appSCE: uma Ferramenta para Classificação da qualidade de evidências usadas em Casos de Garantia de Segurança

Mozart Alves-Júnior[1,2][0000-0002-4865-6581], Sandeison Fernandes[1][0009-0004-5589-3528], Jaelson Castro[1][0000-0002-4635-7297], Alvaro Oliveira[2][0009-0007-8668-4747] and Aldo Nunes[2][0000-0002-3196-3155]
[1]Centro de informática – CIN – Universidade Federal de Pernambuco – UFPE
[2]Centro Universitário CESMAC
[1]{mmaj, lfb, jbc}@cin.ufpe.br, [2]{alvaro2014oliveira, aldonunes001}@gmail.com

Resumo. Os Casos de Garantia de Segurança (CGS) tornaram-se elementos essenciais e indispensáveis na certificação de segurança em diversos domínios de sistemas críticos. Esses processos de certificação são rigorosos e exigem argumentos sólidos, sustentados por um conjunto de evidências de alta qualidade que comprovem a segurança e a adequação do sistema ao seu ambiente de uso específico. No entanto, a avaliação dessas evidências frequentemente depende do julgamento humano, o que pode estar sujeito a vieses cognitivos, comprometendo a validade dos argumentos apresentados. Este trabalho apresenta o appSCE (App for Safety Classification of Evidence), uma ferramenta de código aberto, acessível via web, que segue uma arquitetura cliente-servidor e utiliza tecnologias como TypeScript, React Native, Node.js e Firebase Firestore. O appSCE apoia a abordagem Classify Evidence, que visa classificar a qualidade das evidências de segurança utilizadas na construção dos CGS. O objetivo do aplicativo é facilitar o controle e gerenciamento da classificação das evidências, tornando-as mais dinâmicas e acessíveis, e, desta, contribuir para uma comunicação mais eficaz e confiável entre os stakeholders envolvidos.

Palavra-chave: Evidência, classificação de evidência, qualidade das evidências, Caso de Garantia de Segurança, Certificação de Segurança, viés cognitivo.

1 Introdução

Sistemas críticos, em geral, precisam obter a aprovação de uma entidade independente, como um órgão regulador. Em domínios consolidados, como aviação e dispositivos médicos, é comum a adoção de uma abordagem prescritiva. Neste caso uma agência reguladora define padrões que devem ser seguidos, incluindo processos específicos a serem aplicados durante o desenvolvimento e testes obrigatórios que o sistema deve realizar. Os desenvolvedores e fabricantes, por sua vez, são responsáveis por apresentar evidências de que cumpriram essas exigências, por meio de documentações claras e convincentes que demonstrem a segurança do sistema e fundamentem os argumentos apresentados [1].

O processo de certificação, no entanto, é longo e complexo, em razão do grande volume de informações que precisa ser fornecido. Além disso, o uso de linguagem natural na documentação das argumentações pode introduzir ambiguidades, dificul-

Proceedings of the 28th Workshop on Requirements Engineering (WER2025),
August 20-22, 2025, Rio de Janeiro-RJ, Brazil.
https://doi.org/10.29327/1588952.28-21

tando a análise e avaliação dos argumentos que deveriam assegurar a segurança do sistema. Tais argumentos podem ser comprometidos caso as evidências apresentadas sejam insuficientes para sua sustentação.

Embora os processos de certificação e as normas de segurança venham evoluindo constantemente, ainda é desafiador atender de forma eficaz às exigências de segurança impostas aos sistemas críticos de segurança [2]. A literatura aponta problemas como a necessidade de descrever de forma mais clara e rastreável os objetivos a serem alcançados [3], além do uso de linguagem informal e ambígua, frequentemente influenciada por vieses cognitivos na especificação dos argumentos.

Nesse contexto, novas abordagens, métodos e ferramentas têm sido propostas, com destaque para os Casos de Garantia de Segurança (do inglês *Safety Assurance Case*) [4]. Um Caso de Garantia de Segurança (CGS) visa demonstrar a validade de uma reivindicação de segurança, apresentando um argumento estruturado e fundamentado em evidências de apoio [5]. Essas evidências desempenham um papel crucial na construção da credibilidade necessária para a operação segura de um sistema.

Conforme observado por Kelly [6], argumentos sem evidências de apoio são infundados e, portanto, pouco convincentes. Evidências de baixa qualidade tornam os argumentos inconsistentes, comprometendo a reivindicação de segurança do sistema. Assim, a classificação da qualidade das evidências é essencial para aprimorar a confiabilidade dos argumentos [7].

Sistemas críticos que dependem de software para atingir seus objetivos exigem que os CGSs considerem a contribuição do software para a segurança do sistema. Consequentemente, engenheiros de software devem estar envolvidos na elaboração dos CGSs, abordando a construção, validação e manutenção da segurança desses sistemas. De acordo com Cheng [8], os CGSs atuam como uma ponte entre desenvolvedores de software, analistas de segurança e especialistas em certificação, facilitando a troca de conhecimento entre eles.

Diante desse cenário, foi elaborada uma abordagem denominada ***Classify Evidence***[1], destinada a classificar as evidências utilizadas na construção de um CGS, onde apenas evidências de boa qualidade devem ser empregadas na comprovação dos argumentos, enquanto evidências de baixa qualidade, sujeitas a vieses, devem ser eliminadas ou reformuladas.

Este trabalho apresenta o appSCE (App for Safety Classification of Evidence) que apoia uma abordagem de classificação das evidências utilizadas na construção de CGSs, denominada *Classify Evidence*. Seu objetivo é fornecer uma solução eficiente para avaliar a qualidade das evidências empregadas na especificação dos CGSs, tornando o processo mais estruturado, confiável e rastreável. Além disso, facilita o controle e gerenciamento das evidências, tornando a classificação mais dinâmica e acessível, beneficiando tanto a comunidade acadêmica quanto a indústria.

2 Visão Geral da Abordagem

A abordagem *Classify Evidence* é estruturada em várias etapas, apresentada utilizando um diagrama BPMN (vide Fig. 1). Inicialmente é preciso Obter Evidências. Em seguida serão realizadas as etapas de **Introdução, Apresentação, Análise Crítica,**

[1] https://bit.ly/ClassifyEvidence

Classificação e Cálculo da Relevância da Evidência. Como resultados as evidências poderão ser classificadas em quatro categorias: **Incontestável, Importante, Mediana e Fraca**.

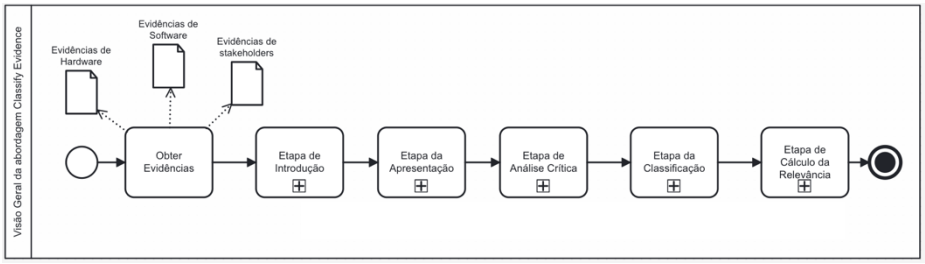

Fig 1. Visão Geral da abordagem Classify Evidence

Na aplicação da abordagem *Classify Evidence*, é crucial verificar, classificar e validar a qualidade das evidências apresentadas. Essa classificação baseia-se nos artefatos de maior valor agregado para a indústria ou órgãos reguladores, como normas, códigos, relatórios técnicos, documentos de requisitos e testes. Portanto, apenas as evidências de boa qualidade (Incontestáveis e Importantes) e livres de vieses serão usadas na validação dos argumentos. A partir dessa avaliação, são identificados os artefatos de maior e menor valor, descartando-se as evidências fracas ou sem comprovação oficial.

2.1 Detalhamento das Etapas da Abordagem Classify Evidence

A seguir serão detalhadas as etapas de Introdução, Apresentação, Análise Crítica, Classificação e Cálculo da Relevância, que no momento são apoiadas pela ferramenta appSCE.

Introdução - Nesta fase, o objetivo é compreender a evidência inicial. Ela deve ser nomeada de forma clara e sucinta, bem como as palavras-chave devem ser listadas para facilitar a rastreabilidade e a futura localização da evidência. Também é necessário descrever brevemente o tema e a importância da evidência no domínio, além de esclarecer sua intenção (vide Fig. 3c e Fig. 3d).

Apresentação- Após a introdução, é necessário aprofundar a análise de como as evidências foram coletadas. Nessa etapa, deve-se descrever de maneira clara, sucinta e objetiva o artefato, especificando as pesquisas confiáveis das quais o artefato foi extraído (autores, data de publicação, tipo de evidência, normas e o link). Também é importante indicar se a avaliação foi realizada por pares e avaliar a consistência da evidência em relação a estudos prévios (vide Fig. 4c).

Análise Crítica - Esta fase envolve uma avaliação crítica detalhada, identificando os pontos fortes, as limitações e as possíveis influências externas sobre as evidências. Nessa etapa, é necessário definir a metodologia, fornecendo exemplos de como descrever a evidência no contexto de um caso de segurança, aplicando-a em documentações de segurança já existentes, e descrevendo recomendações ou técnicas relevantes para o uso da evidência. Além disso, devem ser identificados possíveis vieses ou limitações que, embora não explicitamente mencionados, possam comprometer a validade dos resultados obtidos. Também é importante analisar a existência de potenciais con-

flitos de interesse que possam influenciar a objetividade ou integridade dos resultados apresentados (vide Fig. 4d).

Classificação - Após coletar e organizar as informações das etapas anteriores é essencial avançar para a classificação das evidências com base em três critérios (vide Fig 5a): relevância (mede o grau de aplicabilidade das evidências), cobertura (avalia em que medida as evidências abrangem todas as subdivisões da instância) e força (determina o nível de confiabilidade das evidências).

Cálculo da Relevância - Nesta fase, será necessário avaliar a Gravidade do Perigo (GP), onde o especialista atribui uma pontuação de 1 a 10 (vide Fig. 5b), indicando o impacto da evidência na redução do risco. Também é preciso definir a **Probabilidade de Falha (PF)**, diferenciando a metodologia adotada para hardware e software (vide Fig. 5c), atribuindo pontuação de 1 a 10.

Os especialistas designados para a área correspondente verificarão se a organização adota métricas específicas para o controle de erros e determinarão o nível de maturidade dessas práticas. Esse processo facilita a atribuição de pontuação para a probabilidade de falhas nas evidências, conforme ilustrado na Fig. 5b e Fig. 5c.

Com essas informações, a relevância da evidência será calculada como Incontestável, Importante, Mediana ou Fraca, conforme o preconizado pela abordagem *Classify Evidence* (vide Fig. 5d).

Evidências de categoria **Incontestável e Importante** são consideradas de alta qualidade e geram argumentos menos propensos a desvios sistemáticos do pensamento racional, reduzindo interpretações equivocadas. Já as evidências de categoria **Mediana** ou **Fraca** devem ser revistas ou descartadas.

Nossa proposta assegura que apenas evidências sólidas e confiáveis sejam utilizadas para justificar os argumentos, aumentando a qualidade e robustez dos CGSs. Ao calcular a relevância, a abordagem *Classify Evidence* garante a adequação das evidências, permitindo o desenvolvimento de estratégias precisas e a seleção dos artefatos com maior valor agregado. Com a classificação das evidências, será possível embasar os argumentos de segurança utilizados na construção dos CGSs.

3 Sistema de Classificação de Evidências (appSCE)

Para o gerenciamento e a classificação das evidências associadas a projetos de Casos de Garantia de Software (CGSs), foi desenvolvido o appSCE, uma ferramenta de código aberto para dispositivos móveis, acessível via web. O appSCE segue uma arquitetura cliente-servidor e utiliza tecnologias como TypeScript, React Native, Node.js e Firebase Firestore. Seu objetivo é fornecer uma solução eficiente para avaliar a qualidade das evidências utilizadas na especificação dos CGS. Além disso, facilita o controle e gerenciamento das evidências, tornando a classificação mais dinâmica e acessível, beneficiando tanto a comunidade acadêmica quanto a indústria.

3.1 Detalhamento do AppSCE

No AppSCE, os usuários desempenham duas funções principais: Administrador ou Avaliador (especialista).

Administrador: É responsável pelo cadastro dos avaliadores, atribuindo a área de especialidade de cada um (hardware ou software), conforme ilustrado na Fig. 2. Além

disso, o administrador realiza o cadastro do projeto, incluindo a etapa de introdução das evidências ilustrada na Fig. 3. Nessa etapa, são registradas informações como o tipo, nome, palavras-chave e a contextualização das evidências.

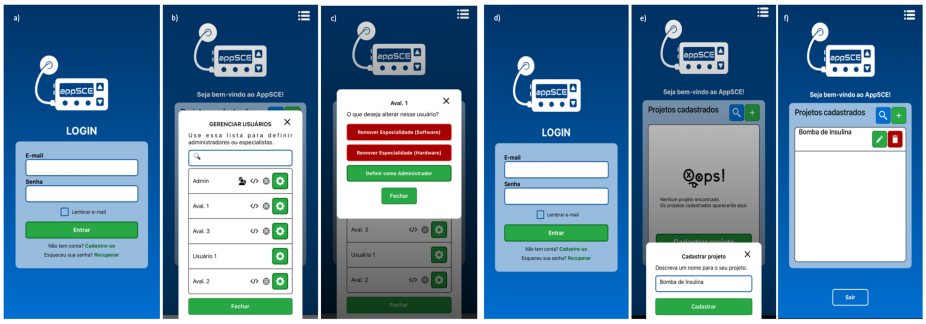

Fig 2. Cadastro do especialista e do projeto no appSCE

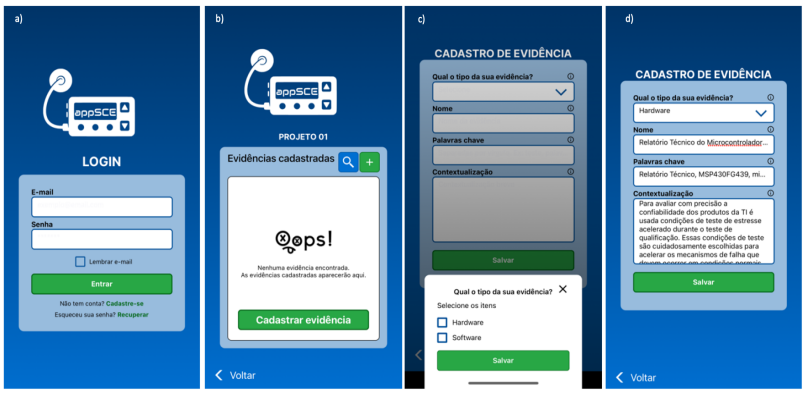

Fig 3. Cadastro das evidências

Avaliador: É o responsável por analisar as evidências destinadas à sua área de especialidade, realizando avaliações detalhadas e contribuindo para a classificação precisa das evidências.

A ferramenta oferece uma abordagem estruturada e eficiente para o gerenciamento das evidências, promovendo uma clara divisão de responsabilidades entre administradores e avaliadores, com foco na garantia da qualidade e precisão no processo de classificação.

Após a criação do projeto e das evidências, é responsabilidade dos avaliadores (especialistas) selecionar e classificar as evidências, seguindo a abordagem *Classify Evidence*, conforme ilustrado na Fig. 4.

Fig 4. Cadastro das evidências

É importante destacar que, dependendo do tipo de evidência (hardware ou software), o sistema direciona os avaliadores para interfaces específicas relacionadas à verificação da probabilidade de falhas. Essa diferenciação ocorre devido à maior complexidade no processo de verificação das falhas em evidências de software.

Através da abordagem *Classify Evidence*, os especialistas indicam se a organização adota métricas específicas para o controle de erros e determinarão o nível de maturidade dessas práticas. Esse processo facilita a atribuição de pontuação para a probabilidade de falhas nas evidências (vide Fig. 5b e Fig. 5c).

Fig 5. Avaliação da evidência de software

A avaliação de evidências de hardware é realizada de forma direta. Como mencionado anteriormente, a probabilidade de falhas está diretamente vinculada a testes de estresse acelerado, projetados para simular e prever mecanismos de falha que poderiam ocorrer em condições normais de uso. Esses testes devem ser informados pelos fabricantes, com estimativas confiáveis sobre o desempenho dos componentes em cenários reais. Na Fig. 6 é ilustrada a avaliação direta da evidência de hardware no que se diz respeito à probabilidade de falha.

Fig 6. Avaliação da evidência de hardware

A abordagem *Classify Evidence* estabelece como critério obrigatório a avaliação em pares. Assim, o appSCE, também passará pelas seguintes etapas:

Análise e Consolidação: As respostas dos dois especialistas são analisadas e organizadas em evidências convergentes ou divergentes.

Segunda Rodada: Os critérios que não obtiveram consenso são revisados por um novo especialista. Nesta etapa, um feedback detalhado é fornecido a todos os especialistas que participaram da rodada anterior, com o objetivo de alcançar consenso. A avaliação pode ser ajustada através do aplicativo.

Resultado Final: As evidências serão classificadas automaticamente. Aquelas que forem consideradas como **incontestáveis** e **importantes** são recomendadas para sustentar os argumentos a serem usados nos CGS. Por outro lado, evidências classificadas como **medianas** ou **fracas** devem ser excluídas ou reformuladas.

Ao final do processo, o appSCE gera um relatório detalhado com a documentação da abordagem *Classify Evidence* para a evidência classificada, podendo ser baixada no formato pdf.

4 Considerações Finais e Trabalhos Futuro

A abordagem *Classify Evidence* não apenas facilita a identificação de evidências de maior valor agregado, mas também organiza e sistematiza o processo de classificação, tornando-o mais rastreável e adaptável a diferentes contextos regulatórios. Evidências bem classificadas têm o potencial de reduzir significativamente os retrabalhos e rejeições em processos de certificação, otimizando recursos e aumentando a confiança dos stakeholders nos sistemas avaliados.

O aplicativo **appSCE**, complementa essa abordagem, sendo uma inovação, ao automatizar e estruturar o gerenciamento das evidências, proporcionando uma experiência mais dinâmica e acessível para os avaliadores. Sua interface facilita a verificação da probabilidade de falhas em componentes de hardware e software, um aspecto crítico para sistemas complexos que operam em ambientes regulamentados. Com essa ferramenta, espera-se não apenas atender às exigências regulatórias, mas também estabelecer novos padrões de clareza, rastreabilidade e confiabilidade nos **CGS**.

Como trabalho em andamento, já em fase de testes, temos a funcionalidade para tratar os vieses cognitivos das evidências a serem usadas nos **CGSs**. Desta forma, será possível quantificar o percentual de influência de viés cognitivo nas evidências inseridas no appSCE.

Nesta etapa estamos utilizando **Large Language Models (LLMs)** integrados estrategicamente com tecnologias e ferramentas sofisticadas, como **Streamlit** e **LangChain**, além de serviços especializados acessíveis por meio das APIs fornecidas pela **OpenAI** e **Groq**, por exemplo. Trata-se de um avanço significativo frente às técnicas tradicionais, que frequentemente se limitam a abordagens simplificadas e superficiais, como análises baseadas meramente na frequência de palavras-chave ou em modelos genéricos pré-treinados para avaliação de sentimentos. Em contraste, a transição para o uso de **LLMs avançados**, tais como **GPT-4** ou os modelos mais recentes oferecidos pela **Groq**, como o **DeepSeek**, permite uma análise muito mais aprofundada e contextualizada.

Link para o Vídeo da Ferramenta: https://bit.ly/appSCE-CE .

Agradecimentos

Este trabalho foi realizado com o apoio do Conselho nacional de Desenvolvimento Cientifico e Tecnológico (CNPq) e da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES).

Referências

1. Rushby, J.:Formalism in safety cases. Making Systems Safer, (2010). Disponível em: http://www.csl.sri.com/users/rushby/papers/sss10.pdf, último acesso: 27/04/2025
2. Porfirio, E.: 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).
3. Alves-junior, M., Lencastre M., Brito, L., Castro, J., Ribeiro M.: Casos de Garantia de Segurança aplicados a sistemas robóticos: revisão sistemática da literatura. In: XXIV WER - Workshop em Engenharia de Requisitos. Brasília. (2021).
4. Denney, E., Pai, G., Habli, I., Kelly, T., Knight, J.:1st International workshop on assurance cases for software-intensive systems (ASSURE 2013). In: 35th International Conference on Software Engineering (ICSE) pp. 1505-1506, (2013).
5. SACM, OMG.: Structured assurance case Metamodel Specification Version 2.0. (2018). disponível em: https://www.omg.org/spec/SACM/2.0/, último acesso: 27/03/2025.
6. Kelly, T.: Arguing safety: a systematic approach to managing safety cases. Tese de Doutorado. University of York. (2001).
7. Rushby, J.: The interpretation and evaluation of assurance cases. Comp. ScienceLaboratory SRI International, Tech. Rep. SRI-CSL-15-01. (2015). Disponível em: https://www.csl.sri.com/~rushby/papers/sri-csl-15-1-assurance-cases.pdf, último acesso: 17/04/2025.
8. Cheng L., Goodrum J., Metoyer M., Cleland-Huang R.: How do practitioners perceive assurance cases in safety-critical software systems? In: CHASE´18: Proceedings of the 11th international workshop on cooperative and human aspects of software engineering.p. 57 – 60, (2018).