USO DE CASOS DE INSEGURANÇA NA AVALIAÇÃO E CERTIFICAÇÃO DE SISTEMAS COMPLEXOS

Lúcio F. Vismari
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica – Universidade de São Paulo
São Paulo, Brasil
lucio.vismari@usp.br

João Batista Camargo Junior
Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica – Universidade de São Paulo
São Paulo, Brasil
joaocamargo@usp.br

RESUMO

Este artigo propõe o uso de Casos de Insegurança (*Unsafety Cases*) – uma abordagem baseada em evidências de insegurança, método científico e a Teoria da Falseabilidade de Popper – como forma de complementar e aprimorar as atuais abordagens de avaliação e certificação de segurança crítica em sistemas de alto risco e críticos em dependabilidade. Além disso, a abordagem proposta pode vir a contribuir com a disciplina de Engenharia de Segurança de Sistemas, evoluindo com os fundamentos e arcabouço metodológico relacionado à engenharia de sistemas complexos.

Palavras-chave: Método Científico, Garantia de segurança crítica, Certificação, Normas, Popper.

ABSTRACT

USING UNSAFETY CASES IN SAFETY ASSESSMENT AND CERTIFICATION OF COMPLEX SYSTEMS. This paper proposes the use of *Unsafety Cases* - an approach based on evidences of unsafety, scientific method and the Popper‟s Theory of Falsifiability - in order to complement and improve the current safety assessment and certification approaches in dependable, high risk critical domains. Moreover, the proposed approach may contribute to the Systems Safety Engineering discipline with the evolution of the foundations and methodological framework related to complex systems engineering.

Keywords: Scientific Method, Safety Assurance, Certification, Standards, Popper.

1. INTRODUÇÃO

Sistemas são projetados para atender necessidades específicas, prestar serviços e executar tarefas necessárias à vida cotidiana. Quando um sistema não é capaz de realizar requisitos desejados e projetados, a missão para a qual foi concebido não pode ser devidamente cumprida. O funcionamento anormal de muitos sistemas do dia-a-dia tem consequências menores, não prejudicando significativamente as pessoas envolvidas ou o ambiente, causando, no máximo, irritação ou decepção. No entanto, o funcionamento anormal de alguns sistemas pode levar a consequências socialmente inaceitáveis, com perdas catastróficas. Sistemas cujo funcionamento anormal pode causar perdas e danos à vida humana e ao ambiente no qual está inserido são definidos como sistemas críticos em segurança (SOMMERVILLE, 2011).

Um estado operacional no qual um sistema pode expor as pessoas e o meio ambiente a um acidente – evento com perdas inaceitáveis – é definido como um estado inseguro ou estado perigoso. Estados inseguros violam a propriedade de segurança de um sistema e, portanto, os riscos relacionados com a segurança devem ser minimizados a níveis considerados aceitáveis por todos os envolvidos e interessados. Os sistemas onde os riscos de perdas superam os benefícios para as partes interessadas tendem a ser retirados de operação ou mesmo não implementados. Assim, a garantia de níveis de risco aceitáveis relacionados à operação de sistemas críticos em segurança demanda abordagens robustas e bem estabelecidas de garantia de segurança (ALMEIDA JR, 2003), aplicadas ao longo de todas as fases do ciclo de vida dos sistemas onde problemas (condições adversas para o correto funcionamento) podem ser introduzidos e se manifestar de forma insegura.

Em geral, essas abordagens de garantia de segurança são baseadas na combinação de duas filosofias: (1) prevenir que problemas (falhas) estejam presentes no sistema e, consequentemente, manifestem-se durante sua operação (com abordagens para evitar e/ou remover falhas); ou (2) quando se manifestarem durante a operação, tolerar todos aqueles problemas (falhas) que não puderam ser removidos ou evitados (com abordagens de tolerância a falhas). Em resumo, o principal objetivo destas abordagens é a de garantir um nível de risco de perdas, produzidas por acidentes, em níveis aceitáveis durante todo o ciclo de vida de sistemas críticos, especialmente em relação à percepção de risco para os usuários.

Abordagens de garantia da segurança variam desde uma compilação das melhores práticas – que contêm processos, métodos e técnicas desenvolvidos e recomendados por organizações (incluindo empresas) e cuja a aplicação é opcional durante o ciclo de vida de sistemas, principalmente as fases de implantação e operação – até um conjunto obrigatório de normas – cujo conteúdo e aplicação são definidos e regulamentados em nível governamental. Percebe-se que essa diferença de abordagem é dependente do domínio de aplicação do sistema de segurança crítica, bem como o país onde será utilizado, uma vez que o risco de perdas relacionadas com um sistema depende do domínio de aplicação para a qual foi desenvolvido. Dado que o risco é ponderado pela relação entre probabilidade contra gravidade da ocorrência de um perigo, a perda potencial de vidas humanas após a ocorrência de eventos incertos em determinadas áreas de aplicação é maior do que em outros. Usinas nucleares e sistemas de transportes são exemplos de áreas de aplicação que têm sistemas críticos em segurança de alto risco, onde a operação anormal desses sistemas tende a causar um grande número de mortos, feridos e danos ambientais catastróficos.

Nesses domínios de aplicação de alto risco, o uso de conjuntos específicos de normas de segurança – onde estão definidas as abordagens de garantia da segurança – é obrigatório e regulamentado em nível governamental. Uma investigação preliminar (VISMARI; CAMARGO JUNIOR, 2012) a respeito de abordagens de garantia de segurança regulamentadas em alguns domínios de aplicação crítica resultou na identificação de um macroprocesso de garantia de segurança, comum a estes domínios, composto por três elementos

principais: uma Base Normativa, uma Autoridade de Segurança e as Partes Interessadas (como os Desenvolvedores e Operadores), conforme ilustrado na Figura 1. A Autoridade de Segurança, geralmente em nível governamental ou transnacional, estabelece (regulamenta) as bases normativas que devem ser cumpridas por todos os envolvidos no domínio de aplicação e em todas as fases do ciclo de vida de seus sistemas. A Base Normativa pode estabelecer tanto o conjunto de requisitos alocáveis ao nível das aplicações – determinando o comportamento e nível de desempenho de segurança que a aplicação deve cumprir, principalmente relacionados com os riscos – quanto os requisitos e procedimentos ao nível dos próprios sistemas críticos de segurança, determinando os requisitos que os sistemas devem atender, bem como os processos de desenvolvimento, fabricação, operação, entre outros. Os envolvidos com o sistema devem cumprir as suas exigências para minimizar as chances de o sistema manifestar problemas que possam comprometer o nível de segurança da aplicação. Pode-se notar que, mesmo no nível do sistema, a base normativa está relacionada com os tipos de sistemas existentes em uma aplicação específica como, por exemplo, sistemas eletroeletrônicos e programáveis, sistemas mecânicos, entre outros.

Na maioria dos domínios de aplicação crítica de alto risco, além dos sistemas serem desenvolvidos, comissionados, operados e mantidos de acordo com os requisitos e procedimentos especificados nas Bases Normativas, suas abordagens de garantia de segurança exigem que a Autoridade de Segurança certifique que estes sistemas críticos cumprem as Bases Normativas, tanto seus requisitos quanto seus procedimentos. Assim, o processo de certificação é utilizado pela Autoridade de Segurança para avaliar se um sistema crítico está em conformidade com as exigências normativas e, portanto, é seguro sob o ponto de vista de aceitação de riscos (Figura 1). Um processo de certificação pode ser aplicado em diferentes estágios do ciclo de vida do sistema – projeto, produção, operação e manutenção – e em seus diversos elementos funcionais e níveis sistêmicos (tanto para os produtos e equipamentos quanto para processos e pessoas). Desta forma, pode-se notar que, além da aplicação mandatória das Bases Normativas pelos envolvidos em todas as fases do ciclo de vida dos sistemas, o **processo de garantia de segurança** possui uma abordagem extra de garantia onde a Autoridade de Segurança ou Organização Independente (ISA) verifica se os sistemas atendem a regulamentação e, portanto, certifica-os como seguros.

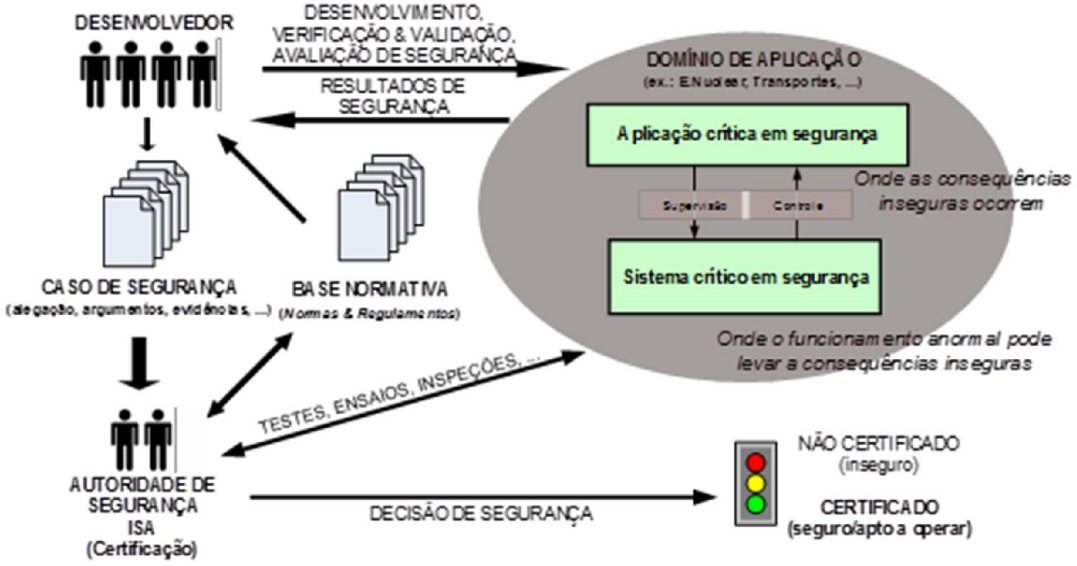


Figura 1 - Macroprocesso de garantia de segurança para domínios de aplicação de alto risco (baseado em Vismari e Camargo Jr (2012)

Desta forma, sistemas em aplicações críticas em segurança parecem ter abordagens de garantia de segurança robustas e bem estabelecidas, muitas deles especificados em bases normativas. Estas abordagens, cujo cumprimento é mandatório (por meio do atendimento compulsório a bases normativas) em diversos domínios de aplicação em muitos países, regem o ciclo de vida destes sistemas, mais especificamente a forma como devem ser especificados, projetados, produzidos, verificados e validados, operados, mantidos e até mesmo descartados. Assim, estas abordagens deveriam ser suficientes para garantir baixos níveis de risco de perdas, tornando raras as ocorrências de incidentes e de acidentes. Contudo, apesar da extensa e quase sempre mandatória base normativa, de abordagens bem estabelecidas e da existência de uma disciplina da engenharia dedicada à garantia da segurança de sistemas, acidentes e condições inseguras continuam ocorrendo a taxas que podem vir a comprometer a percepção de risco das partes envolvidas e interessadas, sobretudo seus usuários, comprometendo a permanência da operação destes sistemas. Por exemplo, nos últimos anos têm se observado na mídia um aumento significativo no número de Recalls de produtos em diversos setores produtivos, em especial no setor automotivo. Uma parcela significativa destes recalls teve como objetivo solucionar problemas de segurança relacionados a software ou a novas tecnologias embarcadas.

Um estudo preliminar levantou a hipótese a respeito das abordagens de garantia de segurança preconizadas pelas bases normativas atuais serem inadequadas para lidar com as novas demandas tecnológicas, sobretudo com aquelas relacionadas às características de complexidade sistêmica (VISMARI; CAMARGO JUNIOR, 2012). Consequentemente, estas abordagens viriam a produzir, cada vez mais, sistemas com níveis de segurança reais (observados quando em operação) abaixo dos níveis justificados pelo desenvolvedor e aceitos pela autoridade de segurança (certificador). Portanto, é um problema tanto para as autoridades de segurança (certificador e regulador) – responsáveis por zelar pela segurança dos envolvidos, sobretudo usuários e ambiente afetado pelo sistema – quanto para os desenvolvedores dos sistemas – onde, além da responsabilidade por perdas e danos produzidos por seus sistemas, devem manter equilíbrio entre a receita e os custos para garantir a segurança – avaliar e decidir se um sistema é seguro (incluindo a definição sobre o que pode ser considerado como aceitavelmente seguro), sobretudo os sistemas considerados complexos.

Casos de Segurança são utilizados como recurso em procedimentos de avaliação para demonstrar a segurança de um sistema. Casos de Segurança (do inglês, *Safety Cases*) vem sendo utilizado em processos de garantia de segurança – sobretudo em procedimentos de avaliação e tomada de decisão sobre o nível de segurança de um sistema para fins de certificação – para justificar, por meio de argumentações lógicas baseada em conjuntos de evidências obtidas por meio de testes, ensaios, análises, auditorias sobre processos, entre outros; que um sistema/produto atende a regulamentação pertinente, em especial aos requisitos de segurança, e, consequentemente, pode ser considerado (certificado) como seguro e apto a entrar em operação (KELLY, 2004). Em geral, o desenvolvedor do sistema é responsável pela elaboração dos Casos de Segurança e por sua apresentação às partes interessadas (ex.: autoridades certificadoras, operadores e/ou usuários finais).

A forma como um Caso de Segurança é elaborado, incluindo seu conteúdo, é dependente do domínio de aplicação no qual está inserido, sobretudo o tipo de regulamentação ao qual determinado sistema está submetido. Independentemente do tipo de regulamentação ao qual um sistema está submetido, a alegação principal na qual qualquer Caso de Segurança se baseia é que "*o sistema é (suficientemente) seguro*". Com isso, os desenvolvedores utilizam o Caso de Segurança como mecanismo documental para demonstrar (validar a *hipótese principal*), por meio de uma série de argumentações sobre um conjunto de evidências (sejam eles testes, ensaios, análises ou outro método pertinente), que sua alegação (hipótese) principal é válida e está correta.

Por analogia, e conforme apresentado por Kinnersly (2011), pode-se considerar um Caso

de Segurança como uma tese científica, onde o elaborador defende uma hipótese (a alegação de que "o sistema é seguro") e, utilizando uma diversidade de experimentos, observações, análises e demais métodos e processos, obtém evidências que, organizadas e apresentadas de forma lógica e estruturada, argumentam (corroboram) a favor da validade da hipótese. Por outro lado, a Teoria do Falseamento de Popper (POPPER, 1934) defende que uma teoria (hipótese) pode apenas ser falseada, nunca validada, com base em observações experimentais. Utilizando esta linha de raciocínio de Popper, pode-se concluir que um Caso de Segurança, por mais que esteja respaldado em evidências experimentais a favor da tese de que "*o sistema é seguro*", jamais conseguirá verificar e justificar que o sistema é realmente seguro. Estas evidências, no máximo, corroboram com a validade da tese defendida. Porém, ainda segundo Popper, basta uma única evidência (teste) que falsifique (rejeite) conclusivamente a tese para que ela seja considerada inválida e, no contexto aqui tratado, que o sistema não é seguro.

Desta forma, entende-se que submeter o conceito de Caso de Segurança à Teoria do Falseamento de Popper – elaborando evidências de insegurança (e ***Casos de Insegurança***) – é uma forma logicamente mais aceitável de lidar com o conceito de Caso de Segurança em processos de avaliação e certificação de segurança em sistemas de aplicação crítica, sobretudo quando as evidências utilizadas na sua construção são obtidas por métodos experimentais (testes, ensaios ou simulações). Além disso, com base na experiência profissional dos autores como avaliadores independentes de segurança crítica de sistemas, acredita-se que esta abordagem seja mais eficiente em um processo de avaliação independente e de certificação de segurança, cuja tarefa é contestar a tese apresentada (Caso de Segurança), e não atuar na corroboração das alegações (hipóteses) apresentadas pelo desenvolvedor.

Portanto, este trabalho propõe o uso de Casos de Insegurança (*Unsafety Cases*) – uma abordagem baseada em evidências de insegurança, método científico e a Teoria da Falseabilidade de Popper – como forma de complementar e aprimorar as atuais abordagens de avaliação e certificação de segurança crítica em sistemas de alto risco. A seção 1 introduziu e contextualizou a proposta. A seção 2 apresenta uma revisão não sistematizada da literatura a respeito do tema proposto. A seção 3 apresenta a proposta de utilização de casos de insegurança na avaliação e certificação de segurança de sistemas complexos. Por fim, a seção 0 faz considerações finais a respeito da proposta aqui apresentada.

2. REVISÃO DA LITERATURA

A aplicação do método científico (hipotético-dedutivo), onde hipóteses teóricas são formuladas e suas predições são testadas e desafiadas contra observações sistemáticas e experimentos controlados – ao conceito de Casos de Segurança foi previamente discutida por Kinnersly (2011). Kinnersly defende conceitualmente a aplicação do mesmo rigor científico à demonstração (garantia) da segurança de sistemas, mostrando, por analogia, que um Caso de Segurança tem a mesma estrutura de uma teoria científica. Contudo, o autor não propõe abordagem ou mesmo recomenda técnicas ou meios para sua aplicação.

Leveson (2011) reforça a especulação de que um caso de insegurança é mais produtivo (eficiente) do que um caso de segurança em um processo de garantia de segurança, dado que demonstrar insegurança (falsear a segurança) é mais viável que demonstrar a segurança. Leveson justifica, utilizando conceitos da psicologia como 'mindset' e 'confirmation bias', que "... it is always possible to find or produce evidence that something is safe. ... (cases) should focus not on showing that the system is safe". Além disso, Leveson apresenta exemplos da ineficiência de um avaliador independente confirmar argumentos produzidos por uma terceira parte. Contudo, assim como Kinnersly, Leveson não propõe abordagem nem mesmo recomenda técnicas ou meios para aplicação de Caso de Insegurança, atendo-se a discutir como a abordagem normativa influencia a garantia de segurança de sistemas.

Corroborando com os achados

preliminares de Vismari e Camargo Jr (2012), pesquisas vêm discutindo as limitações dos métodos tradicionais de engenharia para lidar com características de sistemas complexos. Pesquisas vêm sendo realizadas sobre a ciência da complexidade no contexto da engenharia de sistemas, sobretudo em como as características de sistemas complexos (como evolução, emergência, não linearidade, entre outras) devem ser abordadas no desenvolvimento de Sistemas de Sistemas (SoS) e de sistemas complexos (MALDONADO; GÓMEZ CRUZ, 2012).

Com isso, uma nova área da engenharia vem sendo constituída, com alcunhas como Engenharia de Sistemas Complexos (SHEARD; MOSTASHARI, 2009) ou Engenharia da Complexidade (FREI; SERUGENDO, 2011).

Recentemente, alguns autores vêm discutindo o impacto das características de complexidade sistêmica sobre a segurança de sistemas, tanto no desenvolvimento (LEVESON et al., 2009)(SOMMERVILLE et al., 2012) quanto na investigação de acidentes relacionados aos sistemas sócio-técnicos (DEKKER, 2011). Contudo, percebe-se que não há consenso quanto aos conceitos fundamentais relacionados à engenharia de sistemas complexos, em especial a relação entre as características de complexidade e de segurança além daquelas consolidadas por Perrow (1999), mostrando-se um campo de pesquisa promissor. Essa percepção é reforçada pela literatura recente e relevante na área da segurança, onde a fundamentação da ciência da segurança – antes mesmo da sua relação com a ciência ou a engenharia da complexidade – ainda é tema em discussão (LE COZE; PETTERSEN; REIMAN, 2014).

Por fim, pesquisas preliminares mostraram que a avaliação de segurança e certificação de sistemas complexos tem recebido pouco destaque, e com quase nenhuma profundidade, na literatura.

3. UTILIZANDO CASOS DE INSEGURANÇA NA AVALIAÇÃO E CERTIFICAÇÃO DE SISTEMAS COMPLEXOS

Com base nos resultados obtidos em Vismari e Carmargo Jr (2012), pôde-se notar que as Bases Normativas definem que a Avaliação e a Verificação e Validação (V&V) de sistemas críticos de segurança é responsabilidade tanto da Autoridade de Segurança e dos demais envolvido diretamente com os sistemas. Mas, a forma como as Bases Normativas são aplicadas e as responsabilidades por seus resultados são diferentes para cada um dos envolvidos (ilustrados na Figura 1):

- O Desenvolverdor é responsável pelo desenvolvimento de seus produtos, processos e sistemas, a fim de cumprir os requisitos definidos na Base Normativa. Ele deve justificar, apoiado por evidências produzidas pelas abordagens de avaliação de segurança e V&V definidas na Base Normativa, que os seus sistemas, processos e produtos cumprem as normas e são seguros. A documentação produzida como resultado dessas abordagens é comumente referida como Casos de Segurança (KELLY, 2004).
- A Autoridade de Segurança é responsável por avaliar e se certificar, com base nos Casos de Segurança, se Desenvolvedor cumpriu as normas e procedimentos definidos na Base Normativa e, portanto, seus processos, produtos e sistemas são seguros. Se a Autoridade de Segurança valida as evidências e aprova os casos de segurança, ela certifica que o processo, produto ou sistema em avaliação cumpre os requisitos definidos na Base Normativa, é seguro e, portanto, capaz de operar em seu domínio de aplicação. Além desta verificação de conformidade com base em evidências documentais, a autoridade de segurança pode complementar as evidências (casos) de segurança com novos ensaios e inspeções para, então, emitir a certificação.

A estrutura geral desta abordagem utilizada para identificar condições inseguras e para assegurar o nível de segurança dos produtos e sistemas críticos atuais é ilustrado na Figura 1. Como descrito acima, a identificação de condições inseguras é da responsabilidade do desenvolvedor, que aplica os métodos e processos de avaliação, verificação e validação de segurança definidos na Base Normativa e gera as evidências de segurança (Caso de Segurança) utilizada para

demonstrar que os sistemas desenvolvidos são seguros.

Conforme justificado em Vismari e Camargo Jr (2012), processos, métodos e técnicas definidas para a segurança de avaliação, verificação e validação abordagens na Base Normativa pode não ser eficiente para identificar condições de insegurança dos sistemas atuais. Isso possibilita que problemas permaneçam latente após o desenvolvimento e, assim, eventos inseguros podem ocorrer durante a operação do sistema. No entanto, uma vez que estes métodos e processos são reconhecidos e recomendados pela autoridade de segurança, os resultados obtidos por eles são aceitos e utilizados como evidências de segurança para demonstrar que um sistema é seguro.

Dado que a verificação de conformidade conduzida pela Autoridade de Segurança para a certificação se baseia tanto no Caso da Segurança (evidências e argumentos), produzido pelos desenvolvedores, e em testes e inspeções aplicadas pelo Autoridade de Segurança sobre eles, o processo de garantia de segurança pode estar produzindo **níveis de segurança certificados** maiores do que realmente serão apresentados durante sua operação em um ambiente real. Sobretudo devido o processo de garantia de segurança não ser capaz de identificar potenciais situações de perigo durante a fase de desenvolvimento e certificação.

Conforme apresentado anteriormente, Casos de Segurança são utilizados como insumos do processo de tomada de decisão sobre a abordagem de avaliação de segurança para determinar se o sistema é seguro. Casos de segurança são utilizados pelos desenvolvedores de sistema para demonstrar (documentar) a alegação (tese) – com base em argumentos apoiados por evidências (obtidos a partir de testes, ensaios, análises, auditorias e outros) – que sistema é seguro e capaz de ser colocado em operação. Em geral, o desenvolvedor do sistema é responsável tanto pela elaboração dos Casos de Segurança quanto por sua apresentação às partes interessadas (por exemplo, autoridade responsável pela segurança e certificador independente).

Assim, e por analogia, um Caso de Segurança pode ser considerado como uma teoria científica, onde seu elaborador apresenta uma hipótese (ex.: *o sistema é seguro*) e, usando uma variedade de experimentos, observações, análises e outros métodos e processos, obtém provas (evidências) que, organizadas e apresentadas de uma forma lógica e estruturada, argumentam (corroboram) a favor da validade da hipótese.

Por outro lado, a Teoria de Popper de Falsifiability (POPPER, 1934) argumenta que uma teoria (hipótese) só pode ser falsificada, e não validada, com base em **observações experimentais**. Segundo Popper, nunca será possível demonstrar (validar) a hipótese apresentada em um Caso de Segurança de que "*o sistema é seguro*", independentemente do tipo e quantidade evidências experimentais apresentadas a favor da hipótese. Evidências, no máximo, corroboram a validade da hipótese. No entanto, de acordo com Popper, apenas um único elemento de prova (teste) que falsifique (rejeite) conclusivamente a tese (hipótese) é suficiente para considerá-la inválida (neste caso, definir o sistema como inseguro).

Assim, a aplicação de Teoria da Falsifiability de Popper sobre o conceito de Casos de Segurança – através da produção de provas de insegurança (***Casos de Insegurança***) – é uma maneira logicamente mais aceitável de lidar com o conceito de casos de segurança nos processos de avaliação e certificação da segurança para sistemas críticos de alto risco, especialmente quando as provas utilizadas na sua construção são obtidas por métodos experimentais (ensaios, ensaios e simulações). Além disso, com base na experiência dos autores como avaliadores da segurança independentes (ISA) de sistemas críticos, entende-se que esta abordagem é mais eficiente no processo de avaliação de segurança independente e certificação, cuja tarefa é desafiar a tese apresentada pelo desenvolvedor (Caso de Segurança), e não agir na corroboração das suas alegações (hipóteses).

A aplicação do Método Científico – método hipotético-dedutivo, onde são formuladas hipóteses teóricas e suas predições são testadas e desafiadas contra observações sistemáticas e experimentos controlados – sobre o conceito de casos de segurança foi

previamente discutido por Kinnersly (2011). Kinnersly discute, conceitualmente dizendo, a aplicação do mesmo rigor científico para demonstrar (garantir) a segurança de um sistema. No entanto, o autor não propõe ou mesmo recomendar qualquer abordagem, técnica ou meio para a sua implementação.

Leveson (2011) dá força para a proposição de que a utilização de um **Caso de Insegurança** seria mais produtivo do que um Caso de Segurança em um processo de avaliação independente de segurança, dado que demonstrar insegurança do sistema (falsificar a segurança) é mais viável do demonstrar sua segurança. Leveson justifica, usando conceitos da psicologia como modelos mentais (*mindset*) e tendência a confirmação (*confirmation bias*), que "*... it is always possible to find or produce evidence that something is safe. ... [safety] cases should focus not on showing that the system is safe.*" (LEVESON, 2011). No entanto, assim como Kinnersly, Leveson não propõe qualquer abordagem ou técnica, ou mesmo recomendado meios para a sua aplicação, atendo-se apenas a discutir como as abordagens normativas afetam a garantia de segurança dos sistemas.

Este trabalho contribui com uma abordagem baseada em evidências de insegurança (e, consequentemente, em Casos de Insegurança) a ser utilizada para complementar as abordagens atuais de garantia de segurança, sobretudo análise independente e certificação, de sistemas complexos e críticos em segurança. A Figura 2 ilustra a abordagem proposta, destacando sua contribuição dentro da abordagem atual de garantia de segurança para domínios de aplicação de alto risco.

A proposta inicial deste trabalho é aplicar o método científico – método hipotético-dedutivo, onde hipóteses teóricas são formuladas e suas predições são testadas contra observações sistemáticas e experimentos controlados – ao conceito de Casos de Segurança, previamente discutido por Kinnersly (2011). Contudo, ao invés de desenvolver uma linha de argumentação para confirmar hipóteses, esta abordagem emprega a Teoria do Falseamento de Popper, onde o objetivo será o de refutar – e não o de confirmar – a(s) hipótese(s) apresentada(s) nos Casos de Segurança. Para isso, **testes de segurança** ou outras abordagens a serem desenvolvidas serão utilizados para gerar evidências de insegurança de forma independente àquelas utilizadas pelo desenvolvedor. Pretende-se identificar e utilizar características intrínsecas, relacionadas aos sistemas complexos, para orientar a forma de gerar as evidências.

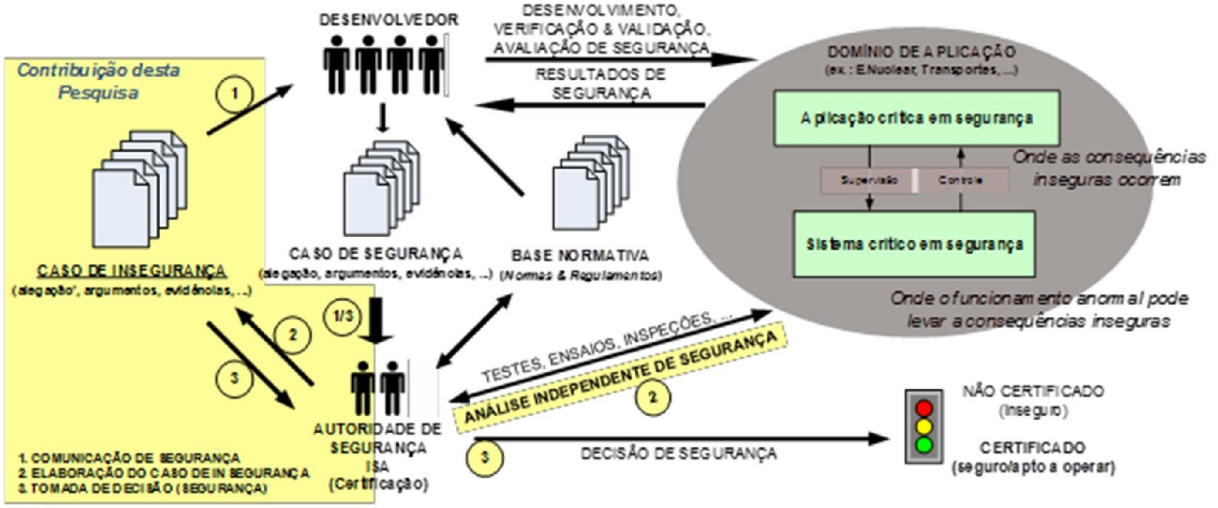


Figura 2 – Proposta de complemento, baseada em Casos de Insegurança, das abordagens atuais de garantia de segurança para domínios de aplicação de alto risco.

4. CONSIDERAÇÕES FINAIS

Este trabalho propôs uma abordagem baseada em evidências insegurança (e, consequentemente, em **Casos de Insegurança**) que complementa as abordagens atuais de avaliação e certificação da segurança. Esta proposta inicial consiste em aplicar o método científico (hipotético- dedutivo), onde são formuladas hipóteses teóricas e suas predições são testadas em observação sistemática e experimentos controlados, sobre o conceito de casos de segurança. No entanto, em vez de hipóteses confirmando (corroborando) os argumentos apresentados nos casos de segurança), esta proposta se respalda na Teoria da Falseabilidade de Popper, onde o objetivo é refutar (e não confirmar) a hipótese apresentada nos processos de segurança. A refutação será baseada em testes de insegurança – ou outras técnicas e métodos a serem investigados e desenvolvidos – para gerar evidências insegurança.

Com base em trabalho anterior (VISMARI; CAMARGO JUNIOR, 2012), foi apresentado o processo de garantia de segurança para sistemas críticos de segurança e seus principais pontos fracos. Com base em argumentos sobre os autores referenciados, a viabilidade da proposta apresentada foi justificada. Como próximos passos, será desenvolvido os detalhes da abordagem metodológica apresentada. Vale ressaltar que as questões a serem investigadas e a abordagem a ser desenvolvido tem o potencial de ser aplicado nos processos de certificação e de garantia de segurança de diversas áreas de aplicação críticas, tais como a automotiva, metroferroviária, aeroespacial e nuclear.

Além disso, este trabalho pode vir a contribuir com a disciplina de Engenharia de Segurança de Sistemas. Neste caso, sua relevância para a engenharia de segurança é a evolução das fundações e estrutura metodológica relacionados com a engenharia de segurança de sistemas complexos que, segundo pesquisas bibliográficas, é uma área inexistente da engenharia, sobretudo devido o tema „sistemas complexos“ estar em estado embrionário na engenharia.

5. REFERÊNCIAS

ALMEIDA JR, J. R. **Segurança em Sistemas Críticos e em Sistemas de Informação – Um Estudo Comparativo**. [s.l.] Escola Politécnica da USP, 2003.

DEKKER, S. The criminalization of human error in aviation and healthcare: A review. **Safety Science**, v. 49, n. 2, p. 121–127, fev. 2011.

FREI, R.; SERUGENDO, G. D. M. Concepts in complexity engineering. **International Journal of Bio-Inspired Computation**, v. 3, n. 2, p. 123, 2011.

KELLY, T. Defining the safety-case concept. **Safety Systems**, v. 14, n. 1, 2004.

KINNERSLY, S. Safety Cases - what can we learn from Science? In: DALE, C.; ANDERSON, T. (Eds.). . **Advances in Systems Safety**. [s.l.] Springer London, 2011. p. 25–40.

LE COZE, J.-C.; PETTERSEN, K.; REIMAN, T. The foundations of safety science. **Safety Science**, v. 67, p. 1–5, ago. 2014.

LEVESON, N. et al. Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems. **Organization Studies**, v. 30, n. 2-3, p. 227–249, 1 fev. 2009.

LEVESON, N. The Use of Safety Cases in Certification and Regulation. **Journal of System Safety (eEdition)**, v. 47, n. 6, p. 13–25, 2011.

MALDONADO, C. E.; GÓMEZ CRUZ, N. A. The complexification of engineering. **Complexity**, v. 17, n. 4, p. 8–15, 19 mar. 2012.

PERROW, C. **Normal Accidents: Living with High-Risk Technologies [Paperback]**. [s.l.] Princeton University Press; Updated Edition edition, 1999.

POPPER, K. **The Logic of Scientific Discovery**. [s.l: s.n.].

SHEARD, S. A.; MOSTASHARI, A. Principles of complex systems for systems engineering. **Systems Engineering**, v. 12, n. 4, p. 295–311, set. 2009.

SOMMERVILLE, I. **SOFTWARE ENGINEERING**. 9th. ed. [s.l.] Addison-Wesley, 2011.

SOMMERVILLE, I. et al. Large-scale complex IT systems. **Communications of the ACM**, v. 55, n. 7, p. 71, 1 jul. 2012.

VISMARI, L. F.; CAMARGO JUNIOR, J. B. **Safety assurance in complex engineered systems: could the current safety standards and regulations be doing our critical systems more unsafe?**II Brazilian Conference on Critical Embedded Systems (CBSEC) - Student Workshop. **Anais**...Campinas, Brazil: 2012