S17, S20, S21]
P4	Tratar da complexidade dos casos de garantia de segurança, certificando que os sistemas agem conforme esperado.	[S02, S09, S10, S11, S14, S20]
P5	Elicitação de requisitos de confiabilidade	[S05, S06, S07, S08, S16, S21]
P6	Elicitação e análise de requisitos na avaliação do risco associado aos perigos	[S01, S02, S03, S07, S08, S11, S21]
P7	Especificação de requisitos de hardware	[S03, S05, S07, S08, S14, S15, S16, S18, S19]
P8	Especificação de requisitos de segurança	[S01, S02, S03, S07, S14, S15, S16, S17, S18, S19, S21]
P9	Falta de padronização na especificação dos requisitos de segurança	[S01, S11, S20]
P10	Falta de técnicas linguísticas para melhorar a especificação e análise de sistemas robóticos	[S02, S11, S12, S18]
P11	Falta de um processo de engenharia de requisitos bem definido para o domínio de sistemas robóticos.	[S02, S03, S12, S13, S14]
P12	Grande número de elementos disponíveis para modelagem devido a diferentes especialistas no domínio	[S01, S02, S03, S09, S10, S11, S18, S20, S21]
P13	Inclusão dos requisitos de segurança e criação dos casos de garantia no início do processo.	[S01, S09, S10, S18]
P14	Métodos de verificação e certificação excessivamente intensivos em tempo e recursos	[S05, S11, S12, S14, S20]
P15	Padronização das terminologias relacionada ao domínio robótico	[S04, S11, S20]
P16	Prototipagem de sistemas robótico para validação de requisitos	[S07, S12]
P17	Requisitos físicos e não funcionais para sistemas robóticos	[S03, S14, S15, S16, S21]
P18	Ferramenta para facilitar a descrição dos casos de garantia	[S02]

Um outro problema relatado é o P12- Grande número de elementos disponíveis para modelagem devido às propostas de diferentes especialistas no domínio. Neste caso, o problema não trata apenas das diversas modelagens existentes e da quantidade de informação de sistemas robóticos, mas também da dificuldade de padronizar o que foi feito por inúmeros especialistas para uma variedade de domínios.

O problema de dificuldade, relatado em P7- Especificação de requisitos de *hardware*, aparece também com uma quantidade de citações significativa com 43%. Há também, em 33% das publicações, o relato de dificuldade para realizar P6-Elicitação e análise de requisitos, especificamente na avaliação do risco associado aos perigos. Completam a lista dos problemas mais citados nas publicações, com 29%, o que se deve tratar da complexidade em P4-Casos de Garantia de Segurança, certificando que os sistemas se comportam de certo modo conforme esperado. Neste caso, não basta apenas especificar se é necessário dominar a complexidade dos sistemas para que se tenha argumentos e evidências que garantam a segurança durante a adaptação constante dos sistemas robóticos. Com o mesmo percentual anterior temos, P5-Elicitação de Requisitos de confiabilidade, que trata de como obter informações detalhadas para garantir a consistência dos requisitos. Outros problemas com menor incidência também são listados na Tabela 5.

5 Conclusão

Esta revisão sistemática da literatura teve como objetivo analisar conceitos, métodos, ferramentas, normas dificuldades e vantagens relacionados à garantia da segurança em sistemas robóticos. A RSL baseou-se em 21 estudos selecionados de um total de 857 trabalhos publicados entre 1985 até janeiro de 2021. Através dela foi possível responder às perguntas e identificar as lacunas na área em questão.

As descobertas mais relevantes desta revisão e suas implicações para pesquisas futuras são as seguintes:

Especificação de requisitos de segurança. Foi verificado que a maioria dos estudos relatam problemas na descrição da especificação de segurança. Portanto, os casos de garantia podem assumir um papel importante na gerência dessas especificações, atestando que as metas e requisitos de segurança sejam completos e corretamente declarados e que forneçam argumentos que justifiquem com base em evidências os requisitos de segurança de sistemas robóticos tornando-os, mais seguros. É necessário que o desenvolvimento dos Casos de Garantia de Segurança seja iniciado o mais cedo possível, isto é, durante as fases da engenharia de requisitos; assim, eles trarão contribuições já nas fases iniciais da especificação.

Padronização de modelos/técnicas/ferramentas. Outro ponto importante é a padronização, seja de técnicas, de modelos ou até mesmo de vocabulário específico para a robótica. O que se vê, de acordo com os artigos analisados, é um grande número de especialistas (nos mais variados domínios) propondo diversos elementos diferentes e, muitas vezes, sem convergências de ideias. A falta de ferramentas comuns e de acesso compartilhado, que socializem Casos de Garantia de Segurança com a comunidade acadêmica e industrial, acarreta muitos projetos distintos e sem integração, o que dificulta novas pesquisas na área da robótica. Portanto, é necessária uma maior integração entre as fontes de pesquisa, padronizando e socializando os projetos; desta forma os estudos em robótica podem ganhar mais força e evoluir.

Complexidade no processo de certificação. O processo de certificação baseado em normas, que regulamenta a segurança para sistemas robóticos, é complexo. Portanto, para que se consiga a validação de uma certificação, deve-se simplificar o processo de geração de evidências de segurança; desta forma, os casos de garantia podem contribuir para que isso seja possível, gerenciando os argumentos necessários.

Lacuna na área de robôs sociais. Percebeu-se que existe uma lacuna importante no que tange a essa área especificamente, pois a grande maioria das publicações da RSL trataram da segurança de sistemas robótico industriais, omitindo a robótica social.

Motivados pelos resultados desta RSL, propomos uma agenda de pesquisa para a comunidade engenharia de requisitos para sistemas robóticos:

1. Pesquisar a relação que dever existir entre os Casos de Garantia de Segurança e as especificações de requisitos de segurança;
2. Desenvolver um processo de engenharia de requisitos de segurança que leve em consideração a necessidade de se criar Casos de Garantia de Segurança para robôs;
3. Criar um meta-modelo de segurança que seja baseado nas principais normas da indústria que tratam de robôs, a fim de facilitar o processo de certificação;
4. Adequar as pesquisas para área da robótica social, uma vez que robôs cognitivos estão sendo desenvolvidos e devem se tornar parte de nossa vida cotidiana. Assim, será necessário garantir que seu comportamento seja adequado, atendendo as normas de segurança.

Como trabalho futuro pretendemos propor uma metodologia de geração de Caso de Garantia de Segurança para Sistemas de Robóticos.

Agradecimentos

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001, Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ), Fundação de Amparo a Ciência e Tecnologia do Estado de Pernambuco (FACEPE).

Referências

1. JACOBS, Theo; VIRK, Gurvinder. ISO 13482-The new safety standard for personal care robots. In: ISR/Robotik 2014; 41st International Symposium on Robotics. VDE, 2014. p. 1-6. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&anumber=6840202&isnumber=6840100.
2. HILLIARD, Rich. Ieee-std-1471-2000 recommended practice for architectural description of software-intensive systems. IEEE, http://standards.ieee.org, v. 12, n. 16-20, p. 2000, 2000.
3. DENNEY, Ewen; PAI, Ganesh; HABLI, Ibrahim; KELLY, Tim; KNIGHT, John. 1st Interntional workshop on assurance cases for software-intensive systems (ASSURE 2013).In: 2013 35th International Conference on Software Engineering (ICSE). IEEE, p. 1505-1506, 2013.
4. ANGERER, Andreas; HOFFMANN, Alwin; ORTMEIER, Frank; VISTEIN, Michael; REIF, Wolfgang. Object-Centric Programming: A New Modeling Paradigm for Robotic Applications. In International Conference on Automation and Logistics, (2009), 18-23.
5. SACM, OMG. Structured assurance case Metamodel Specification Version 2.0. 2013. url https://www.omg.org/spec/SACM/2.0/
6. KITCHENHAM, Barbara; CHARTERS, Stuart. Guidelines for performing systematic literature reviews in software engineering, 2007.
7. WOHLIN, Claes; RUNESON, Per; MOTA, Paulo; ENGSTRÖM, Emelie; MACHADO, Ivan; ALMEIDA, Eduardo. On the reliability of mapping studies in software engineering. Journal of Systems and Software, v. 86, n. 10, p. 2594-2610, 2013.
8. RUSHBY, John. The interpretation and evaluation of assurance cases. Comp. Science Laboratory, SRI International, Tech. Rep. SRI-CSL-15-01, 2015.

9. NAIR, Sunil; LA VARA, Jose Luis; SABETZADEH, Mehrdad; BRIAND, Lionel. An extended systematic literature review on provision of evidence for safety certification. Information and Software Technology, v. 56, n. 7, p. 689-717, 2014. doi.org/10.1016/j.infsof.2014.03.001.
10. NOF, Shimon Y. (Ed.). Handbook of industrial robotics. John Wiley & Sons, 1999.
11. LEVESON, Nancy G. Safeware: system safety and computers. Addison-Wesley, 1995.
12. PORFÍRIO, E. J. Um metamodelo para casos de garantia de sistemas críticos e intensivos em software baseado em análise do conceito inicial de sistemas teóricos. 122 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Goiás, Goiânia, 2019.
13. KEELE, Staffs. Guidelines for performing systematic literature reviews in software engineering. Technical report, Ver. 2.3 EBSE Technical Report. EBSE, 2007.
14. GALSTER, Matthias; WEYNS, Danny; TOFAN, Dan; MICHALIK, Bartosz; AVGERIOU, Paris. Variability in software systems—a systematic literature review. IEEE Transactions on Software Engineering, v. 40, n. 3, p. 282-306, 2013.
15. DYBÅ, Tore; DINGSØYR, Torgeir. Empirical studies of agile software development: A systematic review. Information and software technology, v. 50, n. 9-10, p. 833-859, 2008.
16. ACHIMUGU, Philip; SELAMAT, Ali; BRAHIM, RolianaI; MAHRIN, Mohd. A systematic literature review of software requirements prioritization research. Information and software technology, v. 56, n. 6, p. 568-585, 2014.
17. DERMEVAL, Diego; VILELA, Jéssyka; BITTENCOURT, Ig Ibert; CASTRO, Jaelson; ISOTANI, Seiji; BRITO, Patrick; SILVA, Alan . Applications of ontologies in requirements engineering: a systematic review of the literature. Requirements Engineering, v. 21, n. 4, p. 405-437, 2016.
18. DING, Wei; LIANG, Peng; TANG, Antony; VLIET, Hansvan. Knowledge-based approaches in software documentation: A systematic literature review. Information and Software Technology, v. 56, n. 6, p. 545-567, 2014.
19. DYBA, Tore; DINGSOYR, Torgeir; HANSSEN, Geir K. Applying systematic reviews to diverse study types: An experience report. In:First international symposium on empirical software engineering and measurement. IEEE, p. 225-234, 2007.
20. WOHLIN, Claes; RUNESON, Per; HÖST, Martin; OHLSSON, Magnus; REGNELL, Björn; WESSLÉN, Anders. Experimentation in software engineering. Springer Science & Business Media, 2012.
21. ISO/IEC 15026-2:2011- Systems and software engineering -Systems and software assurance - Part 2: Assurance case.
22. ZAMBONI, Augusto, THOMMAZO, André, HERNANDES, Elis Cristina; FABBRI, Sandra. StArt uma ferramenta computacional de apoio à revisão sistemática. In: Proc.: Congresso Brasileiro de Software, Brazil. 2010. p. 91-96.
23. PESHKIN, Michael; COLGATE, J. Edward. Cobots. Industrial Robot: An International Journal, 1999.
24. ISO10218:2011 - Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots.
25. ISO/IEC 19501:2005 Information technology — Open Distributed Processing — Unified Modeling Language (UML) Version 1.4.2
26. FRIEDENTHAL, Sanford; MOORE, Alan; STEINER, Rick.A practical guide to SysML: the systems modeling language. Morgan Kaufmann, 2014.
27. ATKESON, Christopher G.; SCHAAL, Stefan. Robot learning from demonstration. In:ICML. p. 12-20, 1997.

28. HAVELUND, Klaus; HOLZMANN, Gerard J. Software certification: coding, code, and coders. In: Proceedings of the ninth ACM international conference on Embedded software. p. 205-210., 2011.
29. Japanese Standard, JIS B0187 Service robots- Vocabulary.
30. Japanese Standard, JIS B0186 Mobile robots-Vocabulary.
31. Japanese Standard, JIS BO185 Intelligent robots- Vocabulary.
32. Japanese Standard, JIS B0134 Manipulating Industrial Robots-Vocabulary.
33. Diretiva 2006/42/CE do Parlamento Europeu e do Conselho, 2006, relativa às máquinas e que altera a Diretiva 95/16/CE.
34. IEC 61508-1:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems.
35. ISO 11161:2007/AMD 1:2010 Safety of machinery, Integrated manufacturing systems, Basic requirements.
36. ISO/TS 15066:2016 Robots and robotic devices, Collaborative robots.
37. ISO/IEC 15026-1:2019 - Systems and software engineering -Systems and software assurance e- Part 1: Concepts and vocabulary.
38. ISO/PAS 21448:2019 Road vehicles, Safety of the intended functionality.
39. ISO 26262-12:2018 Road vehicles, Functional safety, Adaptation of ISO 26262 for motorcycles.
40. SAE J3016:2019, automated-driving graphic update.
41. SAE J3088:2017Active Safety System Sensors.
42. BS EN 50126:2017 - Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS).
43. BS EN 50128:2011/A2:2020 - Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems.
44. BS EN 50129:2018 - Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signaling.
45. ISO 13482:2014 - Robots and robotic devices - Safety requirements for personal care robots
46. ISO/TR 23482-1:2020 - Robotics - Application of ISO 13482 -Part 1: Safety-related test methods.
47. RTCA/DO-178B:2011 - Software Considerations in Airborne Systems and Equipment Certification.
48. RTCA/DO-178C:1992 - Software Considerations in Airborne Systems and Equipment Certification.
49. IEC 60601-1-11:2015 - Medical electrical equipment - Part 1-11: General requirements for basic safety and essential performance - Collateral standard: Requirements for medical electrical equipment and medical electrical systems used in the home healthcare environment.
50. IEC 80601-2-78:2019 Medical electrical equipment - Part 2-78: Particular requirements for basic safety and essential performance of medical robots for rehabilitation, assessment, compensation or alleviation.
51. ISO 12100:2010 - Safety of machinery - General principles for design - Risk assessment and risk reduction.
52. GASPARETTO, A.; SCALERA, L. A brief history of industrial robotics in the 20th century. Advances in Historical Studies, v. 8, n. 1, p. 24-35, 2019.
53. ASIMOV, Isaac. I, robot. Spectra, 2004.
54. CECCARELLI, Marco. A historical perspective of robotics toward the future. Journal of Robotics and Mechatronics, v. 13, n. 3, p. 299-313, 2001.