Universidade FUMEC
Faculdade de Ciências Empresariais - FACE
Doutorado em Sistemas de Informação e Gestão do Conhecimento

Avaliação de segurança cibernética no desenvolvimento de software embarcado automotivo: uma abordagem ontológica

Mauricio Vianna de Rezende

Belo Horizonte
2020

Mauricio Vianna de Rezende

Avaliação de segurança cibernética no desenvolvimento de software embarcado automotivo: uma abordagem ontológica

Tese apresentada ao Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC como requisito para a obtenção do título de doutor

Orientador: Prof. Dr. Rodrigo Moreno Marques

Belo Horizonte

2020

Dados Internacionais de Catalogação na Publicação (CIP)

R467a Rezende, Mauricio Vianna de, 1970-

Avaliação de segurança cibernética no desenvolvimento de software embarcado automotivo: uma abordagem ontológica / Mauricio Vianna de Rezende. - Belo Horizonte, 2020.

135 f.: il.; 29,7 cm

Orientador: Rodrigo Moreno Marques

Tese (Doutorado em Sistemas de Informação e Gestão do Conhecimento), Universidade FUMEC, Faculdade de Ciências Empresariais, Belo Horizonte, 2020.

1. Software - Desenvolvimento. 2. Internet das coisas. 3. Cibernética. 4. Ontologia. I. Título. II. Marques, Rodrigo Moreno. III. Universidade FUMEC, Faculdade de Ciências Empresariais.

CDU: 681.5

Ficha catalográfica elaborada pela Biblioteca Universitária-FUMEC

FUMEC

Tese intitulada **"Avaliação de segurança cibernética no desenvolvimento de software embarcado automotivo: uma abordagem ontológica"**, de autoria do doutorando ***Maurício Vianna Rezende*** aprovado pela banca examinadora constituída pelos seguintes professores:

Prof. Dr. Rodrigo Moreno Marques - Universidade FUMEC
(Orientador)

Prof. Dr. Fernando Silva Parreiras – Universidade FUMEC

Prof. Dr. Luiz Cláudio Gomes Maia - Universidade FUMEC

Prof. Dr. Marcello Peixoto Bax – UFMG

Prof. Dr. Maurício Barcellos Almeida - UFMG

Prof. Dr. Fernando Silva Parreiras
Coordenador do Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento da Universidade FUMEC

Belo Horizonte, 14 de fevereiro de 2020.

CAMPUS
Rua Cobre, 200 - Cruzeiro
30310-190 - Belo Horizonte, MG
Tel. (31) 3228-3000
www.fumec.br

Agradecimentos

À minha esposa Maria Lúcia e aos meus filhos Lucas e Thiago, pela paciência e carinho.

Aos Profs. Drs. Fernando Silva Parreiras, Rodrigo Moreno Marques, Maurício Barcellos Almeida, Marcelo Peixoto Bax, Luiz Cláudio Gomes Maia, Marta Kerr Pinheiro e Ana Maria Pereira Cardoso pela inestimável contribuição neste trabalho e paciência.

Aos colegas da FCA que me suportaram desde o início nesta empreitada, pelo tempo dedicado nas discussões e nos grupos focais.

Resumo

A cibersegurança de dispositivos IoT (*Internet of Things*) é uma questão que preocupa desenvolvedores de software e deve ser avaliada durante todo o ciclo de vida do dispositivo para reduzir ameaças e riscos. Um dos mais importantes aspectos da IoT é a própria heterogeneidade das soluções de suas conexões com a internet e as ameaças a que estes sistemas estão expostos. Portanto, proteções em cibersegurança ganham destaque tanto no âmbito dos sistemas legados como dos novos sistemas. CPS (*Cyber-physical systems*) utilizam sensores e atuadores como forma de controlar sistemas do mundo real e trouxeram novos desafios para a IoT. Ataques cibernéticos contra estes dispositivos podem trazer severos danos quando os CPS estão integrados às redes de comunicação e à Internet. Neste contexto, a exemplo do automóvel que emprega CPS para controle de elementos do veículo, uma ameaça cibernética a esses dispositivos pode ter como consequência desde uma parada do veículo até a perda do controle da direção. O ciclo de vida de um CPS automotivo é de algumas dezenas de anos, o que significa que estes dispositivos devem resistir às ameaças cibernéticas atuais e também ser suficientemente flexíveis para se adaptar e evoluir ao longo dos anos, oferecendo proteção contra os ataques cibernéticos durante todo o ciclo de vida. Nesse contexto, uma ontologia que expresse o conhecimento do domínio automotivo e da segurança cibernética aí envolvida pode suportar os desenvolvedores de softwares embarcados no processo de avaliação da cibersegurança de CPS. Este trabalho apresenta a utilização do *framework* da norma SAEJ3061 de avaliação em cibersegurança em softwares embarcados de CPS automotivos por meio de uma abordagem ontológica. O objetivo geral desta pesquisa foi investigar a eficácia da avaliação da cibersegurança por meio de uma ontologia. Nesse sentido, construímos uma ontologia de domínio voltada para cibersegurança (*AutomotiveCyberSecurity*), utilizando o método *OntoforInfoScience*. Durante o processo de desenvolvimento da ontologia, utilizamos o suporte e a validação dos especialistas em cibersegurança da FCA (Fiat Chrysler Automobiles). O resultado deste trabalho foi o maior aproveitamento do relatório de cibersegurança pelos desenvolvedores de CPS automotivo em razão de um maior entendimento sobre as ameaças e os ataques aos CPS.

Palavras-chaves: Segurança Cibernética em IoT; Avaliação em Segurança Cibernética; Ontologia; OntoforInfoScience; SAEJ3061.

Abstract

Internet of Things (IoT) cybersecurity is a matter of concern to software developers and must be evaluated throughout the device lifecycle to reduce threats and risks. One of the most important aspects of IoT is the very heterogeneity of its Internet connection solutions and the threats to which these systems are exposed. Therefore, cybersecurity protections are highlighted in both legacy and new systems. CPS (Cyber-physical systems) use sensors and actuators as a way to control real world systems and have brought new challenges for IoT. Cyber-attacks against these devices can do severe damage when CPS is integrated with communication networks and the Internet. In this context, like the automobile, which employs CPS to control vehicle elements, a cyber threat to these devices can result in vehicle downtime and loss of steering control. Automotive CPS must endure approximately ten of years, meaning that these devices must withstand today's cyber threats and also be flexible enough to adapt and evolve over the years, providing protection against cyber-attacks throughout the lifetime. In this context, an ontology that expresses knowledge of the automotive domain and the cybersecurity involved, can support embedded software developers in the cybersecurity assessment process. This work presents the use of the SAEJ3061 framework for cybersecurity assessment in automotive CPS embedded software through an ontological approach. The overall objective of this research is to improve the effectiveness of cybersecurity assessment supported by ontology. In this sense, we built a cybersecurity domain ontology (AutomotiveCyberSecurity) using the OntoforInfoScience method. During the ontology development process, we use the support and validation of FCA (Fiat Chrysler Automobiles) cybersecurity experts. The result of this work was the increased use of the cybersecurity report by embedded software developers due to a greater understanding of CPS threats and attacks.

Key-words: Cybersecurity; Cibersecurity risk assessment; Ontology; OntoforInfoScience; SAEJ3061.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

AUTOSAR	*AUTomotive Open System ARchitecture*
IoT	*Internet of Things*
CAPEC	*Common Attack Pattern Enumeration and Classification*
CPS	*Cyber Physical Systems*
CVSS	*Common Vulnerability Scoring System*
BFO	*Basic Formal Ontology*
FCA	FIAT Chrysler Automobiles
IFOMIS	Instituto de Ontologia Formal e Ciência da Informação Médica
NHTSA	*National Highway Traffic Safety Administration*
NIST	*National Institute of Standards and Technology*
OWL	*Web Ontology Language*
RES	Registro Eletrônico da Saúde
SAE	*Society of Automotive Engineers*
TARA	*Threat Analysis and Risk Assessment*

Sumário

1 Introdução

IoT (*Internet of Things*) e dispositivos CPS[1] (*Cyber Physical Systems*) conectam o mundo virtual e o físico para resolver problemas complexos e explorar novas tecnologias (ALI; HONG, 2018). CPS empregam componentes físicos para adquirir dados e processá-los para utilizá-los no mundo cibernético, além de controlar e atuar em elementos do mundo real. Os CPS fazem a ponte do mundo físico com o virtual (LEE, 2008), permitindo interações entre os dois mundos pela detecção e atuação (WU; KAO; TSENG, 2011).

Os CPS estão presentes atualmente em diversos domínios, como o de energia, controle industrial e automotivo. Com a conexão da internet, os CPS se aproximaram da IoT e têm contribuído para a melhoria da mobilidade e da conectividade de dispositivos, além de trazer a perspectiva de aprimoramento da segurança nas estradas, entre outras vantagens, por meio de centrais eletrônicas responsáveis pelo controle dinâmico de estabilidade e gerenciamento eletrônico do motor (SCHMITTNER et al., 2015).

A principal diferença entre IoT e CPS é o foco. A IoT foca na conectividade de dispositivos com a infraestrutura da Internet, enquanto o CPS se concentra nos recursos de detecção e atuação dos dispositivos para atingir determinados objetivos em uma aplicação de domínio específico. Para os sistemas CPS funcionarem, eles não precisam estar conectados à Internet, como, por exemplo, um sistema robótico de circuito fechado em uma planta, um sistema de rede inteligente em uma rede local. Atualmente, esses termos são frequentemente usados de forma intercambiável, especialmente nos casos em que sistemas IoT não incorporam apenas um identificador digital aos dispositivos, mas também sensores e atuadores e quando os dispositivos são conectados on-line e conectados entre eles por uma rede (SALIM; HAQUE, 2015).

A avaliação de risco em cibersegurança é mais recente no desenvolvimento de CPS automotivos se compararmos com a avaliação de riscos na internet e na IoT. Como parte desta evolução, as proteções em cibersegurança automobilística assumem papel importante tanto em sistemas legados como em novos desenvolvimentos. É necessário dar maior atenção às fases iniciais do ciclo de vida do produto e à importância do conhecimento do domínio automotivo.

O comitê da SAE[2] para cibersegurança disponibilizou recentemente um guia em

[1] O termo *Cyber Physical Systems* compreende componentes digitais, analógicos, físicos e humanos em interação, projetados para funcionar por meio de física e lógica integradas. O CPS é originário da indústria de manufatura, como por exemplo robôs industriais programados, para detectar seu ambiente e atuar de acordo com as respostas programadas. Os CPS são aplicados em muitas áreas, incluindo saúde, assistência, sistemas de transporte inteligentes, sistema de resgate, vigilância e monitoramento.

[2] A *SAE International, inicialmente estabelecida como a Society of Automotive Engineers*, é uma associação profissional e organização de desenvolvimento de padrões para profissionais de engenharia.

cibersegurança para CPS automotivos, que resultou na norma J3061 (Society of Automotive Engineers, 2016). A referida norma reconheceu a necessidade de um guia para tratar requisitos de segurança cibernética e de um processo de avaliação de riscos. A norma SAEJ3061 utiliza referências em cibersegurança na Internet, redes de computadores e dispositivos IoT, por reconhecer que o conhecimento em cibersegurança nesses domínios interdisciplinares deve ser o ponto de partida para lidar com o tema.

Tendo em vista que a complexidade da cibersegurança voltada para o desenvolvimento de softwares embarcados automotivos exige o uso do conhecimento de forma intensiva (SI-SAID; ROLLAND, 1997) e que a norma J3061 não propôs uma ontologia do conhecimento em cibersegurança para o domínio automotivo, na presente pesquisa propomos uma ontologia (*AutomotiveCyberSecurity*) para se integrar ao processo de avaliação da cibersegurança automotiva. Utilizamos a BFO[3] (*Basic Formal Ontology*) como de nível superior e as orientações de Smith et al. (2015) na definição das entidades continuantes e ocorrentes da ontologia do domínio de cibersegurança *AutomotiveCyberSecurity*. Utilizamos conceitos e relações visando a que a avaliação em cibersegurança possa responder de forma rápida às questões de competência dos envolvidos nas fases do desenvolvimento do software automotivo. Estabelecemos um grupo focal composto por especialistas em avaliação em cibersegurança da FCA (FIAT Chrysler Aumobiles). A ontologia foi utilizada na avaliação das respostas às questões de competência e na integração com o processo do J3061.

A seguir, são apresentados o problema de pesquisa, sua justificativa, o objetivo geral e os objetivos específicos.

1.1 Problema de pesquisa

Existem vários estudos e aplicações de avaliação em cibersegurança na indústria, no setor aeroespacial, na produção e distribuição de energia assim como em redes de computadores IoT e CPS automotivos. Estes estudos visam, principalmente, a avaliar ataques cibernéticos, ameaças e vulnerabilidades em ativos de um determinado domínio. Ativos são definidos como objetos ou partes do veículo que o atacante pode alcançar e trazer prejuízos físicos a seu ocupante.

A cibersegurança deve acompanhar o CPS desde sua concepção, produção, utilização

A ênfase principal dessa entidade está nas indústrias de transporte, como veículos automotores, aeroespaciais e comerciais. Site da associação: www.sae.org. Acesso em 16 de setembro de 2019.

[3] A BFO (*Basic Formal Ontology*) é uma ontologia pequena, de nível superior, projetada para uso no suporte à recuperação, análise e integração de informações em domínios científicos. A BFO é uma ontologia superior genuína. Portanto, ela não contém termos físicos, químicos, biológicos ou outros que se enquadram adequadamente nos domínios de cobertura das ciências especiais. O BFO é usado por mais de 250 empreendimentos orientados a ontologias em todo o mundo. Está disponível em http://basic-formal-ontology.org/. Acesso em 01 de novembro de 2019.

e descarte final. Durante a fase de desenvolvimento de software embutido, engenheiros e programadores lidam com um número elevado de requisitos, em processos em que são exigidos vários *stakeholders* envolvidos e um ciclo de vida de algumas dezenas de anos de utilização.

Stakeholders têm uma vaga ideia de como um CPS automotivo deveria se comportar e quais seus objetivos. Essas intenções são importantes, mas não suficientes para uma engenharia voltada a requisitos e que almeja maior controle sobre os CPS no intuito de protegê-lo contra os ataques cibernéticos.

Por consequência, um necessário formalismo, conceitos e semântica únicos para tratar a cibersegurança são necessários para manter o controle dos processos e facilitar a comunicação entre os *stakeholders*.

A falta de uma comunicação eficiente entre múltiplos *stakeholders* é o principal motivo para ocorrência de falhas de projetos por causar inconsistências em objetivos e requisitos (LAMSWEERDE; DARIMONT; LETIER, 1998). Nossa hipótese é que a avaliação da cibersegurança, suportada por uma ontologia que garanta um entendimento unificado do domínio do conhecimento, é uma ferramenta poderosa para lidar com problemas como inconsistência, ambiguidade e qualidade. Além disso, uma ontologia aplicada à avaliação da cibersegurança pode ser a chave para o compartilhamento de informações entre os vários desenvolvedores de CPS.

Chalé et al. (2011) apontam a ontologia como um caminho para suportar desenvolvedores no entendimento correto da terminologia de um domínio e na implementação do softwares embarcados. Apesar disso, pouco se fez na direção da integração de ontologias e na análise do processo de cibersegurança no desenvolvimento de CPS automotivo.

Diante desse contexto, essa pesquisa objetiva responder à pergunta: **Uma ontologia pode melhorar a eficácia da avaliação em cibersegurança de CPS automotivos?**

Um desafio que reside nesse contexto é a pluralidade de conceitos e ferramentas de desenvolvimento necessárias ao desenvolvimento de um CPS. A aquisição, especificação e evolução de metas e requisitos de diferentes partes interessadas ou fontes, muitas vezes, levam a requisitos incompletos, ambíguos e com falhas. Assim, a capacidade de detectar e reparar inconsistências e garantir a segurança é crucial para uma avaliação em cibersegurança e um desenvolvimento bem-sucedido. Acredita-se, portanto, que ontologias possam fornecer expressividade para capturar requisitos de forma suficiente, permitindo desenvolvê-los em software e avaliá-los (SIEGEMUND, 2014).

1.2 Objetivo da Pesquisa

1.2.1 Objetivo Geral

Neste trabalho, objetiva-se o desenvolvimento de uma ontologia de domínio que integre a avaliação da cibersegurança da norma J3061, visando uma maior eficácia ao processo de desenvolvimento de CPS, suportando os especialistas em cibersegurança a responder questões de competência.

1.2.2 Objetivo específicos

- OBJ1: Analisar as abordagens e aplicações que investigam o uso de ontologias para avaliação de cibersegurança;
- OBJ2: Desenvolver a ontologia proposta (*AutomotiveCyberSecurity*), uma ontologia de domínio na área de cibersegurança para, posteriormente, suportar avaliação em cibersegurança;
- OBJ3: Integrar a ontologia de domínio desenvolvida à ontologia BFO de nível superior;
- OBJ4: Integrar a ontologia de domínio desenvolvida à norma J3061; e
- OBJ5: Avaliar a ontologia proposta em um estudo de caso real com o grupo focal de especialistas em cibersegurança da FCA.

1.3 Tipo de pesquisa

A pesquisa pode ser classificada, em relação à sua finalidade, como aplicada, pois objetiva gerar uma solução tecnológica voltada para avaliação em cibersegurança. Quanto ao procedimento, é um estudo de caso que empregou grupo focal de especialistas para avaliar a contribuição da ontologia de domínio desenvolvida. Em relação à abordagem, a investigação é qualitativa. Quanto ao procedimento técnico da etapa experimental, trata-se de uma pesquisa laboratorial que, num ambiente controlado, aplicou a ontologia em um processo de avaliação em cibersegurança (FONTELLES; SIMÕES; FARIAS, 2009).

1.4 Contribuições da pesquisa

O trabalho em segurança cibernética é de constante atualização e aprendizado. Novos ataques surgem constantemente, utilizando novos vetores. Encarar seriamente o fato de que a realidade do automóvel tenha mudado de uma simples máquina mecânica para um elemento ativo da internet das coisas motiva o trabalho de pesquisa.

Além disso, um desafio na avaliação é a determinação dos ativos e os impactos diretos ou indiretos para os ocupantes do veículo, no caso de um ataque cibernético. Esses ativos podem se comunicar com CPS do automóvel, a exemplo do motor ou de um freio, ambos controlados por dispositivos que podem ser acessados via internet. Sendo assim, o conhecimento sobre ameaças, vetores de ataque e seus níveis de sofisticação, a classificação de risco destas ameaças e as contramedidas são a forma que os especialistas em cibersegurança tem de enfrentar este desafio.

Portanto a contribuição desta pesquisa para os especialistas em avaliação de cibersegurança é o desenvolvimento da ontologia *AutomotiveCyberSecurity* e sua integração ao *framework* da norma J3061 a fim de reunir este conhecimento e suportar a avaliação em cibersegurança com uma ferramenta capaz de inferir este conhecimento através da própria ontologia. Pretende-se que a solução desenvolvida seja ágil e adaptável ao ciclo de vida do produto, permitindo a construção de CPS mais confiáveis, evitando, assim, transtornos aos usuários de veículos, processos judiciais e *recalls*.

Para o usuário de veículos automotores, a contribuição da pesquisa é o aumento da confiabilidade na utilização do automóvel, pois o fabricante de veículos terá, à sua disposição, desde o início do processo de desenvolvimento dos CPS, uma ferramenta que objetiva minimizar riscos de acidentes e aumentar a proteção dos dados do usuário.

Para a área de Ciência da Informação, a pesquisa traz avanços nos estudos empíricos em ontologias aplicadas à avaliação da cibersegurança em IoT. Com essa abordagem, pretendemos avançar nos atuais estudos de ontologias que cobrem o desenvolvimento dos IoTs e as potenciais vulnerabilidades, como descrito por Mozzaquatro, Jardim-Goncalves e Agostinho (2015). Nessa pluralidade de protocolos de comunicação e baixa interoperabilidade dos IoTs desenvolvidos, sem levar em conta a presença de vulnerabilidades, pretendemos harmonizar conceitos e responder a questões de competência dos especialistas em cibersegurança de CPS automotivo.

1.5 Estrutura do documento

A Seção 2 apresenta o referencial teórico e os trabalhos relacionados. A Seção 3 aborda a revisão sistemática de literatura realizada, voltada para a cibersegurança em IoT e CPS. A Seção 4 descreve a metodologia utilizada para o desenvolvimento da ontologia em cibersegurança e o *framework* de avaliação em cibersegurança da norma J3061, suportada pela ontologia. A Seção 5 descreve o desenvolvimento da ontologia, a integração com a ontologia de nível superior, a integração da ontologia e a norma J3061, as questões de competência e a aplicação da *AutomotiveCyberSecurity* pelo grupo de trabalho de especialistas em cibersegurança da FCA. E a Seção 6 traz as conclusões e trabalhos futuros.

2 Referencial Teórico

Nesse capítulo, é apresentado o referencial teórico que sustenta a nossa investigação e seu experimento empírico. Exploramos alguns conceitos ligados à cibersegurança, Ontologia, ontologia de nível superior como a BFO e trabalhos relacionados que utilizam ontologia na avaliação em cibersegurança como solução para lidar com os problemas semânticos originados em grandes equipes, distribuídas em várias tarefas do desenvolvimento de software de IoT, métricas em avaliação de riscos e vulnerabilidades, além de trabalhos que forneceram suporte para normas em avaliação em cibersegurança.

2.1 Por que nos preocupamos com a segurança?

É importante diferenciarmos a segurança em duas partes: *safety* e *security*. As definições de *safety* e *security* variam amplamente em diferentes contextos e comunidades técnicas. Em alguns idiomas, como o português e o espanhol, ambas as palavras são usadas no sentido de segurança. No entanto, mesmo na língua que oferece duas palavras distintas, o significado de cada uma varia consideravelmente de um contexto para outro. Por simplificação, preferimos o conceito dado por Burns, McDermid e Dobson (1992) em que relaciona o objeto ou sistema estudado ao conceito de segurança. Por consequência, um sistema é definido como crítico em segurança (*safety*) se uma falha puder causar dano imediato e direto (físico e material). Por outro lado, um sistema é crítico em segurança (*security*) se uma falha na proteção puder habilitar ou aumentar a capacidade de terceiros de gerar prejuízos. Embora a segurança se concentre em diferentes problemas, causas e consequências, não é mais possível ser verdadeiramente seguro (*safety*) sem também ser protegido (*security*).

2.2 Conceitos de cibersegurança

Kemmerer (2003) afirma que a cibersegurança consiste basicamente de métodos defensivos usado para detectar e impedir possíveis invasores.

A ITU (*International Telecomunications Union*) define cibersegurança como uma coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, riscos, abordagens de gestão, ações, treinamento, melhores práticas, garantia e tecnologias que podem ser usadas para proteger o ambiente cibernético, a organização e

os ativos do usuário (ITU, 2009).

Craigen, Diakun-Thibault e Purse (2014) afirmam que a cibersegurança é um termo amplamente usado, cujas definições são, muitas vezes subjetivas e, às vezes, pouco informativas e definem cibersegurança como uma organização e uma coleção de recursos, processos e estruturas utilizadas para proteger o ciberespaço e sistemas habilitados para o ciberespaço contra ocorrências que desalinham aquilo que é permitido ou amparado por lei com algo que realmente é praticado (desalinhamento *de jure* com o *de facto*).

Ainda, Amoroso (2006) define a segurança cibernética como aquilo que envolve a redução do risco de ataque por *malware* a software, computadores e redes. Isso inclui ferramentas usadas para detectar invasões, interromper vírus, bloquear acesso malicioso, impor autenticação, ativar comunicações criptografadas e assim por diante.

Apesar do termo cibersegurança assumir definições diferentes entre os autores, na maioria delas existe um consenso sobre a capacidade de reduzir riscos através de ferramentas, coleção de recursos e métodos de detecção e melhores práticas, a fim de proteger ativos e evitar invasões. Além disso, não conseguimos pensar em cibersegurança sem mencionar a tríade CIA que envolve a confidencialidade, integridade e disponibilidade.

Segundo Samonas e Coss (2014) a confidencialidade pode ser tratada como a liberação de informação não autorizada: uma pessoa não autorizada é capaz de ler e tirar proveito das informações armazenadas no computador. Essa categoria de preocupação às vezes se estende à "análise de tráfego", na qual o invasor observa apenas os padrões de uso da informação. Tendo esses padrões como referência, o invasor pode inferir algum conteúdo de informação. Essa categoria também inclui o uso não autorizado de um programa proprietário.

Podemos demonstrar a confidencialidade quando, por exemplo, um especialista em cibersegurança lida com segurança cibernética de uma organização, e é responsável pelo acesso a dados confidenciais mantidos somente por pessoas autorizadas. Digamos que esse profissional trabalhe para uma grande empresa financeira que tem concorrentes em todo o mundo e tem agentes de ameaças tentando acessar os segredos comerciais. Verificar se esses segredos comerciais não estão acessíveis para pessoas que não estão autorizadas a acessá-los, é cuidar da confidencialidade.

Firewalls, detectores de intrusão e tecnologias de prevenção de acesso são alguns dos métodos utilizados para garantir a confidencialidade e o acesso à informação somente às pessoas autorizadas.

Integridade, por sua vez, é a modificação não autorizada de informações: uma pessoa não autorizada é capaz de fazer alterações nas informações armazenadas - uma forma de sabotagem. Deve-se notar que, no caso desse tipo de violação, o invasor não vê necessariamente as informações que mudou.

Dentro do mesmo exemplo, o especialista em cibersegurança da mesma organização financeira deve garantir que as pessoas não estejam mexendo nos dados que a organização mantém. De um cliente de uma empresa de cartões de crédito pode ser cobrado um valor $3000 em vez de $30 na sua fatura de forma intencional, acidental ou devido a alguma corrupção do banco de dados. O especialista em cibersegurança deve garantir que os dados não estejam corrompidos e que os backups não tenham sido manipulados incorretamente. Nesse caso, por exemplo, implementam-se rotinas de FIM (*File Integrity Monitors*) através de algoritimos *hash* para verificar se os dados estão seguros e sem violação.

E a disponibilidade é negação de autorização de uso. Um invasor pode impedir que um usuário autorizado se refira ou modifique informações, mesmo que o invasor não consiga se referir, nem modificar as informações, como, por exemplo um especialista em cibersegurança de um site de compras da internet. Sua tarefa é garantir que o site nunca esteja inativo. Organizações como sites de compras não podem lidar com o tempo de inatividade e sofrerão enormes perdas se isso acontecer. Para garantir a disponibilidade, redundâncias e backups são implementadas para garantir que os serviços do site funcionem mesmo se o servidor esteja inativo.

Sem dúvida, existem muitas respostas para o conceito de cibersegurança e principais conceitos como a tríade CIA para a Tecnologia da informação e outros como SAIC (Segurança, disponibilidade, Integridade e Confidencialidade) para IoT. Essas são as estruturas conceituais para as coisas que a cibersegurança está tentando alcançar ou proteger. Na presente pesquisa, cibersegurança é definida como as medidas tomadas para proteger um CPS contra acesso ou ataque não autorizado através de medições de impacto e probabilidade.

2.3 Vulnerabilidade, Riscos e Ameaças

Autores como Herzog, Shahmehri e Duma (2007), Khazai et al. (2014) e Khan e Salah (2018) defendem a importância da cibersegurança nos aspectos de vulnerabilidade, riscos e ameaças. Sendo uma maneira pela qual podemos relacionar de fato os aspectos ligados à proteção e aos riscos envolvidos em razão das vulnerabilidades e ameaças que uma empresa, um sistema ou um IoT pode se envolver no ciberespaço, afetando assim sua integridade, confidencialidade e disponibilidade.

Vulnerabilidade

Safety e *security* receberam muita atenção nos últimos anos. Na indústria, por exemplo, Reason (1990), em seu livro *Human Error*, empregou o conceito de barreiras

de segurança que descreve o isolamento entre o perigo e sua consequência como fatias de queijo suíço, cujos controles de risco de pessoas, instalações e processos são comparados com os furos das fatias de queijo, que representam as falhas ou fraquezas de cada uma das barreiras protetoras existentes (vulnerabilidade). O modelo mostra que nenhuma falha isolada jamais causou um acidente grave, mas, sim, uma sequência de falhas, como exemplificado no vazamento de óleo da planta industrial no Texas *Deepwater Horizon* e muitos outros. Esses eventos catastróficos sempre podem ser atribuídos a várias falhas, seja na planta, nas pessoas ou nos processos (KLETZ; AMYOTTE, 2019). Como uma dessas múltiplas barreiras, nos sistemas de segurança, que são sistemas digitais e frequentemente conectados a uma rede, existe sempre uma preocupação real de que um ataque cibernético direcionado possa desativar ou afetar seu desempenho, causando ou simplesmente criando oportunidade para um grande incidente.

Riscos

Tanto o *safety* quanto *security* lidam com riscos. De acordo com a norma ISO 31004 (ISO31000, 2018), risco é definido como a combinação da probabilidade de um evento (ou perigo ou fonte de risco) e sua consequência. De acordo com esta norma, dois parâmetros importantes são considerados na definição de risco: a fonte de risco e sua consequência. A fonte do risco pode ser acidental ou deliberada, e as consequências podem ser de diferentes tipos: financeiro, ambiental, humano, reputação, privacidade, operacional ou em *safety* (KRIAA, 2016).

Ameaças

Descrevemos informalmente uma ameaça como “uma pessoa ou organização que pretende causar danos”. Mais formalmente, uma ameaça é “um malevolente ator, seja uma organização ou um indivíduo, com um objetivo político, social ou pessoal e algum nível de capacidade e intenção de se opor a um governo estabelecido, a uma organização ou a uma norma social aceita” (MATESKI et al., 2012, p.10).

As ameaças podem ser de tipos diferentes assim como perseguir objetivos diferentes. Dependendo do ambiente em que um sistema de informação ou uma rede esteja localizada e o tipo de informação para a qual foi projetada, diferentes classes de ameaças terão interesse em tentar obter diferentes tipos de informações ou acesso, com base em suas capacidades particulares (MATESKI et al., 2012).

As ameaças são geralmente muito mais fáceis de listar do que de descrever e muito mais fáceis de descrever do que de medir. Como resultado, muitas organizações listam ameaças, poucas as descrevem em termos úteis e menos ainda as medem de maneira

significativa. Isto é particularmente verdade na dinâmica e domínio nebuloso de ameaças cibernéticas - um domínio que tende a resistir a medições fáceis, em alguns casos, parece desafiar qualquer medida.

2.4 Ameças em IoT e CPS

Um dos mais importantes desafios para a adoção da IoT e dos CPS vem da própria heterogeneidade das soluções empregadas para conexão à internet e das ameaças que surgem quando esses sistemas são expostos ao universo da web. Assim, proteções em cibersegurança ganham destaque tanto no âmbito dos sistemas legados como dos novos sistemas (MOZZAQUATRO et al., 2018).

Com a rápida expansão da IoT e dos dispositivos CPS, abrem-se novas e diversificadas perspectivas de usos dessas tecnologias, a exemplo das *Smart Cities*, dos *Smart Grids*, aplicações nos setores automotivo e da saúde. Estamos diante, portanto, de um campo interdisciplinar em que a adequada representação do conhecimento se torna imprescindível para garantir a construção de artefatos de softwares que resolvam problemas relativos aos dispositivos IoT (como a heterogeneidade de soluções e de protocolos de comunicação) e que minimizem os riscos ligados à cibersegurança nesse contexto (IBARRA-ESQUER et al., 2017).

No segmento de veículos, os CPS, integrados aos sistemas automotivos, se conectam à internet e comandam sistemas físicos do automóvel. Esses CPS permitem o controle ativo sobre elementos reais do veículo e estão sujeitos a ameaças cibernéticas. Por consequência, a cibersegurança nesses dispositivos envolve, além de dados privativos, a segurança física dos ocupantes do veículo (ABDULKHALEQ et al., 2017).

Quanto mais os sistemas automotivos são conectados à internet, maior é sua exposição a riscos de penetração maliciosa. Em 2014, mais da metade dos usuários de veículo se mostraram preocupados com a possibilidade de o carro ser manipulado por hackers quando o automóvel estiver conectado à internet. Além disso, mais de 30% dos brasileiros rejeitam a ideia de carros conectados em razão do risco de perda de privacidade (HANNON et al., 2018).

2.5 Avaliação em cibersegurança em CPS Automotivo

O DOT HS 812 do NHTSA (*National Highway Traffic Safety Administration*) (MCCARTHY; HARNETT; CARTER, 2014), a J3061 da SAE (*Society of Automotive Engineers*) (Society of Automotive Engineers, 2016) e NIST.SP.1500-201 do NIST (*National*

Institute of Standards and Technology) (GRIFFOR et al., 2017) são esforços no sentido de propor *frameworks* de avaliação em cibersegurança com o objetivo de compartilhar um vocabulário comum, estrutura e metodologia de análise abrangente.

Esses esforços visam, entre outras coisas, à construção de uma base de conhecimento sobre cibersegurança automotiva, ao desenvolvimento de ferramentas que permitam a pesquisa aplicada nessa área, à facilitação da implementação de melhores práticas eficazes baseadas na indústria, ao fomento ao desenvolvimento de novas soluções, à viabilização do desenvolvimento de requisitos mínimos de desempenho para segurança cibernética automotiva e reunião de dados e fatos fundamentais para a comunidade relacionados à cibersegurança automotiva para informar possíveis atividades futuras de políticas e decisões regulatórias federais.

Em todas as abordagens, verifica-se uma tentativa de captura das funcionalidades que o CPS fornece e as atividades e artefatos necessários para dar suporte à conceitualização, realização e garantir a cibersegurança do CPS em seu ciclo de vida. Essa garantia em termos de *safety* e *security*, é a parte do processo da análise em que os especialistas em cibersegurança discutem os riscos e ameaças, e por fim, produzem relatórios que auxiliam os desenvolvedores de CPS a tomarem contramedidas para eliminar as vulnerabilidades.

2.6 Integração da avaliação em cibersegurança e o ciclo de desenvolvimento do CPS

Em 2016, trabalhos relacionados à aplicação da norma J3061 (BECKERS; DÜRRWANG; HOLLING, 2016; SCHMITTNER et al., 2016; ISLAM et al., 2016; EBERT; LIECKFELDT, 2017) demonstraram a necessidade de integrar o processo de desenvolvimento com a avaliação de cibersegurança em CPS automotivos. Estes esforços de integração tiveram como base o guia instituído pela J3061, que avalia e trata riscos cibernéticos, utilizando-se, como ponto de partida, referências em cibersegurança da Internet, redes de computadores e dispositivos IoT.

A norma J3061 estabeleceu um processo de avaliação em cibersegurança do ciclo de vida do CPS, passando pela fase conceitual, desenvolvimento do CPS, utilização e descarte. Ela determina as ameaças e vulnerabilidades com o objetivo de priorizar as ações e contramedidas de modo a implementar um sistema de gestão que suporte desenvolvedores e especialistas em cibersegurança na determinação e configuração do nível de segurança de que um CPS necessita.

Segundo a norma J3061, a avaliação de cibersegurança no desenvolvimento é um processo complexo que pode ser dividido em três fases: planejamento da cibersegurança,

objetivo de cibersegurança, identificação dos ativos e ameaças; análise de risco e seleção de CPS e as funções de *safety* e *security*; e relatório de cibersegurança.

O planejamento visa a um entendimento comum dos especialistas em cibersegurança em relação aos objetivos de cibersegurança do CPS, que passa então pela identificação de ativos que possam, diante de uma ameaça, expor um risco que pode resultar em dano real de integridade (*safety*).

A análise do risco é uma atividade extensiva que exige conhecimento de vulnerabilidades de sistemas operacionais, históricos de invasões, vetores e passos de um ataque. Esse conhecimento acumulado e registrado é a base que especialistas utilizam para avaliar as ameaças. Na J3061, existem métodos como o TARA (*Threat Analysis and Risk Assessment*) que auxiliam os especialistas a identificar os riscos, de forma a priorizá-los e responder contra que vulnerabilidades o CPS deve ser protegido antes mesmo de ser desenvolvido.

O relatório de cibersegurança é o resultado da atividade da avaliação e contém as recomendações dos especialistas em cibersegurança nas ações que devem ser empregadas durante o ciclo de vida do CPS para evitar vulnerabilidades e ameaças. Entretanto, tanto o processo quanto o relatório são fruto de uma conceitualização que depende intrinsecamente do grupo de especialistas em cibersegurança envolvido no trabalho. Atualmente, os desenvolvimentos de CPS são cada vez mais globais e o resultado do trabalho de avaliação em cibersegurança necessita de uma taxonomia e de conceitos em uma representação mais formal do conhecimento, de forma a garantir que diferentes grupos possam trabalhar ao redor do globo sem cair na armadilha do desentendimento. Sem este entendimento o resultado da análise de cibersegurança pode ser comprometido, gerando vulnerabilidades a serem exploradas por hackers.

2.7 Ontologias e taxonomias

Segundo Gruber (1993), ontologia é a representação formal de uma conceitualização compartilhada. Almeida (2006) enriquece a definição do termo ao explicar que o estudo de ontologias é caracterizado como um ramo de pesquisa que propõe alternativas para representação do conhecimento através de uma série de formalismos capazes de representar conceitos, relações entre os conceitos e a semântica de um domínio do conhecimento que, através de declarações lógicas, podem ser manipuladas por um sistema computacional.

Ontologias oferecem a possibilidade de representar, organizar e desenvolver conjuntos complexos de conhecimento em diferentes áreas do conhecimento. Por meio das ontologias, são criados vocabulários que permitem que sejam feitas inferências a serem processadas através de raciocinadores automáticos (ALMEIDA, 2013).

A estrutura oferecida pela ontologia pode ser entendida como uma representação formal e hierárquica de conceitos que se inter-relacionam em um domínio de conhecimento específico. Componentes comuns de uma ontologia são indivíduos, instâncias ou objetos, classes (conjuntos, coleções, conceitos, classes em programação, tipos de objetos, ou tipos de coisas), propriedades (aspectos, atributos, características, características ou parâmetros dos objetos e classes) e relações (maneiras pelas quais classes e indivíduos podem estar relacionados uns aos outros). Uma vez desenvolvida, esta estrutura abstrata permite ao usuário descrever uma estrutura de domínio do conhecimento, coletando sinônimos, capturando hierarquias como nas taxonomias, estabelecendo relações entre classes e indivíduos (KHAZAI et al., 2014).

Rees (2003) define a taxonomia como uma estrutura hierárquica para auxiliar o processo de classificação de informações. Nas taxonomias, em geral, as informações são principalmente textuais, e seu objetivo principal é sistematizar uma gama de vários elementos em uma estrutura hierárquica.

É importante distinguir as taxonomias das ontologias. Embora as taxonomias possam ser consideradas ontologias simples (MCGUINNESS, 2003), as ontologias são mais aprimoradas do ponto de vista semântico.

Nas taxonomias, preocupa-se com o desenvolvimento de categorias, inserção e recuperação da informação, enquanto nas ontologias, o objetivo é o desenvolvimento de um consenso linguístico do domínio de conhecimento, levando em consideração, além dos relacionamentos taxonômicos adotados na ordenação de classes e subclasses, outros tipos de relações semânticas, como as de associação, derivadas da explicitação das características dos conceitos (VITAL; CAFÉ, 2011).

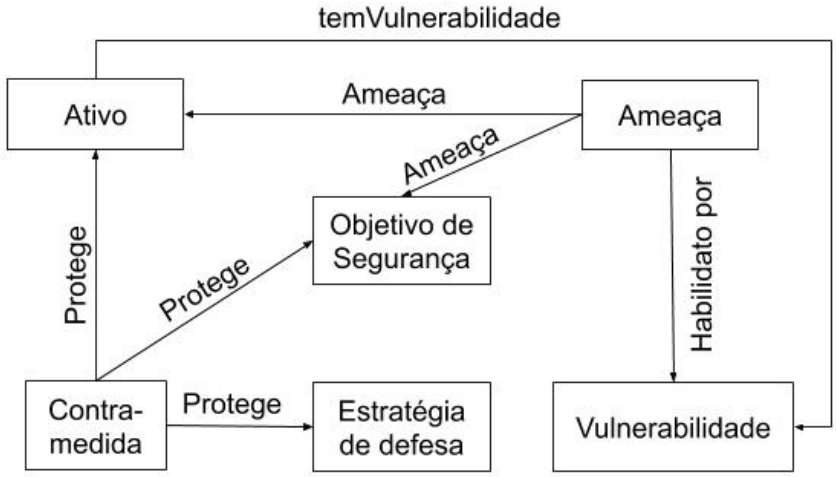
Esse consenso linguístico das ontologias é seguramente um caminho que pode ser percorrido pelos especialistas em cibersegurança de diferentes grupos e nacionalidades. Num desenvolvimento global de CPS, gerando assim a confiabilidade na informação tratada por todos, já que o entendimento da taxonomia e da conceitualização pode ser gerado pelos participantes que entendem o domínio da cibersegurança aplicada em IoT e CPS.

2.8 Ontologias na avaliação de cibersegurança

Soluções baseadas em ontologias têm sido empregadas para enfrentar problemas relativos à cibersegurança e à preservação da privacidade em dispositivos conectados à IoT (FICCO, 2013; ALAM; CHOWDHURY; NOLL, 2011; TAO et al., 2018), bem como para gerir riscos (análise, avaliação e mitigação de riscos) envolvidos nesse universo (EKELHART; FENZ; NEUBAUER, 2009).

Herzog, Shahmehri e Duma (2007), ao proporem uma ontologia em cibersegurança baseada em OWL[1], definiram os componentes clássicos adotados em avaliações de risco em ativos (*assets*), ameaças (*threats*), contramedidas (*counter-measures*), vulnerabilidades (*vulnerabilities*) e suas relações (Figura 1). A ontologia proposta pelos autores, disponibilizada abertamente, pode ser usada como um vocabulário geral, roteiro e dicionário extensível do domínio da segurança da informação. Com sua ajuda, os usuários podem adotar uma linguagem comum com definição de termos e relacionamentos. Além disso, ela é útil para raciocinar sobre relacionamentos entre suas entidades, como, por exemplo, ameaças e contramedidas. A referida ontologia ajuda a responder a perguntas como: Quais contramedidas podem detectar ou impedir a violação da integridade dos dados?

Figura 1 – Trabalhos relacionados - Classes e relações da ontologia de cibersegurança de Herzog et al.



fonte: Adaptado de Herzog, Shahmehri e Duma (2007)

Se compararmos a ontologia de Herzog, Shahmehri e Duma (2007) com a norma J3061, fica evidente que a norma J3061 se limitou a apresentar recomendações e um guia de avaliação de riscos envolvidos em CPS. Nota-se que a referida norma não apresenta uma ontologia do conhecimento em cibersegurança. Apesar de a norma representar o melhor esforço já alcançado para a área de cibersegurança em CPS automotivos, torna-se necessário que os desenvolvedores e os especialistas em cibersegurança tenham conhecimento prévio de outros domínios, como a cibersegurança da internet, para que o guia proposto pela SAE seja mais bem conduzido e aplicado.

Santos, Bax e Pessanha (2010) defendem que o crescimento do número de aplicações na área de saúde aumentou a complexidade informacional, também abrindo caminhos para novas tecnologias que buscam separar o domínio do conhecimento do domínio da

[1] A linguagem de Ontologia da Web (OWL) do W3C é uma linguagem da Web semântica projetada para representar um conhecimento rico e complexo sobre coisas, grupos de coisas e relações entre as coisas.

implementação. Os autores buscaram o contraste entre as ontologias e a norma ISO1306, que define um modelo de informação para comunicar parte ou todo o RES (Registro Eletrônicos da Saúde) de um paciente, preservando o significado clínico original. O trabalho de Santos, Bax e Pessanha (2010) com esta visão do contraste e também da contribuição ontológica sob a norma ISO1306 pode ser também buscado na norma J3061.

2.9 BFO (*Basic Formal Ontology*)

A BFO[2] é uma teoria das estruturas básicas da realidade atualmente desenvolvidas no Instituto de Ontologia Formal e Ciência da Informação Médica (IFOMIS) (GRENON; SMITH, 2004). A BFO é uma ontologia de nível superior, projetada para uso no suporte à recuperação, análise e integração de informações em domínios científicos. Ela não contém termos físicos, químicos, biológicos ou outros que se enquadrem adequadamente nos domínios de cobertura das ciências.

O comitê da norma ISO demonstrou claramente o seu interesse na Ontologia BFO com a publicação da ISO21838[3] como um padrão TLO (*Top-level Ontology*), com claro objetivo de apoiar a integração de ontologias mais específicas que se estendem a partir dela (ORELLANA; MANDRICK, 2019). Uma ontologia de referência visa a fornecer uma representação abrangente das entidades em um determinado domínio, encapsulando o conteúdo terminológico do conhecimento estabelecido, e significa que deste modo, futuramente, poderemos conectar a ontologia do domínio da avaliação de cibersegurança e outras ontologias já existentes em razão da sua interoperabilidade entre os vários domínios promovidos pelas classes da BFO.

A BFO é usada por mais de 130 empreendimentos direcionados à ontologia em todo o mundo e este interesse se estende até a indústria de transformação. A exemplo disto Smith (2019) define uma visão da Ontologia da BFO como exemplo do que a indústria de transformação chama de sistema de produto-serviço. Produtos fornecidos com uma variedade de serviços de ontologia, como atualizações, treinamento, suporte técnico e identificadores permanentes.

A BFO apoia o raciocínio formal e está associada a um conjunto de teorias formais comuns e ao raciocínio espacial qualitativo, potencialmente também de números, não necessitando ser reconstruída para cada domínio sucessivo. Para esse fim, a BFO é capaz de ser aplicada à criação de ontologias de domínio em níveis mais baixos. Na sua essência, o BFO fornece uma descrição formal das distinções entre: a) universal e particular, (b) continuante e ocorrente, (c) dependente e independente e (d) formal e material (SMITH;

[2] Disponível em http://basic-formal-ontology.org. Acesso em 08 de nov. 2019
[3] https://www.iso.org/standard/71954.html acesso em Novembro de 2019

KUMAR; BITTNER, 2005). Apesar de as explicações abaixo se referirem a exemplos da medicina, os conceitos podem ser aplicados a qualquer domínio.

Universais e Particulares

Primeiramente, a BFO distingue universais (também chamados de entidades, tipos, classes, espécies) e particulares (também chamados de indivíduos, exemplos, instâncias, fichas) (SMITH, 2003; BITTNER; DONNELLY; SMITH, 2004). No exemplo de Bittner, Donnelly e Smith (2004), um universal duradouro pode ser exemplificado como o ser humano, o coração, o oxigênio. Os universais ganham e perdem instâncias. Por exemplo, o ser universal humano ganha ou perde instâncias quando uma pessoa nasce ou morre.

Os universais têm instâncias que, na BFO, são, em todos os casos, particulares (entidades localizadas em regiões específicas do espaço e do tempo). Exemplo de Universal é a espécie Escherichia coli, cuja função é aumentar a produção de insulina. Exemplo de Particular é a bactéria Escherichia coli agora existente nesta placa de Petri, cuja função é aumentar a produção de insulina nas células beta do pâncreas (SMITH et al., 2005, P.3).

Além disso, a distinção entre universais e particulares nos permite fornecer um relato mais coerente das relações *is-a* e *part-of*. Assim, a relação entre universais pode ser exemplificada por todo ser humano ser um animal (*human is-an animal*), enquanto a relação entre particulares pode ser exemplificada por seu braço fazer parte do seu corpo (*arm part-of body*).

Continuantes e ocorrentes

Continuantes são entidades que podem ser fatiadas em partes, apenas ao longo da dimensão espacial, produzindo, por exemplo, as partes de sua mesa: pernas, tampo e pregos (ZEMACH, 1970). Algumas qualidades também podem ser divididas dessa maneira, como, por exemplo, a qualidade da cor de um cubo de vidro de Murano.

Ocorrentes, também chamados de eventos, processos, atividades, são marcados pelo fato de nunca existirem completamente em um único instante de tempo. Pelo contrário, são tais que se desdobram em suas sucessivas fases. Por exemplo, o processo de desenvolvimento de um embrião se desdobra através das sucessivas fases distinguidas pelo seu desenvolvimento biológico (SMITH; KUMAR; BITTNER, 2005).

Dependentes e independentes

Uma terceira distinção é aquela entre entidades dependentes e independentes. Isso reflete o fato de que, enquanto algumas entidades (planetas, pessoas, moléculas,

átomos) têm uma capacidade inerente de existir sem o apoio de outras entidades, outras precisam desse apoio para existir: uma infecção viral depende de certas instâncias de um determinado vírus e também do organismo que está infectado; a função de um órgão depende da existência do órgão de que é função (GRENON; SMITH, 2004).

Tanto a distinção contínua/ocorrente quanto a dependente/independente se aplicam ao nível de universais e particulares. Assim, o funcionamento do meu coração aqui e agora (um acontecimento particular) depende do meu coração e de sua função (ambos continuantes específicos), de uma maneira que reflete relações de dependência exatamente paralelas entre os universais correspondentes.

Formal e Material

A biologia lida principalmente com entidades referidas por termos materiais, como por exemplo, célula, núcleo, organismo, morte. As ontologias também lidam com as várias relações formais pelas quais essas entidades materiais estão conectadas (GRENON; SMITH, 2004). Os termos materiais são caracterizados pelo fato de serem aplicados a entidades em apenas um domínio da realidade. Relações formais são caracterizadas por poderem manter relações entre as entidades que abrangem diferentes domínios. Identidade, dependência e instanciação são exemplos de relações formais.

Ontologia de Herzog, BFO e *AutomotiveCyberSecurity*

Com as classes principais da ontologia de Herzog (ativos, vulnerabilidades, ameaças, objetivo de segurança e contramedidas), podemos verificar em qual tipo de entidade as classes da *AutomotiveCyberSecurity* são referenciadas na ontologia BFO.

Primeiramente, todo ativo (*asset*) é uma instância de BFO:Object, ou seja, um material continuante, pois ativos são entidades existentes, e suas instâncias representam os CPS e IoTs. Toda vulnerabilidade (*vulnerability*) é uma instância da BFO:Quality, pois as vulnerabilidades são atribuídos a um CPS e existem durante o ciclo de vida. As ameaças (*threats*) são BFO:Independent Continuant, pois existem independentemente dos ativos e das vulnerabilidades (ex.: podem ser definidas por pessoas, computadores ou mesmo formas de ataques).

Objetivo de segurança (*Security goal*) é um tipo de BFO:Quality, pois indica o nível de cibersegurança necessário para aquele determinado objeto. Contramedida é uma instância de BFO:Process, pois a cada ataque são definidos processos para ativar estratégias de cibersegurança.

Podemos perceber que as classes da ontologia de Herzog são facilmente referenciadas à ontologia de alto-nível da BFO, o que nos traz uma vantagem de podermos construir a

nossa ontologia do domínio da avaliação de cibersegurança e obtermos o mesmo resultado de encaixe na BFO.

2.10 Métricas de avaliação

Além do estudo de ontologias de alto nível e trabalhos de avaliação relacionados à cibersegurança, nota-se uma forte dependência de métricas utilizadas para entender o risco. Um objeto pode ser considerado seguro se conseguirmos medir características que tornam a afirmação verdadeira, a exemplo da J3061.

Homer et al. (2013) defendem que uma semântica clara de métricas é importante na avaliação de cibersegurança, e o desafio é que, muitas vezes, os parâmetros de entrada no modelo de métrica são inevitavelmente imprecisos. Por exemplo, é importante saber a probabilidade de uma vulnerabilidade ser explorada com êxito ao decidir sobre as prioridades de mitigação. Essa probabilidade pode ser caracterizada como a probabilidade de sucesso, assumindo certas habilidades e recursos do invasor. No entanto, essas probabilidades são praticamente impossíveis de obter, portanto, devemos confiar em estimativas imprecisas. Um modelo semântico claro para o cálculo de métricas torna possível interpretar o resultado.

Muito trabalho já foi feito na análise de dados de configuração de rede e identificação de vulnerabilidades para construir gráficos que representem os diversos ataques e seus passos, além de medir a probabilidade de sucesso no ataque (SWILER et al., 2001; POOLSAPPASIT; DEWRI; RAY, 2011; LIU; LIU, 2016). Os gráficos de ataque ilustram o efeito cumulativo das etapas de ataque, mostrando como uma série de etapas individuais pode potencialmente permitir que um invasor obtenha privilégios profundos na rede. Uma limitação dos gráficos de ataque, no entanto, é a suposição de que qualquer vulnerabilidade existente possa ser explorada. Na realidade, existe uma ampla probabilidade de que diferentes vulnerabilidades possam ser exploradas com sucesso por um atacante, dependendo da habilidade do atacante e da dificuldade da exploração. Os gráficos de ataque mostram o que é possível sem qualquer indicação do que é provável.

Com o *Common Vulnerability Scoring System* (CVSS), houve um progresso significativo na padronização e desenvolvimento de métricas para vulnerabilidades individuais (MELL; SCARFONE; ROMANOSKY, 2007). Essas medidas de risco consideram as qualidades específicas de vulnerabilidades como a habilidade necessária para explorar a fraqueza e informações conhecidas sobre a disponibilidade de um ataque.

o CVSS é uma estrutura aberta que trata informações de vulnerabilidade de uma forma operacional. Oferece uma métrica e pontuações padronizadas de vulnerabilidade em diferentes plataformas de software e hardware e um política de gerenciamento de como uma

vulnerabilidade específica deve ser validada e remediada. Além disso, o risco é priorizado, quando a pontuação é calculada, dando à vulnerabilidade uma forma contextual, ou seja, as pontuações de vulnerabilidade representam um risco real para um organização e os usuários sabem a importância de uma determinada vulnerabilidade em relação a outras vulnerabilidades através da priorização.

A principal limitação dessas métricas de vulnerabilidade é que não é possível capturar as interações de segurança das vulnerabilidades no contexto da rede da empresa. Por exemplo, uma vulnerabilidade pode ter uma pontuação CVSS alta, indicando que representa alto risco para um sistema quando a vulnerabilidade é exposta a um invasor. Mas a vulnerabilidade pode residir em um local difícil para um invasor acessar. Da mesma forma, uma vulnerabilidade pode ter uma pontuação CVSS mais baixa, mas está em um local relativamente fácil para um invasor fazer a abordagem. Para refletir com precisão os riscos de segurança que as vulnerabilidades apresentam a um rede corporativa, tanto a medição das propriedades de vulnerabilidades individuais quanto o contexto em que elas aparecem devem ser levados em consideração.

Assim, na análise de cibersegurança é importante considerar métricas e priorizações, mas também o papel dos especialistas em cibersegurança e sua interpretação sobre determinada vulnerabilidade para evitar que o foco de proteção do CPS acabe em recomendações ineficazes que podem não representar vulnerabilidades reais e, consequentemente, um direcionamento de esforço inadequado. Em razão desse papel fundamental exercido pelos especialistas em avaliação de cibersegurança, a semântica das métricas utilizadas torna-se ainda mais importante, evitando o risco de interpretações equivocadas por diferentes profissionais envolvidos na análise.

Os avanços na análise de risco como a J3061, grafos, métricas como a CVSS e semânticas claras presumem a direção que os pesquisadores tomaram na análise de vulnerabilidades e riscos. Por consequência, o caminho na construção de uma ontologia de análise de cibersegurança em CPS deve considerar referências como BFO, CVSS, J3061, além do que foi descrito em ontologias de cibersegurança de Herzog, Shahmehri e Duma (2007) como um caminho claro para o desenvolvimento do nosso trabalho.

3 Revisão Sistemática da Literatura

3.1 Introdução

A revisão sistemática de literatura seguiu o guia proposto por Kitchenham et al. (2009) e foi norteada pela seguinte questão principal:

[QP] Quais abordagens e aplicações têm sido discutidas nas pesquisas que investigam o uso de ontologias para avaliação de cibersegurança?

Justifica-se a questão principal pela necessidade de aprimorar os sistemas de segurança da informação, o que não é tema novo, mas que, cada vez mais, ganha importância e complexidade. Nesse sentido, pressupomos que o uso de ontologias possa trazer significativos avanços para esse campo do conhecimento aplicado.

Sistemas de detecção de intrusão são utilizados desde a década de 80 e métodos como *data mining*, análise de transição de estados, *clustering*, classificação e *neuro-fuzzy* foram utilizados para reduzir falsos alertas e aumentar a confiabilidade em sistemas de segurança na internet (ABDOLI; MEIBODY; BAZOUBANDI, 2010). Raskin et al. (2001) inauguram um novo campo na segurança da informação com o uso da ontologia. Os autores defendem que a ontologia é extremamente promissora como ferramenta de classificação para eventos ilimitados (ABDOLI; MEIBODY; BAZOUBANDI, 2010; MOZZAQUATRO et al., 2018), afirmando que o conhecimento sobre questões de cibersegurança e medidas de prevenção, integrado a uma ontologia abrangente e acessível às ferramentas de monitoramento, pode melhorar a detecção automática de ameaças à rede IoT e ajudar na implementação dinâmica de serviços adequados de proteção.

Para auxiliar a questão principal de pesquisa, foram criadas três questões específicas, para as quais serão buscadas respostas na literatura acadêmica:

[QE1]: Quais taxonomias organizam as bases de conhecimento de ataques e vulnerabilidades no contexto da cibersegurança?

[QE2]: Quais estratégias de avaliação em cibersegurança são suportadas por ontologias de ataques e vulnerabilidades?

[QE3]: Quais métricas de avaliação de cibersegurança em IoT e CPS são adotadas?

As questões específicas propostas se justificam pela necessidade de estabelecer etapas para responder à questão principal e pela necessidade de especificar os elementos aplicados a serem analisados na revisão sistemática de literatura. Ao apresentarmos respostas para

as perguntas específicas, serão discutidos alguns elementos que nos conduzem às respostas para a questão principal.

3.2 Protocolo de pesquisa

O processo de revisão sistemática adotado foi o de busca automática de artigos em anais de conferências e em revistas científicas publicados entre 2001 e 2020. . O período inicial da pesquisa foi escolhido pois o ano de 2001 marca o início da utilização de ontologias na solução de problemas de cibersegurança, ataques e vulnerabilidades em sistemas informativos (RASKIN et al., 2001).

As bases de dados escolhidas foram IEEE[1] , ACM[2] , Elsevier[3] e o portal de periódicos da CAPES[4]. Essas bases foram selecionadas porque elas são conhecidas por incluir estudos empíricos ou literatura de pesquisas nas áreas relacionadas à cibersegurança e às ontologias aplicadas à segurança da informação

As bases de dados escolhidas foram IEEE, ACM, Elsevier, SAE, NHTSA e a própria Capes. Essas bases foram selecionadas por serem conhecidas por incluir estudos empíricos ou literatura de pesquisas nas áreas relacionadas à cibersegurança e às ontologias aplicadas à segurança da informação em software.

Para a pesquisa automática nas bases de dados selecionadas, foram utilizadas as seguintes palavras-chave: “cybersecurity ontology”, “cybersercurity assessment”, “automotive cybersecurity”, “IoT cybersecurity ontology”, “CPS cybersecurity ontology”, "Automotive Cybersecurity Assessment"e “cybersecurity assessment framework”, “taxonomy of cyber attacks”, taxonomy of vulnerabilities”. Adicionalmente, foram utilizadas combinações de palavras por meio de conectores lógicos, que formaram a seguinte string de busca: [cybersecurity ontology AND cybersecurity assessment framework], [cybersecurity ontology AND (IOT OR CPS OR automotive) AND (assessment OR framework)].

Além dos procedimentos acima, optou-se por incluir na RSL, as principais normas de avaliação em cibersegurança em CPS automotivos: norma SAE J3061 e o relatório do NHTSA - DOT HS 812 (*Characterization of Potential Security Threats in Modern Automobiles*), que foram integralmente analisadas em relação às taxonomias que elas citam e empregam[5].

[1] Disponível em: https://ieeexplore.ieee.org/Xplore/home.jsp. Acesso em 06 de jan. 2020.
[2] Disponível em: https://dl.acm.org/. Acesso em 06 de jan. 2020.
[3] Disponível em: https://www.elsevier.com/pt-br. Acesso em 06 de jan. 2020.
[4] Disponível em: http://www.periodicos.capes.gov.br/. Acesso em 06 de jan. 2020.
[5] As referidas normas são adotadas em todo o setor automotivo mundial, incluindo os fabricantes norte-americanos, europeus e asiáticos.

3.2.1 Critérios de inclusão e exclusão

Seguindo o protocolo de Kitchenham et al. (2009), foram selecionados os artigos que passaram por revisão por pares, publicados entre 2001 e 2020, que discutem o uso de ontologias na solução de problemas de avaliação em cibersegurança em Internet, IoT ou CPS, a utilização de taxonomias como forma de organizar bases de dados em ataques e vulnerabilidades, os *frameworks* de avaliação e detecção em cibersegurança em IoT ou CPS automotivos e a utilização de métricas de avaliação de segurança cibernética.

Foram excluídos os artigos que se enquadraram nos seguintes critérios: artigos anteriores a 2001; artigos fora do contexto de cibersegurança, ataques e vulnerabilidades; artigos duplicados do mesmo estudo em revistas diferentes; e dissertações de mestrado, editoriais, prefácios, entrevistas, correspondências, discussões, comentários, cartas, materiais derivados de *workshops* e de painéis.

3.2.2 Avaliação de relevância

Foram definidos critérios de relevância para classificar os artigos selecionados, com peso de 0 a 1 (Quadro 1). Os critérios de relevância foram pesados da seguinte forma: (S)=1 representa que o critério foi totalmente respeitado; (P)=0,5 representa que o critério foi parcialmente respeitado; e (N)=0 representa que o critério não foi respeitado ou desconhecido.

Quadro 1 – Critérios de relevância na classificação de artigos

Critério	**Relevância**
QA1	O artigo responde ou contribui claramente com objetivo da pesquisa?
QA2	O artigo apresenta uma ontologia clara em avaliação de cibersegurança?
QA3	O artigo apresenta um método claro de avaliação de cibersegurança?
QA4	O artigo apresenta evidência de utilização prática em processos de avaliação em cibersegurança?

Fonte: Dados da pesquisa.

Os critérios de relevância da QA1 à Q4 foram avaliados conforme a seguir:

- QA1: S (sim) o artigo reponde ou contribui claramente com o objetivo da pesquisa; P (parcialmente), o artigo responde de forma implícita; N (não), o artigo não responde clara ou de forma implícita ao objetivo da pesquisa e não pode ser facilmente inferido.
- QA2: S (sim), os autores confirmaram no artigo a existência de uma ontologia clara e declarada; P (parcialmente), os autores pesquisaram e confirmaram uma forma de ontologia ou taxonomia mesmo que rudimentar; N (não), os autores pesquisaram e o artigo não inclui alguma referência à ontologia.

Tabela 1 – Artigos recuperados pela RSL

Repositórios	Inicialmente recuperados	Fase 1 (Duplicados)	Fase 2 (Análise Título)	Fase 3 (Análise Resumo)
Capes	320	78	30	8
IEEE	10	5	1	1
Elsevier	15	5	5	5
ACM Digital	433	230	8	1
SAE	4	1	1	1
NHTSA	3	1	1	1
NIST	2	2	2	1
Total	785	320	44	18

Fonte: Dados da pesquisa.

- QA3: S (sim), o artigo apresenta um guia, *framework* ou método de avaliação suportada por alguma ontologia ou taxonomia de avaliação em cibersegurança; P (parcialmente), os autores pesquisaram e confirmaram de forma indireta, a existência de alguma metodologia de avaliação suportada por ontologia; a N (não), não foi possível identificar de forma clara ou indireta a existência de um guia ou método de avaliação.

- QA4: S (sim), o artigo apresenta exemplos práticos de avaliação em cibersegurança com suporte ontológico; P (parcialmente), o artigo apresenta exemplo(s), mesmo que de forma indireta, do uso de ontologia na avaliação em cibersegurança; N (não), não apresenta exemplos.

3.2.3 Processo de Extração

Durante o processo de busca e extração, foram encontrados 785 artigos de acordo com os critérios adotados. Num segundo estágio, removemos artigos duplicados em razão das diferentes bases de dados. Na terceira fase, eliminamos artigos cujos títulos não tinham relação com o tema proposto e, na quarta fase, removemos artigos cujo resumo não apresentava relação com o objetivo da pesquisa.

Foram recuperados 18 artigos após a aplicação dos filtros, de acordo com o protocolo estabelecido, e que respondem as QEs. Após o processo de recuperação, os artigos selecionados foram lidos integralmente e aplicados os critérios de relevância

3.2.4 Classificação dos artigos

Os artigos foram classificados em áreas de interesse que correspondem aos objetivos da pesquisa (Quadro 2) A classificação oferece uma forma de agrupar os artigos conforme

as questões auxiliares desta pesquisa.

Quadro 2 – Classificação dos artigos da RSL

Descrição	Acrônimo
Taxonomia de Ataque e vulnerabilidade	TXN_ATQ
Avaliação Ontologia em cibersegurança	AVAL_ONTO
Métricas de avaliação em cibersegurança	MTR
Frameworks de avaliação em Cibersegurança	FRM_WK

Fonte: Dados da pesquisa.

3.3 Artigos selecionados

A Tabela 2 apresenta o resultado dos artigos selecionados e seus autores, conforme o protocolo proposta na RSL. A Tabela 2 está organizada pela classificação dos artigos conforme proposto no Quadro 2, além dos respectivos repositórios e o peso em relação aos critérios de relevância.

Tabela 2 – Artigos selecionados na RSL

Autor / Ano	Título	Revista / Conferência	Repositório	Classificação
Fenz e Ekelhart (2006)	*Security Ontology: Simulating Threats to Corporate Assets*	*Book Session: Information Systems Security*	Springer	AVAL_ONTO
Abdoli et al. (2010)	*An Attacks Ontology for computer and networks attack*	*Innovations and Advances in Computer Sciences and Engineering*	Springer	AVAL_ONTO
Ficco (2013)	*Security event correlation approach for cloud computing*	*International Journal of High Performance Computing and Networking*	Researchgate	AVAL_ONTO
Georgescu; Smeureanu (2017)	*Using Ontologies in Cybersecurity Field*	*Informática Econômica*	Researchgate	AVAL_ONTO

Continua na próxima página

Tabela 2 – continuação da página anterior

Autor / Ano	Título	Revista / Conferência	Repositório	Classificação
Bergner e Lechner (2017)	*Cybersecurity Ontology for Critical Infrastructures*	*International Conference on Knowledge Engineering and Ontology Development*	SCI	AVAL_ONTO
Balduccini et al. (2018)	*Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems*	*Living in the Internet of Things: Cybersecurity of the IoT*	IEEE	AVAL_ONTO
Tao et al. (2018)	*Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes*	*Future Generation Computer Systems*	MDPI	AVAL_ONTO
Álavarez e Petrovic (2003)	*A new taxonomy of Web attacks suitable for efficient encoding*	*Computer and Security*	Elsevier	TXN_ATQ
Hansman e Hunt (2005)	*A taxonomy of network and computer attacks*	*Computer and Security*	Elsevier	TXN_ATQ
Igure e Willimas (2008)	*Taxonomies of attacks and vulnerabilities in computer systems*	*Communications Surveys & Tutorials*	IEEE	TXN_ATQ
Mozzaquatro (2018)	*An Ontology-Based Cybersecurity Framework for the Internet of Things*	*Sensors*	MDPI	FRM_WK

Continua na próxima página

Tabela 2 – continuação da página anterior

Autor / Ano	Título	Revista / Conferência	Repositório	Classificação
McCarthy et al. (2014)	*Characterization of potential security threats in modern automobiles: A composite modeling approach.*	-	NHTSA	FRM_WK
Schmittner et al. (2016)	*Using SAE J3061 for Automotive Security Requirement Engineering*	*Computer Safety, Reliability, and Security*	Springer	FRM_WK
SAE J3061 (2016)	*Cybersecurity guidebook for cyber-physical automotive systems*	-	SAE	FRM_WK
Wu; Zhang; Cao (2017)	*Safety Guard: Runtime Enforcement for Safety-Critical Cyber-Physical Systems: Invited*	*DAC proceedings*	ACM	FRM_WK
Griffor (2017)	*Framework for Cyber-Physical Systems*	-	NIST	FRM_WK
Razzaq et al. (2014)	*Ontology for attack detection: An intelligent approach to web application security*	Computer and Security	Elsevier	MTR
Homer et al. (2013)	*Aggregating vulnerability metrics in enterprise networks using attack graphs*	ARES proceedings	ACM	MTR

Fonte: Dados da pesquisa.

3.4 Análise e discussão dos resultados da RSL

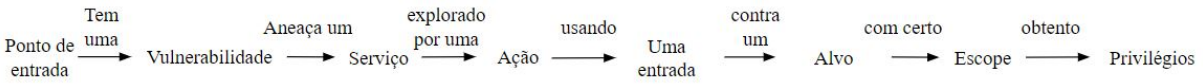
Com os artigos selecionados, foi possível responder às questões de pesquisa propostas, conforme apresentado a seguir.

3.4.1 [QE1]: Quais taxonomias organizam as bases de conhecimento de ataques e vulnerabilidades no contexto da cibersegurança?

Os ataques contra ativos informacionais estão se tornando cada vez mais sofisticados, distribuídos e com rápida difusão. Portanto, é necessário classificá-los por meio de taxonomias. Esse tipo de classificação pode ser usado na execução sistemática da avaliação da cibersegurança de um sistema.

Álvarez e Petrović (2003) propuseram uma taxonomia de ataques na web adequada para uma codificação eficiente, usando como referência o ponto de entrada do sistema, onde existe uma vulnerabilidade que ameaça um serviço, contra um alvo de escopo determinado, obtendo, assim, certo privilégio como permissão administrativa. A taxonomia

Figura 2 – Trabalhos relacionados - Taxonomia de ataques



Fonte: Adaptado de Álvarez e Petrović (2003)

dos autores definiu um esquema semântico de codificação dos ataques na web, removendo redundâncias na sua descrição, o que gerou economia de tempo e memória no processamento. A codificação e a economia no esforço computacional permitiram sua utilização em sistemas de detecção de intrusão como *firewalls*.

Os autores evidenciam que a aplicação de um IDS (*Intrusion Detection System*) pode funcionar melhor com a utilização da taxonomia, pois seu emprego permite que sejam gerados menos falsos alertas que um firewall tradicional. Conforme destacam os autores, a eficácia no bloqueio de ataques e a decisão sobre sua gravidade são cruciais para uma resposta eficaz. A taxonomia ajuda nessa tarefa ao prover um grupo exaustivo de categorias exclusivas por meio das quais os ataques podem ser classificados sem ambiguidade, através de métodos que empregam o esquema de classificação.

Hansman e Hunt (2005) utilizaram a base de dados do projeto CVE[6] (*Common Vulnerabilities and Exposures*) como parte da sua taxonomia de ataque. Corpus como o

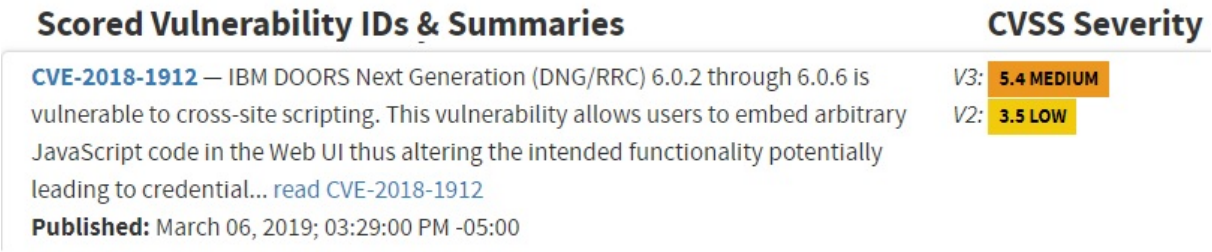
[6] CVE (*Common Vulnerabilities Exposures*) está disponível em http://cve.mitre.org. Acesso em 19 janeiro de 2019.

CVE são extremamente úteis pela sua ampla base de conhecimento sobre vulnerabilidades em diversos sistemas operacionais. O projeto CVE, originalmente proposto por Baker et al. (1999), teve apoio do U.S. Department of Homeland. A comunidade de cibersegurança endossou a importância do CVE via produtos compatíveis (*CVE-compatible*) e em 2011 o DISA (*U.S. Defense Information Systems Agency*) determinou que fabricantes e distribuidores apresentem identificadores CVE em produtos utilizados por aquela agência.

Assim como o CVE, o NVD[7] (*U.S. National Vulnerability Database*) é um banco de dados abrangente sobre vulnerabilidades em cibersegurança, que integra todos os recursos de vulnerabilidade do governo dos EUA disponíveis publicamente e fornece referências à indústria. As informações do NVD podem ser acessadas através de web semântica, e seus dados permitem a automação do gerenciamento de vulnerabilidades, medição de segurança e conformidade. O banco de dados da NVD inclui referências a listas de verificação de segurança, falhas de software relacionadas à segurança, configurações incorretas, nomes de produtos e métricas de impacto.

O CVSS (*Common Vulnerability Scoring System*) disponível no NVD fornece uma estrutura aberta de comunicação das características e impactos das vulnerabilidades em tecnologia da informação (TI). Seu modelo é quantitativo e permite aos usuários uma confiabilidade no processo de avaliação. Assim, o CVSS é bem adequado como um sistema de medição padronizada para indústrias, organizações e governos que necessitem de pontuações consistentes de impacto de vulnerabilidade (Figura 3).

Figura 3 – Sumário das ameaças e avaliação da severidade de acordo com o CVSS



Fonte: https://nvd.nist.gov/ acessado em 06/03/2019.

Em resumo, as taxonomias de ataques nos dão uma visão de padrões de ataques. Podemos dizer que o padrão de ataque é uma sequência de passos do ataque contra uma fraqueza a ser explorada em um software e ajuda a identificar e qualificar o risco de um determinado ataque. Os padrões de ataques se tornaram mais viáveis em termos computacionais após a criação e definição formal de taxonomias como a *Common Attack Pattern Enumeration and Classification* (CAPEC) e CVE (BARNUM, 2012). O Quadro 3

[7] NVD (*US National Vulnerability Database*) está disponível em https://nvd.nist.gov. Acesso em 06 março de 2019.

apresenta um resumo das principais bases de dados que permitem aos desenvolvedores se guiar e compartilhar informações sobre ataques e vulnerabilidades. As bases de dados permitem ao desenvolvedor eliminar ambiguidades e aumentar a precisão, automatizar, integrar e correlacionar dados e processos, permitindo um desenvolvimento rápido de contramedidas.

Quadro 3 – Principais bases de dados em cibersegurança

Recurso	Propósito	Site
CAPEC - *Common Attack Pattern Enumeration and Classification*	Fornece um catálogo publicamente disponível de padrões de ataque, juntamente com um esquema abrangente e taxonomia de classificação	https://capec.mitre.org/
NVD - *National Vulnerability Database*	O NVD é um repositório do governo dos EUA de dados de gerenciamento de vulnerabilidade embasado em padrões representados usando o SCAP (*Security Content Automation Protocol*)	https://nvd.nist.gov/
JVN - *JAPAN Vulnerability Notes*	Fornece informações de vulnerabilidade em japonês e é descrito de acordo com seu próprio esquema em RDF	https://jvn.jp/en/
CVE - *Common Vulnerabilities and Exposures*	Dicionário de descrições padronizadas para vulnerabilidades e exposições	http://cve.mitre.org

Continua na próxima página

Tabela 2 – continuação da página anterior

Recurso	Propósito	Site
CWE - *Common Weakness Enumeration*	Lista de fraquezas comuns de segurança de software desenvolvidas pela comunidade. Ela serve como uma linguagem comum, uma ferramenta de medição para ferramentas de segurança de software e como uma linha de base para esforços de identificação, mitigação e prevenção de fraquezas.	https://cwe.mitre.org/

Fonte: Dados da pesquisa.

3.4.2 [QE2]: Quais estratégias de avaliação em cibersegurança são suportadas por ontologias de ataques e vulnerabilidades?

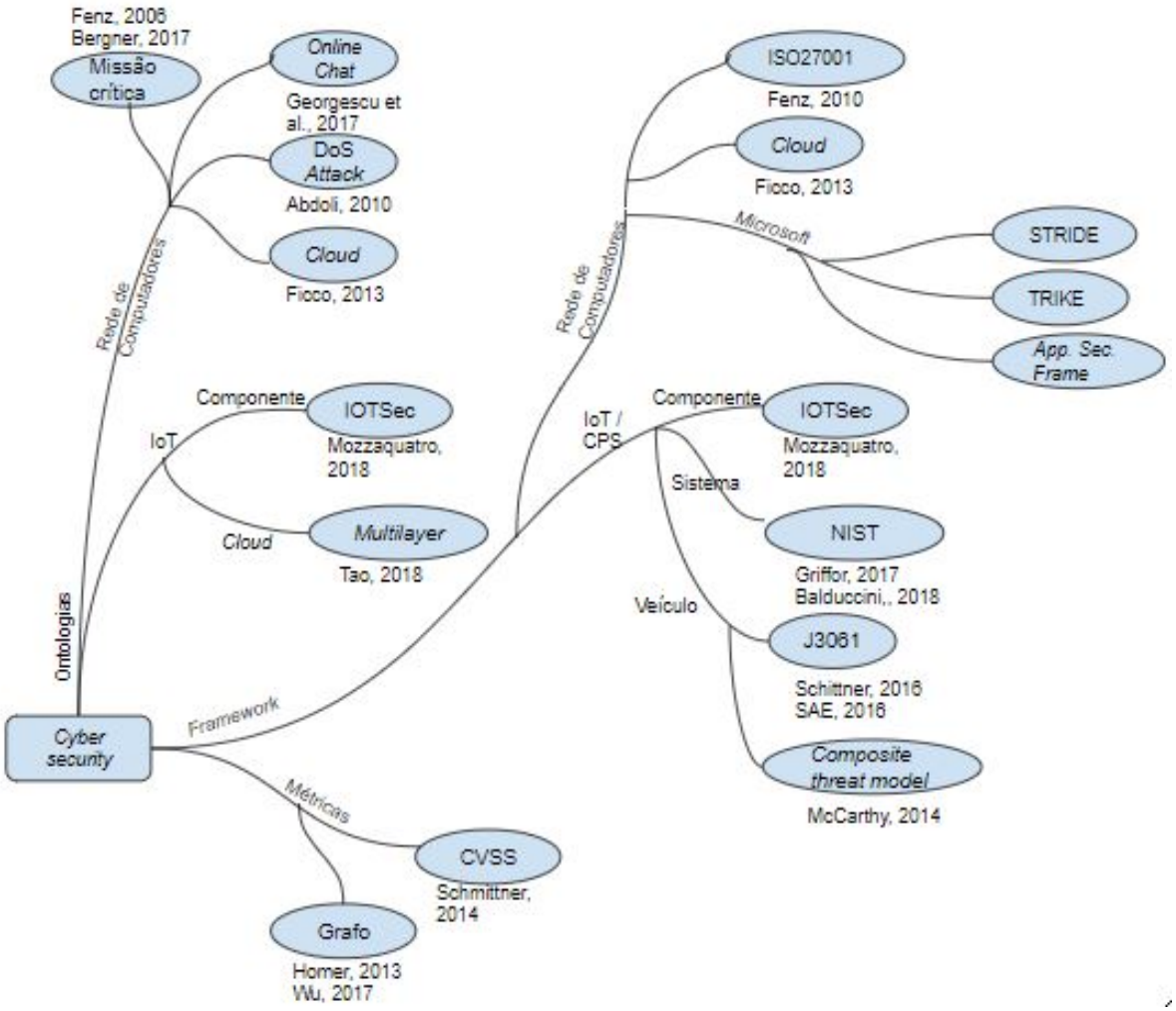
Avaliação de risco é um componente da gestão de segurança da informação voltado para a identificação de ameaças e vulnerabilidades, potenciais impactos decorrentes da perda de confidencialidade, integridade e/ou disponibilidade de ativos de informação.

Na Figura 4, é apresentado um resumo das principais ontologias e métodos de avaliação encontrados durante a revisão sistemática. O critério que utilizamos para a construção da árvore foi baseado na classificação de artigos de Petersen et al. (2008). Os autores recomendam a busca de facetas coincidentes nos artigos e a elaboração de um mapa esquemático para agrupá-los em grupos e subgrupos. O resultado disto é apresentado na Figura 4, com os grupos de ontologias, *frameworks* e métricas, além dos subgrupos de rede de computadores, IoT e CPS automotivos.

A revisão abordou dois grandes construtos: ontologia e *framework* de cibersegurança. Dentro destes construtos, o mapa da Figura 4 fornece os domínios de interesse da revisão sistemática: Rede de computadores e IoT/CPS. Na sequência, descrevemos as pesquisas recuperadas dentro de cada domínio.

Abdoli, Meibody e Bazoubandi (2010) desenharam uma ontologia para ataques em computadores e redes de computadores. Os autores estudaram diferentes números de conexões e *logs* que causaram ataques do tipo DoS (*Denied of Service*). A utilização do *Protegé* e SPARQL suportou análises e raciocínios de sequências de *logs* extensas. A importância desse estudo é que ele não somente comprovou a efetividade da análise

Figura 4 – Principais ontologias e *frameworks* de avaliação em cibersegurança



Fonte: dados da pesquisa

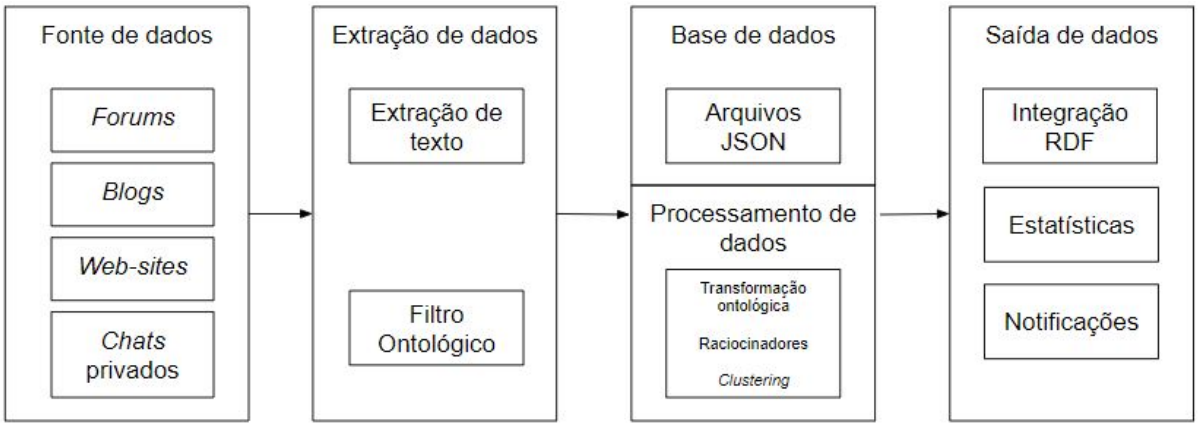
holística que a ontologia proporciona, mas também apresentou uma forma efetiva de integração entre conhecimento sobre tipos de ataques e estudos de casos reais. Nesse tipo de situação, o desafio da equipe de segurança da informação é analisar sequências de informações que envolvem grande quantidade de parâmetros e dados que podem ou não indicar ataques.

Ficco (2013) utilizou a mesma estratégia de análise para computação em nuvem ao investigar passos de ataques através de correlação de eventos de segurança. O processo de detecção de intrusão empregou uma abordagem híbrida capaz de analisar eventos por meio de ontologia para detectar sintomas de intrusão em computação distribuída. Uma *query* foi usada para analisar uma sequência de requisições através de uma base de conhecimento sobre ameaças para decidir quando um comportamento particular representava uma ameaça potencial.

Georgescu e Smeureanu (2017) utilizaram a web semântica para extração de textos

on-line em linguagem natural para detectar atividades de invasores (Figura 5). Os autores encontraram correlação entre atividades dos *hackers* e fontes de informação como fóruns e *chats* privados, resultando em uma forma de extrair informações para avaliação das ameaças que vão além dos bancos de dados da CVE (*Common Vulnerabilities Exposures*) e também do conhecimento adquirido pelos engenheiros de cibersegurança. Na abordagem dos autores, as fontes de informações podem ser fóruns, blogs, *web-sites* e *chats* privados. As informações, extraídas por meio de *scrapers*, foram carregadas em uma ontologia e, em seguida, geradas estatísticas de possíveis atividades atribuídas aos hackers. No sistema desenvolvido pelos autores, são empregados raciocinadores para emissão de notificações, aumentando, assim, a eficiência na análise de uma massa de dados.

Figura 5 – Arquitetura de extração de informações sobre ataques em textos *on-line*



Fonte: Adaptado de Georgescu e Smeureanu (2017)

Mozzaquatro et al. (2018) propuseram um *framework* de avaliação em cibersegurança de componentes básicos utilizados na IoT e seus processos por meio da ontologia IoTSec[8]. Essa ontologia foi desenhada para reunir conhecimento sobre alertas e possíveis ameaças e ataques, prover a capacidade de raciocinar e descobrir dados implícitos em uma informação sobre problemas de cibersegurança.

No exemplo utilizado durante o trabalho, os autores mostraram como o ambiente IoT é frequentemente suscetível às ameaças em uma rede Wi-Fi em razão de pontos de acesso mal configurados, interceptação de dados e negação de serviço. A Figura 6 mostra o resultado da *query* que emprega a ontologia IoTSec. O resultado da consulta mostra as vulnerabilidades em ativos da rede, as criptografias disponíveis e o status atual, reprovado ou seguro.

Tao et al. (2018) propuseram uma ontologia para cibersegurança em IoT, fundamentada em um modelo de arquitetura em nuvem multicamadas, para permitir interações entre os dispositivos IoT em casas inteligentes que geram uma grande quantidade de dados.

[8] disponível em http://iotsec.brunomozza.com/. Acesso em 06 mar. 2019.

Figura 6 – Exemplo de *query* proposta pelo *framework* de Mozzaquatro et al. (2018)

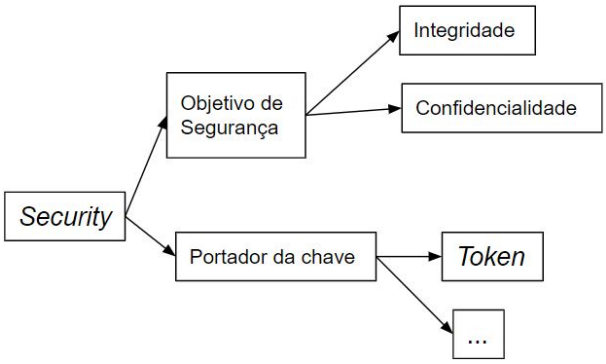
```
SELECT ?ASSET ?VULN ?THREAT ?SECPROP ?SECMEC_1 ?FEATURE_1
WHERE {
  ?VULN iotsec:isVulnerabilityOf ?ASSET .
  ?VULN iotsec:isThreatensBy ?THREAT .
  ?THREAT iotsec:affects ?SECPROP .
  ?SECMEC_1 iotsec:isSecurityMechanismOf ?THREAT .
  ?SECMEC_1 iotsec:hasFeature ?FEATURE_1 .
  ?SECMEC_1 rdfs:label ?SMLabel .
  FILTER regex (?SMLabel, 'WEP')
}
```

ASSET	VULNERABILITY	THREAT	SECURITYPROPERTY	SECMEC_1	FEATURE_1	SM_2	FEAT_2
WiFi	UnauthorizedAccess	Eavesdropping	Authentication	WEP	Deprecated	WPA1	Deprecated
WiFi	UnauthorizedAccess	Eavesdropping	Authentication	WEP	Deprecated	WPA2	Secured

Fonte: Mozzaquatro et al. (2018)

A importância da ontologia criada pelos autores decorre do fato de a heterogeneidade de dispositivos, serviços, protocolos de comunicação, padrões e formatos de dados envolvidos nas casas inteligentes, oriundos de diferentes fornecedores, afetar negativamente a utilização e proliferação da IoT. A ontologia desenvolvida pelos autores suporta a representação dos dados, conhecimentos, serviços de segurança entre o provedor de serviço e os usuários. A ontologia define um grupo comum de vocabulário, um objetivo de segurança, como integridade através de assinatura digital, confidencialidade por encriptação e um *token* de segurança. Por meio da ontologia proposta, fabricantes de dispositivos seriam capazes de definir políticas de segurança, indicando a habilidade de interações e interoperações (Figura 7).

Figura 7 – Ontologia de segurança em IoT de Tao et al. (2018)



Fonte: Adaptado de Tao et al. (2018)

McCarthy, Harnett e Carter (2014) caracterizaram o primeiro modelo de potenciais ataques em veículos automotores. Com o objetivo de aprimorar as melhores práticas de segurança cibernética na indústria automotiva, os autores reuniram informações em uma

base de conhecimento coletivo sobre segurança cibernética automotiva visando a ajudar a descrever os ambientes de risco e ameaças, além de dar suporte a tarefas de acompanhamento usadas para estabelecer diretrizes de segurança durante o desenvolvimento de automóveis.

Os autores desenvolveram ferramentas de avaliação, e requisitos de mínima performance foram desenvolvidos para cibersegurança automotiva, baseando-se nos modelos da *Microsoft Composite Threat Model*, STRIDE, TRIKE e *Application Security Frame* (MCCARTHY; HARNETT; CARTER, 2014).

O *framework* adotado pelos autores foi dividido em duas partes: a primeira identifica as aplicações e sistemas críticos e a segunda determina e analisa as ameaças através de uma matriz de potenciais ataques, nível de sofisticação, dificuldade de implementação e probabilidade de ocorrência.

Schmittner et al. (2016) mostraram a utilização do TARA (*Threat Analysis and Risk Assessment*), que suporta avaliação de risco a partir de um cenário de ataque para ajudar organizações a identificar e avaliar ameaças envolvidas no design em cibersegurança em CPS automotivos, desde a fase de conceito, produção, operação, serviço e de descarte. Nota-se que a avaliação de risco seguida pelos autores é uma adaptação do projeto HEAVENS, proposto por Schmittner et al. (2014), também recomendado pela norma J3061.

Na pesquisa de Schmittner et al. (2016), a avaliação de risco recebeu pontuações conforme: (1) capacidade de execução do ataque; (2) disponibilidade de informação do sistema alvo; (3) acessibilidade ao alvo; e (4) tecnologia necessária para comprometer remotamente um sistema do automóvel (Quadro 4).

Quadro 4 – Principais métricas em avaliação de risco em ativos automotivos

Cenário de ataque	Ameaça	Efeito	Prob. ataque	Severidade	Risco
Ativo: Software/Applicações					
Explorar vulnerabilidades conhecidas no SO ou nos aplicativos remotamente	Instalar *rootkit, Trojan*	Assumir o controle das operações do sistema CPS, alterar parâmetros e acessar dados	9 (2+1+3+3)	4	Alto
Explorar vulnerabilidades conhecidas no SO ou aplicativo remotamente	Apagar componente de software	Reduzir a funcionalidade do CPS	9 (2+1+3+3)	2	Medium

Fonte: Adaptado de Schmittner et al. (2016)

O NIST (*U.S. National Institute of Standards and Technology*) hospedou um grupo

de trabalho público sobre sistemas físicos cibernéticos (CPS) com o objetivo de identificar insumos envolvidos em CPS para definir um *framework*[9] de referência que contivesse definições comuns e facilitasse a interoperabilidade entre tais sistemas.

Balduccini et al. (2018), tendo como referência o trabalho desse grupo, descreveram uma avaliação de fidedignidade através de uma ontologia voltada para *safety*, confiabilidade, *security*, resiliência e privacidade. Merecem destaques no referido trabalho a utilização da ontologia e a avaliação de confiança em um sistema de LKAS (*lane keeping assistant*), ou seja, um sistema que tem por finalidade manter um automóvel dentro da sua pista, utilizando duas câmeras de vídeo. Caso o CPS perceba que o automóvel tenha abandonado sua faixa de rolamento, o sistema assume o volante na tentativa de corrigir a rota do veículo. Esse sistema utiliza câmeras e radares para atuar. Os autores fizeram uma avaliação do sistema por meio de conexões com algumas bases de dados de ameaças e ataques, como proposto por Hansman e Hunt (2005).

Ainda, Balduccini et al. (2018) mostraram, através de um caso de uso, como *hackear* o sistema LKAS e operá-lo externamente, invertendo as imagens gravadas pelas câmeras, o que ocasionou perda de imagens, consequentemente, falha em segurança (*safety*).

Os autores formalizam o sistema em dois níveis (Figura 8): (L1) *aspects* e *concerns* e (L2) *properties*, o que pode ser aplicável a qualquer CPS. Nesse *framework*, os autores puderam estabelecer dependências e restrições entre os níveis, através de uma codificação lógica utilizada pelo raciocinador. No caso da inversão de gravação das câmeras, a declaração de dependência entre as propriedades sugere perda de integridade, caracterizando falha de segurança e desligamento do sistema.

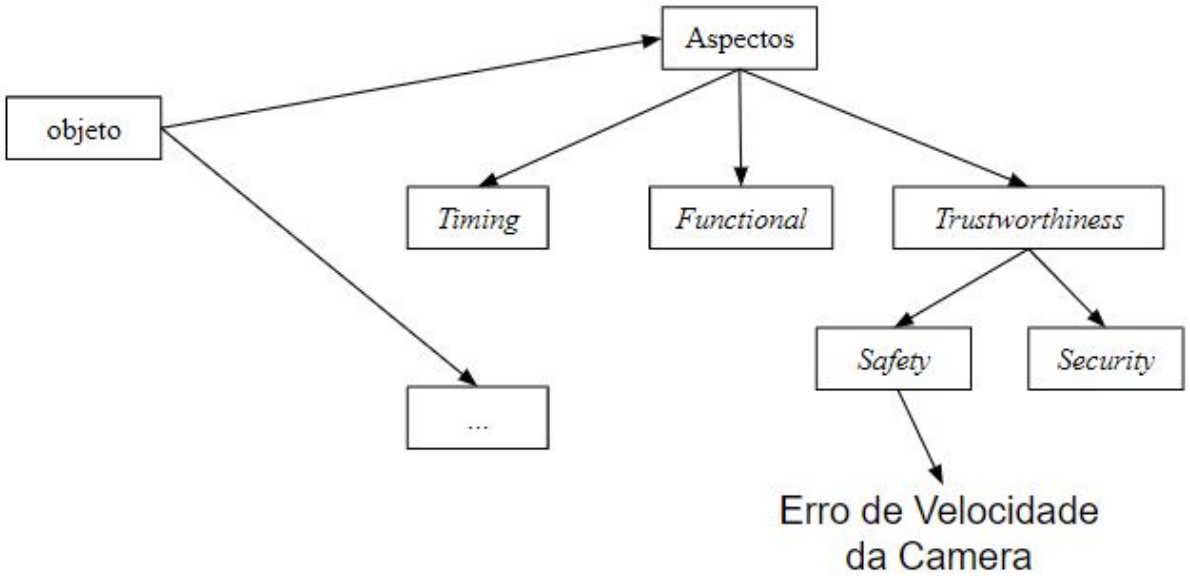
3.4.3 [QE3]: Quais métricas de avaliação em cibersegurança em IoT e CPS são adotadas?

Durante a análise da QE1, algumas métricas de avaliação já foram apontadas, como aquelas apresentadas no projeto HEAVENS, de Schmittner et al. (2014), no CVSS do NVD e nos modelos *Microsoft STRIDE*. Além dessas já citadas, métricas que empregam grafos também são importantes ferramentas para avaliação de ataques complexos, nos quais hackers precisam seguir vários passos até conseguir um ataque bem-sucedido.

Wu, Zhang e Cao (2017) utilizaram grafos para suportar administradores de TI a combater os ataques cujos alvos são vários servidores. A combinação de máquinas e serviços em redes corporativas é cada vez mais complexa e, nesse contexto, se torna uma tarefa difícil para administradores avaliar a segurança geral da rede. Para manter a segurança e a disponibilidade da infraestrutura, um vocabulário e soluções automatizadas comuns

[9] O *framework* do NIST está disponível em https://www.nist.gov/. Acesso em: 25/mar. 2019

Figura 8 – Ontologia simplificada de *concern* do CPS LKAS de Balduccini

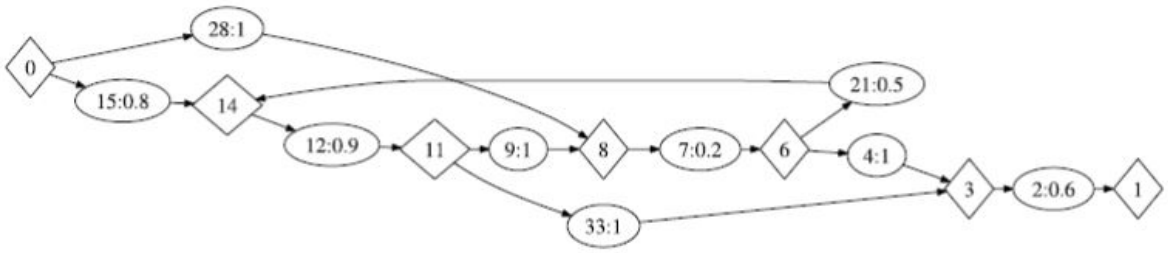


Fonte: Adaptado de Balduccini et al. (2018)

são uma importante ferramenta para troca de conhecimento de segurança e análise de possíveis ataques. Destarte, gráficos de ataque ajudam a ilustrar os caminhos de ataques de vários estágios, que são potencialmente complexos. Além disso, um grafo pode ajudar a quantificar uma sequência de requisições a uma rede distribuída, o que torna mais objetiva a análise de possíveis ameaças a um sistema.

Homer et al. (2013) agregaram métricas de avaliação de risco a redes corporativas para os gráficos de ataque, com o objetivo de trazer informações objetivas para respostas a questões, como, por exemplo: se uma determinada modificação for feita na rede corporativa, ela se torna mais ou menos vulnerável? Os autores se basearam em métricas da CVSS (*Commom Vulnerability Scoring Systems*), combinando-as com os possíveis passos de um provável ataque, gerando métricas de risco de segurança através de pontos cumulativos de cada passo do ataque (Figura 9). No exemplo, o privilégio inicial do atacante é 0 (Internet) e, para ganhar o privilégio 14 (*workstantion*), é necessário lançar o *exploit* 15 (*victim browse a malicious website*) que tem com uma probabilidade de 80% de chance de sucesso dada pela CVSS (na notação do grafo 15:0,8). O próximo passo do ataque é ganhar o privilégio 11, 8, 6 e 3, através de outros mecanismos de *exploit*, até o atacante chegar ao privilégio 1 (*root*). A métrica gerada é o somatório dos passos de 0 até 1, e seus relativos pesos nos dão a dimensão do risco. Essa métrica pode nortear ações de administradores através de ações para mitigar ou eliminar a vulnerabilidade.

Figura 9 – Grafo de ataque e as métricas geradas a cada passo utilizando a CVSS



0: Attacker Located internet
1: execCode(dbServer, root)
2: remote exploit of CVE-2009-2446
3: netAccess(dbServer,tcp,3306)
4: multi-hop access
6: execCode(webServer,apache)
7: remote exploit of CVE-2006-3747]
8: net Access(webServer, tcp,80)
9: multi-hop access
11: execCode(workStation, user Account)
12: remote exploit of CVE-2009-1918
14: access Malicious Input (WorkStation, user, IE)
15: victim browse a malicious website
21: victim browse a compromised website
28: direct network access
33: multi-hop access

Fonte: Homer et al. (2013)

3.5 Conclusões da RSL

O uso de ontologias em cibersegurança é defendido por vários autores pela rapidez e pela forma holística de tratar muitos parâmetros na avaliação dos riscos envolvidos. A representação formal pode suportar desenvolvedores e também estabelecer um conhecimento formal e compartilhado sobre ataques e vulnerabilidades.

Em todos os trabalhos que foram objeto de análise na RSL realizada, denota-se a clara necessidade de organização ontológica para facilitar e unificar o entendimento dos *stakeholders* envolvidos na tarefa de avaliar riscos e implementar soluções para cibersegurança, sejam elas direcionadas para uma rede de computadores, IoT ou CPS.

Respondendo de maneira ampla à questão de pesquisa colocada, os artigos que abordam a avaliação em cibersegurança podem ser classificados em dois grupos principais. No primeiro, os autores utilizam ontologias na etapa de desenvolvimento de sistemas para avaliação dos requisitos de segurança (MCCARTHY; HARNETT; CARTER, 2014; SCHMITTNER et al., 2016; MOZZAQUATRO et al., 2018; TAO et al., 2018). Num segundo grupo de artigos, estão as pesquisas referentes aos sistemas em operação. Nesses casos, seja na internet ou em IoT, os autores utilizam ontologias com o suporte de raciocinadores para identificar padrões e prever ataques (HANSMAN; HUNT, 2005; GEORGESCU; SMEUREANU, 2017; BALDUCCINI et al., 2018).

Tanto no desenvolvimento quanto na operação, os domínios influenciaram na construção das ontologias. Por exemplo, no caso de um IoT ou um CPS trabalhando

em multicamadas, a ontologia de Tao et al. (2018) e o *framework* de sistema do NIST de Griffor et al. (2017) mostraram-se mais adequados à solução, ao passo que o mesmo CPS/IoT no domínio do componente poderia ser mais adequado ao IoTSec, de Mozzaquatro, Jardim-Goncalves e Agostinho (2015).

Tanto no desenvolvimento quanto na operação, as avaliações de cibersegurança utilizam métricas reconhecidas pelo mercado como o CVSS [10] e o CVE[11]. Essas métricas estão disponíveis através de bases de conhecimento sobre ameaças e vulnerabilidades do NVD (*National Vulnerability Database*) e CWE (*Common Weakness Enumeration*) e são utilizadas pelos autores como referência para lidar com vulnerabilidades a serem corrigidas (HANSMAN; HUNT, 2005; GEORGESCU; SMEUREANU, 2017; HOMER et al., 2013; BALDUCCINI et al., 2018).

Os trabalhos em cibersegurança na internet pavimentaram os estudos realizados posteriormente em IoT, CPS e, consequentemente, no mundo automotivo. A adoção rápida do NHTSA como padrão de análise em cibersegurança e a elaboração de procedimentos como o HEAVENS da norma J3061 mostram a importância do tema no setor automotivo.

Apesar de a aplicação da IoT no domínio automotivo ser relativamente recente, os conhecimentos já consolidados sobre cibersegurança no ambiente da internet e as pesquisas já realizadas sobre ontologias de cibersegurança são fundamentais para o avanço das investigações sobre cibersegurança em CPS automotivos. A utilização de ontologias para suporte da avaliação de cibersegurança e para desenvolvimento de software embarcado automotivo é fundamental para a melhoria da qualidade desse tipo de software e para redução de potenciais vulnerabilidades dos automóveis.

Quanto a isto, o *framework* da norma J3061, com as métricas de CVSS e as ontologias do IoTSec de Mozzaquatro et al. (2018), e a ontologia em multicamadas de Tao et al. (2018) se mostram adequados como base de partida para uma avaliação em CPS.

[10] Fonte: https://nvd.nist.gov/. Acesso em 06/03/2019
[11] Fonte: https://cwe.mitre.org/. Acesso em 06/03/2019

4 Metodologia

4.1 Introdução

Nesta seção discutiremos a metodologia que utilizamos para alcançar os objetivos específicos e também como relacionamos estes objetivos para comprovar nossa hipótese de que a avaliação da cibersegurança, suportada por uma ontologia, pode contribuir na construção de um entendimento unificado do domínio do conhecimento, sendo uma ferramenta poderosa para lidar com problemas como inconsistência, ambiguidade e qualidade.

A RSL da Seção 3 abordou a literatura de diversas áreas que contribuíram para responder o OBJ1, nas análise das abordagens e aplicações que investigam o uso de ontologias para avaliação de cibersegurança, provando ser uma área de exploração, nos mostrando a direção das pesquisas desta área de conhecimento e o caminho que devemos seguir na nossa pesquisa. Seguindo os argumentos de Fontelles, Simões e Farias (2009), nossa pesquisa é uma pesquisa aplicada se valendo de ferramentas utilizadas na construção da ontologia *AutomotiveCyberSecurity* e o estudo de caso real com grupo focal.

O restante da presente seção está organizado no sentido de descrever a metodologia utilizada para a responder ao OBJ2, no desenvolvimento da ontologia *AutomotiveCyberSecurity*, ao OBJ3 e ao OBJ4 na integração da ontologia de domínio da BFO e à norma J3061 e ao OBJ5 na avaliação pelo grupo focal de especialista em cibersegurança da FCA.

4.2 Metodologia *OntoForInfoScience* no desenvolvimento de ontologia de domínio

A metodologia proposta para a construção da ontologia de *AutomotiveCyberSecurity* utilizou os passos da *OntoforInfoScience* de Mendonca (2015).

Mendonca (2015) propõe um protocolo em nove etapas: avaliação da necessidade, especificação, aquisição e extração do conhecimento, conceitualização, fundamentação ontológica, formalização da ontologia, avaliação da ontologia, documentação e disponibilização. Para efeito deste trabalho, descrevemos brevemente as etapas da *OntoforInfoScience* no processo de desenvolvimento da ontologia de domínio.

4.2.1 Avaliação de necessidade

A etapa de avaliação da necessidade é uma etapa preliminar da metodologia de construção da *OntoForInfoScience* na qual os especialistas pelo desenvolvimento da ontologia devem fazer uma avaliação real do projeto na procura da resposta à pergunta - "O projeto a ser desenvolvido e seu contexto necessitam ou demandam a construção de uma ontologia? Ou a criação de outro instrumento de representação, tal como um tesauro, seria suficiente?"

Segundo Mendonca (2015), a resposta a essa pergunta, embora trivial, é essencial para nortear os especialistas na construção da ontologia. No caso do OBJ2 o nosso projeto corresponde à indexação e à recuperação de informação em um contexto dinâmico para descrição de recursos do domínio do conhecimento da avaliação de cibersegurança, sendo fundamental a utilização de ontologias.

A resposta a esta pergunta nos remete às etapas seguintes da metodologia.

4.2.2 Documento de especificação

Nesta etapa faremos a descrição do objetivo da ontologia e a representação do conhecimento, os usuários, o rigor formal e o escopo de cobertura através de questões de competência.

O método *OntoForInfoScience* dedica alguns *templates* para auxiliar o desenvolvedor da ontologia na confecção da documentação. Além dos *templates*, com o passo-a-passo, envolvemos os especialistas em avaliação de cibersegurança com o objetivo de obtermos uma melhor cobertura nas questões de competência.

As questões de competência, de forma resumida, auxiliam ao desenvolvedor da ontologia na sua validação, ou melhor, perguntas que os especialistas de domínio normalmente enfrentam no processo da aplicação do conhecimento envolvido às quais a ontologia deve ser capaz de responder. Para ajustar as questões de competência, utilizamos o método DELPHI (SKULMOSKI; HARTMAN; KRAHN, 2007), que tem a capacidade de buscar consenso entre especialistas através de rodadas de entrevistas em da busca da priorização das questões de competência relevantes para nossa ontologia.

4.2.3 Aquisição e extração do conhecimento

Para aquisição e extração do conhecimento utilizamos a análise informal e formal de textos de especificação técnica de CPS automotivos, normas e manuais técnicos como a J3061 e entrevistas com especialistas da FCA na busca de compreensão de conceitos

de domínio, com o objetivo de construirmos um glossário que registre o conhecimento extraído.

Na extração destes conceitos, utilizamos o suporte do *Rapidminer*[1] de forma a automatizar este processo de construção de glossário através de mineração de dados.

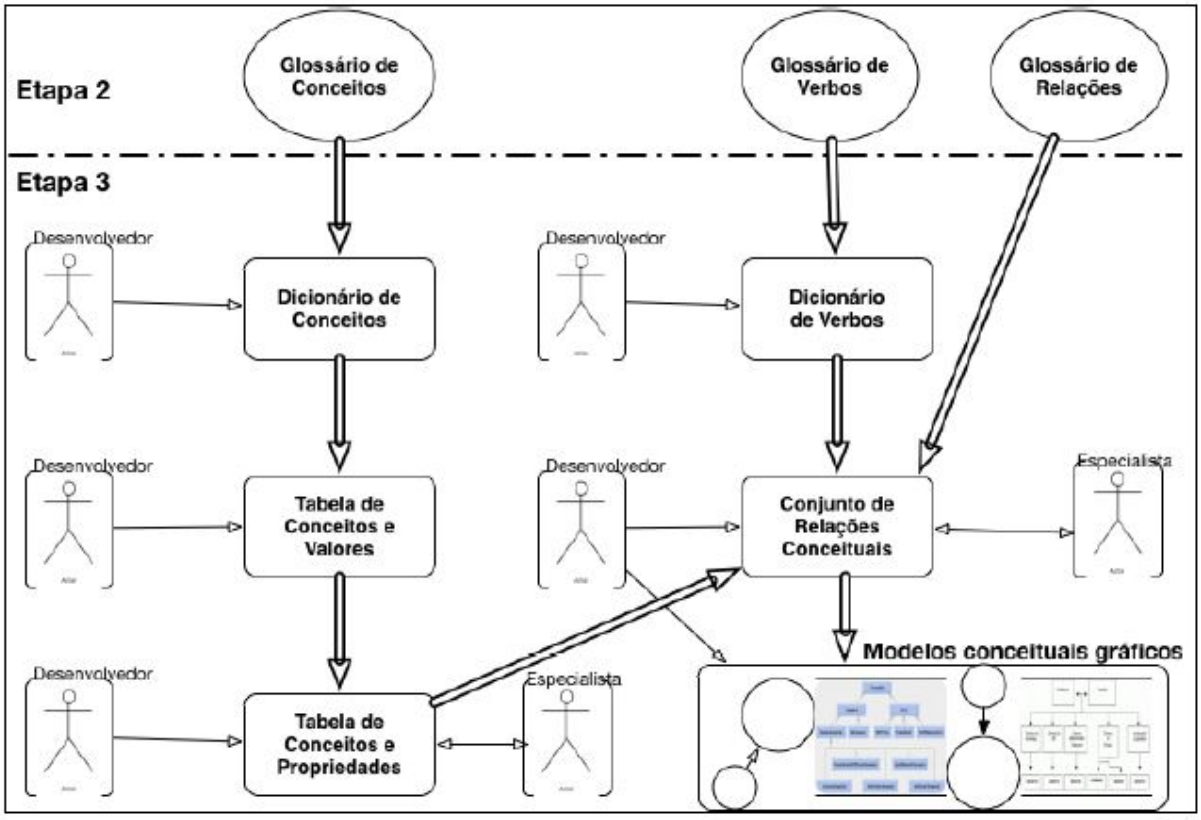
Por fim, como etapa consolidadora dos conceitos e das relações extraídas dos candidatos à ontologia desenvolvida, elaboramos três glossários (conceitos, verbos e relações).

4.2.4 Conceitualização

A etapa de conceitualização seguiu o metodologia da *OntoforInfoScience*, que descreve o processo de transformação dos conceitos em um modelo conceitual gráfico (Figura 10).

Elaboramos encontros entre o desenvolvedor da ontologia e os especialistas em avaliação em cibersegurança da FCA para desenvolvermos a etapa 3, descrita na Figura 10, e a elaboração do modelo conceitual final que será utilizado posteriormente para a fundamentação e formalização da ontologia.

Figura 10 – Etapa de conceitualização da metodologia *OntoForInfoScience*



Fonte: Mendonca (2015, p.199)

[1] Disponível em https://rapidminer.com. Acesso em 21 abr. 2019.

A etapa de conceitualização tem como saída uma tabela de conceitos, valores e propriedades. Propriedades de um conceito ou classe são características que permitem diferenciar um conceito do outro no domínio sob estudo. Nesta etapa, ainda de forma descritiva e textual, não é necessário especificar explicitamente propriedades tais como: tipo de valores das classes (numérico, *string*, booleano), domínio e imagem, cardinalidade (MENDONCA, 2015).

4.2.5 Fundamentação ontológica

Sugere-se pelo método o uso de ontologias de fundamentação, cuja prática é, geralmente, bem aceita e incentivada na área. Esta etapa sugere uma abordagem filosófica. No nosso trabalho, utilizamos a BFO como ontologia de alto nível como fundamento para a nossa pesquisa. Anteriormente, descrevemos a BFO em trabalhos relacionados que fizeram o uso da BFO em questões similares como a transformação produto-serviço e as norma ISO21838, tornando a escolha mais adequada a este trabalho.

4.2.6 Formalização da ontologia

Na etapa de formalização utilizamos a lógica descritiva da OWL como linguagem. A Linguagem de Ontologia da Web do W3C[2] (OWL) é uma linguagem da Web Semântica projetada para representar conhecimento rico e complexo sobre coisas, grupos de coisas e relações entre elas.

Nesta etapa construímos a taxonomia geral da ontologia, definimos propriedades descritivas das classes, definição formal para cada classe, definição das propriedades de dados das classes e definimos propriedades e relações ontológicas.

Para esta etapa utilizamos o *Protégé*[3] 5.2.0, desenvolvido pela universidade de Stanford. O *Protégé* é uma plataforma gratuita e de código aberto que fornece a uma comunidade crescente de usuários um conjunto de ferramentas para construir modelos de domínio e aplicativos baseados em conhecimento de ontologias.

Criamos, posteriormente, algumas instâncias que foram utilizadas com o grupo focal para a avaliação da ontologia. Para a etapa de avaliação e respostas às questões de competência, utilizamos o *plugins* fornecidos com o *Protégé*: o raciocinador SPARQL (HermiT 1.3.8.413) e o SPARQL Query.

[2] O *World Wide Web Consortium* (W3C) é uma comunidade internacional que desenvolve padrões abertos para garantir o crescimento da Web a longo prazo. Disponível em https://www.w3.org/ Acesso em 12 de Novembro de 2019.

[3] Disponível em https://protege.stanford.edu/products.php. Acesso em 12 de Novembro de 2019.

4.2.7 Avaliação da ontologia

A avaliação do projeto ontológico obedeceu a um conjunto de critérios e parâmetros definidos pela *OntoForInfoScience* (MENDONCA, 2015, p.246). O primeiro critério verifica a adequação ao mundo real, avaliando o compromisso ontológico, especificação, validação especializada e expansibilidade. O segundo critério verifica a corretude ontológica através dos parâmetros de completude, integridade, consistência, precisão e documentação.

A aplicação destes critérios é apresentado na documentação formal da ontologia *AutomotiveCyberSecurity* na Seção de 5.5.1, sendo registrados na ontologia formalizada pelo *Protégé* que fornece recursos que auxiliam na identificação de problemas de integridade, imprecisão e inconsistências no conteúdo ontológico.

Utilizamos também o grupo focal e questionários especificamente preparados (Anexo 1) para avaliação da ontologia conforme descrito na Seção 4.5.3.

4.2.8 Documentação da ontologia

Utilizamos o *template* da *OntoForInforScience* de Mendonca (2015, p.249) para a documentação, que foi apresentado durante a Seção 5, tendo requirido nas etapas de documentação de especificação, documentos de referência, modelos conceituais, ontologias reutilizadas, conteúdo ontológico e métricas de avaliação.

4.2.9 Disponibilização da ontologia

O projeto ontológico foi gerado utilizando o OWL-DL (Turtle) e disponibilizado como anexo deste trabalho. Utilizamos o identificador IRI - *Internationalized Resource Identifier* da ontologia como atributo "contributor", com um acrônimo "AUT"para facilitar as *queries* em SPARQL.

4.3 Integração da ontologia de domínio desenvolvida segundo a ontologia BFO de nível superior

Foi escopo deste projeto uma primeira integração à BFO como ontologia de alto-nível. Discutimos em termos filosóficos as classes e seus universais e particulares, continuantes e ocorrentes, dependentes e independentes, formal e material para identificarmos a partonomia das classes da *AutomotiveCyberSecurity*. Neste trabalho, ainda que inicial, procuramos ter uma primeira abordagem de integração para permitir futuramente a conexão com

ontologias que utilizaram a BFO como ontologia de alto nível, também para agregar ontologias compatíveis que possam contribuir com o a evolução deste trabalho.

Para cumprir o [OBJ3], utilizamos o guia[4] da BFO (*Basic formal Ontology*) do usuário da BFO para suportar a criação da ontologia de domínio. As ontologias de referência UCO e OntoReq foram então adaptadas e conectadas à ontologia de alto nível para termos uma ontologia que a longo prazo se beneficie da transversalidade da BFO.

Descrevemos as condições que devem ser satisfeitas pelas entidades, conforme análise feita anteriormente na ontologia de Herzog, Shahmehri e Duma (2007) para as classes anteriormente definidas (Ativo, ameaça, vulnerabilidade, Objetivo de cibersegurança e contramedida).

4.4 Integração da ontologia de domínio desenvolvida segundo a norma J3061

Utilizamos a J3061 como um guia de avaliação em cibersegurança em CPS automotivo e propusemos uma forma de conectar os passos da avaliação ao conteúdo ontológico através de esquemas simples como colocado por Beckers, Dürrwang e Holling (2016). Descrevemos as fases de avaliação em cibersegurança e a integração em alto-nível que será utilizada posteriormente no grupo focal para avaliação da ontologia proposta neste trabalho.

4.5 Avaliação da ontologia proposta em um estudo de caso real

Propusemos um grupo focal formado por especialistas em cibersegurança da FCA. O grupo é composto, na sua maioria, por engenheiros de software e hardware, especialistas em ciber-ataques e desenvolvedores de softwares embarcados, com experiência de mercado de mais de dez anos em cibersegurança de IoTs e CPS. O grupo é dividido em várias sedes da FCA no Brasil, sendo responsável por todos os desenvolvimentos e análise em cibersegurança dos produtos produzidos e vendidos no mercado da América Latina.

4.5.1 Composição do grupo

Para composição do grupo focal, convidamos representantes da área de cibersegurança da FCA para avaliar a proposta conceitual em um estudo de caso real. Representando

[4] O guia do usuário da BFO pode ser encontrado em https://github.com/bfo-ontology/BFO/wiki, acesso em 08 de novembro de 2019.

a empresa, 30 representantes do grupo de cibersegurança confirmaram presença para realizar o experimento. Os 30 representantes, compostos por desenvolvedores de softwares embarcados e especialistas em cibersegurança, foram divididos em três grupos de dez pessoas e cada grupo focou na avaliação em cibersegurança, utilizando um CPS do veículo automotor e explorando suas vulnerabilidades em relação aos ativos e ataques sugeridos pelo autor.

4.5.2 Avaliação das questões de competência

Dentro de cada grupo de trabalho, foi proposta uma análise em cibersegurança dos ativos em relação a algumas ameaças selecionadas para um determinado CPS automotivo que utiliza Wi-Fi como meio de ataque. O suporte de um exemplo real auxiliou o grupo a formular as questões de competência e trata-se, sendo, então, de uma forma de auxiliar na definição do escopo e das características da ontologia.

O método utilizado para formular as questões de competência proposto foi descrito na Seção 4.2.2 e nas avaliações que se seguiram. Os especialistas em desenvolvimento de softwares embarcados e avaliação em cibersegurança foram capazes de checar as propostas de avaliação de risco dos ativos, levando em consideração o conteúdo desenvolvido, confrontando o arquétipo da ontologia com a documentação de origem (especificações dos CPS automotivos).

O resultado após a utilização do método DELPHI pode ser visto na Seção 5 - Desenvolvimento da ontologia.

4.5.3 Avaliação da ontologia para um estudo de caso real

Selecionamos os ataques da CAPEC-466: *Leveraging Active Man in the Middle Attacks to Bypass Same Origin Policy*, CAPEC-615: *Evil Twin Wi-Fi Attack*, CAPEC-158: *Sniffing Network Traffic*.

Em relação às vulnerabilidades a esses CPS, selecionamos algumas vulnerabilidades presentes na CWE: CWE-201 *Information Exposure Through Sent Data*, CWE-521: *Weak Password Requirements*, CWE-300: *Channel Accessible by Non-Endpoint, 'Manin-the-Middle'* e CWE-319: *Cleartext Transmission of Sensitive Information*.

No ABOX da *AutomotiveCyberSecurity*, com as ameaças e vulnerabilidades anteriormente descritas, para promover a análise de cibersegurança suportada pela ontologia, colocamos à disposição do grupo focal as ferramentas da proposta conceitual.

Após o *workshop* e rodar a avaliação em cibersegurança utilizando a proposta de integração da ontologia e a J3061, os integrantes do grupo focal responderam questionários

com o objetivo de comprovar se o modelo representa o conhecimento em avaliação em cibersegurança. Os questionários foram preparados a respeito de diferentes orientações e apresentados no Anexo 1. Os questionários e a fundamentação da sua utilização foram adaptados segundo proposta de Almeida (2006).

- Questionário [Q1]: fundamentado em questões de competência;
- Questionário [Q2]: fundamentado em critérios de qualidade de informação; e
- Questionário [Q3]: fundamentado na taxonomia de objetivos educacionais.

O objetivo de [Q1], fundamentado nas questões de Competência, é normalmente utilizado em metodologias para desenvolvimento de ontologias para apreender o escopo da ontologia nas fases iniciais de sua construção. Essas questões delimitam a abrangência da ontologia de forma que a recuperação da informação ocorra dentro das expectativas e que a estrutura cumpra a função a que se propõe. O Q1 orienta responder ao descrito anteriormente em 4.2.7 da avaliação o critério de adequação ao mundo real, verificando a corretude ontológica.

O Questionário [Q1] apresentou aos funcionários questões de competência que a ontologia concebida era capaz de responder e solicitou que eles avaliassem se tais questões atenderiam a suas expectativas. Os resultados positivos indicariam que a ontologia seria capaz de responder sobre o conhecimento necessário para suporte à execução da avaliação em cibersegurança.

O Questionário [Q2] foi utilizado para medir critérios da Qualidade da Informação para avaliar a credibilidade, a completude da informação, a corretude, a objetividade, a atualidade, a relevância e a compreensão. Segundo Almeida (2006) o questionário [Q2] é normalmente utilizados para avaliar a usabilidade de sistemas, aplicativos e sites. Essa avaliação, na maioria dos casos, enfatiza a adequação das funcionalidades de um sistema ao usuário, mas também propõe critérios relacionados apenas a conteúdo.

Já o Questionário [Q3] utilizou a Taxonomia de Objetivos Educacionais e estabeleceu uma hierarquia de objetivos de aprendizado. Segundo Almeida (2006), a hierarquia identifica o que uma pessoa foi capaz de aprender sobre um assunto, através de um espectro que identifica como a pessoa consegue usar o que aprendeu. Esse espectro consiste de seis categorias, que representam desde o nível considerado mais baixo de apreensão do conhecimento, de simples recuperação, denominado conhecimento; a níveis intermediários, denominados compreensão, aplicação, análise; e até o nível mais alto, denominado avaliação. Com esta abordagem, avaliou-se se a *AutomotiveCyberSecurity* realmente apreendeu o conhecimento no contexto da organização.

A coleta de dados para a realização da pesquisa foi feita durante o *workshop* promovido pela FCA utilizando o grupo focal. O formato dos questionários está apresentado

no Anexo 1. Todos os itens analisados receberam notas de 1 a 5, em que 1 quer dizer não concordo e 5 concordo totalmente.

A cada etapa do processo de avaliação e utilização da ontologia, o grupo focal teve a oportunidade de checar os questionários e avaliar a ontologia utilizando os questionários [Q1..Q3]. A notas foram posteriormente compiladas e as médias de cada resposta analisadas com o objetivo de avaliar os critérios de adequação ao mundo real e ao rigor ontológico, descritos na Seção de 5.5.1 - resultados.

Resumimos as etapas que percorremos para responder às questões e aos objetivos que propusemos no trabalho, com o intuito de responder à nossa questão principal e à hipótese de que a ontologia realmente nos trará vantagem necessária na questão da avaliação em cibersegurança. Na próxima seção, mostramos a execução da metodologia e a atividade do grupo focal.

5 Desenvolvimento

Neste capítulo, o leitor encontrará o desenvolvimento da ontologia *AutomotiveCybersecurity*, as análises de integração da ontologia e BFO e J3061, a avaliação do trabalho pelo grupo focal através dos questionários e *workshop* e as questões de competência através de evidências em SPARQL, que resultaram das perguntas elaboradas durante a construção da ontologia e, por fim, algumas considerações sobre o desenvolvimento.

5.1 Desenvolvimento da *AutomotiveCyberSecurity*

No desenvolvimento da ontologia *AutomotiveCyberSecurity* propusemos vários encontros entre o desenvolvedor da ontologia e o grupo focal de especialistas em cibersegurança da FCA. As interações foram colocadas segundo a necessidade do próprio grupo, até que ele se sentisse seguro na condução de uma avaliação utilizando a ontologia dentro do guia da norma J3061. Nas seções seguintes, mostramos os resultados da condução do método *OntoForInfoScience*.

5.1.1 Definições de especificação

A *AutomotiveCyberSecurity* é uma ontologia de domínio que representa o conhecimento relativo à cibersegurança e requisitos de implementação de software de CPS automotivos, mais especificamente, dos requisitos de alto e baixo nível que devem ser estudados durante o processo de avaliação de risco dos ataques cibernéticos. Seu escopo geral abrange elementos da arquitetura veicular, funções, barramentos de comunicação, componentes, ativos, vetores de ataque, padrões de ataque, ameaças, vulnerabilidades e impactos.

Os usuários da ontologia são engenheiros de sistemas automotivos e de funções veiculares, engenheiros de softwares embarcados, validadores, especialistas em cibersegurança automotiva e fornecedores de componentes automotivos e softwares embarcados. A utilização da ontologia *AutomotiveCyberSecurity* visa ao suporte ao processo de avaliação em cibersegurança de CPS. A *AutomotiveCyberSecurity* é uma ontologia de domínio, com médio rigor formal, representada em OWL. O ponto de partida são os requisitos e o processo de captura dos requisitos de alto e baixo nível e limitam-se ao domínio de software do padrão AUTOSAR[1].

[1] Disponível em https://www.autosar.org/ acesso em 12 de Novembro de 2019

O método *OntoforInfoScience* define um escopo de cobertura através de questões de competência para deixar claros o propósito geral e os objetivos específicos a que a ontologia deve atender. No caso da *AutomotiveCyberSecurity*, as questões ligadas à competência são:

1) Quais as funções veiculares e ativos que envolvem impactos diretos ou indiretos para os ocupantes do veículo no caso de um ataque cibernético?

2) Quais os barramentos mais importantes que podem ser acessados através de vetores de ataque?

3 Quais padrões de ataque resultam em impactos que podem trazer prejuízos à segurança da informação?

4) Qual o nível de sofisticação do ataque?

5) Como classificar um ataque?

5.1.2 Documentos de referência

Os documentos de referência para o estudo foram as especificações utilizadas para comunicar a especificação técnica do fabricante (arquitetura veicular, componentes eletroeletrônicos automotivos, especificações de funções veiculares) à norma J3061, além dos sites da CAPEC e NIST. Na etapa da construção dos glossários de conceitos e do dicionário, foi utilizada a ferramenta de processamento de texto do RAPIDMINER[2] para extração automática de candidatos e posterior elaboração manual de conceito, verbos e relações.

5.1.3 Modelos Conceituais

No Quadro 5, apresentamos uma parte dos conceitos após a extração dos documentos citados na etapa anterior, definições e valores verificados pelos engenheiros de sistemas e pelos especialistas em cibersegurança.

Partindo de Herzog, Shahmehri e Duma (2007) e com o suporte da BFO, construímos um meta-modelo da *AutomotiveCyberSecurity*, Figura 11, que foi implementado em OWL, utilizando o Protégé. Posteriormente, a ontologia construída foi utilizada num estudo de caso descrito na Seção 5.5.1.

[2] Disponível em https://rapidminer.com. Acesso em 21 abr. 2019.

Quadro 5 – Parte dos conceitos e valores da *AutomotiveCyberSecurity*

ID	Conceito	Freq.	Sinônimo	Definição	Valores
1	*Ignition*	13236	*Key Position*	Posição em que se encontra a chave no comutador de ignição e suas transições durante a operação. Descreve a conexão física e também o sinal disponível na CAN em relação ao sinal físico do comutador de ignição.	KEY_OFF 30 15 CRANK
2	*Bcm*	9072	*Body Computer* *Body Control*	Unidade eletrônica de Computador de Bordo. Controla o acionamento de cargas internas do habitáculo e o transporte de mensagens entre barramentos.	-
3	*Engine*	4944	-	Descreve o motor térmico	
4	*Ipc*	3014	*Cluster* *Instrument Panel Cluster* *Quadro de Instrumentos*	Unidade eletrônica responsável pela informativa de bordo e sinalização de espias	-
5	*Condition*	2336	*Conditions*	Premissas que devem ser satisfeitas para que determinada máquina de estado execute	-
6	*Brake*	2146	*Break Pedal* *Break Pedal switch*	Chave ou switch capaz de gerar informação da posição do pedal de freio	ON, OFF
7	*Fail*	1982	*Error*	Condição ou estado de falha relevado, determinado por uma central da arquitetura,	*Present, absent, Intermitent*
8	*diagnosis*	1676	*Diagnose*	Algoritmo de diagnose que determina condição de funcionamento	-
9	*Speed*	1631	-	Velocidade do veículo. Velocidade média das quatro rodas do veículo.	0-FFFF

Fonte: Dados da pesquisa.

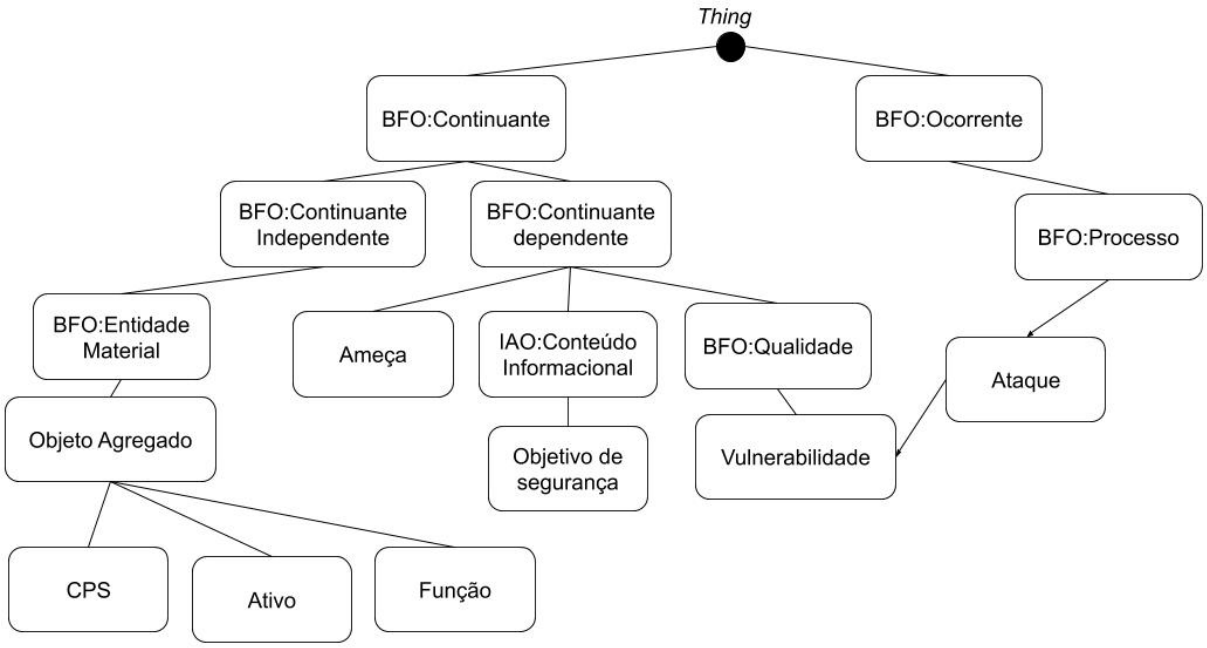
5.1.4 Ontologias reutilizadas

Durante o processo de construção da ontologia, foi utilizada a OntoReq, desenvolvida por Siegemund et al. (2011), em que são definidas importantes classes como Requisito(*Função*), *RequirementArtifact* e *Attribute* e a UCO (SYED et al., 2016), que contribuíram com relevantes classes como Ataque(*Attack*) (BFO:Processo), Ameaça (*Threat*) (BFO:Continuante dependente), Vulnerabilidade (*Vulnerability*) (BFO:Qualidade). Dentro da norma J3061, definimos também os Ativos (*Asset*) (Objeto agregado em BFO:Entidade Material).

5.1.5 Conteúdo ontológico

Para a construção da Taxonomia geral, dicionário de classes e relações ontológicas, foi utilizado o editor OWL-DL Protégé (MUSEN, 2015). Também foram importadas as

Figura 11 – Partonomia de classes da ontologia *AutomotiveCyberSecurity*



Fonte: O autor

classes da ONTOReq[3] e UCO[4]. A versão 1.0.0 da ontologia *AutomotiveCyberSecurity* conta com 1032 axiomas e 168 classes (Figura 12).

Figura 12 – Métricas da ontologia 0.5*AutomotiveCyberSecurity*

Ontology metrics:

Metrics	
Axiom	1032
Logical axiom count	627
Declaration axioms count	358
Class count	168
Object property count	95
Data property count	60
Individual count	38
Annotation Property count	4
DL expressivity	ALCROIQ(D)

Fonte: O autor

[3] Disponível em https://nbn-resolving.org/urn nbn:de:bsz:14-qucosa-162704. Acesso em 08 de novembro de 2019

[4] Disponível em https://github.com/ucoProject/UCO, acesso em 08 de novembro de 2019

5.1.6 Métricas de avaliação

Segundo previsto na metodologia do *OntoforInfoScience*, a ontologia *AutomotiveCyberSecurity* foi avaliada em relação aos critérios de adequação ao domínio do conhecimento em avaliação de cibersegurança e corretude ontológica. Para isto, foram elaborados encontros com os especialistas em desenvolvimento de CPS automotivo e também especialistas em cibersegurança da FCA (FIAT Chrysler Automobiles) com o objetivo de avaliar a ontologia segundo os critérios da metodologia de Mendonca (2015).

Em relação aos parâmetros de avaliação, obedeceu-se ao compromisso ontológico utilizando a OntoReq e a UCO como fundamentação. Além disso, a ontologia foi avaliada em relação à natureza, utilizando classes e relações genuinamente ontológicas. Foram evitados conceitos intuitivos pela utilização da revisão em pares dos especialistas, com o objetivo de harmonizar conceitos existentes nas ontologias de fundamentação e conceitos já utilizados nas documentações de especificações técnicas da montadora.

Com o mesmo suporte dos especialistas, avaliamos as questões de competência (Seção 4.5.3), o grau de abrangência da ontologia e dos indivíduos das classes. O grau de representatividade do mundo real da *AutomotiveCyberSecurity* foi considerado aceitável[5]. No caso da FCA, o processo de validação da ontologia passa por duas etapas. A primeira, já concluída, foi a avaliação das classes em relação ao principal componente da arquitetura, etapa essa que obteve resultado satisfatório na representação do domínio automotivo.

Na Seção 5.5.1, mostramos a execução da avaliação em cibersegurança com o suporte ontológico, discutido na proposta conceitual, já integrada ao processo de desenvolvimento do CPS.

5.2 Integração da ontologia de domínio desenvolvida segundo a ontologia BFO de nível superior

Durante a execução do OBJ3, procuramos descrever as classes da ontologia de domínio e suas principais classes demonstradas, Figura 11, e sua relação com a BFO. Procuramos incluir uma descrição breve do significado que as classes têm para a nossa ontologia de domínio e um pequeno exemplo de objetos que podem ser encontrados nestas classes.

[5] Leitor pode encontrar mais detalhes na Seção 5.5.1

5.2.1 CPS (*Cyber Physical System*)

CPS (Objeto agregado) conceitualmente reúne todas os IoTs e CPS automotivos. São entidades que existem ao longo de todo o ciclo de vida do produto, não importando a situação temporal, e desempenham atividades de integração entre o mundo físico e o mundo virtual.

5.2.2 Ativos (*Asset*)

Ativos (Objeto agregado) são entidades controladas por CPS. Podem representar objetos da segurança (*safety*) como uma direção elétrica ou um freio ABS (*anti-block system*) e também objetos de *security* como os quadros de instrumentos (IPC) e as unidades de multimídia (*head units*). Ambos os objetos (ABS e IPC) podem ser acessados via *wireless* (Wi-Fi), através das redes de comunicação do veículo, e representam o objetivo dos ataques.

Seus atacantes tentam explorar as vulnerabilidades dos CPS e suas redes de comunicação para atingir os ativos e ganhar o controle da situação. Numa situação semelhante a essa, a J3061, no processo de avaliação de risco, sinaliza a necessidade de controlabilidade pelo usuário ou motorista em casos em que a severidade das consequências indique risco de morte, mesmo quando o atacante tenha ganho o acesso ao ativo. Por consequência, a propriedade de severidade no ativo é um importante passo para priorizar ameaças e ataques.

5.2.3 Ameaça (*Threat*)

Mapeamos a ameaça em *BFO:Continuante dependente*, discutido anteriormente em Herzog, Shahmehri e Duma (2007). As ameaças aos ativos podem ser expressas como pessoas, computadores e formas de ataques. Na *AutomotiveCyberSecurity*, a ameaça representa o atacante (*Attacker*). São caracterizados por atores maliciosos, incluindo uma intenção presumida ou um comportamento observado historicamente.

É importante termos um histórico de comportamentos, pois dificilmente um atacante pode ser identificado. Presumir comportamentos nos dá a chance de antecipar um movimento. O histórico de ataques passa então a ser uma parte importante da pesquisa e também é o diferencial de uma avaliação em cibersegurança, pois as fraquezas são identificadas por históricos de comportamentos de atores maliciosos.

5.2.4 Vulnerabilidade (*Vulnerability*)

A vulnerabilidade é uma instância da BFO:qualidade, pois as vulnerabilidades são atribuídas a um CPS e existem durante o ciclo de vida do CPS. Representam as fraquezas encontradas ou mesmo conhecidas de aplicações anteriores ou similares, que podem ser a referência para a análise de cibersegurança.

Informações presentes da CWE (*Common Weakness enumeration*), como a descrição da vulnerabilidade, modo de introdução e potencial mitigação, são também utilizadas na ontologia, sendo igualmente importantes para o reconhecimento do modo como os atacantes utilizam a vulnerabilidade em seu favor para ganhar o controle do CPS.

5.2.5 Objetivo de segurança (*Security goal*)

Objetivo de segurança é um tipo de IAO:Conteúdo informacional[6], pois entra como nível de cibersegurança necessário para aquele determinado ativo e o plano informacional da segurança desejada para cada CPS. É um produto do nível de impacto (*impact level*) e o nível de ameaça (*threat level*) utilizado no processo de avaliação de cibersegurança da norma J3061.

A IAO (*Information Artifact Ontology*) é uma ontologia de nível médio que descreve entidades de informação relacionadas à medicina, originalmente desenvolvida no contexto da iniciativa da OBI (*Ontology for Biomedical Investigations*) (ALMEIDA; MENDONÇA; AGANETTE, 2013) e pode ser relacionada à BFO como um BFO:Continuante dependente.

A probabilidade de exposição em um ativo que exige um nível de controlabilidade total no caso de falhas da CPS é determinada pela missão do CPS. A controlabilidade é explicada pelos especialistas da cibersegurança como nas questões de competência: quais as funções veiculares e ativos que envolvem impactos diretos ou indiretos para os ocupantes do veículo no caso de um ataque cibernético?

5.2.6 Ataque (*Attack*)

Ataque é um BFO:Process e define o uso de uma vulnerabilidade por um adversário, com o objetivo de causar um impacto técnico negativo. A CAPEC (*Common Attack Pattern Enumeration and Classification*) define vários ataques no domínio do software, como, por exemplo, falsificação de credenciais através de manipulação (CAPEC-226).

A CAPEC226 mostra como um invasor manipula uma credencial de acesso existente para obter o controle de um aplicativo. As credenciais permitem que os usuários

[6] Todas essas ontologias biomédicas podem ser encontradas no portal OBO Foundry. Disponível na Internet em: http://www.obofoundry.org/. Acesso em: 12 de Novembro de 2019.

identifiquem-se a um serviço após uma autenticação inicial, sem precisar reenviar as informações de autenticação (geralmente um nome de usuário e senha) com cada mensagem. Um invasor pode conseguir manipular uma credencial captada de uma conexão existente para obter acesso a um servidor de destino. Por exemplo, uma credencial na forma de um *cookie* da web pode ter um campo que indica os direitos de acesso de um usuário. Ajustando manualmente esse *cookie*, um usuário poderá aumentar seus direitos de acesso ao servidor. O invasor pode ainda manipular uma credencial existente para aparecer como um usuário diferente. Como resultado, um invasor pode ser capaz de se passar por outro usuário ou elevar suas permissões a um serviço direcionado. Por consequência, a classe Ataque consegue descrever o processo resultante da exploração de uma vulnerabilidade por um atacante.

5.2.7 Considerações

Dentro do escopo do OBJ3 deste trabalho consideramos que o estágio atual de integração entre BFO e *AutomotiveCyberSecurity* é ainda inicial mas satisfatório para evitar de cometer erros ontológicos que sejam propagados, no sentido de proteger a ontologia de domínio e suas futuras evoluções além suportar a integração com outras ontologias existentes.

5.3 Integração da ontologia de domínio desenvolvida segundo a norma J3061

Com o objetivo [OBJ4] da pesquisa, propomos um método para integração da ontologia *AutomotiveCyberSecurity* com o guia da norma J3061 de avaliação em cibersegurança. Nesse sentido, seguimos a proposta de Beckers, Dürrwang e Holling (2016), que nos permite integrar diferentes processos e diferentes times, mantendo um vocabulário comum. Mostramos o passo a passo do *framework* da norma J3061 e as classes e algumas relações pertinentes à ontologia.

A norma J3061 estabelece um processo de avaliação em cibersegurança dos ativos desde a fase de conceito, determinando as ameaças e o objetivo de cibersegurança, de modo a implementar um sistema de gestão que suporte os especialistas em cibersegurança na determinação e configure o nível de cibersegurança de que um CPS necessita.

Segundo a norma J3061, a avaliação de cibersegurança é um processo que pode ser divido em três fases:

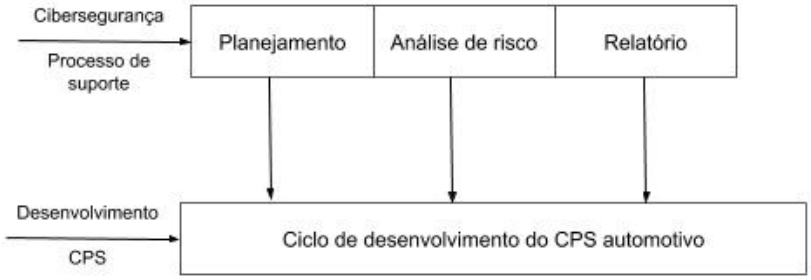
- Planejamento da cibersegurança, objetivo de cibersegurança, identificação dos ativos

e ameaças;

- Análise de risco e *Controls selection*[7]; e
- Relatório de cibersegurança.

A adaptação da norma J3061 proposta por Beckers, Dürrwang e Holling (2016) visa à integração das fases de avaliação em cibersegurança descritas acima e ao ciclo de vida do desenvolvimento do CPS. Um ciclo de vida de um dispositivo CPS geralmente é dividido em especificação do sistema (através da captura de requisitos de software), desenvolvimento do software, integração e, por fim, verificação e validação (Figura 13).

Figura 13 – *Framework* do processo de avaliação em cibersegurança



fonte: O autor

Pretende-se oferecer uma ontologia que suporte todo o processo de avaliação de cibersegurança durante todo o ciclo da Figura 13, com o objetivo de ser uma avaliação mais assertiva, que ofereça aos desenvolvedores um retorno rápido às questões de ameaças e ataques. Acredita-se que este instrumento, se bem definido e bem estruturado, seja capaz de reduzir a probabilidade de um potencial ataque cibernético que coloque em risco o ocupante do veículo.

A seguir, descrevemos algumas etapas dentro de cada fase do *framework* da J3061 - planejamento, avaliação de risco e relatório - e como ele se integra ao processo de desenvolvimento do CPS.

5.3.1 Fase de planejamento

Na fase de planejamento (*planning*), é definido o escopo de cibersegurança pela descrição do CPS a ser desenvolvido, Figura 14, tendo como base uma definição do escopo de cibersegurança e do nível de segurança exigido para estes CPS.

[7] *Controls Selection* é um termo do domínio do desenvolvimento em CPS automotivo e refere-se às funções que o CPS deve realizar durante o ciclo de vida (exemplo: um CPS relacionado com o controle de estabilidade do veículo deve ser capaz de realizar a função de frear as rodas do veículo de forma autônoma e independente do motorista)

Ainda na Figura 14, a iniciação do ciclo de planejamento de cibersegurança inclui o desenvolvimento de um programa de atividades durante o ciclo de vida. O escopo e os objetivos de segurança precisam ser definidos para as maiores ameaças em potencial. Por exemplo: se uma ameaça em potencial for um acionamento malicioso do freio, então o maior nível de objetivo em cibersegurança será prevenir ou reduzir a ocorrência de uma freada inesperada, ou mitigar as potenciais consequências deste ataque. Uma vez definidos o escopo e os objetivos, a estratégia de cibersegurança pode ser então perseguida durante o desenvolvimento do CPS.

Figura 14 – Fase de planejamento da cibersegurança

fonte: O autor

O nível de segurança exigido depende do contexto e também da comunidade de desenvolvedores envolvidos no projeto. Além disso, níveis de segurança dependem das tecnologias que podem estar presentes no veículo para alcançar determinada proteção. Por exemplo, a um canal de comunicação criptografado pode ser atribuída uma determinada pontuação em relação a um canal que não utilize esse processo. O mesmo pode ser feito para troca de senhas com *tokens*, criptografia de *hardware* e *gateways*.

A norma J3061 não visa à classificação destes artifícios e à sua pontuação, até porque a evolução dos métodos de ataques e os ativos envolvidos mudam ao longo do tempo. Consequentemente, teríamos uma escala em constante mudança. Isso também abre a oportunidade para, na fase de planejamento, discutir também a frequência com que devemos revisitar um projeto para reavaliar a cibersegurança ao longo do ciclo de vida do produto.

5.3.2 Fase de avaliação de risco

A fase de avaliação do risco visa à identificação dos ativos e à análise das ameaças. No caso da segurança do ocupante (*safety*), podemos nos basear na norma ISO 26262, que define o potencial de dano para o ocupante do veículo que um determinado CPS pode ocasionar em caso de falha. Mas podemos expandir o conceito de *safety* também para outros componentes que não estão necessariamente relacionados com a segurança do ocupante, como, por exemplo, as centrais multimídia que contêm dados do usuário,

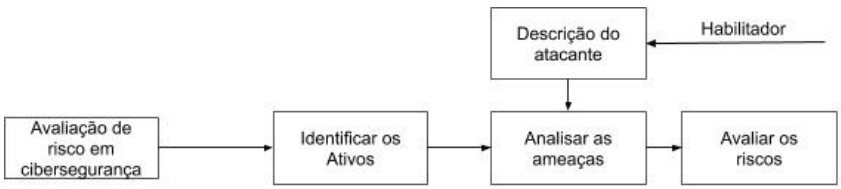
a localização via GPS ou mesmo a possibilidade de um atacante fazer uma compra de um produto utilizando um celular conectado ao veículo. Enfim, são vários os ativos que um atacante pode alcançar. O importante é que, desde a fase de planejamento, sejam discutidos e definidos o escopo e o nível que se quer alcançar em cibersegurança em relação aos ativos que correm risco.

Na Figura 15, podemos ver as etapas de avaliação de risco e a interface com o processo de desenvolvimento do software automotivo. Tendo como referência a especificação do componente e requisitos de software, podemos identificar os ativos e também iniciar a análise das ameaças, segundo as vulnerabilidades que um atacante pode explorar.

O habilitador do processo é o conhecimento sobre ataques e ameaças dos especialistas em cibersegurança. Mas também podemos utilizar uma base de dados de ataques conhecidos para entender as necessidades de proteção em relação às etapas de um ataque. Essas bases de dados, disponíveis em locais como o CAPEC e o NIST, podem ser conectadas ao *framework* por uma ontologia em cibersegurança.

Na análise das ameaças, o *framework* da J3061 prevê a utilização do *Threat Analysis and Risk Assessment* (TARA) de Schmittner et al. (2016), com o objetivo de identificar potenciais ameaças e avaliar o risco associado a elas. O objetivo pode ser declarado em termos do que evitar. O conceito de cibersegurança inclui uma estratégia de alto nível definida na fase de planejamento que possa ser satisfeita posteriormente na fase de desenvolvimento do produto. Tendo como base essa estratégia de alto nível, podemos elencar os requisitos de cibersegurança a serem atingidos.

Figura 15 – Fase de avaliação de risco



fonte: O autor

Dentro ainda da análise de risco proposta pela norma J3061, utiliza-se a ferramenta HEAVENS (Society of Automotive Engineers, 2016) para ranquear as ameaças e poder guiar os engenheiros sobre os requisitos de segurança e as prioridades que devem ser observadas durante o processo de desenvolvimento. No Quadro 6 mostramos um exemplo de análise de risco através de um cenário de ataque de Schmittner et al. (2016). No exemplo a seguir, com o objetivo de modificar parâmetros e acessar dados, o atacante tenta explorar a vulnerabilidade conhecida de um sistema operacional ou aplicação remota para instalar um *rootkit* e ganhar o controle de uma determinada central eletrônica do veículo.

Quadro 6 – Avaliação de risco HEAVENS

Cenário de ataque	Ameaça	Efeito	*Threat Level* (TL)	*Impact Level* (IL)	*Security Level* (SL)	Ativo
Explorar uma vulnerabilidade conhecida de um sistema operacional ou aplicação remotamente	Instalar rootkit	Ganhar controle da ECU, modificar parâmetros e acesso à dados	3	4	High	Aplicativo de Software

Fonte: Adaptado de Schmittner et al. (2016)

Na Figura 16, o nível de segurança é uma interseção entre o TL (*Threat Level*) e o IL (*Impact Level*), conforme análise por HEAVENS, determinando o SL (*Security Level*) necessário para o ativo. O SL então determina o próximo passo da metodologia, ou seja, os requisitos de cibersegurança necessários para cada ameaça analisada.

Figura 16 – Nível de segurança definido por IL (*Impact Level*) e TL (*Threat Level*)

Security Level (SL)		Impact Level (IL)				
Threat Level (TL)		0	1	2	3	4
	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

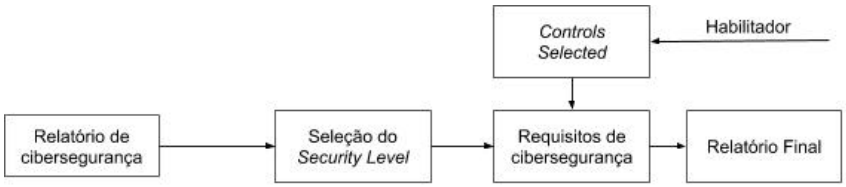
Fonte: Society of Automotive Engineers (2016)

5.3.3 Fase do relatório de cibersegurança

A última fase do *framework* consiste em elencar os requisitos de cibersegurança e sua rastreabilidade em relação aos requisitos de desenvolvimento de software embarcado automotivo.

Na Figura 18, representamos as etapas do relatório dos requisitos de cibersegurança determinados pelo nível de segurança selecionado pelos especialistas em cibersegurança e as potenciais ameaças discutidas anteriormente durante o processo de HEAVENS. Os requisitos de cibersegurança se relacionam com os controles disponíveis para evitar uma ameaça ou proteger a arquitetura do veículo contra ela. Isso parece óbvio, mas é necessário identificar quais controles disponíveis são capazes de executar a tarefa. Por fim, temos

Figura 17 – Fase de compilação dos requisitos de cibersegurança



Fonte: O autor

a realimentação do sistema de requisitos de desenvolvimento do CPS. Isto estabelece a rastreabilidade do requisito de cibersegurança dentro do processo de confecção do software e sua posterior integração e validação.

Neste *framework*, a rastreabilidade é a chave para a implementação segura dos requisitos de software, pois não trata a cibersegurança de uma maneira isolada ou marginal, mas assegura, desde o princípio e em todas as fases do ciclo de vida do desenvolvimento, o cuidado com a cibersegurança e sua aplicação prática.

5.3.4 Suporte ontológico da *AutomotiveCyberSecurity*

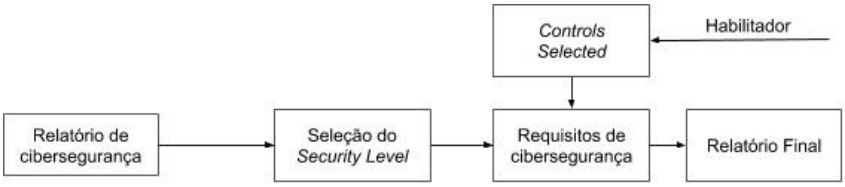
Discutimos passo a passo o *framework* da norma J3061 e as adaptações de Beckers, Dürrwang e Holling (2016) em relação às etapas de desenvolvimento de software e à avaliação de cibersegurança. Entretanto, a norma J3061 se limitou a apresentar recomendações e um guia de avaliação de riscos envolvidos em cibersegurança e no desenvolvimento de softwares embarcados. Nota-se que a referida norma não apresenta uma ontologia do conhecimento em cibersegurança para o domínio automotivo. Apesar de a norma representar o melhor esforço já alcançado para a área de cibersegurança em CPS automotivos, torna-se necessário que os desenvolvedores de CPS e os especialistas em cibersegurança tenham conhecimento prévio de outros domínios, como a cibersegurança da internet, para que o guia proposto pela SAE J3061 seja mais bem conduzido e aplicado.

Assim sendo, a utilização da ontologia neste contexto traz ainda duas vantagens. A primeira vantagem é em relação à análise das ameaças, geralmente feita por especialistas em sessões de *brainstorming*. A ontologia *AutomotiveCybsersecurity* deve ser capaz de percorrer, de forma mais abrangente, uma ampla base de conhecimentos em cibersegurança e

disponibilizar, durante a discussão sobre ativos e análise de risco, o conhecimento a respeito de ataques e ameaças, além de manter uma taxonomia entre os diversos desenvolvedores de software e cibersegurança. A segunda vantagem é a rastreabilidade, de modo a evitar interpretações que eventualmente possam levar a falhas ou inconsistências entre o requisito de software e a análise em cibersegurança.

A Figura 16 representa o *framework* completo da solução com a integração do processo de desenvolvimento de software, representado em alto nível. O processo em questão está alinhado ao padrão aberto de desenvolvimento AUTOSAR[8], possibilitando às empresas OEMs (*Original Equipment Manufacturer*) e fornecedores de autopeças uma rápida migração. Com o objetivo de permitir a análise de risco de cibersegurança

Figura 18 – Desenvolvimento de CPS integrado à análise de risco de ameaças através do suporte ontológico da *AutomotiveCyberSecurity*



Fonte: O autor

concomitantemente ao desenvolvimento de software automotivo, torna-se necessário a criação de uma ontologia de cibersegurança automotiva que integre o conhecimento sobre entidades como arquitetura eletrônica veicular e seus barramentos, requisitos automotivos e cibersegurança, no intuito de suportar o processo durante cada etapa da referida metodologia.

Neste contexto, a ontologia *AutomotiveCyberSecurity* parte da arquitetura veicular e seus barramentos de comunicação, adicionando classes da ontologia de requisitos funcionais e não funcionais de Siegemund (2014) e também da ontologia UCO, além do modelo do NHTSA (*Composite Threat Model*).

Posteriormente, procedemos à aplicação da metodologia integrada num exemplo real de desenvolvimento de software embarcado e análise de ameaças para comprovarmos a eficácia do método de avaliação de cibersegurança proposto. Nossa proposta de solução aplicada é a avaliação da cibersegurança em um exemplo real de desenvolvimento sobre um CPS automotivo, com a utilização da ontologia proposta e suporte do grupo de especialistas em desenvolvimento de CPS e especialistas em cibersegurança da FCA.

[8] AUTOSAR (*AUTomotive Open System ARchitecture*) é uma parceria mundial de desenvolvimento entre fabricantes de veículos, fornecedores, prestadores de serviços e empresas dos setores de eletrônica automotiva, semicondutores e software. Disponível em https://www.autosar.org/ acesso em 12 de Novembro de 2019

Para fins desta pesquisa, utilizamos a solução em uma parte da especificação textual do CPS correlato durante um *workshop* promovido no segundo semestre de 2019. O resultado foi evidenciado no relatório de cada etapa e, por fim, no *Report Security Level Controls*, nas respostas para as questões de competência propostas pelos especialistas em cibersegurança e os questionários do grupo focal (Seção 5.5.1).

5.4 Questões de competência

Durante o *workshop* com os especialista de cibersegurança da FCA, respondemos as questões de competência feitas anteriormente pelos próprios especialistas e ranqueadas utilizando o método DELPHI que discutimos durante a Seção 4.2.2, e as repetimos aqui:

.QC1 - Quais as funções veiculares e ativos que envolvem impactos diretos ou indiretos para os ocupantes do veículo no caso de um ataque cibernético?;

.QC2 - Quais os barramentos mais importantes que podem ser acessados através de vetores de ataque?;

.QC3 - Quais padrões de ataque resultam em impactos que podem trazer prejuízos à segurança da informação?;

.QC4 - Qual o nível de sofisticação do ataque?;

.QC5 - Como classificar um ataque?

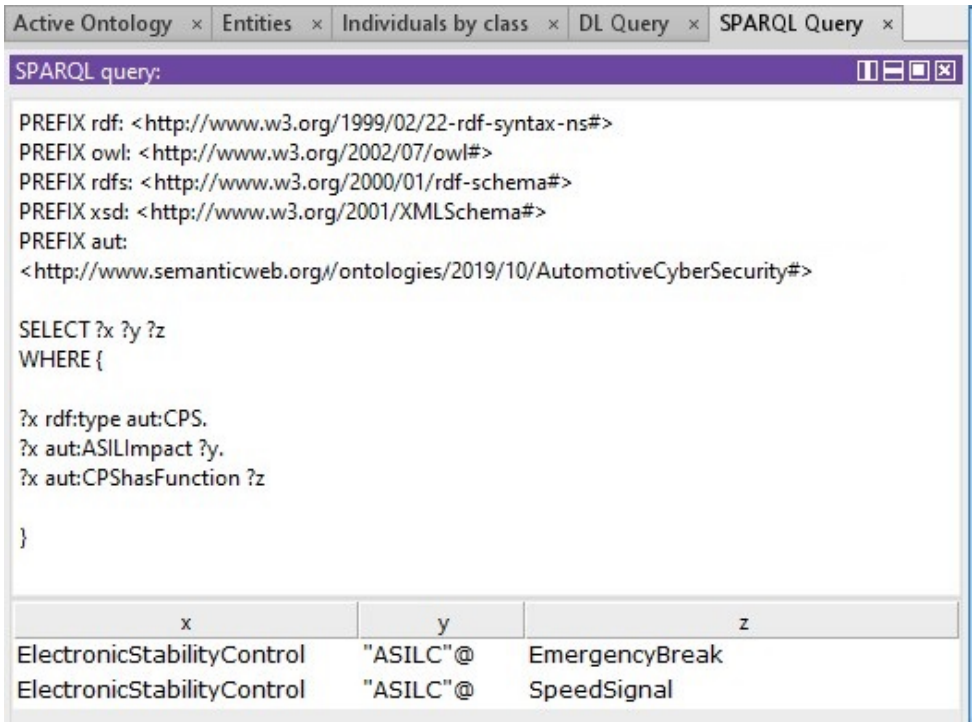
Carregamos a ABOX com alguns exemplos de ataques e vulnerabilidades a fim de utilizamos o SPARQL para confrontar nossas respostas com o grupo. No caso dos ataques temos a CAPEC-466: *Leveraging Active Man in the Middle Attacks to Bypass Same Origin Policy*, CAPEC-615: *Evil Twin Wi-Fi Attack*, CAPEC-158: *Sniffing Network Traffic* e para as vulnerabilidades em CPS, presentes na CWE: CWE-201 *Information Exposure Through Sent Data*, CWE-521: *Weak Password Requirements*, CWE-300: *Channel Accessible by Non-Endpoint, 'Manin-the-Middle'* e CWE-319: *Cleartext Transmission of Sensitive Information*.

Nas avaliações das questões de competência, os especialistas em desenvolvimento de softwares embarcados e cibersegurança foram capazes de checar as propostas de especificação segundo o conteúdo desenvolvido, confrontando a metodologia TARA e seus passos ao arquétipo da ontologia e também em relação à documentação de origem (especificações de componentes da arquitetura veicular).

Desenvolvemos uma *query* que utilizou uma base ABOX simples, carregada para mostrar a eficácia da ontologia na análise. Para a questão [QC1] , utilizamos uma *query*

em SPARQL simples para mostrar os CPS que envolvem algum impacto para o veículo durante o ataque (Figura 19).

Figura 19 – *Query* – [QC1] Funções veiculares e ativos que envolvem impactos diretos ao ocupante do veículo



Fonte: O autor.

A reposta à *query* retorna ao CPS - *ElectronicStabilityControl* com um Impacto ASILC definido pela ISO26262 como crítico em *safety* para o ocupante e duas funções envolvidas: *EmergencyBreak*, que tem por finalidade executar uma parada do veículo frente a uma emergência, e a função *SpeedSignal*, definida como a função que processa a velocidade do veículo.

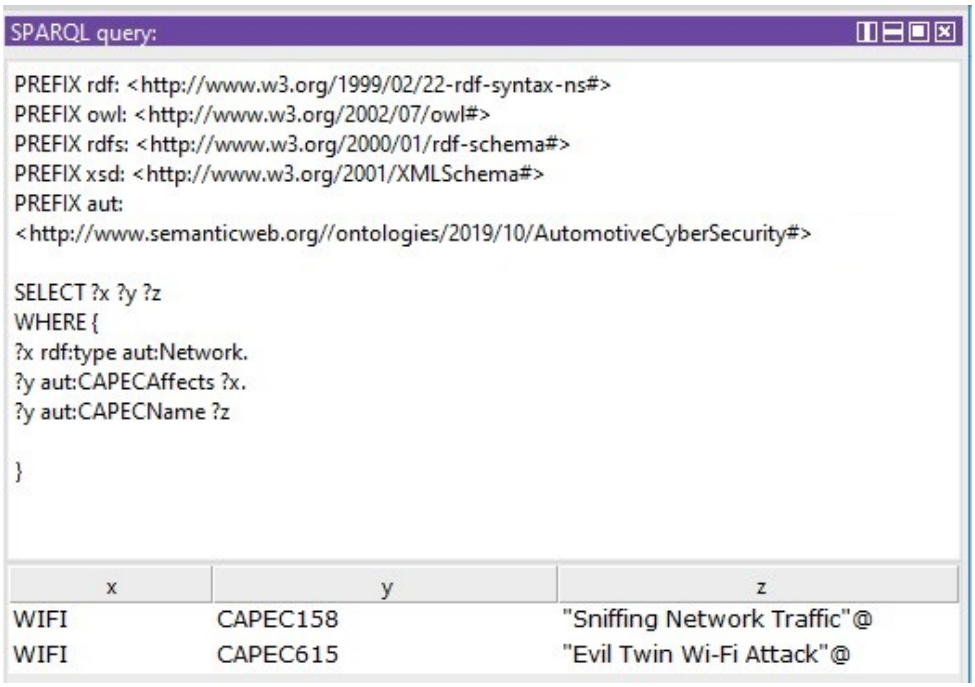
Nesta *query*, o resultado para um analista em cibersegurança tem a finalidade de evidenciar quais funções devem ser consideradas em uma avaliação em cibersegurança como prioritárias.

Para responder à pergunta [QC2] , elaboramos uma *query* em SPARQL também simples, que investiga os vetores de ataque da CAPEC relacionados aos barramentos de comunicação (Figura 20).

A resposta à *query* devolveu a comunicação através do Wi-Fi e de dois vetores de ataque (o CAPEC158 e o CAPEC615), que exploram vulnerabilidades do protocolo Wi-Fi. O primeiro é um *sniffer* de rede e o segundo tenta emular o SSID da rede para se passar pelo CPS e se conectar com o dispositivo ou o ativo.

A questão [QC3] pode ser respondida com uma *query* similar a [QC2] envolvendo

Figura 20 – *Query* que raciocina vetores de ataque que estão relacionados com os barramentos de comunicação



Fonte: O autor.

os ataques e o impacto que eles podem gerar pela propriedade ASILImpact.

Mais uma vez o impacto que afeta *safety* e *security* são, respectivamente, o ASIL C e B. A Figura 21 mostra as funções dos CPS (*ElectronicsStabilityControl* e o *BodyComputerModule*) envolvidas, que são a *EmergencyBreak*, *SpeedSignal* e *Immobilizer*, sendo que a última processa a codificação da chave de ignição e libera a partida do motor do veículo.

No caso da quarta questão [QC4] , o nível de sofisticação pode ser representado pela quantidade de passos para execução, pelo nível de privilégios que permitem ao atacante o controle total do CPS, pelo nível de *skills* necessários para executar o ataque e também pelos recursos necessários para ele. Podemos responder a esta questão utilizando a classificação de *skill* e severidade disponível em bases de vulnerabilidade e ataques como o CVE e CAPEC.

Na Figura 22, podemos verificar o resultado da *query* em SPARQL para o nível de sofisticação de cada ataque. Observa-se o nível de sofisticação na resposta na tabela em “z” e “u” correspondendo ao *skill* necessário para executar o ataque e também a severidade que ele pode provocar. Por uma questão de simplificação de resultado, mostramos os ataques à rede Wi-Fi, já identificada nas questões de competência anteriores.

No caso da [QC5] , podemos ver a severidade na coluna “u” da Figura 22, que indica o nível de severidade que um ataque pode representar. Os especialistas em cibersegurança podem então classificá-lo pela severidade e mitigar as ameaças.

Figura 21 – *Query* dos padrões de ataque e impactos em *Safety*

SPARQL query:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX aut:
<http://www.semanticweb.org/ontologies/2019/10/AutomotiveCyberSecurity#>

SELECT ?x ?y ?z
WHERE {

?x rdf:type aut:CPS.
?x aut:ASILImpact ?y.
?x aut:CPShasFunction ?z


}
```

x	y	z
ElectronicStabilityControl	"ASILC"@	EmergencyBreak
ElectronicStabilityControl	"ASILC"@	SpeedSignal
BodyComputerModule	"ASILB"@	Immobilizer

Fonte: o autor.

Figura 22 – *Query* para [QC4] – Nível de sofisticação dos ataques

SPARQL query:

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX owl: <http://www.w3.org/2002/07/owl#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
PREFIX aut:
<http://www.semanticweb.org/ontologies/2019/10/AutomotiveCyberSecurity#>

SELECT ?x ?y ?z
WHERE {

?x rdf:type aut:CPS.
?x aut:ASILImpact ?y.
?x aut:CPShasFunction ?z


}
```

x	y	z
ElectronicStabilityControl	"ASILC"@	EmergencyBreak
ElectronicStabilityControl	"ASILC"@	SpeedSignal
BodyComputerModule	"ASILB"@	Immobilizer

Fonte: O autor.

Considerações sobre as questões de competência e *AutomotiveCyberSecurity*

Apesar do êxito das *queries*, denota-se que foram interrogações às triplas, bastante simples. Isso não retira o mérito da resposta, mas podemos perceber que a ontologia pode oferecer muito mais que respostas simples, já que o SPARQL nos permite responder a questões bastante complexas. Entretanto o simples fato de termos uma concordância entre os desenvolvedores e os especialistas em avaliação de cibersegurança e a questão de uma semântica única para ser utilizada por várias equipes multidisciplinares e espalhadas ao redor do mundo já é um avanço e um resultado bastante eficiente para esta etapa do projeto.

A transformação do veículo automotivo em um componente IoT com a integração da arquitetura veicular à internet e a utilização de protocolos como o das redes sem fio Wi-Fi (IEEE 802.11) impõem aos desenvolvedores de componentes eletrônicos automotivos o desafio de lidar com a cibersegurança e adaptar as ferramentas de desenvolvimento de CPS automotivo a este novo contexto de ameaças pervasivas.

No desenvolvimento da *AutomotiveCyberSecurity*, o suporte da metodologia *OntoforInfoScience* como instrumento de apoio foi fundamental no processo, já que os especialistas em desenvolvimento de CPS e cibersegurança automotiva, em geral, não são oriundos da área de Ciência da Informação. Assim, foi possível executar a metodologia integralmente e validar a ontologia.

A proposta de integração da J3061 e a ontologia foram testadas durante o *workshop* com os profissionais da FCA (Seção 5.5.1), tendo suportado tanto a avaliação como também no entendimento às respostas das questões de competência.

A seguir, entramos mais na avaliação pelo grupo focal durante o *workshop* e nas respostas aos questionários que avaliarão a ontologia nas questões de adequação à realidade e formalismo.

5.5 Avaliação da *AutomotiveCyberSecurity* pelo grupo focal

Além da questões de competência, o grupo focal discutiu a adequação da ontologia ao mundo real e a corretude ontológica, a definição textual e a definição formal. O resultado do trabalho do grupo resultou também na melhoria da ontologia proposta e da metodologia de integração à norma J3061. Os resultados são apresentados pelos questionários da Seção 5.5.3.

Em relação à integridade e consistência, a *AutomotiveCyberSecurity* foi considerada pelos especialistas em desenvolvimento de CPS e cibersegurança bastante coesa com o domínio automotivo e os tipos definidos, apesar de serem, em parte, oriundos de

outras ontologias, representam, de maneira formal, o requisito automotivo em razão da sua transversalidade de entendimento. Além disso, verificarmos a polissemia, ciclos hierárquicos, classes genéricas e recursividade.

Para garantir a precisão e evitar sinônimos em conceitos, utilizamos algumas classes (*deprecated*) para harmonizar e consolidar termos mais atuais entre os especialistas, além de suportar a disseminação de uma definição mais rigorosa sobre um conceito.

5.5.1 Estudo de caso real com o grupo focal

Como atividade prática de avaliação da efetividade da *AutomotiveCyberSecurity*, aplicamos a proposta conceitual num ambiente real, utilizando como objeto de estudo a FCA (Fiat Chrysler Automobiles) no Brasil. A FCA é uma montadora de veículos automotores e de desenvolvimento de projetos de engenharia de veículos, motores e transmissões. Dentro da área de desenvolvimento de projetos, há as áreas de cibersegurança, que avaliam o desenvolvimento e os riscos envolvidos no ciclo de vida do produto. O grupo de cibersegurança foi composto conforme a Seção 4.5.3.

Dentro do cada grupo de trabalho, foi proposta uma análise em cibersegurança dos CPS em relação a algumas ameaças selecionadas, conforme descrito na nossa metodologia, que utilizam Wi-Fi como meio de comunicação. O objetivo foi avaliarmos o resultado da avaliação de cibersegurança suportada pela ontologia *AutomotiveCyberSecurity* e a integração à norma J3061. Os resultados foram coletados através dos questionários, conforme mencionado anteriormente na Seção 4.2.7.

O processo inteiro foi executado durante *workshop* promovido dentro da FCA com os integrantes do grupo focal, no mês de novembro de 2019 (Figura 23).

Figura 23 – Grupo Focal durante o *workshop* de avaliação em cibersegurança

Fonte: O autor.

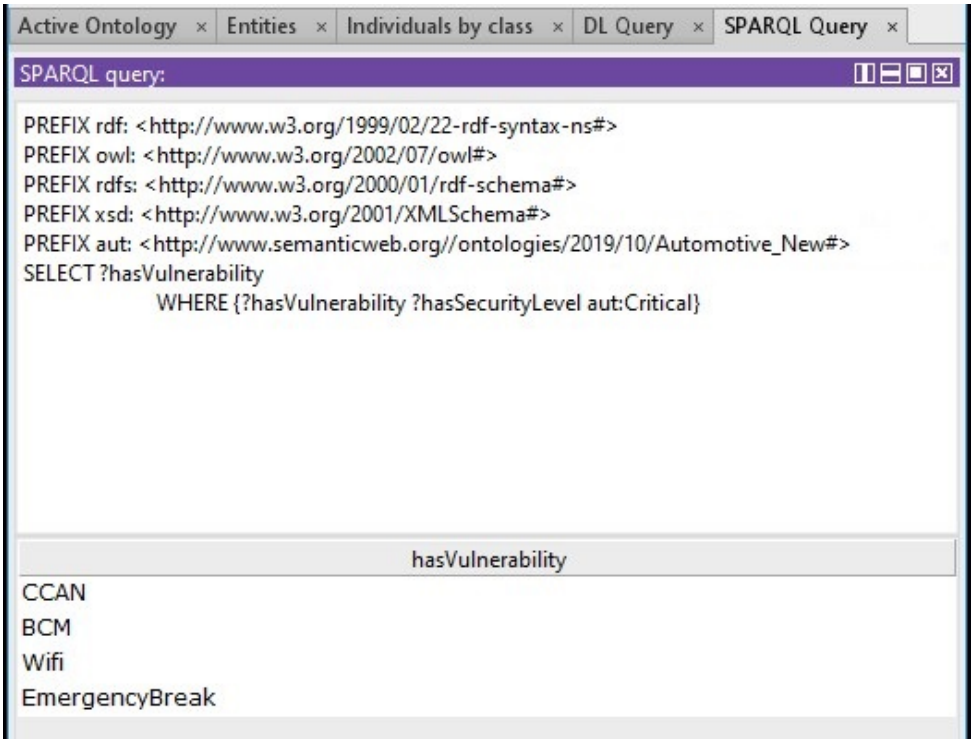
5.5.2 Execução do *workshop* e avaliação em cibersegurança

Executamos as três fases da avaliação em cibersegurança com os grupos separadamente e posteriormente confrontamos as respostas dos grupos como forma de garantir a efetividade da proposta conceitual.

Como primeira parte do *workshop*, os três grupos focais fizeram o planejamento, a definição do escopo de cibersegurança e o nível de risco dos ativos, conforme nossa proposta de integração com a J3061 . Os especialistas utilizaram o processo da J3061 para planejar a avaliação de cibersegurança e como resultado desta etapa, tivemos uma visão clara de como a ontologia *AutomotiveCyberSecurity* pode responder ao planejamento de risco através da ontologia e do raciocinador.

Para comprovar este fato mostramos os riscos eleitos como "*Critical*" como saída para a definição de escopo, através da *query* elaborada conforme a Figura 24. O nível de cibersegurança *Critical* respondido neste exemplo pelo raciocinador foram o CPS BCM, a função *EmergencyBreak* e as redes de comunicação CCAN, BCAN e Wi-Fi. Certamente existem outras funções veiculares e CPS que merecem o mesmo nível de avaliação. Entretanto, para tornar a discussão mais ampla dentro da fase de avaliação do risco, selecionamos a função *EmergencyBreak* e a rede Wi-Fi para identificarmos ameaças e vulnerabilidades que devem receber atenção dos especialistas em cibersegurança.

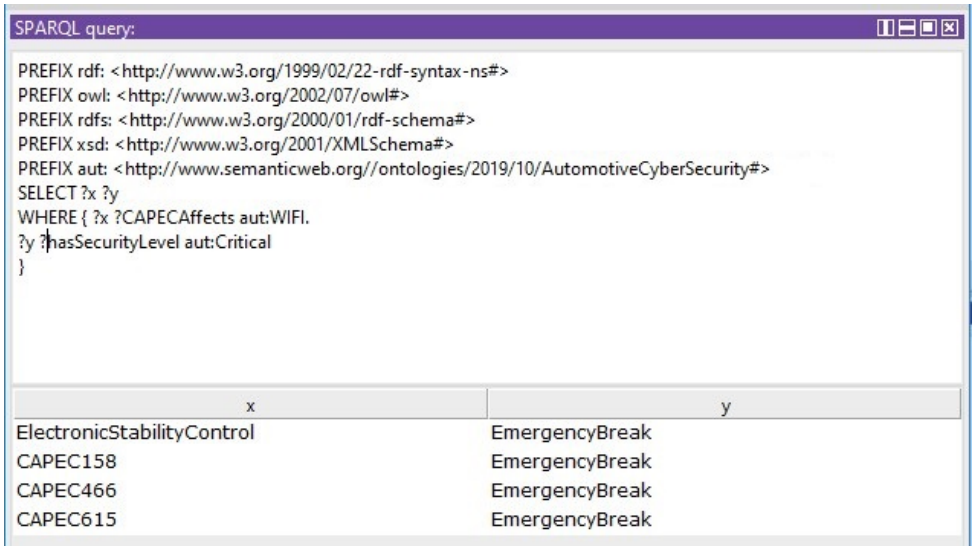
Figura 24 – *Query* com a avaliação dos especialistas na definição em nível de segurança



Fonte: O autor.

Os ativos identificados pela ontologia passaram então pela análise de vulnerabilidade e ameaças através do TARA. Na identificação de ameaças, carregamos a ontologia com os itens do CAPEC 466, 615 e 158, com o objetivo de suportar a análise dos especialistas com respostas produzidas pela *AutomotiveCyberSecurity*. Para suportar o grupo focal, utilizamos o raciocinador e a *query* da Figura 25. O resultado da *query* suportou os especialistas a classificar os riscos relacionados à rede Wi-Fi.

Figura 25 – *Query* dos ataques relacionados à rede Wi-Fi com nível de segurança crítico.



Fonte: O autor.

Na Figura 7, mostramos o resultado da análise TARA feita pelo grupo focal, compilado utilizando a saída do raciocinador. O resultado do *Security Level (SL)* final é carregado novamente na ontologia para suportar a próxima etapa da avaliação na seleção do nível de cibersegurança necessário e a priorização das ameaças e vulnerabilidades que fazem parte da recomendação no relatório final.

Priorizamos no grupo focal o nível Alto (*High*) de cibersegurança. Na Figura 26, podemos verificar, após o carregamento da ABOX e o retorno do raciocinador, sobre as ameaças para cada análise feita no TARA. Nesse caso, o raciocinador retornou os objetos CAPEC 466 e 615 para a rede Wi-Fi.

A última etapa da nossa proposta de integração da ontologia e a avaliação em cibersegurança se beneficiaram do raciocinador e do resultado mostrado na Figura 26 para elaboração do relatório final. A vantagem da proposta conceitual e da utilização da *AutomotiveCyberSecurity* é que a avaliação se tornou um processo recursivo, podendo ter várias iterações a cada nova ameaça ou vulnerabilidade conhecida.

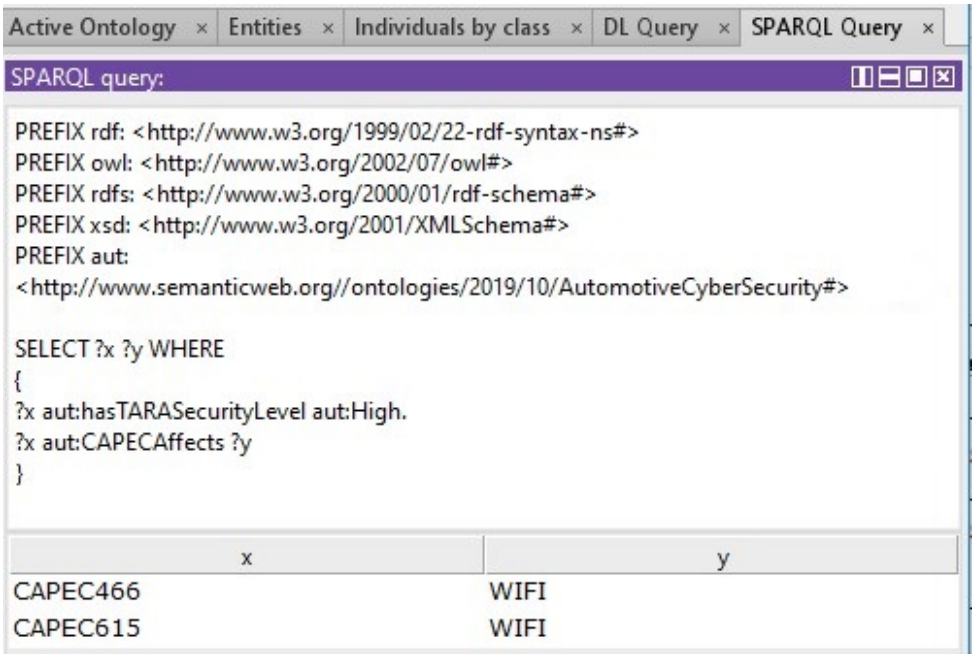
Com esta simplificação, a energia necessária para a nova iteração é significativamente menor e o grupo de desenvolvimento do CPS pode reagir rapidamente a cada nova ameaça identificada.

Quadro 7 – Análise TARA em relação às ameaças devolvidas pelo raciocinador

Cenário de ataque	Ameaça	Efeito	*Threat Level (TL)*	*Impact Level (IL)*	*Security Level (SL)*	Ativo
CAPEC158	*Sniffing Network Traffic*	Expor dados sensíveis pela rede Wi-Fi	3	4	Médio	*EmergencyBreak*
CAPEC466	*Man in the middle*	Requisição não autorizada usando *cookies, JAVA script*	3	5	Alto	*EmergencyBreak*
CAPEC615	*Evil Twin WIFI*	Agindo com o *accesspoint* e expondo chaves de segurança do Wi-Fi	4	4	Alto	*EmergencyBreak*

Fonte: o autor.

Figura 26 – *Query* que recupera a rede e os ataques com nível de segurança definido em *High*



Fonte: O Autor.

5.5.3 Avaliação do Grupo focal - Questionários

Com o objetivo de entendermos a reação do grupo focal em relação à proposta de integração e à ontologia, aplicamos três questionários: [Q1], fundamentado em questões de competência; [Q2], fundamentado em critérios de qualidade de informação; e [Q3], fundamentado na taxonomia de objetivos educacionais. Como descrito na metodologia, a função deste questionários é avaliar a aderência da ontologia ao mundo real e também o formalismo da *AutomotiveCyberSecurity*.

Os questionários foram respondidos integralmente por todos os participantes do grupo focal após a realização do encontro e após rodarmos o processo de avaliação em cibersegurança com o suporte da *AutomotiveCyberSecurity*. Tendo em mãos o conjunto de entrevistas, o pesquisador preparou o agrupamento de sínteses e resultados.

As respostas foram orientadas em uma escala de 1 a 5, em que 1 corresponde a "não atende" e 5 corresponde a "atende totalmente". Os resultados foram organizados em uma tabela com a média de cada resposta.

Avaliação das questões de competência pelo grupo focal - questionário [Q1]

Compilamos os resultados das avaliações das questões de competência elaboradas pelo grupo focal. Apresentamos no Quadro 8 o resultado final com a média aritmética das respostas.

Quadro 8 – Resultado do questionário [Q1] – questões de competência

Pergunta	Nota
1) A ontologia suportou a identificação das funções veiculares e os ativos que envolvem impactos diretos ou indiretos para os ocupantes do veiculo no caso de um ataque cibernético?	4,1
2) Foram identificados os barramentos de comunicação mais importantes que podem ser acessados através de vetores de ataque?	4,2
3) A ontologia foi capaz de mostrar os padrões de ataque que resultam em impactos e prejuizos ao *safety* e *security*?	4,7
4) Foram identificados os niveis de sofisticação dos ataques?	3,8
5) Os ataques foram classificados de forma clara no contexto do desenvolvimento do CPS?	4,8
6) De modo geral, como você avalia a utilização da proposta no trabalho de avaliação em cibersegurança?	4,5

Fonte: O autor.

Considerando que a escala de 1 a 5, em que 1 é não concordo e 5 é concordo totalmente, podemos observar, pelo resultado de cada pergunta uma média de 4,6. Ou seja, *AutomotiveCyberSecurity* foi capaz de atender a questões comuns que os especialistas em avaliação de cibersegurança fazem durante o processo de avaliação seguindo a J3061.

Verifica-se que a maior aderência da ontologia vem da classificação de forma clara dos ataques. Isso provavelmente é devido ao raciocinador conseguir inferir através de triplas e de uma forma bem simplificada os ataques. Sem o auxilio da ontologia, um especialista deveria retirar este conhecimento através de banco de dados ou por experiências passadas no desenvolvimento, depois ranqueá-las e relacioná-las com o CPS para testar a pertinência ou não ao contexto da avaliação. Por consequência, a ontologia se mostrou superior ao executar o raciocinador e poder inferir a pertinência e todos os passos intermediários de uma maneira bem simplificada.

Ainda, a menor nota dada pelos especialistas vem do nível de sofisticação dos ataques. Acreditamos que a forma como carregamos o ABOX possa ter influenciado o resultado. O corpus limitado pode ter esse efeito, pois não escolhemos o nível de sofisticação de fato. Outra consideração é ainda a possibilidade de profissionais de avaliação de segurança esperarem um relatório já automatizado com todas as saídas elaboradas de maneira que o conhecimento retornado fosse consumido de forma simplificada. Certamente, no estágio atual do projeto, não planejamos saídas automatizadas, mas p conhecimento de valor para ser utilizado como entrada no processo de avaliação de cibersegurança, porém a resposta abre o caminho para melhorias que podem ser planejadas em um trabalho futuro.

As outras respostas ao questionário e as notas alcançadas nos permitem afirmar que, do ponto de vista da avaliação das questões de competência, acreditamos que a ontologia tenha respondido totalmente e com um boa aderência ao mundo real. Isso pode ser visto pelas respostas do raciocinador e também pela nota média obtida nesta etapa do trabalho.

Avaliação da qualidade da informação representada pela ontologia - questionário [Q2]

No Quadro 9, consta o resultado da avaliação da qualidade da informação na interpretação dos especialistas em avaliação de cibersegurança. O resultado é extremamente positivo pelo fato de o grupo focal ter sido exposto pela primeira vez, dessa forma, ao processo de avaliação.

O resultado obtido indica que a ontologia foi capaz de preservar um conhecimento relevante para os respondentes e apresentá-lo de forma adequada, de acordo com os critérios utilizados.

Outra observação são as notas de volume apropriado, corretude e atualidade. Quando perguntado ao grupo o motivo de tal valor, a resposta consensual foi atribuída ao corpus limitado. Certamente, um corpus mais completo poderia mudar a opinião do grupo focal. Entretanto, para fins de avaliação da proposta conceitual, o resultado com o corpus limitado foi positivo e mostra que a carga total de vulnerabilidades e de ameaças poderia tornar a análise de cibersegurança mais efetiva.

Destacamos aqui o critério de interpretação. Apesar de o grupo focal ter tido,

Quadro 9 – Avaliação da qualidade da informação – Questionário [Q2]

Média para cada Orientação	Nota
1) Volume apropriado	3,5
2) Credibilidade	4,2
3) Completude	4
4) Corretude	3,9
5) Interpretação	4,2
6) Objetividade	4
7) Atualidade	3,9
8) Relevância	4,5
9) Compreensão	3,9

Fonte: O autor.

pouca exposição à ontologia e do curto espaço de tempo do *workshop*, foi possível verificar, através do questionário, que tanto as questões de competência quanto às perguntas feitas pelo grupo ao raciocinador, através de SPARQL denotam um rápido entendimento de cada especialista e a interpretação dos resultados oriundos das *queries*. Consideramos que a facilidade do uso da interpretação é um fator positivo para uma rápida adoção da ontologia num processo de avaliação em cibersegurança de um CPS.

Resultado quanto ao aprendizado – questionário [Q3]

No Quadro 10, apresentamos o resultado da avaliação das questões do aprendizado. Podemos observar que o grupo focal avalia que a *AutomotiveCyberSecurity* foi capaz de apreender o conhecimento de avaliação em cibersegurança e suportar o grupo durante o processo da proposta conceitual.

Quadro 10 – Avaliação quanto ao aprendizado – questionário [Q3]

Média para cada Orientação	Nota
1) Conhecimento	4,2
2) Compreensão	4,1
3) Aplicação	3,8
4) Análise	4,1
5) Síntese	3,9
6) Avaliação	4,1

Fonte: O autor.

Acreditamos que a nota mais baixa dada pelo grupo, na questão de aplicação, refere-se à novidade da metodologia e às poucas iterações feitas, utilizando a ontologia. Quando perguntado ao grupo focal, a resposta foi a quantidade de ameaças a serem analisadas através das *queries*. Entretanto, acreditamos que seja a força da ontologia, pois apesar das poucas iterações feitas pelo grupo utilizando a ontologia, ela simplifica o trabalho de avaliação em razão ao seu aprendizado do conhecimento através de triplas. O raciocinador pode apresentar respostas sempre mais complexas e abrangentes num contexto de avaliação em CPS, isso porque ameaças e métodos de ataque vão surgindo

com o tempo, e a ontologia é capaz de capturar isso de uma forma prática, ligando o conhecimento adquirido aos novos cenários de uma forma dinâmica, ou seja, ameaças podem evoluir utilizando uma pluralidade de artifícios, mas a ontologia é capaz de formar novas triplas que podem capturar este conhecimento de uma forma mais flexível.

Mais uma vez, a nota dada à síntese, quando perguntado ao grupo focal, retorna como um método novo e de necessário amadurecimento, o que não desabona o método, mas aponta um caminho para uma evolução consistente.

A notas dadas ao conhecimento, compreensão, análise e avaliação mostram a força da ontologia na questão do aprendizado e o que *AutomotiveCyberSecurity* pode oferecer a longo prazo. O questionário [Q3] mostra uma ligação também com o mundo real, pois o aprendizado foi feito dentro do contexto de uma aplicação em questões reais do grupo focal, o que de certa forma contribui para o número elevado de notas altas. Acreditávamos que o corpus limitado poderia influenciar a nota nestas questões, mas contrariamente à nossa crença, o grupo focal conseguiu comprovar o aprendizado da ontologia indiferentemente do tamanho do corpus.

5.5.4 Considerações finais sobre o trabalho do grupo focal

A atividade durante o *workshop* conduzida conforme exposto em nossa metodologia e os resultados obtidos mostraram um caminho bastante promissor para a ontologia como suporte ao processo de avaliação em cibersegurança. Podemos com isto comprovar, através do grupo focal, as atividades desenvolvidas (questões de competência e questionários) e a efetividade da *AutomotiveCyberSecurity* na questão que colocamos como hipótese do nosso trabalho.

A vantagem que conseguimos perceber da utilização da ontologia em relação ao método tradicional é certamente a definição formal de classes, axiomas, objetos e suas propriedades, reduzindo consideravelmente o conflito entre os representantes do grupo focal no entendimento individual de cada um. Proporcionou ainda, através do raciocinador, uma rápida leitura da informação necessária em cada etapa do processo de avaliação.

Essa leitura da informação, na verdade é um conhecimento adquirido através de experiências passadas em outras avaliações de cibersegurança ou base de dados externas como a CAPEC e CVE. E mais, com a vantagem de poder evoluirmos o conhecimento de uma forma flexível, através da ontologia e suas triplas. Sendo assim, acreditamos que tenhamos conseguido, nesta etapa, a comprovação da nossa hipótese.

6 Conclusões e trabalhos futuros

O contínuo aumento da utilização de IoT e CPS automotivo conectando o mundo virtual e físico, contribuiu para a melhoria da mobilidade, conectividade e segurança (SCHMITTNER et al., 2015), mas também trouxe ameaças e ataques cibernéticos com que devemos lidar durante o seu ciclo de vida.

A norma J3061, utilizou-se de referências em domínios multidisciplinares (Internet e redes de computadores) como ponto de partida para lidar com o tema da avaliação em cibersegurança. Além disso, a pluralidade de ataques e a complexidade de sistemas como o automotivo exigem o uso de conhecimento de forma intensiva (SI-SAID; ROLLAND, 1997), deste modo, concluímos que o a ontologia se propunha como um caminho promissor para essa questão (CHALÉ et al., 2011).

Assim propusemos nossa hipótese de que **uma ontologia pode melhorar a eficácia da avaliação em cibersegurança de CPS automotivos**. Conduzimos esse trabalho para verificar e comprovar, através de objetivos claros, a hipótese apresentada. Analisamos a eficácia da ontologia no processo de avaliação em cibersegurança e as diversas abordagens que alguns autores tiveram sobre o tema, o que nos suportou no desenvolvimento da ontologia *AutomotiveCyberSecurity* e serviu de insumo para a execução dos outros objetivos específicos a que nos propusemos.

Avançamos na questão da avaliação em cibersegurança, garantindo a conexão entre os requisitos de projeto e os conhecimentos sobre ameaças e vulnerabilidades, como a CAPEC e CVE.

Trabalhos de avaliação em cibersegurança como o de Schmittner et al. (2016) podem se beneficiar de uma significativa melhoria se utilizarmos a ontologia *AutomotiveCyber-Security*, pois harmoniza o conhecimento do domínio de avaliação em cibersegurança em CPS, aproveitando-se da definição formal de classes, axiomas, objetos e suas propriedades. Além disso, a ontologia *AutomotiveCyberSecurity* pode ser extensível a outras normas de avaliação como a DOT HS 812 do NIST, de Griffor et al. (2017), e as caracterizações de ameaças do NHTSA, de McCarthy, Harnett e Carter (2014).

Além das ontologias, verificamos a importância das métricas no resultado da avaliação em cibersegurança. Essa questão, ainda dentro da nossa investigação da RSL, nos permitiu entender métodos de classificações de risco como o TARA, exemplificado pela Society of Automotive Engineers (2016). Essa evidência da métrica sugeriu que nossa ontologia deveria suportar a análise de cibersegurança dentro do TARA, orientando-nos também na construção da *AutomotiveCyberSecurity*.

6.1 Desenvolvimento da ontologia

Segundo os passos da *OntoForInfoScience* de Mendonca (2015) para realizar a *AutomotiveCyberSecurity*, concluímos que o método foi realmente eficiente e nos auxiliou nas questões mais difíceis, como os modelos conceituais, dicionário de classes e relações ontológicas. Além do método, foram imprescindíveis na construção da ontologia a contribuição e o conhecimento dos especialistas em avaliação de cibersegurança. Sem isso, acreditamos que o resultado seria inexpressivo.

O documento de especificação da ontologia trouxe uma organização formal do escopo, limitou expectativas e respondeu de maneira objetiva à necessidade da construção da ontologia. Consideramos o documento de especificação da *OntoForInfoScience* muito importante dentro do método, pois auxilia na avaliação prévia sobre a real necessidade de sua criação, através de uma questão básica - "O projeto a ser desenvolvido e seu contexto necessitam ou demandam a construção de uma ontologia? Ou a criação de outro instrumento de representação, tal como um tesauro, seria suficiente?"

A resposta a essa pergunta, embora trivial, é essencial para nortear os especialistas na construção da ontologia. Como discutido na seção de metodologia, nosso projeto corresponde à indexação e à recuperação de informação em um contexto dinâmico para a descrição de recursos do domínio do conhecimento da avaliação de cibersegurança, sendo fundamental para a utilização de ontologias.

Os documentos de referência têm maior influência no resultado geral da construção. No nosso caso, utilizamos especificações de desenvolvimento de CPS bastante detalhadas, o que nos possibilitou um carregamento maior dos dicionários e uma abrangência maior na construção da taxonomia, classes e relações.

O resultado foi conferido pelo grupo focal durante o *workshop*, através dos questionários e das questões de competência. Para questões de competência, utilizamos o método DELPHI para eleger, em consenso, as perguntas mais importantes entre os especialistas, posteriormente categorizadas em [QC1..QC5]. Concluímos, durante o curso da execução das *queries*, que a clareza e a simplicidade das respostas trouxeram segurança e efetividade na utilização da ontologia. Esse fato foi, de certa forma, um catalisador no grupo focal e nos deu a credibilidade necessária para continuarmos o trabalho de análise com maior grau de engajamento. Acreditamos que esta seja a resposta ao método de construção e feche a questão da eficácia da *OntoForInfoScience* e o resultado de produção da ontologia de domínio.

Nas questões de competência, acreditamos que tenhamos alcançado o resultado e respondido a todas as perguntas colocadas pelos especialistas. Apesar do resultado animador, percebemos que um ABOX mais carregado de informações nos traria uma

melhor aplicação das questões. Não estabelecemos um limite, aqui, da quantidade mínima, mas com base nas respostas e no resultado alcançado nos questionários de representação do mundo real, acreditamos que traria um maior benefício um ABOX com maior quantidade de exemplos.

Mesmo, assim, considerando as repostas das *queries*, conseguimos separar as funções que têm impacto direto no ocupante do veículo, e os vetores de ataque relacionados com os seus barramentos de comunicação e o nível de sofisticação exigido por estes ataques. Esta importante informação auxilia tanto a avaliação em cibersegurança, quanto no futuro, podendo ser estendida à análise em *safety* (ISO26262).

6.2 Integração à ontologia de nível superior - BFO

Foi evidenciado como as classes da *AutomotiveCyberSecurity* são aderentes à ontologia BFO de nível superior [OBJ1], restando para uma futura etapa, aprofundarmo-nos no tema, até mesmo porque a *AutomotiveCyberSecurity* tem a pretensão de poder se integrar a outras ontologias de segurança da informação que se relacionem com à BFO.

Neste trabalho classificamos as principais classes: (1) CPS, Ativo e Função como objetos agregados e Continuante dependente, (2) Ameaça como Continuante dependente, (3) Objetivo de segurança como um conteúdo informacional da IAO, (4) Vulnerabilidade como Qualidade e (5) Ataque um Processo.

O guia de integração de Smith et al. (2015) foi fundamental na análise e compreensão das entidades e universais. Acreditamos que o trabalho de aderência seja inicial, pois se limitou a referenciar as classes da BFO (Seção 5.2). Este resultado trouxe maior segurança na construção da ontologia *AutomotiveCyberSecurity*, sem erros de integração, e facilitou nosso entendimento das classes e o propósito da existência de cada uma.

6.3 Integração à J3061

Mostramos como a ontologia *AutomotiveCyberSecurity* se integrou à avaliação da cibersegurança da norma J3061, trazendo maior eficácia ao processo, e suportou os especialistas em cibersegurança na avaliação de questões de competência colocadas durante o desenvolvimento da ontologia e também na execução da proposta de integração pelo grupo focal.

Focamos na metodologia da norma J3061 e na adaptação proposta por Beckers, Dürrwang e Holling (2016) na integração de processos. No nosso caso, a avaliação é

subdividida em 3 partes: (1) Planejamento da cibersegurança, (2) Análise do risco e (3) relatório final. Nossa ontologia proporcionou suporte em todas as fases do processo.

Na fase de planejamento de risco, propusemos aos especialistas em avaliação de cibersegurança de focarmos nos riscos considerados críticos aos ativos. A ontologia suportou os especialistas na priorização dos riscos, através do raciocinador, e as respostas sobre quais objetos estariam envolvidos nessa fase de planejamento (Figura 15 da Seção 5.5.1).

Na fase seguinte de análise de risco, a ontologia suportou o processo do TARA na identificação de ameaças como a CAPEC 466, 615 (Quadro 7 da Seção 5.5.1). O resultado trouxe maior consistência ao Nível de segurança (SL) carregado pela ontologia na fase anterior.

Em seguida os especialistas compilaram o relatório de análise e recomendações necessárias para solucionar os problemas de vulnerabilidades durante o desenvolvimento do CPS. Como descrevemos anteriormente, concluímos que a integração do processo de avaliação da J3061 com a ontologia *AutomotiveCyberSecurity* simplifica o processo, pois traz consistência entre as fases pela da aplicação da ontologia, e a energia necessária para uma nova iteração é significativamente menor. Com isso o grupo de desenvolvimento do CPS pode reagir rapidamente a cada nova ameaça identificada.

6.4 Desenvolvimento do Grupo focal

A atividade prática do grupo de focal concentrou-se nas questões da adequação ontológica ao mundo real e sobre a corretude ontológica, definição textual e definição formal. Além disso, o grupo contribuiu no desenvolvimento da nossa primeira versão da *AutomotiveCyberSecurity*.

Testamos a integração à norma J3061 conforme proposto por Beckers, Dürrwang e Holling (2016) e os resultados foram apresentados pelos questionários da Seção 5.5.3 e pelas *queries* à ontologia. A vantagem do nosso método é que ele não é intrusivo, mas complementar à atividade de avaliação em cibersegurança. Tanto os passos dados durante o processo de avaliação quanto as perguntas feitas pelo grupo focal nos mostraram isso claramente.

O estudo de caso real concentrado em um CPS automotivo, utilizando ataques carregados no ABOX, proporcionou, ao grupo, insumos para não somente executar o processo, mas também como suporte no momento de responder aos questionários.

Comprovamos que a ontologia foi capaz de correlacionar os riscos considerados críticos pelos especialistas, e o que se encontrou na consulta à ontologia foram os barramentos de comunicação C-CAN e B-CAN, a rede Wi-Fi e a função *EmergencyBreak* do

veículo (Figura 24). Separamos então, conforme a resposta do raciocinador, a rede Wi-Fi como objeto de estudo, e novamente conduzimos o trabalho com a ajuda do raciocinador à procura dos ataques relacionados com o Wi-Fi considerados críticos. Nesta nova interação o raciocinador retornou o Controle de estabilidade do veículo e três ataques da CAPEC (158, 466 e 615) relacionados ao *EmergencyBreak* (Figura 25).

Após todas as interações com a ontologia, os especialistas em avaliação em cibersegurança foram capazes de realizar o processo do TARA com o apoio da *AutomotiveCyberSecurity*, finalizando o relatório de cibersegurança com o SL=Alto (Nível de Segurança) para os ataques CAPEC466 e CAPEC 615 (Quadro 7). Esta evidência nos mostrou como o grupo focal foi beneficiado pela utilização da nossa ontologia durante o processo de avaliação e pelo consenso no relatório final. Certamente provando a eficácia do método.

Além disso, utilizamos os questionários para poder fechar a atividade do grupo e responder às duas questões colocadas (adequação ao mundo real e formalismo ontológico), que colaboram na comprovação da nossa hipótese sobre a ontologia e melhoria da eficácia da avaliação em cibersegurança.

O objetivo dos questionários foi termos uma evidência da reação do grupo focal à proposta de integração e à ontologia, através do questionário [Q1], fundamentado em questões de competência, [Q2], em critérios de qualidade de informação, e [Q3], fundamentado na taxonomia de objetivos educacionais (ver Seção 5.5.3).

As respostas foram orientadas em uma escala de 1 a 5, em que 1 corresponde a "não atende" e 5 corresponde a "atende totalmente". Os resultados foram organizados em uma tabela com a média aritmética de cada resposta.

O questionário [Q1] obteve média 4,6, ou seja, *AutomotiveCyberSecurity* foi capaz de atender à questões comuns que os especialistas em avaliação de cibersegurança fazem durante o processo de avaliação quando seguem a J3061. O questionário [Q2], com média 4,0, respondeu à avaliação da qualidade da informação, demonstrando que o raciocinador foi capaz de trazer respostas relevantes para os especialistas do domínio. Finalmente, o questionário [Q3], também com média 4,0, respondeu à questão do aprendizado, mostrando a força da ontologia em relação ao conhecimento, compreensão e análise.

Os pontos fortes levantados pelo grupo foram: (1) a classificação dos ataques de forma clara, diminuindo o número extremamente alto de passos na atividade de relacionar os ataques, experiências passadas e ranqueamento, (2) a identificação dos padrões de ataques e (3) a identificação dos ativos em risco, o que denota uma forte correlação com o mundo real. Ainda foi destacada pelos especialistas a forma simples e direta como a ontologia mostrou resultados, mesmo com a pouca familiaridade com a integração à J3061 e ao raciocinador.

Os pontos a melhorar ficaram por conta da limitada amostra do ABOX carregado,

o nível de sofisticação dos ataques e sua aplicação. Esta última talvez seja o ponto em que podemos propor, futuramente, uma interface mais amigável para que os especialistas em avaliação tenham uma forma mais simplificada de interação com a ontologia, evitando comandos diretos em SPARQL. Além disso, integrar as bases de conhecimento da CAPEC para evitar a carga manual dos objetos.

6.4.1 Considerações finais

A pesquisa partiu da seguinte indagação: Uma ontologia pode melhorar a eficácia da avaliação em cibersegurança de CPS automotivos? Podemos afirmar que a pergunta foi respondida plenamente, utilizando a ontologia *AutomotiveCyberSecurity*, o que ficou comprovado durante a avaliação da proposta pelo grupo focal em razão das evidências coletadas durante o desenvolvimento dos objetivos colocados neste trabalho.

Para tornar o processo de avaliação da norma J3061 mais eficaz, foi necessário estabelecer uma ontologia que integrasse as informações sobre o processo de avaliação de cibersegurança, tornando o desenvolvimento do CPS automotivo mais robusto, além de assegurar a consistência da informação e a rastreabilidade durante toda a análise de cibersegurança.

Essa prevenção e a comunicação rápida entre os agentes promovendo o desenvolvimento automotivo são, portanto, uma necessidade. Jamais existirá um sistema totalmente imune a penetrações e isento de ameaças, mas cabe ao profissional que desenvolve CPS automotivos a mitigação de riscos por meio de ações conscientes e coordenadas que este trabalho pode também promover.

Esperamos que este trabalho possa colaborar com a comunidade de desenvolvimento de CPS automotivos e também de cibersegurança no desenvolvimento de uma ontologia abrangente, capaz de permitir um melhor entendimento do domínio de conhecimento em cibersegurança, resultando em um desenvolvimento de CPS mais robusto e, consequentemente, automóveis menos vulneráveis a ataques e a ameaças cibernéticas.

Por fim, espera-se uma maior participação do veículo automotor na internet das coisas ao longo dos anos. O projeto e o desenvolvimento da engenharia do futuro exigem suportar este avanço, que envolve autonomia, funcionalidade, usabilidade, confiabilidade e cibersegurança. Por consequência, pesquisas na área da Ciências da informação podem ajudar a acelerar este desenvolvimento em colaboração com as disciplinas acadêmicas de computação, comunicação, controle e outras engenharias.

6.5 Trabalhos futuros

Consideramos que demos um passo adiante na avaliação em cibersegurança em CPS automotivo, mas este provavelmente foi somente o começo. Durante o trabalho mencionamos algumas melhorias que poderíamos fazer, entre elas o contínuo desenvolvimento da ontologia, interfaces mais amigáveis para os especialistas e extensão da nossa proposta às normas como a de *safety* (ISO26262).

Referências

ABDOLI, F.; MEIBODY, N.; BAZOUBANDI, R. An Attacks Ontology for computer and networks attack. In: SOBH, T. (Ed.). *Innovations and Advances in Computer Sciences and Engineering*. [S.l.]: Springer Netherlands, 2010. p. 473–476. ISBN 978-90-481-3658-2. Citado 2 vezes nas páginas 41 e 51.

ABDULKHALEQ, A. et al. Using STPA in Compliance with ISO 26262 for Developing a Safe Architecture for Fully Automated Vehicles. *arXiv:1703.03657 [cs]*, mar. 2017. Citado na página 31.

ALAM, S.; CHOWDHURY, M. M.; NOLL, J. Interoperability of security-enabled internet of things. *Wireless Personal Communications*, v. 61, n. 3, p. 567–586, 2011. Citado na página 34.

ALI, N.; HONG, J.-E. Failure Detection and Prevention for Cyber-Physical Systems Using Ontology-Based Knowledge Base. *Computers*, v. 7, n. 4, p. 68, dez. 2018. ISSN 2073-431X. Citado na página 21.

ALMEIDA, M. B. Um modelo baseado em ontologias para representação da memória organizacional. *Perspectivas em Ciência da Informação*, v. 11, n. 3, p. 449–449, dez. 2006. ISSN 1413-9936. Citado 5 vezes nas páginas 33, 68, 115, 117 e 119.

ALMEIDA, M. B. Revisiting ontologies: A necessary clarification. *Journal of the American Society for Information Science and Technology*, v. 64, n. 8, p. 1682–1693, ago. 2013. ISSN 15322882. Citado na página 33.

ALMEIDA, M. B.; MENDONÇA, F. M.; AGANETTE, E. C. INTERFACES ENTRE ONTOLOGIAS E CONCEITOS SEMINAIS DA CIÊNCIA DA INFORMAÇÃO: EM BUSCA DE AVANÇOS NA ORGANIZAÇÃO DO CONHECIMENTO. p. 22, 2013. Citado na página 77.

ÁLVAREZ, G.; PETROVIĆ, S. A new taxonomy of Web attacks suitable for efficient encoding. *Computers & Security*, v. 22, n. 5, p. 435–449, jul. 2003. ISSN 01674048. Citado na página 48.

AMOROSO, D. *Cyber Security*. New Jersey: Silicon Press, 2006. Citado na página 28.

BAKER, D. W. et al. The Development of a Common Enumeration of Vulnerabilities and Exposures. In: *Recent Advances in Intrusion Detection*. Virginia: MITRE, 1999. p. 35. Citado na página 49.

BALDUCCINI, M. et al. Ontology-Based Reasoning about the Trustworthiness of Cyber-Physical Systems. In: *IET Conference Proceedings*. London: IET Digital Library, 2018. ISBN 978-1-78561-843-7. Citado 4 vezes nas páginas 56, 57, 58 e 59.

BARNUM, S. Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX). *Mitre Corporation*, v. 11, p. 1–22, 2012. Citado na página 49.

BECKERS, K.; DÜRRWANG, J.; HOLLING, D. Standard Compliant Hazard and Threat Analysis for the Automotive Domain. *Information*, v. 7, n. 3, p. 36, jun. 2016. ISSN 2078-2489. Citado 7 vezes nas páginas 32, 66, 78, 79, 83, 101 e 102.

BITTNER, T.; DONNELLY, M.; SMITH, B. Individuals, universals, collections: On the foundational relations of ontology. In: *Proceedings of the Third Conference on Formal Ontology in Information Systems*. [S.l.: s.n.], 2004. p. 37–48. Citado na página 37.

BURNS, A.; MCDERMID, J.; DOBSON, J. On the Meaning of Safety and Security. *The Computer Journal*, v. 35, n. 1, p. 3–15, fev. 1992. ISSN 0010-4620, 1460-2067. Citado na página 27.

CHALÉ, H. et al. Reducing the Gap Between Formal and Informal Worlds in Automotive Safety-Critical Systems. *INCOSE International Symposium*, v. 21, n. 1, p. 1306–1320, jun. 2011. ISSN 23345837. Citado 2 vezes nas páginas 23 e 99.

CRAIGEN, D.; Diakun-Thibault, N.; PURSE, R. Defining Cybersecurity. *Technology Innovation Management Review*, p. 9, 2014. Citado na página 28.

EBERT, C.; LIECKFELDT, D. Risk-Oriented Security Engineering. p. 18, 2017. Citado na página 32.

EKELHART, A.; FENZ, S.; NEUBAUER, T. Aurum: A framework for information security risk management. In: *2009 42nd Hawaii International Conference on System Sciences*. [S.l.]: IEEE, 2009. p. 1–10. Citado na página 34.

FICCO, M. Security event correlation approach for cloud computing. *International Journal of High Performance Computing and Networking 1*, v. 7, n. 3, p. 173–185, 2013. Citado 2 vezes nas páginas 34 e 52.

FONTELLES, M. J.; SIMÕES, M. G.; FARIAS, S. H. METODOLOGIA DA PESQUISA CIENTÍFICA: DIRETRIZES PARA A ELABORAÇÃO DE UM PROTOCOLO DE PESQUISA. p. 8, 2009. Citado 2 vezes nas páginas 24 e 61.

GEORGESCU, T.; SMEUREANU, I. Using Ontologies in Cybersecurity Field. *Informatica Economica*, v. 21, n. 3, p. 5–15, 2017. ISSN 1453-1305. Citado 4 vezes nas páginas 52, 53, 58 e 59.

GRENON, P.; SMITH, B. SNAP and SPAN: Towards Dynamic Spatial Ontology. *Spatial Cognition & Computation*, v. 4, n. 1, p. 69–104, mar. 2004. ISSN 1387-5868, 1542-7633. Citado 2 vezes nas páginas 36 e 38.

GRIFFOR, E. R. et al. *Framework for Cyber-Physical Systems: Volume 1, Overview*. Gaithersburg, MD, 2017. NIST SP 1500-201 p. Citado 3 vezes nas páginas 32, 59 e 99.

GRUBER, T. R. A translation approach to portable ontology specifications. *Knowledge Acquisition*, v. 5, n. 2, p. 199–220, jun. 1993. ISSN 10428143. Citado na página 33.

HANNON, E. et al. *What's Driving the Connected Car | McKinsey*. 2018. Https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car. Citado na página 31.

HANSMAN, S.; HUNT, R. A taxonomy of network and computer attacks. *Computers & Security*, v. 24, n. 1, p. 31–43, fev. 2005. ISSN 01674048. Citado 4 vezes nas páginas 48, 56, 58 e 59.

HERZOG, A.; SHAHMEHRI, N.; DUMA, C. An ontology of information security. *International Journal of Information Security and Privacy (IJISP)*, v. 1, n. 4, p. 1–23, 2007. Citado 6 vezes nas páginas 29, 35, 40, 66, 72 e 76.

HOMER, J. et al. Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security*, v. 21, n. 4, p. 561–597, set. 2013. ISSN 18758924, 0926227X. Citado 4 vezes nas páginas 39, 57, 58 e 59.

IBARRA-ESQUER, J. et al. Tracking the evolution of the internet of things concept across different application domains. *Sensors*, v. 17, n. 6, p. 1379, 2017. Citado na página 31.

ISLAM, M. M. et al. A Risk Assessment Framework for Automotive Embedded Systems. In: . [S.l.]: ACM Press, 2016. p. 3–14. ISBN 978-1-4503-4288-9. Citado na página 32.

ISO31000. *ISO 31000 RISK MANAGEMENT*. 2018. Https://www.iso.org/iso-31000-risk-management.html. Citado na página 30.

ITU. *Overview of Cybersecurity. Recommendation ITU-T X.1205*. [S.l.], 2009. Citado na página 28.

KEMMERER, R. A. Cybersecurity. In: IEEE. *25th International Conference on Software Engineering, 2003. Proceedings.* [S.l.], 2003. p. 705–715. Citado na página 27.

KHAN, M. A.; SALAH, K. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, v. 82, p. 395–411, maio 2018. ISSN 0167739X. Citado na página 29.

KHAZAI, B. et al. VuWiki: An Ontology-Based Semantic Wiki for Vulnerability Assessments. *International Journal of Disaster Risk Science*, v. 5, n. 1, p. 55–73, mar. 2014. ISSN 2095-0055, 2192-6395. Citado 2 vezes nas páginas 29 e 34.

KITCHENHAM, B. et al. Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, v. 51, n. 1, p. 7–15, 2009. Citado 2 vezes nas páginas 41 e 43.

KLETZ, T.; AMYOTTE, P. *What Went Wrong?: Case Histories of Process Plant Disasters and How They Could Have Been Avoided*. [S.l.]: Butterworth-Heinemann, 2019. Citado na página 30.

KRIAA, S. Joint safety and security modeling for risk assessment in cyber physical systems. p. 173, 2016. Citado na página 30.

LAMSWEERDE, A. V.; DARIMONT, R.; LETIER, E. Managing conflicts in goal-driven requirements engineering. *IEEE Transactions on Software Engineering*, v. 24, n. 11, p. 908–926, 1998. ISSN 00985589. Citado na página 23.

LEE, E. A. Cyber physical systems: Design challenges. In: *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*. [S.l.]: IEEE, 2008. p. 363–369. Citado na página 21.

LIU, S.-c.; LIU, Y. Network security risk assessment method based on HMM and attack graph model. In: IEEE. *2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. [S.l.], 2016. p. 517–522. Citado na página 39.

MATESKI, M. et al. Cyber threat metrics. *Sandia National Laboratories*, 2012. Citado na página 30.

MCCARTHY, C.; HARNETT, K.; CARTER, A. *Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach*. Washington, 2014. Citado 5 vezes nas páginas 31, 54, 55, 58 e 99.

MCGUINNESS, D. Ontologies Come of Age. In: *The Semantic Web: Why, What, and How*. Two thousand, third. [S.l.]: MIT Press, 2003. p. 171–194. Citado na página 34.

MELL, P.; SCARFONE, K.; ROMANOSKY, S. A Complete Guide to the Common Vulnerability Scoring System Version 2.0. p. 24, 2007. Citado na página 39.

MENDONCA, F. M. Ontoforinfoscience: Metodologia para construção de ontologias pelos cientistas da informação-Uma aplicação prática no desenvolvimento da ontologia sobre componentes do sangue humano (HEMONTO). 2015. Citado 7 vezes nas páginas 61, 62, 63, 64, 65, 75 e 100.

MOZZAQUATRO, B. et al. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors*, v. 18, n. 9, p. 3053, 2018. Citado 7 vezes nas páginas 11, 31, 41, 53, 54, 58 e 59.

MOZZAQUATRO, B.; Jardim-Goncalves, R.; AGOSTINHO, C. Towards a reference ontology for security in the internet of things. In: *Measurements & Networking (M&N), 2015 IEEE International Workshop On*. [S.l.]: IEEE, 2015. p. 1–6. Citado 2 vezes nas páginas 25 e 59.

MUSEN, M. A. The protégé project: A look back and a look forward. *AI Matters*, v. 1, n. 4, p. 4–12, jun. 2015. ISSN 23723483. Citado na página 73.

ORELLANA, D.; MANDRICK, W. The Ontology of Systems Engineering: Towards a Computational Digital Engineering Semantic Framework. *Procedia Computer Science*, v. 153, p. 268–276, 2019. ISSN 18770509. Citado na página 36.

PETERSEN, K. et al. Systematic Mapping Studies in Software Engineering. *School of Engineering, Blekinge Institute of Technology. University of Bari, Italy*, v. 8, p. 68–77, 2008. Citado na página 51.

POOLSAPPASIT, N.; DEWRI, R.; RAY, I. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, IEEE, v. 9, n. 1, p. 61–74, 2011. Citado na página 39.

RASKIN, V. et al. Ontology in information security: A useful theoretical foundation and methodological tool. In: *Proceedings of the 2001 Workshop on New Security Paradigms*. [S.l.]: ACM, 2001. p. 53–59. Citado 2 vezes nas páginas 41 e 42.

REASON, J. *Human Error*. [S.l.]: Cambridge university press, 1990. Citado na página 29.

REES, R. V. Clarity in the usage of the terms ontology, taxonomy and classification. In: *CIB W78's 20th International Conference on Construction IT*. Waiheke Island, New Zealand: [s.n.], 2003. (W78:2003, v. 284), p. 1–8. ISBN 0-908689-71-3. Citado na página 34.

SALIM, F.; HAQUE, U. Urban computing in the wild: A survey on large scale participation and citizen engagement with ubiquitous computing, cyber physical systems, and Internet of Things. *International Journal of Human-Computer Studies*, v. 81, p. 31–48, set. 2015. ISSN 10715819. Citado na página 21.

SAMONAS, S.; COSS, D. THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY. *Journal of Information System Security*, v. 10, n. 3, 2014. Citado na página 28.

SANTOS, M. R.; BAX, M. P.; PESSANHA, C. Uma Leitura Ontológica da Norma ISO 13606 para o Registro Eletrônico de Saúde. p. 14, 2010. Citado 2 vezes nas páginas 35 e 36.

SCHMITTNER, C. et al. Security application of failure mode and effect analysis (FMEA). In: *International Conference on Computer Safety, Reliability, and Security*. [S.l.]: Springer, 2014. p. 310–325. Citado 2 vezes nas páginas 55 e 56.

SCHMITTNER, C. et al. Using SAE J3061 for Automotive Security Requirement Engineering. In: *Computer Safety, Reliability, and Security*. [S.l.]: Springer International Publishing, 2016. p. 157–170. ISBN 978-3-319-45480-1. Citado 6 vezes nas páginas 32, 55, 58, 81, 82 e 99.

SCHMITTNER, C. et al. A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems. In: . [S.l.]: ACM Press, 2015. p. 69–80. ISBN 978-1-4503-3448-8. Citado 2 vezes nas páginas 21 e 99.

SI-SAID, S.; ROLLAND, C. Guidance for requirements engineering processes. In: GOOS, G. et al. (Ed.). *Database and Expert Systems Applications*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997. v. 1308, p. 643–652. ISBN 978-3-540-63478-2 978-3-540-69580-6. Citado 2 vezes nas páginas 22 e 99.

SIEGEMUND, K. *Contributions To Ontology-Driven Requirements Engineering*. Tese (PhD Thesis) — Citeseer, 2014. Citado 2 vezes nas páginas 23 e 84.

SIEGEMUND, K. et al. Towards Ontology-driven Requirements Engineering. p. 15, 2011. Citado na página 73.

SKULMOSKI, G. J.; HARTMAN, F. T.; KRAHN, J. The Delphi method for graduate research. *Journal of Information Technology Education: Research*, Informing Science Institute, v. 6, n. 1, p. 1–21, 2007. Citado na página 62.

SMITH, B. The logic of biological classification and the foundations of biomedical ontology. In: *Invited Papers from the 10th International Conference in Logic Methodology and Philosophy of Science, Oviedo, Spain*. [S.l.: s.n.], 2003. p. 19–25. Citado na página 37.

SMITH, B. Ontology as Product-Service System Lessons Learned from GO, BFO and DOLCE. p. 9, 2019. Citado na página 36.

SMITH, B. et al. *Basic Formal Ontology 2.0: Specification and User's Guide*. 2015. Https://github.com/ BFO-ontology/BFO. Citado 2 vezes nas páginas 22 e 101.

SMITH, B. et al. Relations in biomedical ontologies. *Genome Biology*, v. 6, n. 5, p. R46, 2005. ISSN 14656906. Citado na página 37.

SMITH, B.; KUMAR, A.; BITTNER, T. Basic Formal Ontology for Bioinformatics. p. 16, 2005. Citado na página 37.

Society of Automotive Engineers. SAE J3061: Cybersecurity guidebook for cyber-physical automotive systems. *SAE-Society of Automotive Engineers*, 2016. Citado 5 vezes nas páginas 22, 31, 81, 82 e 99.

SWILER, L. P. et al. Computer-attack graph generation tool. In: IEEE. *Proceedings DARPA Information Survivability Conference and Exposition II. DISCEX'01*. [S.l.], 2001. v. 2, p. 307–321. Citado na página 39.

SYED, Z. et al. UCO: A Unified Cybersecurity Ontology. p. 8, 2016. Citado na página 73.

TAO, M. et al. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*, v. 78, p. 1040–1051, 2018. ISSN 0167-739X. Citado 6 vezes nas páginas 11, 34, 53, 54, 58 e 59.

VITAL, L. P.; CAFÉ, L. M. A. Ontologias e taxonomias: diferenças. *Perspectivas em Ciência da Informação*, v. 16, n. 2, p. 115–130, jun. 2011. ISSN 1413-9936. Citado na página 34.

WU, F.-J.; KAO, Y.-F.; TSENG, Y.-C. From wireless sensor networks towards cyber physical systems. *Pervasive and Mobile computing*, v. 7, n. 4, p. 397–413, 2011. Citado na página 21.

WU, S.; ZHANG, Y.; CAO, W. Network security assessment using a semantic reasoning and graph based approach. *Computers & Electrical Engineering*, v. 64, p. 96, 2017. ISSN 0045-7906. Citado na página 56.

ZEMACH, E. M. Four ontologies. In: *Mass Terms: Some Philosophical Problems*. [S.l.]: Springer, 1970. p. 63–80. Citado na página 37.

Apêndices

APÊNDICE A – Questionários

Questionário QC1

Leia as possibilidades abaixo e informe em que medida atendem às necessidades existentes no contexto de trabalho da avaliação em cibersegurança, de acordo com a escala a direita. Na escala:

- O número 1 corresponde a "não atende"
- O número 5 corresponde a "atende totalmente".

Ao final, caso deseje, você pode sugerir outras questões que julgue relevantes.

Figura 27 – Questionário 1

Pergunta	**Nota**
1) A ontologia suportou a identificação das funções veiculares e os ativos que envolvem impactos diretos ou indiretos para os ocupantes do veículo no caso de um ataque cibernético?	1..5
2) Foram identificados os barramentos de comunicação mais importantes que podem ser acessados através de vetores de ataque?	1..5
3) A ontologia foi capaz de mostrar os padrões de ataque que resultam em impactos e prejuízos ao safety e security?	1..5
4) Foram identificados os níveis de sofisticação dos ataques?	1..5
5) Os ataques foram classificados de forma clara no contexto do desenvolvimento do CPS?	1..5
6) De modo geral, como você avalia a utilização da proposta no trabalho de avaliação em cibersegurança?	1..5

Há alguma consideração que você queira propor para a melhoria do método?

fonte: Adaptado de Almeida (2006)

Questionário QC2

Leia as possibilidades abaixo e informe em que medida atendem às necessidades existentes no contexto de trabalho da avaliação em cibersegurança, de acordo com a escala a direita. Na escala:

- O número 1 corresponde a "não atende"
- O número 5 corresponde a "atende totalmente"

Ao final, caso deseje, você pode sugerir outras questões que julgue relevantes.

Figura 28 – Questionário 2

Quanto ao volume:

Pergunta	Nota
7) O volume da informação é suficiente para suas necessidades?	
8) O volume da informação atende a suas necessidades?	
9) O volume da informação é grade ou pequeno?	

As perguntas em azul estão repetidas. Vale verificar.

Quanto à credibilidade

Pergunta	Nota
10) A informação é digna de confiança?	
11) A informação tem credibilidade?	

Quanto à completude

Pergunta	Nota
12) A informação inclui todos os valores necessários?	
13) A informação é completa?	
14) A informação é suficientemente completa para suas necessidades?	
15) A informação cobre as necessidades de suas tarefas?	

Quanto à corretude

Pergunta	Nota
16) A informação é correta?	
17) A informação é precisa?	
18) A informação é confiável?	

Quanto à interpretação

Pergunta	Nota
19) É fácil interpretar o que a informação significa?	
20) A informação é fácil de interpretar?	
21) As unidades de medida para a informação são claras?	
22) A informação codificada é fácil de interpretar?	

Quanto à objetividade

Pergunta	Nota
23) A informação é baseada em fatos?	
24) A informação é objetiva?	
25) A informação apresenta uma visão imparcial?	
26) A informação codificada é difícil de interpretar?	

Quanto à atualidade

Pergunta	Nota
27) A informação é suficientemente atual para seu trabalho?	
28) A informação é oportuna?	
29) A informação é atualizada?	

Quanto à relevância

Pergunta	Nota
30) A informação é útil para seu trabalho?	
31) A informação é relevante para seu trabalho?	
32) A informação é apropriada para seu trabalho?	
33) A informação é aplicável a seu trabalho?	

Quanto à compreensão

Pergunta	Nota
34) A informação é fácil de entender?	
35) A informação é apropriada para seu trabalho?	
36) A informação é de fácil apreensão?	
37) O significado da informação é fácil de compreender?	

Alguma outra consideração que você queira acrescentar sobre a informação?

fonte: Adaptado de Almeida (2006)

Questionário QC3

Leia as possibilidades abaixo e informe em que medida atendem às necessidades existentes no contexto de trabalho da avaliação em cibersegurança, de acordo com a escala a direita. Na escala:

- O número 1 corresponde a "não atende"
- O número 5 corresponde a "atende totalmente"

Ao final, caso deseje, você pode sugerir outras questões que julgue relevantes.

Figura 29 – Questionário 3

Quanto ao conhecimento

Pergunta	Nota
1) Os princípios do assunto em questão estão presentes?	
2) Termos e conceitos usados em meu trabalho estão presentes?	
3) Procedimentos do meu trabalho estão presentes?	

Quanto à compreensão

Pergunta	Nota
4) Os termos estão corretamente definidos?	
5) E possível explicar o assunto verbalmente?	
6) E possível justificar fatos a partir dos termos?	

Quanto à aplicação

Pergunta	Nota
7) A informação pode ser aplicada em meu trabalho?	
8) A informação pode ser aplicada em novas situação do meu trabalho?	

Quanto à análise

Pergunta	Nota
9) A informação permite identificar falhas de raciocínio?	
10) A informação permite identificar o todo e suas partes?	
11) A estrutura da informação é adequada?	
12) A hierarquia de termos e de relações é coerente?	

Quanto à Síntese

Pergunta	Nota
13) A informação possibilita escrever a respeito do assunto?	
14) A informação possibilita elaborar soluções para problemas?	
15) A informação possibilita novas formas de classificação de ideias dentro do assunto?	
16) A informação permite produzir uma linguagem única sobre o assunto?	

Quanto à avaliação

Pergunta	Nota
17) A informação permite julgar a adequação de conclusões?	
18) A informação permite julgar um fato com base em parâmetros internos e externos?	
19) A informação não permite conclusões adequadas?	

Há alguma outra consideração que você queira acrescentar sobre a informação?

fonte: Adaptado de Almeida (2006)

APÊNDICE B – Ontologia em OWL

```
@prefix aut: <http://www.semanticweb.org/aut/ontologies/2019/10/AutomotiveCyberSecurity#> .
@prefix owl: <http://www.w3.org/2002/07/owl#> .
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix xml: <http://www.w3.org/XML/1998/namespace> .
@prefix xsd: <http://www.w3.org/2001/XMLSchema#> .
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@base <http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity> .

<http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity> rdf:type owl:Ontology ;
owl:imports <http://www.semanticweb.org/ontologies/2012/4/test_ontology.owl> ,
<http://ffrdc.ebiquity.umbc.edu/ns/ontology/> .

#################################################################
#    Object Properties
#################################################################

###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECAffects
:CAPECAffects rdf:type owl:ObjectProperty ;
              rdfs:domain :CAPEC ;
              rdfs:range :Network .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CPShasFunction
:CPShasFunction rdf:type owl:ObjectProperty ;
                rdfs:domain :CPS ;
                rdfs:range :Function .
```

```
###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CPShasISOImpact
:CPShasISOImpact rdf:type owl:ObjectProperty ;
                 rdfs:domain :CPS .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CPShasNetwork
:CPShasNetwork rdf:type owl:ObjectProperty ;
               rdfs:domain :CPS ;
               rdfs:range :Network .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#FunctionHasCPS
:FunctionHasCPS rdf:type owl:ObjectProperty ;
                rdfs:domain :Function .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#hasAttacker
:hasAttacker rdf:type owl:ObjectProperty ;
             rdfs:domain :CAPEC .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#hasSecurityLevel
:hasSecurityLevel rdf:type owl:ObjectProperty ;
                  rdfs:domain :Function .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#hasTARASecurityLevel
:hasTARASecurityLevel rdf:type owl:ObjectProperty ;
                      rdfs:domain :CAPEC .
```

```
###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#hasVulnerability
:hasVulnerability rdf:type owl:ObjectProperty ;
                  rdfs:domain :Network .


#################################################################
#    Data properties
#################################################################

###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#ASILImpact
:ASILImpact rdf:type owl:DatatypeProperty ;
            rdfs:domain :CPS .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECDescription
:CAPECDescription rdf:type owl:DatatypeProperty ;
                  rdfs:domain :CAPEC .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECID
:CAPECID rdf:type owl:DatatypeProperty ;
         rdfs:domain :CAPEC .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECMitigation
:CAPECMitigation rdf:type owl:DatatypeProperty ;
                 rdfs:domain :CAPEC .
```

```
###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECName
:CAPECName rdf:type owl:DatatypeProperty ;
           rdfs:domain :CAPEC .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECResourceRequired
:CAPECResourceRequired rdf:type owl:DatatypeProperty ;
                       rdfs:domain :CAPEC .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECSeverity
:CAPECSeverity rdf:type owl:DatatypeProperty .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPECSkill
:CAPECSkill rdf:type owl:DatatypeProperty ;
            rdfs:domain :CAPEC .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CWEDescription
:CWEDescription rdf:type owl:DatatypeProperty ;
                rdfs:domain :CWE .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CWEID
:CWEID rdf:type owl:DatatypeProperty ;
       rdfs:domain :CWE .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CWEMitigation
```

```
:CWEMitigation rdf:type owl:DatatypeProperty ;
               rdfs:domain :CWE .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CWEName
:CWEName rdf:type owl:DatatypeProperty ;
         rdfs:domain :CWE .


#################################################################
#    Classes
#################################################################

###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPEC
:CAPEC rdf:type owl:Class .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CPS
:CPS rdf:type owl:Class .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CWE
:CWE rdf:type owl:Class .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#Function
:Function rdf:type owl:Class .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#Network
```

```
:Network rdf:type owl:Class .


#################################################################
#    Individuals
#################################################################

###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#ASILB
:ASILB rdf:type owl:NamedIndividual .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#ASILC
:ASILC rdf:type owl:NamedIndividual .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#BCAN
:BCAN rdf:type owl:NamedIndividual ,
              :Network .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#BLUETOOTH
:BLUETOOTH rdf:type owl:NamedIndividual ,
                    :Network .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#BodyComputerModule
:BodyComputerModule rdf:type owl:NamedIndividual ,
                            :CPS ;
                    :CPShasFunction :Immobilizer ;
                    :CPShasNetwork :CCAN ,
```

```
                                :WIFI ;
                    :hasSecurityLevel :Critical ;
                    :ASILImpact "ASILB" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPEC158
:CAPEC158 rdf:type owl:NamedIndividual ,
                   :CAPEC ;
          :CAPECAffects :WIFI ;
          :hasTARASecurityLevel :Medium ;
          :CAPECMitigation """Obfuscate network traffic through encryption to prevent its readability by network sniffers.
Employ appropriate levels of segmentation to your network in accordance with best practices.""" ;
          :CAPECName "Sniffing Network Traffic" ;
          :CAPECResourceRequired "A tool with the capability of presenting network communication traffic e.g., Wireshark,
          :CAPECSkill "Low" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPEC191
:CAPEC191 rdf:type owl:NamedIndividual ,
                   :CAPEC ;
          :hasTARASecurityLevel :High ;
          :CAPECID 191 .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPEC466
:CAPEC466 rdf:type owl:NamedIndividual ,
                   :CAPEC ;
          :CAPECAffects :WIFI ;
          :hasTARASecurityLevel :High ;
          :CAPECDescription "An attacker leverages a man in the middle attack in order to bypass the same origin policy
```

protection in the victim's browser. This active man in the middle attack could be launched, for instance,
when the victim is connected to a public WIFI hot spot. An attacker is able to intercept requests and responses
between the victim's browser and some non-sensitive website that does not use TLS. For instance, the victim
may be checking flight or weather information. When an attacker intercepts a response bound to the victim,
an attacker adds an iFrame which is possibly invisible to the response referencing some domain with sensitive
functionality and forwards the response to the victim. The victim's browser than automatically initiates
an unauthorized request to the site with sensitive functionality. The same origin policy would prevent making
these requests to a site other than the one from which the Java Script came, but the attacker once again uses
active man in the middle to intercept these automatic requests and redirect them to the domain / service with
sensitive functionality. Any persistent cookies that the victim has in his or her browser would be used for these
unauthorized requests. The attacker thus actively directs the victim to a site with sensitive functionality.
When the site with sensitive functionality responds back to the victim's request, an active man in the middle
attacker intercepts these responses, injects his or her own malicious Java Script into these responses,
and forwards to the victim's browser. In the victim's browser, that Java Script executes under the restrictions
of the site with sensitive functionality and can essentially be used to continue to interact with the sensitive site.
So an attacker can execute scripts within the victim's browser on any domains the attacker desires.
The attacker is able to use this technique to steal cookies from the victim's browser for whatever site
the attacker wants. This applies to both persistent cookies and HTTP only cookies unlike traditional XSS attacks.
An attacker is also able to use this technique to steal authentication credentials for sites that only encrypt
the login form, but do not require a secure channel for the initial request to get to the page with the login form.
Further the attacker is also able to steal any autocompletion information. This attack pattern can also be used
to enable session fixation and cache poisoning attacks. Additional attacks can be enabled as well." ;
:CAPECID 466 ;
:CAPECMitigation """Design: Tunnel communications through a secure proxy

Design: Trust level separation for privileged / non privileged interactions e.g., two different browsers, two different users, two different operating
:CAPECSeverity "Medium" ;
:CAPECSkill "Low" .

```
###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPEC595
:CAPEC595 rdf:type owl:NamedIndividual ,
                  :CAPEC ;
          :CAPECAffects :WIFI ;
          :hasTARASecurityLevel :High ;
          :CAPECDescription "In this attack pattern, an adversary injects a connection reset packet to one or both ends of a
                  target's connection. The attacker is therefore able to have the target and/or the destination server sever the
                  connection without having to directly filter the traffic between them." ;
          :CAPECName "Connection RESET" ;
          :CAPECSeverity "HIGH" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CAPEC615
:CAPEC615 rdf:type owl:NamedIndividual ,
                  :CAPEC ;
          :CAPECAffects :WIFI ;
          :hasTARASecurityLevel :High ;
          :CAPECDescription "Adversaries install Wi-Fi equipment that acts as a legitimate Wi-Fi network access point.
                  When a device connects to this access point, Wi-Fi data traffic is intercepted, captured, and analyzed.
                  This also allows the adversary to act as a \"man-in-the-middle\" for all communications." ;
          :CAPECMitigation "Commercial defensive technology that monitors for rogue Wi-Fi access points, man-in-the-middle
                  attacks, and anomalous activity with the mobile device baseband radios." ;
          :CAPECName "Evil Twin Wi-Fi Attack" ;
          :CAPECSeverity "Low" ;
          :CAPECSkill "None" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CCAN
:CCAN rdf:type owl:NamedIndividual ,
               :Network ;
```

```
      :hasVulnerability :CWE201 .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CWE201
:CWE201 rdf:type owl:NamedIndividual ,
                 :CWE ;
        :CWEDescription "The accidental exposure of sensitive information through sent data refers to the transmission
                of data which are either sensitive in and of itself or useful in the further exploitation of the system through
                standard data channels." ;
        :CWEID 201 ;
        :CWEMitigation "Specify which data in the software should be regarded as sensitive. Consider which types of
                users should have access to which types of data." ;
        :CWEName "Information Exposure Through Sent Data" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#CWE521
:CWE521 rdf:type owl:NamedIndividual ,
                 :CWE ;
        :CWEDescription "The product does not require that users should have strong passwords, which makes it easier
                for attackers to compromise user accounts." ;
        :CWEID 521 ;
        :CWEMitigation """Phase: Architecture and Design

Enforce usage of strong passwords. A password strength policy should contain the following attributes:
Minimum and maximum length;
Require mixed character sets alpha, numeric, special, mixed case;
Do not contain user name;
Expiration;
No password reuse.
Phase: Architecture and Design
```

```
Authentication mechanisms should always require sufficiently complex passwords and require that they be
 periodically changed."""" ;
        :CWEName "Weak Password Requirements" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#Cluster
:Cluster rdf:type owl:NamedIndividual ,
                  :CPS .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#Critical
:Critical rdf:type owl:NamedIndividual .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#ElectronicStabilityControl
:ElectronicStabilityControl rdf:type owl:NamedIndividual ,
                                     :CPS ;
                            :CPShasFunction :EmergencyBreak ,
                                            :SpeedSignal ;
                            :CPShasNetwork :WIFI ;
                            :hasSecurityLevel :Critical ;
                            :ASILImpact "ASILC" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#EmergencyBreak
:EmergencyBreak rdf:type owl:NamedIndividual ,
                         :Function ;
                :hasSecurityLevel :Critical .
```

```
###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#EngineControlModule
:EngineControlModule rdf:type owl:NamedIndividual ,
                              :CPS ;
                     :CPShasNetwork :CCAN ;
                     :ASILImpact "ASILC" .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#FuelCutOff
:FuelCutOff rdf:type owl:NamedIndividual ,
                     :Function ;
            :hasSecurityLevel :Critical .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#HeadUnit
:HeadUnit rdf:type owl:NamedIndividual ,
                   :CPS .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#High
:High rdf:type owl:NamedIndividual ,
               owl:Thing .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#Immobilizer
:Immobilizer rdf:type owl:NamedIndividual ,
                      :Function .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#Low
```

```
:Low rdf:type owl:NamedIndividual ,
              owl:Thing .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#Medium
:Medium rdf:type owl:NamedIndividual ,
                 owl:Thing .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#NetworkManagement
:NetworkManagement rdf:type owl:NamedIndividual ,
                            :Function ;
                   :hasSecurityLevel :Critical .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#ReverseGear
:ReverseGear rdf:type owl:NamedIndividual ,
                      :Function ;
             :hasSecurityLevel :Critical .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#SpeedLimiter
:SpeedLimiter rdf:type owl:NamedIndividual ,
                       :Function ;
              :hasSecurityLevel :Critical .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#SpeedSignal
:SpeedSignal rdf:type owl:NamedIndividual ,
                      :Function ;
```

```
            :hasSecurityLevel :Critical .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#StopAndStart
:StopAndStart rdf:type owl:NamedIndividual ,
                       :Function ;
              :hasSecurityLevel :Critical .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#TorqueCalculation
:TorqueCalculation rdf:type owl:NamedIndividual ,
                            :Function ;
                   :hasSecurityLevel :Critical .


###  http://www.semanticweb.org/Aut/ontologies/2019/10/AutomotiveCyberSecurity#WIFI
:WIFI rdf:type owl:NamedIndividual ,
               :Network ;
      :hasVulnerability :CWE201 ,
                        :CWE521 .


###  Generated by the OWL API version 4.2.8.20170104-2310 https://github.com/owlcs/owlapi
```