Uma Abordagem para Alinhamento de Requisitos de Segurança e Proteção de Sistemas IoT Críticos

Ernesto Fonseca Veiga[1]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)
Goiânia – GO – Brazil

ernestoveiga@ufg.br

Abstract. *The complexity and heterogeneity of IoT systems have given rise to new challenges in the Requirements Engineering (RE) process, such as the joint treatment of security and protection requirements, essential in most of these systems, especially those considered critical. Given the lack of studies that meet this objective, this work presents a proposal for an approach to align security and protection requirements of critical IoT systems, which aims to reduce the complexity of carrying out the RE process for engineers and developers of these systems.*

Resumo. *A complexidade e heterogeneidade dos sistemas IoT tem dado origem a novos desafios no processo de Engenharia de Requisitos (ER), como o tratamento conjunto de requisitos de segurança e proteção, essenciais em grande parte destes sistemas, principalmente aqueles considerados críticos. Diante da carência de estudos que atendam esse objetivo, este trabalho apresenta uma proposta de abordagem para alinhamento de requisitos de segurança e proteção de sistemas IoT críticos, que visa reduzir a complexidade na realização do processo de ER para engenheiros e desenvolvedores destes sistemas.*

1. Introdução

A crescente integração entre infraestruturas de software, hardware e comunicação atribui novas preocupações e características específicas aos sistemas de Internet das Coisas (IoT) e Ciberfísicos (CPS)[1]. Estes sistemas são considerados complexos em várias dimensões, pois operam em ambientes dinâmicos, com alta heterogeneidade de dispositivos e de comunicação [Nguyen-Duc et al. 2019]. Enquanto essa complexidade dos sistemas IoT está aumentando constantemente, o processo de Engenharia de Requisitos (ER) que compreende a descoberta, análise, documentação e validação dos seus serviços e restrições, torna-se também cada vez mais difícil e desempenha um papel fundamental no projeto e desenvolvimento desses sistemas [Binder et al. 2021, Fritz et al. 2019].

Com o objetivo de exemplificar essas características em um domínio de aplicação, e melhorar o entendimento da problemática que será tratada neste trabalho, adotemos o seguinte cenário ilustrativo no domínio de veículos autônomos (VAs):

[1]Os termos "Internet das Coisas" (IoT) e "Sistemas Ciberfísicos" (CPS) têm origens distintas, mas definições sobrepostas, ambas se referindo a tendências na integração de capacidades digitais, incluindo conectividade de rede e capacidade computacional, com dispositivos e sistemas físicos [Greer et al. 2019]. Neste trabalho consideramos o entendimento de equivalência entre IoT e CPS. Por este motivo, para simplificar o texto, padronizamos a sigla IoT como referência aos dois termos.

VAs possuem grande quantidade de sensores, de diferentes tipos, responsáveis pelas entradas de dados no sistema, tais como radares, sonares, sensores de detecção de luz e alcance, GPS, acelerômetro, câmeras, dentre outros. Esses dados são essenciais, pois é a partir do seu processamento em tempo-real que o VA pode entender o contexto e o ambiente em que se encontra para tomar decisões. Além disso, ele controla uma série de atuadores responsáveis por mecanismos como aceleração, frenagem e direção, usados para realizar ações orquestradas de acordo com os dados lidos e processados (ex.: acelerar, manter-se na faixa correta e parar). Em muitos casos, um VA pode também interagir com outros veículos, sistemas e mesmo com pessoas e o próprio ambiente. Esse sistema atua de maneira intensa durante todo o período que o VA estiver em operação, para simplesmente se deslocar com segurança no trânsito, o que mostra sua complexidade. Qualquer decisão equivocada pode colocar em risco as pessoas e o ambiente, neste caso o trânsito, que é altamente dinâmico. Dessa forma, esses sistemas precisam lidar com a alta heterogeneidade de componentes e ambientes dinâmicos desde a sua concepção, o que reflete diretamente na complexidade do processo de ER.

Neste contexto, como primeiro passo desta pesquisa na investigação do processo de ER para sistemas IoT, foi conduzido um mapeamento sistemático da literatura (MSL), cujos resultados preliminares podem ser analisados em [Veiga and Bulcão-Neto 2022][2]. O estudo realizado seguiu um protocolo desenvolvido juntamente com especialistas em ER com objetivo de permitir a identificação das principais tendências, práticas (métodos e técnicas), nível de maturidade e contribuições dos estudos, além de questões em aberto no estado da arte de ER para sistemas IoT.

Buscando identificar lacunas de pesquisa quanto à ER desses sistemas, uma das informações extraídas foi o tipo de requisito abordado em cada estudo revisado. A análise desses dados revelou uma forte preocupação desses sistemas com requisitos de proteção (*security*[3]) e também a necessidade de que estes sejam projetados e operados sob uma visão de alinhamento com segurança (*safety*) [Wolf and Serpanos 2018]. Neste contexto, segurança é "a capacidade do sistema de operar sem falhas que possam causar danos a pessoas ou ao seu ambiente" enquanto proteção é definida como "a capacidade do sistema em se proteger contra intrusão acidental ou deliberada", destacando a sua relação com as questões de segurança da informação e privacidade [Avizienis et al. 2004].

Complementando o cenário apresentado, podemos citar alguns exemplos de requisitos de segurança e proteção (em alto nível) para os sistemas de VAs:

Requisitos de segurança: *a redundância de sistemas de hardware e software (garantir que, em caso de falha de um componente, o VA continue operando com segurança); e a detecção e prevenção de colisões (sensores devem detectar e prever colisões com outros veículos, objetos ou pedestres).*

Requisitos de proteção: *o controle de acesso (sistemas de VAs devem ter protocolos robustos de autenticação para garantir que apenas pessoas autorizadas possam acessar e controlar o veículo); e proteção contra ataques (tanto de hackers quanto de sistemas maliciosos que possam comprometer a segurança do veículo, passageiros e pedestres).*

Requisito que implica diretamente na segurança e na proteção*: a verificação de integridade (VAs devem monitorar constantemente a integridade do software e dos dados processados de modo a detectar eventuais falhas ou ataques).*

[2]Disponível em: `https://bityli.com/hI2mel`

[3]Na literatura também é encontrada a expressão "segurança da informação" como tradução para *security*. Adotaremos o termo "proteção" no intuito de facilitar a separação entre as traduções de *security* e *safety*.

Historicamente, os esforços em segurança e proteção surgiram de comunidades distintas e eram considerados de maneira independente. Entretanto, a integração de software e hardware para criar esses tipos de sistemas abriu uma vasta gama de problemas que exigem o tratamento conjunto desses requisitos [Wolf and Serpanos 2018]. Por exemplo, o ataque que viole a proteção de um sistema IoT pode gerar também ameaças à sua segurança, produzindo ações inesperadas ou fora de controle, que causem danos a pessoas ou ao ambiente com o qual o sistema interage.

Dessa forma, tratar as relações existentes entre segurança e proteção tem se tornando essencial em sistemas IoT complexos, que não podem ser considerados seguros se não forem também protegidos, como é o caso dos automóveis autônomos, veículos aéreos não tripulados, dentre outros [Mailloux et al. 2019]. Além disso, o tratamento desses requisitos é imprescindível em sistemas considerados críticos, que são aqueles cujas falhas podem levar a ferimentos ou morte de pessoas, danos ao ambiente, divulgação de informações não autorizadas e perdas financeiras graves [Sommerville 2015].

1.1. Problema

O estudo de [Kavallieratos et al. 2020] destaca que uma combinação fraca dos requisitos de segurança e proteção pode resultar no projeto e desenvolvimento insatisfatórios de um sistema e, possivelmente, em danos ao ecossistema IoT. Neste sentido, [Sadvandi et al. 2012] citam ainda que diversos problemas metodológicos podem surgir de processos de segurança e proteção desconectados, tais como: i) multiplicidade e inconsistências de concepção e projeto, devido ao tratamento independente dessas disciplinas, muitas vezes realizado por diferentes equipes, para o mesmo sistema; e ii) atividades de análise redundantes, devido ao uso de vocabulários distintos para as mesmas tarefas.

A revisão conduzida por [Lisova et al. 2019] reforça essa visão, identificando que segurança e proteção podem influenciar negativamente uma à outra. Portanto, analisar sua interação de maneira eficiente significa reduzir o esforço que precisa ser investido para alcançar um sistema seguro e protegido. Os resultados da pesquisa também ressaltam a necessidade de mais esforços em abordagens de co-análise desses requisitos em todas as áreas de aplicação e também na sua avaliação.

A análise conjunta de segurança e proteção envolve ainda importantes relações que podem surgir entre estes requisitos e devem ser consideradas. [Pièrre-Cambacédès 2010] resume as interações entre segurança e proteção em quatro tipos: i) *dependência condicional*, quando o cumprimento dos requisitos de segurança condiciona o nível de proteção ou vice-versa (proteção condiciona a segurança); ii) *reforço mútuo*, quando medidas tomadas para fins de segurança também contribuem para a proteção ou vice-versa (proteção contribui para a segurança); iii) *antagonismo*, quando os requisitos de segurança e proteção, considerados em conjunto, levam a situações conflitantes; e iv) *independência*, quando não há interação entre os requisitos de segurança e proteção. Por exemplo:

> ***Dependência condicional**: [ameaça à proteção] após explorar com sucesso uma vulnerabilidade do sistema de entretenimento do VA, um usuário não autorizado acessa indevidamente o sistema; [risco à segurança] o atacante pode causar ameaças de interrupção, tornando parte do sistema indisponível, ou de alteração, modificando algum ativo do sistema; [consequência da relação] o ataque a uma vulnerabilidade do VA pode causar o seu mau funcionamento e possíveis riscos aos seus ocupantes e ao trânsito.*

***Reforço mútuo**: [requisito de proteção] o sistema de um VA precisa ser capaz de detectar e registrar ataques realizados por sistemas externos; [requisito de segurança] o VA precisa detectar e registrar possíveis situações de falha para evitar acidentes e se antecipar a situações de perigo; [consequência da relação] o registro e tratamento de eventos e atividades em um VA é um requisito necessário tanto aos componentes de segurança quanto de proteção, reforçando-se entre eles.*

***Antagonismo**: [ameaça à proteção e risco à segurança acontecendo simultaneamente] em caso de um ataque externo, o sistema de proteção do VA mantém todas as portas trancadas para evitar um possível furto do veículo ou dos pertences dentro dele; porém, se durante esse ataque o VA estiver se deslocando e for detectada uma colisão, ou outro tipo de acidente com risco aos passageiros, o veículo deve manter as portas destrancadas para facilitar a saída ou resgate dos seus ocupantes; [consequência da relação] há um conflito entre os requisitos de segurança e proteção, ameaçando o funcionamento correto do sistema.*

Com base nos desafios identificados por [Pièrre-Cambacédès 2010, Lisova et al. 2019], o problema de pesquisa a ser investigado nesta proposta é a *carência de abordagens de ER que auxiliem as atividades de análise e especificação dos requisitos de segurança e proteção para sistemas IoT críticos, e permitam o tratamento das interações existentes entre estes requisitos desde a sua concepção*.

1.2. Questão de Pesquisa e Objetivos

Dado o problema apresentado, este trabalho visa responder a seguinte questão de pesquisa: "é possível definir uma abordagem de ER voltada à análise e especificação das interações de requisitos de segurança e proteção para sistemas IoT críticos?".

Assim, o objetivo geral desta pesquisa de doutorado é produzir uma abordagem de ER que contemple as atividades de análise e especificação das interações entre requisitos de segurança e proteção para sistemas IoT críticos. Para tal, definem-se como objetivos específicos deste trabalho: i) definir técnica e artefato de análise conjunta de requisitos de segurança e proteção, conforme os tipos de interações entre esses requisitos; ii) definir técnica e artefato de especificação de requisitos que documente o alinhamento entre requisitos de segurança e proteção; e iii) experimentar e avaliar a abordagem de análise e especificação elaboradas em i e ii com exemplos de sistemas IoT críticos.

2. Procedimentos Metodológicos

Essa pesquisa de doutorado está dividida em 4 fases subsequentes, que são apresentadas na Figura 1, a saber: 1) informativa, 2) analítica, 3) proposicional e 4) avaliativa.

No intuito de aprofundar a análise dos resultados do MSL conduzido na fase informativa desta pesquisa por [Veiga and Bulcão-Neto 2022], foi aplicado o método de Síntese Temática, com base em [Dixon-Woods et al. 2005], que contribuiu para consolidar as evidências encontradas, por meio de análise qualitativa dos dados extraídos dos estudos mapeados. Foi identificada grande preocupação com requisitos não funcionais (RNFs), onde segurança e proteção predominam como os mais importantes no processo ER de sistemas IoT, mas ainda com poucos trabalhos que os tratam de forma integrada.

No momento desta publicação o trabalho se encontra no estágio final da fase analítica, com o estudo das abordagens existentes para co-análise de requisitos de segurança e proteção. Para compreender o estado da arte sobre ER de segurança e proteção de sistemas IoT e identificar lacunas existentes, encontra-se em andamento uma revisão sistemática da literatura (RSL). Esse trabalho de revisão tem como ponto de partida uma busca empregando a técnica de *snowballing forward* [Wohlin 2014] a partir dos

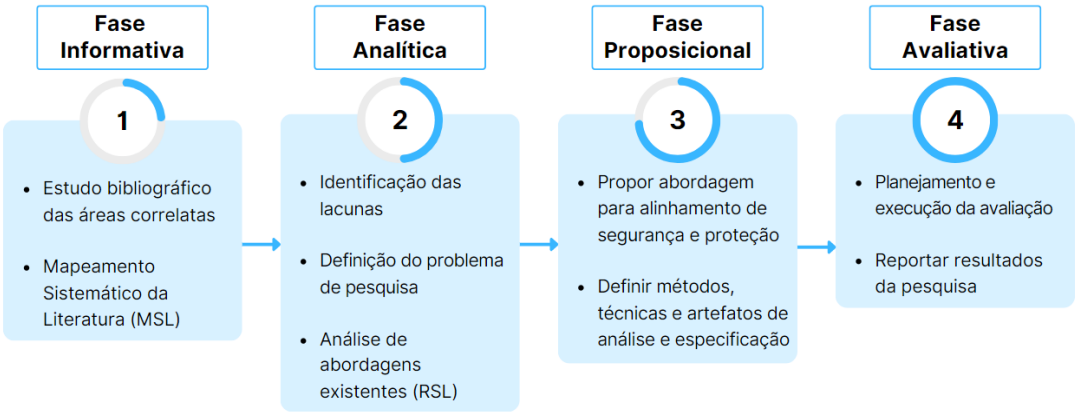

Figura 1. Fases da pesquisa de doutoramento.

14 estudos iniciais (analisados no MSL, que tem como foco principal os requisitos de segurança e/ou proteção). Essa busca identificou 142 novos trabalhos, dos quais 36 foram selecionados como relevantes para a extração de dados, que se encontra em andamento.

A partir dessa RSL serão melhor definidas as atividades de ER a serem tratadas por esta pesquisa, bem como o tipo de abordagem a ser realizada. Até o momento foram identificados gargalos quanto as etapas de análise[4] e especificação destes requisitos. Muitas das abordagens propostas, analisadas até o momento, não realizam um processo de análise abrangente [Japs 2020] ou são dependentes de domínio [Kavallieratos et al. 2020], e ainda trazem poucos resultados práticos em relação à especificação conjunta dos requisitos de segurança e proteção [Japs 2020, Kavallieratos et al. 2020], que servirá como base para o projeto e desenvolvimento de sistemas IoT críticos.

A proposta desse trabalho, a ser detalhada na fase proposicional, deverá cobrir as lacunas identificadas na RSL, de modo a contribuir tanto para a evolução acadêmica da área, como também para os seus praticantes, visando reduzir a complexidade do trabalhos de engenheiros de software e desenvolvedores que precisam lidar com requisitos de segurança e proteção em sistemas IoT críticos. Por fim, as metodologias de experimentação que serão aplicadas na fase avaliativa da pesquisa serão analisadas e definidas posteriormente, de acordo com a abordagem proposta para o processo de ER.

3. Proposta de Solução

De modo geral, os requisitos de segurança enfatizam o desencadeamento acidental de perigos que podem infingir danos às pessoas, enquanto os requisitos de proteção se preocupam com a natureza maliciosa de ataques e ameaças que levam a impactos negativos sobre os ativos de um sistema [Asplund et al. 2019]. A relação entre segurança e proteção vem da sobreposição entre essas perspectivas, por exemplo, quando danos são infligidos a pessoas como parte de um ataque ou como efeito colateral acidental do mesmo. Compreender essas relações é muito importante para sistemas IoT críticos, uma vez que eles permitem a interação com processos físicos por meio de sistemas e software [Wolf and Serpanos 2018, Mailloux et al. 2019]. Entretanto, conforme discutido por meio do cenário da Seção 1, a complexidade destes sistemas torna desafiador o seu processo de ER, exigindo o desenvolvimento e avaliação de novas abordagens.

[4] Alguns dos estudos sobre segurança e proteção incluem elicitação como parte das atividades de análise.

Os resultados do MSL mostraram apenas dois estudos consideraram a integração de requisitos de segurança e proteção para sistemas IoT [Japs 2020, Kavallieratos et al. 2020]. A análise preliminar da RSL mostra um crescimento significativo dessa preocupação, com 9 estudos publicados entre 2021 e 2022, que consideram algum tipo de relação entre estes requisitos. Entretanto, como uma área de pesquisa recente e em desenvolvimento, ainda não existem métodos e técnicas consolidadas para a realização das tarefas necessárias, o que leva muitos destes estudos a adaptarem ou reutilizarem conhecimentos da engenharia de segurança/proteção e novos processos experimentais para as atividades de ER.

A partir da análise de estudos recentes (MSL e RSL em andamento) pudemos identificar lacunas e limitações quanto as atividades de análise e principalmente especificação conjunta de requisitos de segurança e proteção. Grande parte dos estudos ainda não realiza um processo de análise abrangente levando em consideração os diferentes tipos de relações e impacto mútuo entre segurança e proteção destacados por [Pièrre-Cambacédès 2010, Lisova et al. 2019]. Esse cenário se agrava quanto à especificação, que é ainda menos explorada por esses estudos.

Buscando avançar o estado da arte e da prática nessa área de pesquisa, a proposta de solução deste trabalho de doutorado consiste na definição e avaliação de uma abordagem sistemática, bem como dos artefatos necessários, para a realização de uma análise abrangente e a produção da especificação de requisitos de segurança e proteção de sistemas IoT críticos, que possa ser aplicada a diferentes subdomínios. No momento atual da pesquisa estão sendo investigados métodos e técnicas que possam contribuir para o desenvolvimento da abordagem proposta. Nesse ponto existe o desafio de alinhamento das diferentes perspectivas relacionadas a este objetivo, uma vez que precisam ser levadas em consideração tanto as preocupações das atividades de ER quanto as necessidades específicas de engenharia de proteção e segurança, no contexto de sistemas IoT críticos.

Diferentes caminhos para condução dessa abordagem tem sido considerados, buscando avaliar os seus benefícios e limitações. Os estudos analisados apontam diferentes tipos de abordagens de especificação para requisitos de proteção, por exemplo, que podem ser adotados de acordo com as necessidades específicas do projeto ou da complexidade sistema, como os modelos formais, amplamente adotados para sistemas críticos.

4. Trabalhos Relacionados

Com foco nos requisitos de proteção, [Hofbauer et al. 2019] apresentam uma abordagem para criação de aplicações seguras onde definem-se os requisitos e controles, que formam um catálogo referente a um caso de uso de acesso remoto da Indústria 4.0. A abordagem, entretanto, não explora a interseção com requisitos de segurança que podem ser afetados neste domínio. Ainda neste contexto, o trabalho de [Hansch et al. 2019] evidencia que a arquitetura de comunicação de sistemas de Internet das Coisas Industrial (IIoT) apresenta sérios desafios de proteção, especialmente na comunicação entre máquinas, locais de produção e produtos inteligentes. Ataques e falhas nestes sistemas mostram que é necessária uma ER de proteção rigorosa para atender ao cenário de ameaças cada vez maior e em rápida evolução, porém, o estudo não aborda a relação com requisitos de segurança.

O trabalho de [Japs 2020], cujo grupo de pesquisa possui estudos correlatos na RSL, cobrem as atividades de elicitação e análise de requisitos de segurança e proteção,

com ênfase para a necessidade de uma cooperação eficiente entre *stakeholders* e propondo uma abordagem baseada em modelos para a identificação dos requisitos. Entretanto as contribuições ainda são limitadas quanto a análise das relações entre esses requisitos e não cobrem a sua especificação. A segunda abordagem que trata a segurança e proteção no contexto do MSL realizado, é o método SafeSec Tropos, proposto no estudo de [Kavallieratos et al. 2020], e adotado nos estudos correlatos do grupo, que tem como objetivo facilitar a análise conjunta de requisitos de segurança e proteção, modelando o sistema para ambos os propósitos e identificando potenciais conflitos entre os requisitos. Apesar de propor um método de análise mais robusto, a abordagem é dependente de domínio e não contempla como a especificação destes requisitos pode ser realizada.

A proposta apresentada neste artigo visa explorar as lacunas de pesquisa existentes quanto à análise das diferentes relações entre requisitos de proteção e segurança para diferentes domínios de sistemas IoT críticos e também a sua especificação.

5. Contribuições Esperadas

Ao final dessa pesquisa espera-se alcançar como contribuições: i) uma abordagem de ER para sistemas IoT críticos que permita o alinhamento de requisitos de proteção e segurança; e ii) modelos de artefatos para análise e especificação de segurança e proteção para sistemas IoT críticos, que permitam o tratamento das diferentes relações entre estes requisitos, incluindo a identificação e resolução de conflitos, desde a etapa inicial de projeto destes sistemas. Como contribuição parcial desta pesquisa foi publicado um mapeamento sistemático da literatura que investiga o processo de ER de sistemas IoT/CPS [Veiga and Bulcão-Neto 2022] e apresenta um panorama geral sobre o estado da arte e da prática, identificando tendências, problemas e lacunas de pesquisa. Esse estudo está sendo complementado através de uma RSL (descrita na Seção 2), cujos resultados deverão ser submetidos para publicação em congresso da área ou revista especializada.

6. Conclusões e Trabalhos Futuros

Foi apresentada neste trabalho uma proposta de abordagem para alinhamento de requisitos de segurança e proteção de sistemas IoT críticos com apoio aos diferentes tipos de relações entre estes requisitos. Essa proposta é embasada nos resultados de um MSL conduzido no início do doutoramento e em uma RSL em andamento, cujas lacunas de pesquisa identificadas apontam a necessidade de tratamento conjunto dos requisitos de segurança e proteção, ainda pouco explorada no contexto de sistemas IoT críticos.

O trabalho encontra-se andamento, em fase de investigação de abordagens que contribuam para a co-análise análise e especificação conjunta de requisitos e segurança e proteção para sistemas IoT críticos. Após a definição da abordagem, pretende-se verificar a possibilidade de aplicação desta pesquisa para validação e avaliação em projetos do Centro de Excelência em Inteligência Artificial[5] (CEIA), que atualmente desenvolve projetos voltados para sistemas IoT críticos em diferentes subdomínios de aplicação.

Esta pesquisa está sendo realizada no contexto de um trabalho de doutorado que teve início em março de 2021 e possui data prevista de conclusão para março de 2025.

[5]https://ceia.ufg.br/

Referências

Asplund, F., McDermid, J., Oates, R., and Roberts, J. (2019). Rapid Integration of CPS Security and Safety. *IEEE Embedded Systems Letters*, 11(4):111–114.

Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, pages 11–33.

Binder, C., Polanec, K., Brankovic, B., Neureiter, C., Lastro, G., and Lüder, A. (2021). Enabling Model-Based Requirements Engineering in a Complex Industrial System of Systems Environment. In *2021 26th IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA)*, page 1–6. IEEE Press.

Dixon-Woods, M., Agarwal, S., Jones, D., Young, B., and Sutton, A. (2005). Synthesising qualitative and quantitative evidence: a review of possible methods. *Journal of health services research & policy*, 10(1):45–53.

Fritz, S., Weber, F., and Ovtcharova, J. (2019). A Guideline for the Requirements Engineering Process of SMEs Regarding to the Development of CPS. In *2019 8th International Conference on Industrial Technology and Management (ICITM)*, pages 85–94.

Greer, C., Burns, M., Wollman, D., and Griffor, E. (2019). Cyber-Physical Systems and Internet of Things.

Hansch, G., Schneider, P., Fischer, K., and Böttinger, K. (2019). A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications. In *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 325–332.

Hofbauer, D., Ivkic, I., Maksuti, S., Aldrian, A., and Tauber, M. (2019). On the Cost of Security Compliance in Information Systems. *CoRR*, abs/1905.06122.

Japs, S. (2020). Security & Safety by Model-based Requirements Engineering. In *2020 IEEE 28th International Requirements Engineering Conference (RE)*, pages 422–427.

Kavallieratos, G., Katsikas, S., and Gkioulos, V. (2020). SafeSec Tropos: Joint security and safety requirements elicitation. *Computer Standards & Interfaces*, 70:103429.

Lisova, E., Šljivo, I., and Čaušević, A. (2019). Safety and Security Co-Analyses: A Systematic Literature Review. *IEEE Systems Journal*, 13(3):2189–2200.

Mailloux, L. O., Span, M., Mills, R. F., and Young, W. (2019). A Top Down Approach for Eliciting Systems Security Requirements for a Notional Autonomous Space System. In *2019 IEEE International Systems Conference (SysCon)*, pages 1–7.

Nguyen-Duc, A., Khalid, K., Shahid Bajwa, S., and Lønnestad, T. (2019). Minimum Viable Products for Internet of Things Applications: Common Pitfalls and Practices. *Future Internet*, 11(2).

Pièrre-Cambacédès, L. (2010). *Des relations entre sûreté et sécurité*. PhD thesis, Télécom ParisTech.

Sadvandi, S., Chapon, N., and Pièrre-Cambacédès, L. (2012). Safety and Security Interdependencies in Complex Systems and SoS: Challenges and Perspectives. In *Complex Systems Design & Management*, pages 229–241, Berlin, Heidelberg. Springer Berlin Heidelberg.

Sommerville, I. (2015). *Software Engineering*. Pearson, 10th edition.

Veiga, E. F. and Bulcão-Neto, R. F. (2022). Engenharia de Requisitos de Sistemas IoT e Ciber-Físicos: Resultados Preliminares. In *Anais do WER22 - Workshop em Engenharia de Requisitos*, page 1–14.

Wohlin, C. (2014). Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. In *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, EASE '14, New York, NY, USA. Association for Computing Machinery.

Wolf, M. and Serpanos, D. (2018). Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. *Proceedings of the IEEE*, 106(1):9–20.