UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO ACADÊMICO DO AGRESTE

PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

GERALDO ALMIRO DE ARAUJO NETO

GERENCIAMENTO DE RISCOS NA INDÚSTRIA 4.0: análise de ameaças em sistemas produtivos

Caruaru

2020

GERALDO ALMIRO DE ARAUJO NETO

GERENCIAMENTO DE RISCOS NA INDÚSTRIA 4.0: análise de ameaças em sistemas produtivos

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre em Engenharia de Produção.

Área de concentração: Otimização e Gestão da Produção.

Orientador: Prof. Dr. Marcelo Hazin Alencar

Caruaru

2020

Catalogação na fonte:
Bibliotecário – Raul César de Melo - CRB/4 - 1735

A663g Araújo Neto, Geraldo Almiro de.
Gerenciamento de riscos na indústria 4.0: análise de ameaças em sistemas produtivos / Geraldo Almiro de Araújo Neto. – 2020.
115 f.; il.: 30 cm.

Orientador: Marcelo Hazin Alencar.
Dissertação (Mestrado) – Universidade Federal de Pernambuco, CAA, Programa de Pós-Graduação em Engenharia de Produção, 2020.
Inclui Referências.

1. Inovações tecnológicas. 2. Internet das coisas. 3. Administração de risco. 4. Segurança de sistemas. I. Alencar, Marcelo Hazin (Orientador). II. Título.

CDD 658.5 (23. ed.) UFPE (CAA 2020-039)

GERALDO ALMIRO DE ARAUJO NETO

GERENCIAMENTO DE RISCOS NA INDÚSTRIA 4.0: análise de ameaças em sistemas produtivos

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de mestre em engenharia de produção.

Aprovada em: 17 / 02 / 2020.

BANCA EXAMINADORA

_____

Prof. Dr. Marcelo Hazin Alencar (Orientador)
Universidade Federal de Pernambuco

_____

Prof. Dr. Thalles Vitelli Garcez (Examinador Interno)
Universidade Federal de Pernambuco

_____

Prof. Dr. Rodrigo Joé Pires Ferreira (Examinador Externo)
Universidade Federal de Pernambuco

DEDICATÓRIA

Dedico essa dissertação a minha família que sempre apoiou minhas decisões, em especial minha mãe (Vânia), que sempre demonstrou que a educação deveria ser minha maior busca.

In memoriam, dedico a minha avó Vicência, que foi uma das pessoas mais importantes da minha vida.

AGRADECIMENTOS

Agradeço de coração a todos que fizeram parte desse percurso.

Agradeço a minha mãe, meu pai e meus avós sempre presentes e buscando constantemente reconhecer meus esforços e me incentivar para o caminho da educação.

Agradeço a minha noiva – Tayse Mesquita – pelo incentivo, carinho, dedicação, companheirismo e paciência ao longo desses dois anos, fazendo com que todos os esforços aplicados se tornassem mais leves a cada palavra de conforto.

Agradeço aos grandes amigos que fiz nesse período, Bruno, Dallas, Deborah e Saulo, pela forte parceria que desenvolvemos e pelo esforço que todos desprenderam ao colaborar e complementar de forma ainda mais rica esse período de aprendizado.

Agradeço ao professor e orientador Marcelo Hazin Alencar pela paciência e dedicação ao longo desse tempo, buscando aperfeiçoar-me cientificamente, profissionalmente e de forma humana a todo tempo.

Agradeço a Facepe – Fundação de Amparo a Ciência e Tecnologia de Pernambuco, pelo apoio financeiro a este trabalho, por processo de número: IBPG-0592-3.08/17. Proporcionando subsídio necessário às minhas atividades.

Agradeço a todos os professores da Universidade Federal de Pernambuco, especialmente ao corpo docente do PPGEPCAA – Programa de Pós-graduação em Engenharia de Produção do Centro Acadêmico do Agreste.

Por fim, agradeço a todos os meus amigos e colegas, me eximindo da responsabilidade de não citar um a um por risco de omitir alguém importante nessa etapa da minha vida.

RESUMO

A indústria 4.0 tem provocado mudanças profundas nos sistemas produtivos, trazendo consigo, em conjunto com o avanço da industrialização digital, algumas problemáticas, tais como: ataques maliciosos a processos de fabricação, acidentes de trabalhos entre humanos e robôs, vazamento de informações confidenciais e aumento da incerteza dos resultados. Considerando essa perspectiva, esta pesquisa propõe um *framework* para auxiliar a escolha de estratégias eficientes para a análise, controle e gerenciamento dos riscos emergentes nas tecnologias digitais da quarta revolução industrial. A construção do *framework* teve como base a estruturação de informações obtidas a partir de duas revisões sistemáticas da literatura com análise de mais de 100 artigos como forma imparcial de identificar, analisar e interpretar os dados relevantes sobre as ameaças presentes na indústria 4.0 e as ferramentas de análise sistêmica de risco STAMP e STPA. Ao todo foram apresentadas 67 possíveis vulnerabilidades nos processos industriais digitais, contribuindo na escolha de estratégias eficientes para a análise, controle e gerenciamento dos riscos emergentes nas tecnologias digitais da quarta revolução industrial e auxiliando os processos de gerenciamento de riscos em sistemas produtivos que fazem uso destas tecnologias.

Palavras-chave: Indústria 4.0. Riscos emergentes. Gerenciamento de riscos. STAMP. STPA.

ABSTRACT

Industry 4.0 has caused profound changes in productive systems, bringing with it, along with the advancement of digital industrialization, some problems, such as: malicious attacks on manufacturing processes, work accidents between humans and robots, leakage of confidential information and increased uncertainty of results. Considering this perspective, this research proposes a framework to help choose efficient strategies for the analysis, control and management of emerging risks in digital technologies of the fourth industrial revolution. The construction of the framework was based on structuring information obtained from two systematic reviews of the literature with analysis of more than 100 articles as an impartial way of identifying, analyzing and interpreting the relevant data on the threats present in industry 4.0 and the tools of systemic risk analysis STAMP and STPA. Altogether 67 possible vulnerabilities in digital industrial processes were presented, contributing to the choice of efficient strategies for analysis, control and management of emerging risks in digital technologies of the fourth industrial revolution and assisting the risk management processes in productive systems that make use of these technologies.

Keywords: Industry 4.0. Emerging Risks. Risk Management. STAMP. STPA.

LISTA DE ILUSTRAÇÕES

Fluxograma 1 – Sequência de atividades aplicadas no estudo..... 23
Quadro 1 – Pilares da indústria 4.0 e suas características..... 28
Quadro 2 – Tecnologias e soluções da indústria 4.0..... 29
Figura 1 – Modelo de maturidade da indústria 4.0..... 32
Figura 2 – Ligações e principais componentes estruturais de um CPS..... 43
Figura 3 – Estrutura básica de análise e gerenciamento de riscos..... 49
Figura 4 – Influência dos incidentes desastrosos e o desenvolvimento das ferramentas de segurança em risco..... 51
Quadro 3 – Tipos de ataques aplicados à sistemas da indústria 4.0..... 55
Quadro 4 – Incidentes de ciber-ataques a empresas e outras organizações..... 56
Figura 5 – Loop básico de controle do STAMP..... 60
Figura 6 – Etapas básicas da técnica STPA..... 64
Figura 7 – Processo de revisão sistemática da literatura..... 69
Quadro 5 – Questionamentos pesquisa 1 – ameaças das tecnologias digitais..... 70
Quadro 6 – Questionamentos pesquisa 2 - modelo STAMP e técnica STPA..... 71
Quadro 7 – Palavras-chave e combinação de termos para pesquisa sobre riscos às tecnologias da indústria 4.0..... 71
Quadro 8 – Grupos de palavras-chave e combinação de termos da pesquisa sobre STAMP e STPA..... 72
Fluxograma 2 – Etapas do processo de refino da pesquisa indústria 4.0..... 73
Fluxograma 3 – Etapas do processo de refino da pesquisa STAMP - STPA..... 74
Quadro 9 – Riscos, ameaças e vulnerabilidades da indústria 4.0..... 76
Quadro 10 – Número de ameaças por tecnologia facilitadora da indústria 4.0..... 77
Quadro 11 – Relação entre ameaças e tecnologias da indústria 4.0..... 78
Gráfico 1 – Número de ataques hackers nas tecnologias da indústria 4.0 por ano.... 79
Gráfico 2 – Número de publicações relacionadas aos STAMP e a STPA por ano... 80
Quadro 12 – Domínio de aplicação do estudo de revisão sistemática das ferramentas STAMP e STPA..... 82
Figura 8 – Número de publicações por país..... 84
Figura 9 – Diagrama de Venn para relação entre campos de aplicação do estudo.. 89

Fluxograma 4 – Framework para análise de riscos e decisões gerenciais de segurança em organizações industriais digitais..... 91
Figura 10 – Sistema de controle de ameaças para incertezas de custos da digitalização industrial..... 94
Figura 11 – Sistema de controle de ameaças para vulnerabilidades de falta de padrão entre tecnologias..... 95
Figura 12 – Modelo de controle de ameaças e ataques maliciosos advindas da rede de internet mundial..... 96
Figura 13 – Sistema de controle de vulnerabilidades para falta de confiabilidade na transmissão de informações..... 98
Figura 14 – Sistema de controle de riscos para acessos não autorizados e vazamento de informações..... 99
Figura 15 – Sistema de controle de riscos para movimentações robóticas inseguras..... 100
Figura 16 – Sistema de controle para eliminar ameaças de mal dimensionamento de equipamentos..... 101
Figura 17 – Sistema de controle para eliminar falhas em sensores e dispositivos de monitoramento..... 102
Figura 18 – Sistema de controle para limitar o impacto dos riscos naturais ou ambientais..... 103

LISTA DE SIGLAS

3D	*3D Printing*	Impressão 3D
5G	-	5ª Geração
AcciMap	*Accident Map*	-
AGVs	*Automated Guided Vehicles*	Veículo Autoguiado
AI	*Artificial Intelligence*	Inteligência Artificial
AM	*Aditive Manufacturing*	Manufatura Aditiva
AMP	*Advanced Manufacturing Processes*	Processos Avançados de Manufatura
APT	*Advanced Persistent Threat*	Advanced Persistent Threat
BD	*Big Data*	-
CC	*Cyber Component*	Componente Cibernético
CN	*Cloud Computing*	Computação em Nuvem
CNC	*Computer Numeric Control*	Controle Numérico Computadorizado
CPS	*Cyber Physical Systems*	Sistemas Ciber-Físicos
CTA	*Cognitive Task Analysis*	Análise Cognitiva deTarefas
CVE	*Common Vulnerabilities and Exposures*	Vulnerabilidades e Exposições Comuns
CWA	*Cognitive Work Analysis*	Análise Cognitiva do Trabalho
D2D	*Device to Device*	Dispositivo para Dispositivo
DCS	*Distributed Control System*	Sistemas de Controle Distribuído
DMZ	*DeMilitarized Zone*	Zona Desmilitarizada
DoS	*Denial Of Service*	Ataque de Negação de Serviço
EWaSAP	*Early Warning Sign Identification Approach*	Abordagem de Identificação de Sinal de Alerta Precoce
FLSA	*Failure Logic Synthesis and Analysis*	Síntese e Análise de Lógica de Falha
FMEA	*Failure Mode and Effect Analysis*	Análise de Modos de Falhas e Efeitos
FRAM	*Functional Resonance Analysis Method*	Método de Análise de Ressonância Funcional
HAZOP	*Hazard and Operability Study*	Estudo de Perigos e Operabilidade
HC	*Human Component*	Componente Humano
HFACS	*Human Factors Analysis and Classification System*	Sistema de Análise e Classificação de Fatores Humanos
HMI	*Human Machine Interface*	Interface Homem-Máquina
HRA	*Human Reliability Analysis*	Análise de Confiabilidade Humana
HTTPS	*Hyper Text Transfer Protocol Secure*	Protocolo de Transferência de Hipertexto Seguro
I4.0	*Industry 4.0*	Indústria 4.0

ICS	*Information and Comunication Systems*	Sistemas de Comunicação e Informação
IEC	*International Electrotechnical Commission*	Comissão Eletrotécnica Internacional
Indice IP	*Protection Index*	Indice de Proteção
IoT	*Internet of Things*	Internet das Coisas
Ipsec	*IP Security Protocol*	Protocolo de Segurança IP
ISO	*International Organization for Standardization*	Organização Internacional de Normalização
M2M	*Machine to Machine*	-
NER	*New and Emerging Risks*	Riscos Novos e Emergentes
NR	-	Normas Regulamentadoras
NSE	*Naturals Engineering and Sciences*	Ciências Naturais e Engenharia
P&G	*Procter & Gamble*	-
PBs	*Petabyte*	-
PC	*Program Component*	Componente de Programação
PLC	*Power Line Communication*	Controladores Lógicos Programáveis
RFID	*Radio-Frequency Identification*	Identificação por Radiofrequência
RiskSOAP	*Risk Situation Awareness Provision*	Provisão e conscientização da situação de risco
RPN	*Risk Priority Number*	Número de Prioridade de Risco
SCADA	*Supervisory Control and Data Acquisition*	Sistemas de Supervisão e Aquisição de Dados
SLR	*Systematic Literature Review*	Revisão Sistemática da Literatura
SQL	*Structured Query Language*	Linguagem de Consulta Estruturada
STAMP	*System-Theoretic Accident Model and Processes*	Modelo e Processos de Acidentes Teóricos do Sistema
STPA	*Systems-Theoretic Process Analysis*	-
STS	*Sociotechnical System*	Sistema Sociotécnico
TBs	*Terabyte*	-
TCP	*Transmission Control Protocol*	Protocolo de Controle de Transmissão
TI	*Information Technology*	Tecnologia da Informação
VPN	*Virtual Private Network*	Rede Virtual Privada
WEF	*World Economic Forum*	Fórum Econômico Mundial
WoS	*Web of Science*	-
ZBs	*Zettabyte*	-

SUMÁRIO

1. INTRODUÇÃO 14

1.1. Justificativa e relevância 18

1.2. Objetivos 20

1.2.1. Objetivo Geral 20

1.2.2. Objetivos Específicos 20

1.3. Metodologia de pesquisa 21

1.4. Estrutura da pesquisa 23

2. FUNDAMENTAÇÃO TEÓRICA 25

2.1. Indústria 4.0 25

2.2. Tecnologias da indústria 4.0 31

2.2.1. Internet das coisas 32

2.2.2. Big data 35

2.2.3. Computação em nuvem 36

2.2.4. Inteligência artificial 37

2.2.5. Robótica 38

2.2.6. Manufatura aditiva 39

2.2.7. Sistemas ciber-físicos 40

2.3. Gerenciamento de riscos 43

2.4. Riscos emergentes na indústria 4.0 51

2.5. STAMP - STPA 57

2.5.1. STAMP 57

2.5.2. STPA 61

3. REVISÃO SISTEMÁTICA DA LITERATURA 65

3.1. Apresentação da metodologia 65

3.2. Metodologia de revisão sistemática da literatura aplicada no estudo 67

3.3. Relatório da revisão - Análise dos resultados da pesquisa sobre ameaças às tecnologias da indústria 4.0 73

3.4. Análise dos resultados – metodologia STAMP e técnica STPA 78

3.5. Relação entre pesquisas: a solução para as vulnerabilidades da indústria 4.0 83

4. ***FRAMEWORK PROPOSTO PARA APOIO AO GERENCIAMENTO DE RISCOS NA INDÚSTRIA 4.0*** 85
4.1. Apresentação geral do problema 85
4.2. Status de digitalização industrial 86
4.3. Apresentação do framework proposto e desenvolvimento dos resultados .. 86
5. ***CONCLUSÕES E TRABALHOS FUTUROS*** 103
5.1. Conclusões 103
5.2. Limitações do estudo 105
5.3. Estudos futuros 106
REFERÊNCIAS 107

1. INTRODUÇÃO

As novas tecnologias digitais, fundamentadas nos computadores, softwares e redes, estão causando rupturas à terceira revolução industrial. Tecnologias mais sofisticadas e integradas estão transformando a sociedade e a economia global (SCHWAB, 2016).

De acordo com Schwab (2016) e Caruso (2017), há três razões pelas quais as transformações de hoje não representam apenas um prolongamento da terceira revolução industrial, mas sim a chegada de uma quarta transformação, também chamada de Indústria 4.0. A velocidade de evolução das tecnologias – com múltiplas inovações, cada vez mais qualificadas, interconectadas e multifacetadas, causando uma evolução exponencial, diferentemente das demais revoluções industriais. A amplitude e profundidade das mudanças – com a combinação da revolução digital e as inúmeras tecnologias que quebram paradigmas econômicos, sociais e biológicos sem precedentes, trazendo a modificação de todos os seres irreversivelmente e transformando integralmente sistemas de produção, segurança, controle e gestão. E, o impacto sistêmico da tecnologia na sociedade – ocasionando uma transformação sistêmica não apenas nas empresas ou indústrias, mas na sociedade, nas relações interpessoais e nos governos.

A primeira revolução industrial é entendida como a revolução que ocasionou o desenvolvimento da mecanização, iniciou-se no século 18 e deu início também aos processos de fabricação com a utilização do vapor de água. A segunda revolução industrial surgiu com o crescimento do uso da eletricidade na indústria, que permitia a produção em massa por meio de linhas de montagem e padronização do trabalho durante o início do século 20. Já a terceira revolução industrial trouxe a tecnologia da informação (TI) para a fabricação e com o crescente uso de computadores e outros dispositivos eletrônicos na indústria foi elevado de forma ainda mais acentuado o grau de automação nas duas últimas décadas do século 20 (QIN, 2016; REIS e KENETT, 2018).

Considerando as revoluções anteriores e seus aspectos disruptivos, em 2011 o governo federal alemão anunciou a Indústria 4.0 como uma das principais iniciativas de sua estratégia de alta tecnologia. Então, esse novo período de expansão industrial foi considerado a quarta revolução industrial, que se desenvolve sobre o sucesso da terceira revolução industrial e aproveita o notável desenvolvimento tecnológico sobre as tecnologias digitais, como a

cibernética, a internet das coisas, o armazenamento e a computação em nuvem, o sensoriamento remoto e os novos processos de produção, como a manufatura aditiva (REIS e KENETT, 2018).

Até então, o tópico Indústria 4.0 tornou-se famoso entre muitas empresas, centros de pesquisa e universidades, levando assim a discussão da nova revolução industrial que ocorre neste momento (BAHRIN et al., 2016). Diversos países adotaram termos análogos para caracterizar a nova era de desenvolvimento tecnológico e industrial, como a indústria 4.0 na Alemanha, a revolução robótica no Japão, a fábrica do futuro na França, a fábrica digital no Reino Unido e a manufatura avançada nos Estados Unidos (GORECKY *et al*., 2014).

É um conceito comum para todos que a Indústria 4.0 traga imensos benefícios – o que não é uma exceção às revoluções industriais anteriores – mas, diferente das revoluções precedentes, a quarta revolução industrial, se apresenta com uma taxa de desenvolvimento tecnológico exponencial, que busca antecipar-se aos desafios, mesmo quando difíceis de prever, com alta convergência de tecnologias, que se complementam e são capazes de integrar a rápida comunicação com a grande geração e processamento de dados, não considerando apenas a comunicação M2M, mas a crescente interação entre máquinas e humanos. As máquinas e seus componentes tornam-se cada vez mais autônomas e auto-organizáveis, transformando ambientes de manufatura em sistemas ainda mais complexos, com uma enorme gama de problemas e demandas e com uma necessidade de gerenciamento ainda maior. Tal necessidade não levará a um futuro em que as instalações de produção não terão trabalhadores, ao contrário, as pessoas deverão se integrar na estrutura ciber-física industrial, de modo que suas competências e habilidades individuais possam ser completamente exploradas, no entanto, grandes desafios ainda se apresentam, devido as atuais políticas de regulamentação, à velocidade do progresso governamental e principalmente as resoluções de políticas burocráticas, não globais e reativas (GORECKY *et al*., 2014; MORRAR *et al*., 2017).

Mesmo com alguns desafios à frente, a Indústria 4.0 tem atraído altos níveis de investimento na fabricação inteligente. Mais da metade dos fabricantes mundiais tem investido nas atividades de digitalização industrial, somando um montante de pelo menos 100 milhões de dólares nos últimos anos (TUPTUK e HAILES, 2018). E com o crescente nível de investimentos a indústria está começando a ver recompensas. De acordo com os especialistas da empresa de consultoria em tecnologia Capgemini (2017), a fabricação inteligente ajudou as indústrias a alcançar ganhos de produtividade de até 20%, enquanto alcançaram simultaneamente ganhos de qualidade superiores a 15%, possibilitando a exequibilidade de ganhos com as fábricas inteligentes ultrapassando os 500 bilhões de dólares e podendo alcançar

1,5 trilhões nos próximos cinco anos, assim acreditam os investidores (ROSSMANN *et al*., 2017).

Considera-se que a base para esse crescimento é a utilização de tecnologias digitais, como internet das coisas, computação em nuvem, análise de dados, aprendizado de máquina, inteligência artificial, sistemas ciber-físicos e *big data*. Para todas essas tecnologias, a IoT tem importância fundamental, pois fornece a ponte entre o domínio digital e o domínio físico de plantas industriais (TUPTUK e HAILES, 2018). Quando há a combinação dessas tecnologias sinergicamente as condições para o desenvolvimento dos processos de fabricação inteligente são concebidas, então, os componentes de fabricação são capazes de se comunicar de forma autônoma uns com os outros e se auto ajustar em suas operações, a fim de adaptar-se à distúrbios, exigências e restrições das flutuações de mercado, da demanda e do fornecimento (REIS e KENETT, 2018).

O crescimento exponencial das novas tecnologias digitais e da conectividade entre as máquinas e os trabalhadores, trouxe também a necessidade de medidas atualizadas para garantir a segurança dos sistemas industriais, do meio ambiente e da proteção à saúde contra os riscos laborais (BROCAL *et al*., 2018). Dada a novidade dessas novas tecnologias e dada a possibilidade de desenvolvimento de novas aplicações diariamente, o gerenciamento de segurança e a análise de riscos precisam ser atualizadas constante e frequentemente. Assim, novas abordagens teóricas e metodológicas são desenvolvidas para garantir a segurança dos processos digitais e pesquisas empíricas fornecem a evidência científica fundamental para enfrentar os riscos atuais e potenciais que o uso das novas aplicações tecnológicas trazem (GASPAR e GIGER, 2019).

De acordo com Brocal e Sebastian (2015), os processos da indústria 4.0 podem gerar não só os riscos ocupacionais tradicionais, mas outros riscos, chamados NERs (*New and Emerging Risks*). Segundo os autores, foi possível identificar e analisar 171 NERs compatíveis com os processos presentes na indústria 4.0. A definição de NERs pode ser entendida como qualquer risco ocupacional, produtivo ou ambiental, novo e crescente que surja com uma nova perspectiva industrial relativa à indústria 4.0 (BROCAL *et al*., 2018).

Os NERs podem ser definidos também como qualquer risco ocupacional, novo e que tem sua probabilidade de ocorrência aumentando com o passar dos anos. Isso significa que o novo risco era desconhecido e agora está sendo causado por novos processos, novas tecnologias, novos tipos de locais de trabalho ou uma mudança social ou organizacional. Mas

os NERs podem também surgir por outras fontes, como são os casos das ameaças identificadas à longa data, mas que só foram considerados importantes no momento atual, seja para a sociedade ou em uma organização, isso faz com que o conhecimento científico do estudo de riscos seja revisto e possa identificar antigas possibilidades de perigo antes desconsideradas como um novo e emergente risco. E, por fim, um NER pode ser identificado também quando o risco está aumentando, seja com o aumento da probabilidade de exposição ao perigo que conduz ao risco ou ao efeito do perigo para a saúde e segurança do trabalhador, do processo ou da organização em si (HOUTMAN *et al*., 2019).

O surgimento dos NERs foram observados nos processos avançados de manufatura e foi percebido que as abordagens tradicionais funcionavam bem para os sistemas mais simples do passado, mas houveram mudanças significativas nos novos tipos de sistemas e essas mudanças ampliaram os limites da engenharia, ocasionando novos tipos de riscos e aumento significativo da complexidade dos sistemas (LEVESON, 2012). Com o aumento das tecnologias digitais observou-se que os métodos de análise e controle de riscos tradicionais apresentavam algumas limitações para os atuais sistemas produtivos. Não exaurem todos os possíveis cenários de falha, são métodos extremamente trabalhosos e sofrem por limitações de natureza humana, como: erros de avaliação, falhas nos treinamentos e fadiga dos operadores, mas, como apresentam uma estrutura sólida e consolidada no tratamento de riscos são usados como base para o desenvolvimento de novos métodos de segurança. Dessa forma, surgem outras possibilidades para a análise e o gerenciamento de riscos, o desenvolvimento de abordagens sistêmicas, o uso de ferramentas inteligentes para a segurança, o desenvolvimento de modelagens de processos com uso das árvores de falhas, entre outros (CAMERON *et al*., 2017).

No entanto, segundo Chidambaram (2016), muitas organizações ainda não descobriram que as abordagens probabilísticas tradicionais não se adaptaram para o tratamento das novas causas de falhas e acidentes. Dada essa necessidade, de desenvolvimento de métodos e técnicas de análise de riscos que superassem as limitações das abordagens tradicionais, surgiram algumas ferramentas que ampliam a análise de riscos para uma visão mais sistêmica dos processos organizacionais. Podem ser citados o método FRAM (*Functional Resonance Analysis Method*), a abordagem AcciMap (*Accident Map*), o modelo HFACS (*Human Factors Analysis and Classification System*), a metodologia RiskSOAP (*Risk Situation Awareness Provision*), o método STAMP (*System-Theoretic Accident Model and Processes*), a técnica STPA (*Systems-Theoretic Process Analysis*), etc.

Buscando entender as necessidades presentes no gerenciamento da segurança e no tratamento adequado de riscos na Indústria 4.0, idealizou-se um estudo sobre as ferramentas de análise sistêmica de riscos STAMP e STPA e a sua aplicação às vulnerabilidades das tecnologias da indústria 4.0, para tratar e controlar riscos e ameaças. Com o objetivo de restringir o escopo do trabalho a pesquisa foi realizada em duas frentes, em uma delas elaborou-se uma revisão sistemática da literatura sobre as ameaças presentes nas tecnologias 4.0, na outra se analisou as ferramentas STAMP e STPA, construindo-se uma revisão sistemática da literatura para compreender seus conceitos, aplicações e a interface dessas ferramentas com as tecnologias presentes na indústria 4.0. Foram reunidos, em ambas as pesquisas, estudos dos últimos 10 anos sobre os temas, para identificar suas aplicações, restrições, principais autores e principalmente as lacunas existentes nas pesquisas sobre os temas.

1.1. Justificativa e relevância

As organizações industriais estão percebendo que precisam do apoio tecnológico para melhorar a forma como trabalham e para permanecer competitivas em um mercado cada vez mais volátil. A tendência de digitalização está sendo incluída nas organizações e estas estão tomando medidas para melhorar a eficácia da força de trabalho através da introdução de novas tecnologias, incluindo os três principais pilares da indústria moderna como objetivos para seu desenvolvimento. A otimização dos processos, o consumo otimizado de recursos e a criação de sistemas autônomos complexos, introduzindo a aplicação da internet das coisas e das tecnologias digitais como cerne para seus avanços (MOURTZIS e VLACHOU, 2018).

As principais organizações representantes da indústria 4.0 em todo o mundo, sejam elas instituições públicas ou privadas, acreditam que os efeitos das tecnologias digitais trarão grandes benefícios para à produtividade e grandes oportunidades econômicas e de trabalho com o avanço tecnológico (CARUSO, 2017). Para isso, a possibilidade de soluções digitais com menor custo permitirá que o monitoramento das atividades dos trabalhadores, das operações das máquinas e dos processos de transformação torne empresas mais competitivas atendendo simultaneamente a demanda do mercado e a entrega de produtos, no entanto, essas tecnologias ainda tem um longo caminho a percorrer para tornar os seus custos aceitáveis para todos (MONOSTORI, 2014; NAGY *et al*., 2018).

Segundo uma pesquisa aplicada por Nagy e outros (2018), os principais fatores que impedem as organizações de usar soluções digitais são: 1. os níveis de custos dessas tecnologias, tanto para implantação, quanto para manutenção – as empresas sentem que as

novas tecnologias apresentam custos incertos, principalmente pela falta de padrões e pelo risco da rápida obsolescência. 2. a segurança dos dados – um fator potencial de riscos, especialmente quando se trata de dados externos ou dados sensíveis de clientes. E, 3. a qualificação inadequada da força de trabalho – uma barreira ainda longe de ser resolvida e um fator impeditivo para a propagação da indústria 4.0. Assim, percebe-se que todos esses fatores estão relacionados com a inexistência de métodos, normas, protocolos e demais processos de padronização que garantam a interconexão entre sistemas atuais e sistemas tecnológicos digitais.

As indústrias brasileiras encontram-se atualmente, no patamar da Indústria 2.0. Ao compararmos os índices de exportação do Brasil com relação a outros países com maiores desenvolvimentos industriais, como por exemplo, a Alemanha (país em que as indústrias já estão se adequando ao patamar da Indústria 4.0), pode ser percebida uma diferença notória. A inclusão de novas tecnologias como estratégia para o desenvolvimento das indústrias brasileiras será primordial para garantir a competitividade e aumentar a participação do Brasil no mercado mundial. Mas o estado de desenvolvimento tecnológico brasileiro impede o avanço das tecnologias digitais industriais. Para o Brasil, considerando o atraso tecnológico, existe a oportunidade de ultrapassar algumas etapas e migrarmos diretamente para a indústria 4.0. Contudo, os riscos são enormes. Primeiramente, é preciso capacitar a mão de obra e habilitá-la a atender às demandas dessa nova indústria. Ademais, é necessário criar novos mecanismos regulatórios para que a indústria possa se desenvolver. No entanto, dado o atual arranjo econômico onde o vencedor leva tudo, corre-se um sério risco de ter a indústria nacional ainda mais deteriorada, uma vez que empresas estrangeiras inseridas nessa cadeia global de suprimentos serão mais competitivas e terão maior possibilidade de conquistar mercados hoje protegidos por governos locais (YAMADA e MARTINS, 2018).

Dessa forma, considerando o panorama da indústria 4.0 no cenário mundial, a crescente evolução da discussão sobre o tema e os novos problemas que surgem com a sua expansão, justifica-se a construção de um *framework* que possibilite a análise e a avaliação dos novos riscos da indústria 4.0 e que possa ser aplicada na indústria nacional, para limitar os riscos descritos e tornar o país capaz de competir com melhores chances de vitória com o mundo. A metodologia STAMP com aplicação da técnica STPA será utilizada nesse desenvolvimento, por se tratar de uma metodologia moderna e com grande potencial para ampliar as características de segurança nos processos digitais. Visualiza-se como principal objetivo dessa construção, simplificar as decisões estratégicas sobre a análise, controle e gerenciamento dos

riscos, para auxiliar administradores, gerentes, engenheiros e tomadores de decisão na escolha de ferramentas e ações para a manutenção da segurança industrial digital.

Pretende-se, com a proposição do *framework*, identificar os riscos das interações homem-máquina na indústria 4.0 em um contexto industrial e indicar as melhores estratégias de análise, controle e gerenciamento para o tratamento dos riscos emergentes. Ressalta-se que os riscos cibernéticos e de TI não serão considerados de forma abrangente, mas a impossibilidade da separação entre a quarta revolução industrial e as tecnologias da informação na indústria 4.0 torna a análise semelhante para os diversos casos, assim, a influência desses riscos poderá ser considerada no estudo.

Estima-se também que diversos outros benefícios possam ser alcançados ao fim da pesquisa. Benefícios econômicos, por proporcionar maior agilidade nas decisões técnicas de análise, controle e gerenciamento de riscos na indústria 4.0. Benefícios sociais, por possibilitar a escolha de medidas adequadas para a segurança dos operadores no ambiente de trabalho e, benefícios de natureza científica, por agrupar em um único estudo os conceitos de indústria 4.0 e as metodologias de gerenciamento sistêmico de riscos, aplicando a técnica STPA para o tratamento destes riscos no contexto tecnológico atual.

1.2. Objetivos

Os objetivos da pesquisa são expostos a seguir, indicando a principal finalidade do trabalho. O objetivo geral indica o que se pretende alcançar com a pesquisa e os objetivos específicos indicam qual o caminho a ser percorrido, para ao fim alcançar-se o objetivo primordial.

1.2.1. Objetivo Geral

Desenvolver um *framework* para auxiliar a escolha de estratégias eficientes para a análise, controle e gerenciamento dos riscos emergentes nas tecnologias digitais da quarta revolução industrial.

1.2.2. Objetivos Específicos

- Identificar os principais riscos presentes na indústria 4.0 por meio de uma revisão sistemática da literatura.
- Identificar as tecnologias digitais que apresentam mais vulnerabilidades e a influência dessas aos riscos presentes na indústria 4.0.

- Identificar as principais influências das ameaças e vulnerabilidades presentes nas tecnologias digitais da indústria 4.0.
- Identificar as principais características da metodologia STAMP e a técnicas STPA comuma revisão sistemática da literatura.
- Identificar os principais domínios de aplicação e os estudos mais relevantes sobre a metodologia STAMP e a técnica STPA.
- Elaborar um *framework* para auxiliar na mitigação de riscos das tecnologias da indústria 4.0, com a aplicação da metodologia STAMP e da técnica STPA.

1.3. Metodologia de pesquisa

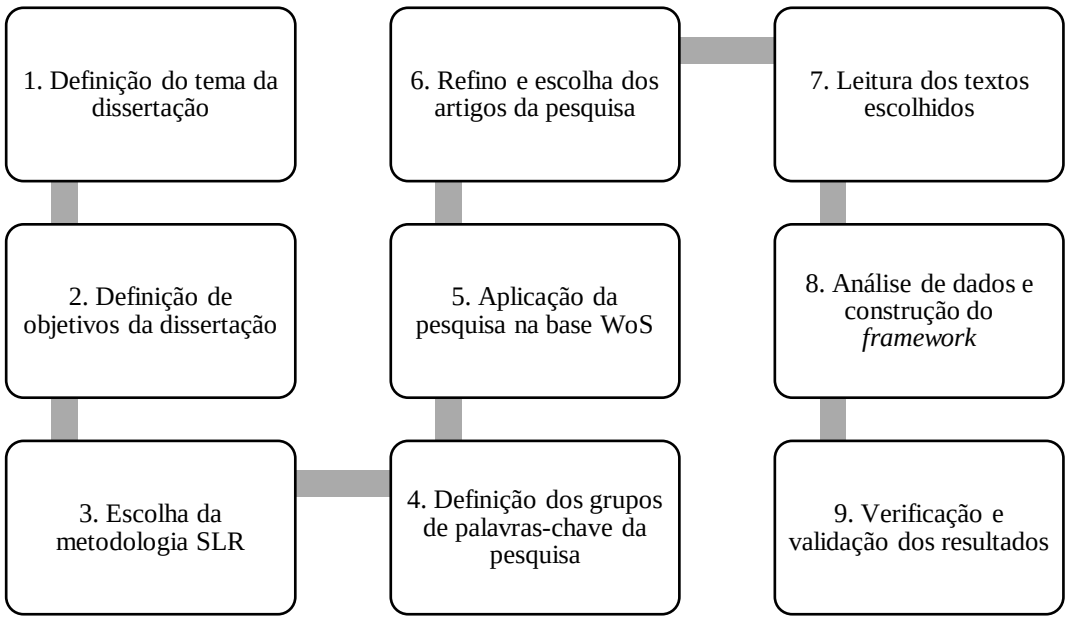
De acordo com Gil (2002), metodologia pode ser definida como procedimentos a serem seguidos na realização de uma pesquisa, já o termo pesquisa pode ser caracterizado como o procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos. Observando tais afirmações, metodologia da pesquisa pode ser entendida como a aplicação de procedimentos racionais e sistemáticos com o objetivo de responder questionamentos antes desconhecidos.

Segundo Silva e Meneses (2005) existem várias formas de classificar as pesquisas científicas. Podem ser classificadas quanto sua natureza (básica ou aplicada), quanto à forma de abordagem do problema (qualitativa ou quantitativa), quanto aos seus objetivos (exploratória, descritiva ou explicativa) e quanto aos seus procedimentos técnicos (bibliográfica, documental, experimental, levantamento, estudo de caso, *expost-facto*, pesquisa-ação ou participante). Seguindo a classificação sugerida pelos autores, a atual pesquisa pode ser caracterizada como uma pesquisa básica, de abordagem quantitativa e qualitativa, com objetivos exploratórios e descritivos e seguindo procedimentos bibliográficos.

Outras classificações podem ser encontradas na literatura, como a sugerida por Severino (2017), indicando que as pesquisas científicas podem ser classificadas como: pesquisa qualitativa ou quantitativa; pesquisa etnográfica; pesquisa participante; pesquisa-ação; estudo de caso; análise de conteúdo (bibliográfica, documental, experimental e de campo); pesquisa de natureza (exploratória, descritiva e explicativa); e, pesquisa por objetivo. Seguindo a classificação desse autor e considerando os objetivos do trabalho, pode-se classificar o estudo como pesquisa qualitativa e quantitativa, bibliográfica, exploratória e descritiva.

A construção do trabalho como um todo deverá seguir um processo de revisão bibliográfica. Na Fluxograma 1 pode ser entendido melhor quais as etapas serão realizadas na construção do trabalho, posteriormente serão mais bem explicadas todas as etapas do processo de revisão sistemática da literatura.

Fluxograma 1 - Sequência de atividades aplicadas no estudo



Fonte: Esta pesquisa (2019)

Na aplicação da pesquisa do estudo optou-se pela metodologia de Brereton e outros (2007), por ter ampla utilização nos trabalhos de revisão sistemática da literatura. A revisão sistemática da literatura é uma forma de revisar estudos anteriores relacionados a uma área de pesquisa específica, capaz de identificar, analisar e interpretar dados relevantes usando uma metodologia imparcial, confiável, rigorosa e auditável. O procedimento de revisão sistemática engloba três etapas.

1. Planejar a revisão bibliográfica;
2. Conduzir a revisão, e;
3. Construir o relatório da revisão.

A aplicação da revisão sistemática da literatura que será apresentada no trabalho está dividida em cinco tópicos, no primeiro serão apresentados os conceitos teóricos da metodologia científica de revisão sistemática e será definida a metodologia que será adotada no estudo. O segundo tópico mostrará as etapas iniciais da aplicação da pesquisa, levando em consideração

os objetivos das duas revisões realizadas, analisar as ameaças e vulnerabilidades das tecnologias da indústria 4.0 e explorar as aplicações das ferramentas de análise sistêmica de riscos STAMP e STPA. No terceiro e quarto tópico serão explicadas as etapas finais da aplicação das duas revisões realizadas, o terceiro tópico mostrará os dados encontrados na pesquisa referente as ameaças e vulnerabilidades presentes nas tecnologias digitais da indústria 4.0 e o quarto tópico deverá expor, de acordo com a etapa dois da aplicação da revisão sistemática da literatura, onde ocorre as principais aplicações das ferramentas de análise sistêmica de riscos, assim como seus principais autores. A etapa cinco da aplicação da metodologia buscará fazer um paralelo entre as duas áreas, possibilitando um melhor entendimento de como o STAMP e o STPA podem auxiliar nas ações de segurança das tecnologias da indústria 4.0.

A aplicação da revisão foi feita na base de dados *Web of Science* (WoS), uma base de dados com serviço de indexação de citações científicas *on-line*. Essa base foi escolhida por ser muito extensa e robusta quando são consideradas revistas nas áreas de Ciências Naturais e Engenharia (NSE) (MONGEON e PAUL-HUS, 2016). Dessa forma, como a área de ciências naturais e engenharia tem ligação direta com o estudo e é uma disciplina importante para as pesquisas em riscos e indústria 4.0, escolheu-se a plataforma *Web of Science*.

1.4. Estrutura da pesquisa

A presente dissertação está estruturada em cinco capítulos, que discorrem sobre o tema proposto, constroem metodologicamente a análise planejada e por fim concluem o trabalho com seus resultados.

No capítulo um são apresentados: introdução (que explica o contexto no qual o trabalho está inserido), justificativa do estudo sobre o tema (incorporando nesse tópico os conceitos mundiais e nacionais para indicar a relevância do tema para a sociedade e para o mercado), os objetivos da pesquisa, que são divididos em dois grupos, objetivo geral, que apresenta o proposito amplo e mais complexo da dissertação e objetivos específicos, que apresentam os fins da pesquisa de forma detalhada e com menor complexidade de realização. Por fim é apresentado ainda no capítulo um uma breve discussão sobre a metodologia utilizada e como o texto está estruturado, considerando todos os tópicos relevantes do estudo.

O capítulo dois apresentará a fundamentação teórica do estudo, abordando conceitos aprofundados sobre: indústria 4.0, tecnologias digitais presentes na indústria 4.0, riscos emergentes, metodologia STAMP e técnica STPA. No capítulo três será descrita a metodologia

para a realização da pesquisa e do desenvolvimento do trabalho, o contexto e as etapas das pesquisas aplicadas, a descrição das atividades e o desenvolvimento do *framework* planejado.

No capítulo quatro será apresentado o modelo proposto, indicando as principais tecnologias da indústria 4.0, os riscos, ameaças e vulnerabilidades presentes nas tecnologias da nova revolução industrial e a revisão bibliográfica dos estudos sobre as ferramentas STAMP e STPA para análise, controle e gerenciamento de riscos.

No capítulo cinco serão desenvolvidas as conclusões, as considerações finais da pesquisa, as principais limitações do estudo e as sugestões para trabalhos futuros. Por fim, são indicadas as referências utilizadas na construção do texto e do *framework* proposto.

2. FUNDAMENTAÇÃO TEÓRICA

Nesse capitulo será apresentada a base teórica utilizada na construção do trabalho, partido dos conceitos básicos da indústria 4.0 e tecnologias digitais facilitadoras, chegando as ameaças e riscos que alcançam tais tecnologias e apresentando uma metodologia e uma técnica que poderá sanar ou reduzir as ameaças digitais presentes no atual cenário industrial.

2.1. Indústria 4.0

A primeira revolução digital iniciou-se com o controle supervisório baseado em computadores, que foi testado pela primeira vez no final da década de 1950. Em 1970 os microprocessadores, possibilitaram os primeiros sistemas de controle distribuído (DCS), mas apenas com o aumento do poder computacional nos últimos 15 anos houve um desenvolvimento fenomenal na conexão industrial. A internet e os aplicativos para *smartphones* geraram mudanças drásticas no mercado consumidor e o que hoje é conhecido como digitalização ou transformação digital pode ser entendida também como segunda revolução digital (ISAKSSON *et al*., 2018).

A experiência com a atual segunda fase da revolução digital tornou possível a digitalização de objetos físicos de diversos tipos em digitais. Numa perspectiva primariamente tecnológica, fala-se em um contexto amplo sobre IoT e CPS visando um enorme potencial anteriormente desconhecido para muitas áreas e para diferentes aplicações, como habitação, sistemas médicos, sistemas de transporte, sistemas produtivos industriais em geral, redes globais de dados, aplicativos interativos, processos logísticos, coordenação e gerenciamento avançado controlados de forma remota, etc. (HIRSCH-KREINSEN, 2016).

A relação entre as duas revoluções digitais e as três revoluções industriais anteriores só apresentou interface nos últimos 20 anos. As três primeiras revoluções industriais caracterizaram-se pela produção mecânica, sempre dependentes da água, da energia a vapor, da utilização de mão de obra em massa, da energia elétrica e da utilização de eletrônica, respectivamente alinhada a produção automatizada. Já a quarta revolução industrial teve sua primeira conceitualização proposta em 2011, com o objetivo do desenvolvimento industrial digital da economia alemã. Esta nova revolução pode ser diferenciada das demais pela sua dependência ao uso de sistemas digitais de comunicação, apresentando grande conexão com a segunda revolução digital (LUKAC, 2015; BOYES *et al*., 2018).

Alguns autores, como: Rubmann e outros (2015), Chong e outros (2018), Kamble e outros (2018), Moktadir e outros (2018) e Nagy e outros (2018) creditam o desenvolvimento da indústria 4.0 à algumas tecnologias, que formam os pilares da quarta revolução industrial. Os robôs automatizados, a simulação com uso da realidade virtual, os sistemas de integração horizontal e vertical, a internet das coisas, os serviços em nuvem (computação e armazenamento), a manufatura aditiva, a realidade aumentada e o *big data*. Todas essas tecnologias monitoradas por uma central de controle definida como sistema ciber-físico, que projetam o mundo físico no mundo virtual e descentralizam a tomada de decisões operacionais, com uso de máquinas autônomas. Essas são descritas de forma conceitual na Quadro 1.

Quadro 1 – Pilares da indústria 4.0 e suas características

Pilares da Indústria 4.0	Descrição
Robótica avançada	Robôs industriais autônomos que trabalham em cooperação. Numerosos sensores integrados e interfaces adaptativas e responsivas.
Manufatura aditiva	Impressão 3D, particularmente para peças de substituição e protótipos. Instalações 3D descentralizadas para reduzir as distâncias de transporte e inventário.
Realidade aumentada	A realidade aumentada para manutenção, logística, e todos os tipos de procedimentos operacionais padrão. Exibição de informação de apoio e indicadores em tempo real, através de telas e vidros.
Simulação	Simulação de redes e cadeias de valor. Otimização com base em dados em tempo real de sistemas inteligentes. Digitalização de processos industriais e simulação da produção.
Integração horizontal e vertical	Integração de dados entre empresas com base em normas de transferência de dados. Condição prévia para uma cadeia de valor totalmente automatizada (do fornecedor ao cliente, para gerenciamento e compras).
Internet das coisas	Rede de máquinas e produtos conectados a internet. Comunicação multidirecional entre objetos em rede.
Computação em nuvem	Gestão de grande volume de dados em sistemas abertos. Comunicação em tempo real para sistemas de produção.
Cyber segurança	Operação em redes e sistemas abertos. Alto nível de comunicação entre máquinas, produtos e sistemas inteligentes.
Big Data	Avaliação completa dos dados disponíveis em tempo real para apoio à decisão e otimização.

Fonte: Adaptado de Chong e outros (2018)

Inúmeros autores tentam identificar as tecnologias que compõem o cerne da indústria 4.0, mas o termo é um coletivo para várias tecnologias e conceitos de organização da cadeia de

valor. Então, Pfohl e outros (2015) realizaram uma pesquisa bibliográfica e identificaram algo a mais na indústria 4.0, distinguiram mais de 60 tecnologias relacionadas a este conceito, todas podendo ser classificadas em grupos com características especificas, como: (1) dados e conexão, (2) análises e inteligência artificial, (3) interações homem-máquina, e (4) parque automatizado de máquinas. Alguns desses exemplos podem ser visualizados na Quadro 2, que demostra os principais componentes dessas tecnologias (CHEN *et al*., 2012; LEE *et al*., 2014; SZOZDA, 2017).

Quadro 2 - Tecnologias e soluções da indústria 4.0

Grupos de tecnologias da indústria 4.0	**Tecnologias da indústria 4.0**
Dados e conexão	Grandes bancos de dados (*big data*) - armazenamento de dados, processamento e cálculos. Internet das Coisas (IoT) e comunicação entre máquinas (*Machine to Machine*) - conexão e transferência de informações/dados. Tecnologias em nuvem (*Cloud technology*) - centralização do armazenamento e virtualização de dados armazenamento.
Análise e inteligência artificial	Digitalização e automação de trabalhos baseados no conhecimento - uso de inteligência artificial e aprendizado de máquina. Análise avançada - algoritmos e disponibilidade de dados aprimorados, implementação de sistemas avançados de mineração de dados usados principalmente para previsões.
Interação Homem-Máquina	Interfaces de toque e novas interfaces gráficas - possibilidade de comunicação rápida usando dispositivos portáteis. Realidade virtual - uso de óptica, incluindo óculos de realidade aumentada, na indústria, por exemplo em um armazém.
Parque de máquinas automatizado	Novas oportunidades de produção – impressoras 3D – ampla variedade de materiais, maior precisão e qualidade, possibilidade de obter imediatamente peças de reposição ou matérias-prima. Robótica avançada - uso de inteligência artificial, automação total da produção, uso da tecnologia M2M Armazenamento de energia – produção e armazenamento de energia, realizando atividades diárias nas empresas

Fonte: Adaptado de Chen e outros (2012); Lee e outros (2014); Pfohl e outros (2015); Yu e outros (2016); Szozda, (2017)

Como apresentado anteriormente, o objetivo da indústria 4.0 não difere das demais revoluções, almejando alcançar melhorias em termos de automação, eficiência operacional e

eficácia da produção (NAGY *et al*., 2018; SLUSARCZYK, 2018). Assim, diversos autores tentam especificar quais os fatores-chave que impulsionam a indústria 4.0. Kumar e outros (2018), indica que o avanço da indústria 4.0 é estimulado por quatro interruptores chave: o aumento surpreendente no volume de dados, de grande poder computacional e conectividade acelerada; o surgimento de análises e capacidades de *business intelligence* para auxílio na tomada de decisão; as novas formas de interação homem-máquina, com interfaces mais intuitivas e amigáveis, possibilitando a interação por toque e utilizando sistemas de realidade aumentada; e, a melhoria na transferência de instruções digitais para o mundo físico, tais como a robótica avançada e a impressão tridimensional (*3D Printing* ou manufatura aditiva).

Para atender as demandas dos mercados atuais, os avanços nas tecnologias de comunicação e informação foram necessários, possibilitando dessa forma aumentar o grau de automação e digitalização da produção e dos processos industriais. O gerenciamento de toda a cadeia de valor de forma mais eficiente e com maior garantia de qualidade só se tornou possível com a melhoria desses processos de produção e automação digital. Essas tarefas requerem sistemas inteligentes e sensores que informam as máquinas como elas devem funcionar e como serão envolvidas em cada etapa do processo de fabricação. Os processos devem ser autogeridos em um sistema modular descentralizado e em sistemas embarcados inteligentes com intercâmbio de dados e informações, tanto diretamente como através da nuvem e essas operações devem envolver a conexão com a internet e com todas as demais ferramentas tecnológicas da indústria 4.0 (SILVA *et al*., 2018).

Por esses e diversos outros motivos o conceito de indústria 4.0 tornou-se essencial no atual cenário industrial global. De acordo com a pesquisa apresentada por Maryska e outros (2018), englobando a maioria das empresas globais praticantes da indústria 4.0, foi indicado que estas estão vendo a internet das coisas como uma atividade estratégica (56%), que tem como principais motivações para sua implementação: o aumento da produtividade (24%), o tempo de mercado (redução do ciclo de vida, 22,5%) e a melhoria da automação de processos (21,7%). A pesquisa também identificou que 63% das empresas lançarão projetos focados na internet das coisas no próximo ano e 76% das empresas dizem que a tecnologia da internet das coisas será crítica para o seu sucesso em um futuro próximo. Já Graetz e Michaels (2015) realizaram uma análise em dezessete países e conseguiram demonstrar que os efeitos de robôs industriais sobre o crescimento econômico e ganhos de produtividade são claros. Popp e outros (2018) verificou que o uso dos processos de TI aumenta a produção industrial, resultando em

crescimento de receita e lucro, bem como maior qualidade dos produtos e melhor desempenho com a introdução de novas ferramentas.

Os principais atributos da indústria 4.0 concentram-se na internet das coisas aplicada a sistemas industriais para interconectar objetos, máquinas e seres humanos em fábricas inteligentes, com tarefas colaborativas que são incentivadas por altas taxas de produção e da minimização de custos. A interação entre os componentes presentes na indústria é alcançada através da introdução de sistemas ciber-físicos, esses componentes captam grande quantidade de dados gerados por sensores e trabalham na execução de algoritmos, mas, como *trade-off* geram um dos maiores desafios globais atuais, o *big data* (BORGIA, 2014; LU, 2017; RODA-SANCHEZ *et al*., 2018).

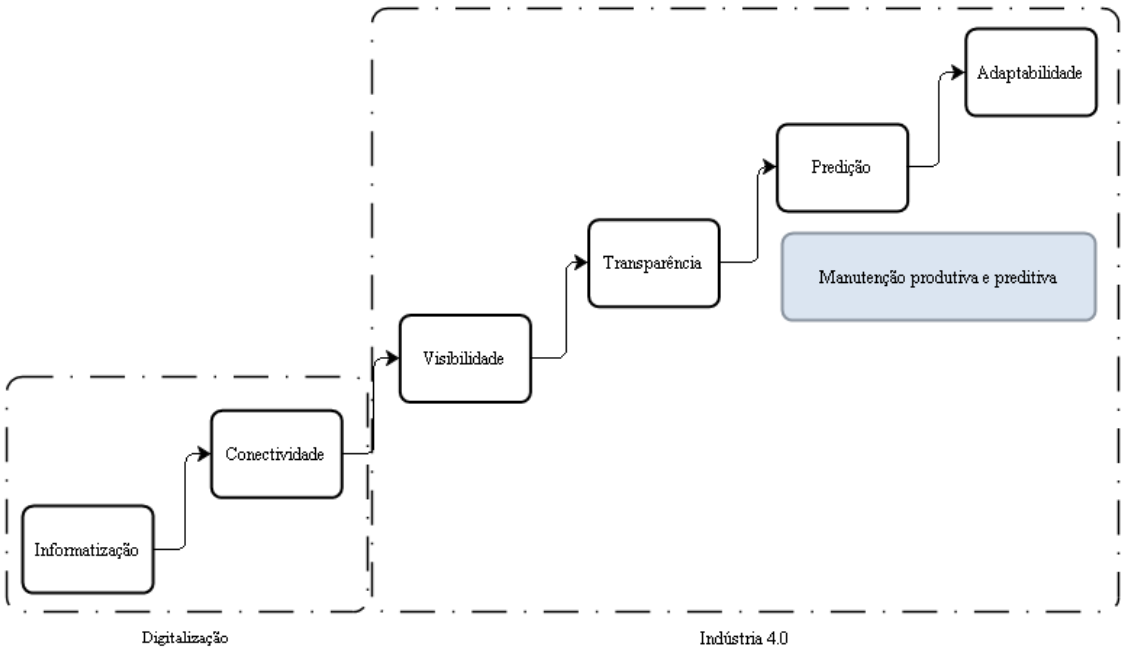
No entanto, assim como há grandes desafios ainda a serem solucionados para a indústria 4.0, não sobram apenas benefícios e elogios às tecnologias digitais, junto a esse paradigma os sistemas de comunicação e informação (ICS) enfrentam novos desafios devido ao aumento do número de dispositivos interconectados. A separação dos ICS e da TI influenciou a eficiência operacional, a redução de custos de implantação e desenvolvimento de sistemas e a resiliência dos processos produtivos, mas trouxe consigo uma exposição crescente aos riscos, com novas ameaças cibernéticas (CORBO *et al*., 2017).

Dessa forma, a segurança não pode mais ser vista como um produto que pode ser comprado e adicionado ao sistema, em vez disso, é necessário um processo de desenvolvimento que se inicia com características de segurança ainda na fase de concepção e deve permear todos os processos de desenvolvimento dos sistemas produtivos. É um processo contínuo, a detecção de uma simples emergência de segurança ou novas ameaças de vulnerabilidade pode incentivar uma revisão completa da segurança de todo o sistema, que só poderá ser alcançada a partir da perspectiva de concepção do projeto. Naturalmente, a complexidade para adicionar ou remover subsistemas modulares nos sistemas fabris tradicionais complica ainda mais esse desenvolvimento de processos seguros (TUPTUK e HAILES, 2018).

Considerando essas necessidades de segurança, na concepção do projeto da fábrica digital, indica-se o desenvolvimento dos processos de segurança ainda em uma das atividades iniciais do modelo de maturidade. O desenvolvimento da indústria 4.0 permeia duas etapas, a etapa inicial, considerada fase de digitalização, é composta por duas atividades que devem ser realizadas para garantir o desenvolvimento do projeto de inteligência fabril, as atividades de informatização e conectividade. Alcançando a fase de maturidade de digitalização, mais quatro

atividades devem ser completadas, tornando assim os sistemas industriais complexos não vulneráveis, que irão apoiar significativamente o desenvolvimento dos meios produtivos. São as atividades de visibilidade, transparência, predição e adaptabilidade. A Figura 1 indica o modelo de maturidade que é indicado para avaliação dos sistemas industriais digitais. (RODSETH *et al*., 2017).

Figura 1 - Modelo de maturidade da indústria 4.0



Fonte: adaptado de Rodseth e outros (2017)

Outros autores também tentam classificar a maturidade organizacional da indústria 4.0, como Nagy e outros (2018). Os autores indicam que a mudança cultural nas empresas com o foco na quarta revolução industrial tende a seguir passos subsequentes que ao fim alcançam o objetivo principal. O primeiro desses passos é visto como a aplicação de ferramentas e tecnologias em redes, para garantir a transparência, proteção e segurança de todo o processo de negócio. A integração horizontal, com conectividade em tempo real e cooperação com a rede de colaboradores internos é tido como um passo seguinte, posteriormente deve-se pensar em integração vertical, que envolve a cooperação com os parceiros na cadeia de suprimento, seja *bottom-up* ou *top-down*, incluindo todos em uma conexão digital e, por fim, transformar o modelo de negócio e objetivar o principal ponto cultural - foco nos clientes.

A fábrica inteligente proposta na literatura representa um sistema de manufatura inteligente, flexível, extensível e confiável, que pode autonomamente perceber as informações

do mundo físico e compreender o seu significado, interagindo com o ambiente e garantido a conformidade e a confiabilidade, mas nem sempre esse conceito por completo é aplicável, na maioria dos casos um longo caminho deve ser percorrido para se alcançar essa definição (WAN *et al*., 2018). Em 2016, foi realizada uma pesquisa sobre a indústria 4.0 global, com a participação de dois mil especialistas de 26 países, esses foram questionados sobre como suas empresas irão explorar as oportunidades proporcionadas pela digitalização. A maioria das empresas pesquisadas (52%) indicou que o maior obstáculo para a implementação da indústria 4.0 é a falta de uma estratégia de desenvolvimento clara para os processos de produção e para os processos logísticos, ambos com total dependência dos seus executivos chefe para a introdução das tecnologias digitais (NAGY *et al*., 2018).

Dessa forma, identifica-se a necessidade de auxiliar os decisores na tomada de melhores e mais assertivas decisões, para que as tendências de personalização, individualização e flexibilidade em massa sejam alcançadas, ultrapassando os desafios que os modos de produção tradicionais apresentam. E uma das principais barreiras identificadas é a segurança, por isso almeja-se construir o *framework* idealizado e proporcionar antecipadamente uma forma de eliminar as principais problemáticas já na implantação das tecnologias facilitadoras da indústria 4.0 (DU *et al*., 2018).

A partir dos conceitos da indústria 4.0 discutidos e com as apresentações sobre suas principais tecnologias facilitadoras, torna-se necessário uma discussão mais aprofundada de tais tecnologias. Assim, o próximo tópico discutirá as características intrínsecas dos principais pilares da indústria 4.0, e como essas tecnologias se complementam para formar o maior paradigma disruptivos já visto na indústria produtiva mundial, a integração entre revolução digital e industrial.

2.2. Tecnologias da indústria 4.0

Com o avanço da tecnologia podemos perceber que a fabricação tradicional tem seus dias de atuação contados com o advento da quarta revolução industrial, e isto ocorre visto a transformação do modelo tradicional para um ecossistema digital. Nessa transformação, a IoT, os CPSs, o *cloud computing* e o *big data* detêm um papel importante. O de desenvolver novos horizontes em direção à digitalização industrial, permitindo que procedimentos automatizados e de comunicação, por meios que não eram viáveis no passado, interliguem os sistemas de produção e as cadeias de abastecimento, constituindo assim um sistema completo que funciona como um todo integrado (MOURTZIS e VLACHOU, 2018).

Confirmando tal afirmação, descobriu-se que na última década, a IoT e os sistemas ciber-físicos tornaram-se generalizados e essa ação teve um impacto sobre diversos aspectos da vida cotidiana. Conceitos como *Smart Home, Smart Car* e *Smart City* tornaram-se familiares também para a população no geral, e o papel das novas tecnologias digitais que constituem a espinha dorsal da quarta revolução industrial se tornou ainda mais concreto, transformar radicalmente a forma como as empresas tradicionais e mecanizadas funcionam e como as interações com as ferramentas digitais são exercidas (ATZORI *et al*., 2010; STANKAVIC, 2014; PILLONI, 2018).

Segundo Schwab (2016), as mudanças nos sistemas produtivos serão tão profundas que, na perspectiva da história da humanidade, nunca houve um momento tão potencialmente promissor ou perigoso para todos. O autor atribui esse desenvolvimento a três principais categorias. Categoria física, digital e biológica, todas inter-relacionadas, interativas e prontas para causar rupturas nunca vistas. Dentre essas categorias se destacam algumas tecnologias digitais que terão maior foco no seu desenvolvimento. Dentro da categoria física estão os veículos autônomos, a impressão em 3D, a robótica avançada e os novos materiais sintéticos. A categoria digital está representada pela internet das coisas, redes inteligentes, conexão entre dispositivos distintos, possibilidade de tornar veículos, casas, empresas, hospitais, escolas e cidades inteligentes e dialógicas e pela evolução das comunicações com o uso da internet em todo e qualquer dispositivo. Já a categoria biológica engloba tecnologias com a capacidade de interferir e modificar os seres vivos, como a biologia e engenharia genética, a biologia sintética, a mudança genética dos seres, os modificando e adaptando-os a condições adversas e a possibilidade de xenotransplantes, repondo órgãos perdidos com o uso de órgãos de outras espécies.

Considerando as novas possibilidades que a indústria 4.0 conduz, faz necessário analisar algumas tecnologias que são o cerne desse desenvolvimento. Como a internet das coisas, os sistemas ciber-físicos, a computação em nuvem, os robôs, o *big data*, a impressão 3D ou manufatura aditiva e a inteligência artificial.

2.2.1. Internet das coisas

A internet das coisas refere-se ao fornecimento de dispositivos com sensores, que lhes dão a capacidade de comunicar e se tornarem participantes ativos em uma rede de informação. A aplicação da tecnologia de internet das coisas transforma produtos *stand-alone* (sem conexão ou com dependência de rede) em inteligentes e sempre conectados com a *web* (PORTER e

HEPPELMAN, 2014; KAMP e PARRY, 2017; RYMASZEWSKA *et al*., 2017; BRESSANELLI, 2018). O conceito internet das coisas envolve todos os objetos físicos ligados entre si dentro em uma estrutura de rede e torna esses capazes de coletar dados e compartilhá-los com os outros (HSIEH *et al*., 2016; HUNG-LIN *et al*., 2018).

IoT é um conceito que descreve a computação transformadora, modificando objetos comuns em dispositivos conectados. A internet das coisas é geralmente descrita como a tecnologia disruptiva que solucionará a maioria dos problemas da sociedade de hoje, com soluções para as cidades inteligentes, transporte inteligente, controle de poluição, saúde, entre outros (SISSINI *et al*., 2018). No entanto, o termo e os planos devem ser feitos com cuidado, pois inúmeros problemas advêm com a aplicação da IoT.

O conceito de internet das coisas foi ouvido pela primeira vez em 1999, durante uma apresentação realizada por Kevin Ashton para a Procter & Gamble (P&G). Daí em diante, IoT tornou-se um novo paradigma para o desenvolvimento de comunicação social e industrial. A internet das coisas tem o intuito de ligar milhões de objetos de qualquer tipo à uma conexão em rede e potencializar grandes mudanças em nossas vidas, com ganhos de produtividade, melhorias na saúde, melhoras na eficiência, redução do consumo de energia e aumento do conforto em nossas casas, carros e até mesmo cidades (ATZORI *et al*., 2010; MOLANO *et al*., 2017).

No estudo em questão, tende-se a diferenciar entre a internet de consumo pessoal e social da internet industrial, por ambas terem características distintas e a forma de criação de valor também ser distinta para as partes. Para a internet social – de consumo pessoal – suas características são baseadas principalmente na interação sociais entre as pessoas, buscando aproximar e solucionar problemáticas de comunicação, na maioria dos casos o valor criado por esse meio vem a partir de anúncios e comercialização de produtos digitais. Já a internet industrial, interessante e relevante apenas para um seletivo grupo, caracteriza-se por construir a integração dos mundos físico e digital. O surgimento de outras tecnologias facilitadoras também ampliou o uso da internet industrial e possibilitou a maior utilização por organizações, com a aplicação de sensores, *software*, aprendizado de máquina, comunicação M2M e demais tecnologias para coleta, análise e compartilhamento de dados, rompendo as barreiras do mundo físico e convertendo objetos físicos em dados informatizados (BOYES *et al*., 2018).

A internet das coisas é atualmente uma visão onipresente, está em pauta nas diversas áreas de trabalho, estendendo-se desde o panorama acadêmico às agendas dos executivos e em

feiras de negócios da indústria. O termo descreve a visão de que praticamente todos os objetos se tornam inteligentes e conectados (ATZORI *et al*., 2010; MATTERN e FLOERKEMEIER, 2010; WEINBERGER *et al*., 2016).

A Indústria 4.0 adota a internet das coisas para uso na fabricação e com isso apresenta um grande potencial para melhorar a produtividade, eficiência, inteligência de fábricas e instalações industriais. Portanto, um sistema industrial inteligente é composto por dois componentes principais: os sistemas virtuais e os sistemas físicos. Os sistemas virtuais incluem infraestruturas de controle, redes e computação que permitem a operação, interconexão e inteligência dos sistemas industriais. Já os sistemas físicos são os sistemas de manufatura e automação que utilizam dispositivos industriais para realizar tarefas de produção e automação designadas por seus operadores que estão nos controles virtuais (LASI *et al*., 2014; LEE *et al*., 2015; XU *et al*., 2018). Qualquer sistema que exclui os fatores humanos inerentes à implantação e gerenciamento de segurança é sempre susceptível à falha, assim como ocorreu no desenvolvimento da segurança dos sistemas de TI, é essencial que a tecnologia de internet das coisas no meio corporativo incorpore a segurança desde o início, integrado com funcionalidades, e não como uma dimensão secundária (TUPTUK e HAILES, 2018).

Consequentemente, todo o potencial da internet das coisas não poderia ser explorado sem interação com outras tecnologias. Por exemplo, a tecnologia do *big data*, a mais capaz de lidar com as enormes quantidade de dados que os sensores da internet das coisas podem produzir, assim como a inteligência artificial é necessária para processar e analisar dados advindos da internet das coisas em tempo real e os sistemas ciber-físicos são essenciais para integrar o trabalho homem-máquina, que podem ser baseada em gestos, voz e diversos comandos interativos conectados e integrados aos dispositivos e ao mundo. Dessa forma, a ampliação da utilização em escala produtiva faz da internet das coisas o grande diferencial para a ruptura da terceira para a quarta revolução industrial (MANOGARAN *et al*., 2018; MARYSKA *et al*., 2018).

De acordo com Fleisch e outros (2014) e Weinberger e outros (2016), no presente, a internet das coisas pode ser usada pelas organizações de três maneiras diferentes. Aplicando o gerenciamento de alto padrão – aumentando a eficiência, qualidade e flexibilidade de seus processos organizacionais, bem como melhorando a gestão de relacionamento com clientes e fornecedores. Enriquecendo seu portfólio de produtos com a adição de tecnologias de sensores e atuadores para oferecer os chamados produtos digitalmente carregados – buscando oferecer aos seus clientes soluções inteiramente novas, aprimoradas e com maior proposta de valor que

as ofertas existentes. E, fornecendo e compartilhando tecnologias de IoT com seus parceiros comerciais – permitindo assim que os demais integrantes da cadeia produtiva se tornem participantes de sucesso no próprio ecossistema.

Alguns analistas de tecnologia preveem que mais de vinte bilhões de dispositivos estarão conectados à internet até 2020 e com esse avanço exacerbado também surgirão novas preocupações, que já foram discutidas anteriormente (MOURTZIS *et al*., 2016; QI e TAO, 2018). A IoT depende de um grande número de tecnologias de suporte, como a identificação por rádio frequência (RFID), os sensores sem fio para monitoramento de condições operacionais, os sensores para fornecimento de informações de localização e a computação em nuvem, para processamento e armazenamento da grande quantidade de dados que é gerada por tais dispositivos de apoio (ATZORI *et al*., 2010; GUBBI *et al*., 2013; LEE e LEE, 2015; GOBBO *et al*., 2018). Com essa grande quantidade de dados gerados atualmente pelos meios de produção é indispensável o uso dos sistemas de armazenamento e análise contínua de dados, convencionalmente chamados de *big data*. (GUBBI *et al*., 2013; REINHART *et al*., 2013; TORO *et al*., 2015; NAGY *et al*., 2018).

2.2.2. *Big data*

Gao e outros (2018), Liang e outros (2018) e Xu e outros (2018), indicam que o *big data* na indústria 4.0 refere-se ao grande volume, a velocidade acelerada e veracidade dos dados recolhidos a partir dos sensores, atuadores e dispositivos, mas, a tecnologia *big data* pode ser interpretada também como um grande aglomerado de dados gerados pelos sistemas digitais. Esse grande conjunto de informações é diferenciado das demais formas de armazenamento de dados por conter características muitos especificas. O volume, a variedade, a velocidade e o valor, os quatro Vs do *big data* (GANTZ e REINSEL, 2011; CHEN *et al*., 2014; GANDOMI e HAIDER, 2015; QI *et al*., 2018).

O volume refere-se a escala de dados, variando de vários PBs (mil TB) para ZBs de informações (um bilhão de TB). Variedade significa que o tamanho, conteúdo, formato e as aplicações dos dados são diversificados, por exemplo, dados estruturados que incluem dígitos, símbolos e tabelas, dados semiestruturados como árvores de dados, gráficos e documentos XML e dados não estruturados, como registros, áudios, vídeos, documentos e imagens. Velocidade é referente a geração rápida de dados e o seu processamento que requer alta velocidade de atualização. Valor significa importância, como a extração de informação valiosa a partir de dados massivos através de algoritmos poderosos. Todas essas características são a

chave para melhorar a competitividade, mas uma merece destaque nos cenários atuais, pois a velocidade é a vida das empresas e é necessária para a transformação da indústria 4.0 acontecer (GANTZ *et al*., 2011; CHEN *et al*., 2014; GANDOMI e HAIDER, 2015; QI *et al*., 2018).

Com isso, para se alcançar um nível adequado do uso do *big data* industrial deve-se inicialmente garantir a sua base, a coleta de dados. Mas esse passo inicial experimenta também suas dificuldades para se desenvolver. A capacidade de integração entre diferentes dispositivos, equipamentos e fornecedores, a diversidade das estruturas de comunicação e os diferentes níveis de inteligência dos dispositivos dificultam o estabelecimento de um fluxo de dados refinado para análise estatística posterior e para o aprendizado de máquina (WAN *et al*., 2018).

A tecnologia do *big data* visa primordialmente proporcionar o armazenamento e a análise de grandes conjuntos de dados, sejam estes estruturados ou não estruturados, permitindo que novos conhecimentos sobre a produção sejam desenvolvidos, identificando problemas antecipadamente ou criando modelos mais precisos baseados em dados robustos. Então, de acordo com Yan e outros (2017), o *big data* industrial oferece a oportunidade de explicar completamente o estado de um processo de fabricação, utilizando a inteligência das técnicas de processamento e previsão de dados, e com isso melhorar o desempenho da tomada de decisão dos sistemas.

Mas esse grande volume de dados não pode ser analisado e fornecer informações sem seus elementos de apoio, assim, abre-se espaço para a tecnologia de computação em nuvem, onde têm-se a principal forma de armazenamento de dados sociais e por onde são transmitidos os principais elementos do *big data* advindos da IoT.

2.2.3. Computação em nuvem

A computação em nuvem é tida como uma tecnologia facilitadora da indústria 4.0 por apoiar fortemente outras tecnologias, como o *big data*, IoT, IA, etc. Tecnologias essenciais para a transformação da indústria digital. Sua combinação com a internet para a manufatura industrial permite o estabelecimento de fábricas, produtos e serviços inteligentes que atendam às necessidades e anseios dos sistemas produtivos atuais e de seu público (GARRIDO-HIDALGO *et al*., 2018).

A computação em nuvem é uma tecnologia moderna que permite o acesso onipresente, conveniente e de rede sob demanda a um conjunto compartilhado de recursos de computação configuráveis, como redes, servidores, armazenamento, arquivos, aplicativos e serviços. Esses

recursos podem ser rapidamente acessados e liberados com o mínimo esforço de gerenciamento ou pela interação do provedor de serviços com os agentes desse processo (MELL e GRANCE, 2011).

É permitido na computação em nuvem que aplicativos de software e dados não sejam instalados fisicamente na planta, mas em qualquer lugar por meio de conexão de internet, isso permite o uso de recursos de computação muito mais poderosos, administração remota mais fácil e reduz o risco de investimento, sem que haja necessidade de dispêndio de capital em *hardware* pelas empresas (ISAKSSON *et al*., 2018).

No entanto, em um ambiente de produção complexo, os mecanismos de distribuição de recursos como a computação em nuvem afetam não só a eficiência da produção, mas também o consumo de energia, fazendo com que a desordem causada por essa falha de alocação de recursos provoque interrupções e perdas. Alguns pontos são importantes também como problemáticas da computação em nuvem, por exemplo, o balanceamento de carga da nuvem para *hosts* físicos, prejudicando o processamento de tarefas e consequentemente a eficiência computacional da organização (WAN *et al*., 2018).

O *big data* e a computação em nuvem são tecnologias que caminham lado a lado com o desenvolvimento digital da indústria, mas para auxiliar esses componentes de transmissão e armazenamento de dados são necessárias tecnologias que exploram, analisam e decidem sobre tais, por isso tem-se como tecnologia de grande importância pra a indústria 4.0 a inteligência artificial e as técnicas avançadas de análise de dados.

2.2.4. Inteligência artificial

A inteligência artificial é uma ciência orientada ao design de máquinas inteligentes e tem o intuito de explicar o comportamento da inteligência, como ocorre em humanos e outros animais. Define-se como objetivo da IA construir uma teoria das capacidades humanas de processamento de informações, para assim, desenvolver máquinas inteligentes (NILSSON, 2014). Em seu sentido amplo, a inteligência artificial refere-se a capacidades abstratas associadas à solução de problemas e que não requer necessariamente uma referência ao mundo físico. Um robô autônomo pode usar ferramentas de inteligência artificial para resolver seus problemas, mas está fundamentado no ambiente físico que compartilha com outros objetos. Uma inteligência artificial em si pode usar um robô autônomo para implementar uma solução criada ou coletar dados para resolver um problema, mas também não precisa se ater no mundo físico para isso (LAWLESS *et al*., 2017).

IA é também um campo relevante e em crescimento para a digitalização industrial. Esse campo é composto por várias metodologias e técnicas de representação e capacidade de análise humana, como, árvores de decisões, regressões lineares e redes neurais, possibilitando que dispositivos físicos obtenham resultados eficazes na entrega de novos serviços e aplicações inteligentes para os cenários de negócios (MOZZAQUATRO *et al*., 2018).

A IA pode ser aplicada para as fábricas inteligentes em grande medida. A implementação dessa tecnologia na indústria produz mudanças significativas nos processos organizacionais, incluindo: dispositivos inteligentes, incorporados com inteligência artificial, sensoriamento de máquinas mais precisas e confiáveis, mecanismos de colaboração com a tomada de decisão, capacidade de raciocínio autônoma e métodos de processamento de dados com base nos algoritmos de inteligência artificial avançada, como a aprendizagem profunda, que demonstram ser mais precisos e eficientes que humanos (WAN *et al*., 2018).

No entanto, para que a inteligência artificial possa alcançar seus objetivos e facilitar a forma de trabalho industrial, há necessidade de tornar físico suas decisões e suas ações, em grande parte das situações. Dessa forma, o uso de robôs com inteligência artificial como uma das tecnologias facilitadoras da indústria 4.0 é indispensável em diversos setores, como: aviação, fabricação de automóveis, setor de defesa, etc.

2.2.5. Robótica

A robótica é uma área de estudo interdisciplinar reconhecida desde meados dos anos 1900. Na década de 1970, a primeira onda de robôs industriais passou da comunidade de pesquisa para o chão de fábrica, esses robôs foram automatizados para superar problemas de segurança devido a suas limitações sensoriais e de processamento e melhorados para interagir de forma mais amigável com humanos (LAWLESS *et al*., 2017).

A tecnologia da robótica é de grande influência para a indústria 4.0. Segundo Wan e outros (2018) o desenvolvimento da tecnologia de robótica industrial e o número de robôs móveis utilizados nas fábricas aumenta constantemente. No ambiente de fabricação complexo, a otimização de um processo com uso de robôs não só influencia a eficiência do sistema, mas também está intimamente relacionada com o consumo de energia, custo, tempo e outros fatores correlacionais. A disseminação dos robôs e da inteligência artificial ajudou a construir processos de trabalho menos monótonos, essas tarefas são realizadas com precisão por máquinas com custos financeiros significativamente mais baixos em longo prazo (GUBBI *et al*., 2013; REINHART *et al*., 2013; TORO *et al*., 2015; NAGY *et al*., 2018).

Em um estudo apresentado por Erdei e outros (2018) realizado no ano de 2015 em dezessete países, demonstrou-se claramente a possibilidade de ganhos econômicos e de produtividade com o uso de robôs industriais. Ainda de acordo com algumas opiniões e com o próprio estudo foi possível indicar que as novas tecnologias promovem a preservação do emprego, quando a integração é realizada de forma amistosa, e promovem ainda um crescimento das oportunidades com maior grau de qualificação.

Devido à transformação digital do setor manufatureiro linhas robóticas estão cada vez mais flexíveis, baseando-se em comunicação M2M, dessa forma, novas possibilidades para lidar com falhas estão sendo descobertas, permitindo que robôs, unidades de transporte e peças de trabalho se comuniquem umas com as outras continuamente, compartilhando informações sobre o seu estado atual e permitindo um reconhecimento dinâmico das configurações do sistema de produção (MULLER *et al*., 2017a; MULLER *et al*., 2017b).

Com o avanço tecnológico os robôs tendem a ser inteligentes e cooperativos, com uso constante da inteligência artificial em um futuro próximo. Por um lado, robôs podem interagir naturalmente com os seres humanos, por outro lado, os robôs podem cooperar com as pessoas na produção industrial. Com base nisso, o conceito de colaboração homem-máquina surgiu como resultado, e foram gradualmente aceitos por diversas organizações. Consequentemente, nos últimos anos, os robôs colaborativos são utilizados em várias cadeias produtivas, tais como linhas de produção em massa, linhas automotivas, produção contínua, etc. (DU *et al*., 2018).

Um dos maquinários robóticos mais usados atualmente na indústria é a impressora 3D, com ela desenvolveu-se processos de prototipagem e desenvolvimento de peças de reposição rápidos e eficientes. Por conta de tais características a manufatura aditiva é uma das tecnologias com maior demonstração de resultados na indústria 4.0, facilitando e promovendo a cultura tecnológica digital industrial.

2.2.6. Manufatura aditiva

A manufatura aditiva ou como pode ser popularmente chamada por impressão 3D, é um processo de fabricação aditiva que produz objetos camada por camada. Existem vários tipos de impressão em 3D. Reconhecidamente, os tipos mais divulgados utilizam materiais termoplásticos ou poliméricos para extrusão e formação de produtos, que são endurecidos imediatamente após sua aplicação (CHONG *et al*., 2018).

Em seu conceito inicial, a impressão 3D era usada principalmente para aplicações de prototipagem. No entanto, com uma profunda pesquisa sobre impressão 3D de material metálico, os pesquisadores começaram a transformar a tecnologia de prototipagem em um método de fabricação controlável e com bom desempenho. Em um futuro próximo imagina-se que as indústrias combinem diferentes técnicas de fabricação, incluindo processos aditivos, equivalentes e subtrativos, e as integrem em uma forma de fabricação ou consigam combinar essas técnicas na cadeia de produção (LU *et al*., 2015).

A história da fabricação aditiva é relativamente curta, quando comparada com a fabricação tradicional, subtrativa. Um dos primeiros protótipos de uma máquina de impressão 3D foi criado há menos de 30 anos, indicando que um grande potencial pode ser desenvolvido com a aplicação da tecnologia. No entanto, o futuro promissor dessa tecnologia também torna imprevisível seu impacto na indústria tradicional (LU *et al*., 2015).

As problemáticas atuais encontradas na manufatura aditiva são relacionadas principalmente com o tamanho limitado dos componentes de construção, as taxas de construção lentas, o esforço elevado para o design dos produtos, a definição dos parâmetros do processo, a precisão dimensional, os métodos de pós-tratamento necessários como acabamento superficial e a qualidade do pó e dos materiais usados para a produção. Mas tais limitações estão relacionadas principalmente com a funcionalidade das impressoras 3D, em uma visão industrial essas tecnologias estão conectadas e inseridas em redes remotas, que conversão e trocam dados com todas as demais tecnologias (BERGER, 2013; DUDA e RAGHAVAN, 2016).

Para unificar todas as tecnologias já discutidas anteriormente, definiu-se um conceito que engloba os sistemas tecnológico em uma só concepção, muitas vezes confundido como sinônimo da indústria 4.0, os sistemas ciber-físicos.

2.2.7. Sistemas ciber-físicos

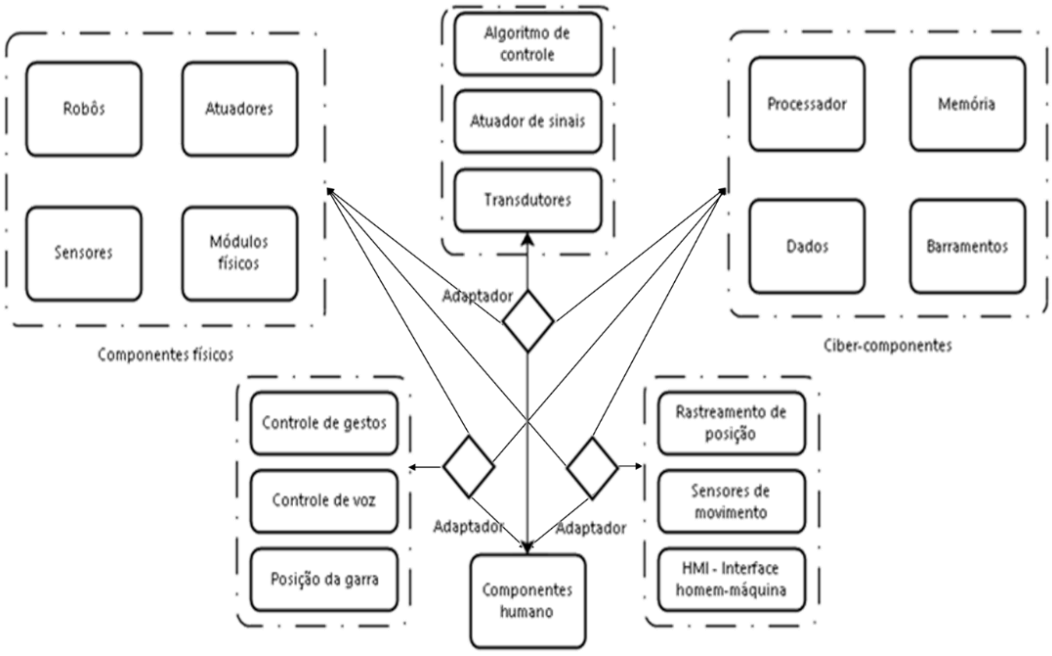
Os sistemas ciber-físicos (CPS) são os principais componentes de integração entre as tecnologias digitais já citadas no texto. Eles são definidos como sistemas que interagem com o mundo físico e o seu homólogo digital (SISSINI *et al*., 2018). Os sistemas ciber-físicos compreendem um conjunto de interações entre os componentes físicos e digitais, que podem ser centralizados ou distribuídos, proporcionando uma combinação de funções de detecção, de controle, de computação e de rede. Todos esses com tendência a influenciar os resultados no mundo real através de processos físicos (BOYES *et al*., 2018). Um CPS tem total integração

das capacidades computacionais e físicas, o que faz com que os recursos físicos sejam capazes de computar, comunicar e controlar informação no mundo virtual (TAO e ZHANG, 2017).

Os CPS são componentes de tecnologia de informação com autonomia e inteligência, com o intuito principal de monitorar os processos físicos, tomar decisões descentralizadas, desencadear ações de comunicação e cooperação entre e com os seres humanos em tempo real. Isso facilita melhorias fundamentais para os processos industriais envolvidos na fabricação, na engenharia, na cadeia de fornecimento, no consumo de materiais e no gerenciamento do ciclo de vida dos produtos (GUBBI *et al*., 2013; REINHART *et al*., 2013; TORO *et al*., 2015; NAGY *et al*., 2018).

Funcionais, interconectados e atuando através de sistemas com fio ou sem fio, os CPS conseguem conversar com outros agentes do processo em uma linguagem própria, assim, os sistemas ciber-físicos usam uma conexão interativa homem-máquina para cooperar através da rede de internet e comunicar-se entre as suas três entidades componentes de forma tecnológica e adaptativa. A disposição de um CPS completo é indicada na Figura 2, bem como seus principais módulos, componentes humanos, componentes físicos e componentes computacionais (CHAO *et al*., 2011; PIRVU *et al*., 2016; KHALID *et al*., 2018).

Figura 2 - Ligações e principais componentes estruturais de um CPS



Fonte: adaptado de Khalid e outros (2018)

Confirmando a validade da estrutura apresentada, Gobbo e outros (2018) e Gunes e outros (2014) afirmam que, tecnicamente, os CPS consistem em quatro elementos principais: elementos cibernéticos (computadores e softwares), que permitem que os dispositivos físicos possam se tornar objetos inteligentes, elementos de redes computacionais, que permitem aos objetos inteligentes se comunicarem uns com os outros e com o meio ambiente, elementos de sensoriamento e atuação incorporados em objetos inteligentes e, não menos importante, o meio ambiente do sistema como um todo, que captura as informações das transmissões e repassa para os demais componentes.

Os CPS são responsáveis pela fusão entre o mundo físico e o conhecimento abstrato (gestão, otimização, controle e processamento de dados). Nesse sentido, sistemas reais e virtuais são conectados por meio de dados, que são então transformados em informações e, eventualmente, são capazes de tomar decisões de gerenciamento e suporte (JIANG e YIN, 2018; STORTI *et al*., 2018). Eles compreendem as máquinas inteligentes e sistemas de armazenamento e instalação de produção, que são capazes de trocar informações de forma autônoma, desencadeando ações de controle de uns para outros de forma independente (CARUSO, 2017).

Em um processo industrial os CPS podem desempenhar o papel dos sistemas de automação, controle, diagnóstico, manutenção e assistência de forma rentável, assim, a interação com máquinas, aparelhos e atuadores no âmbito da Indústria 4.0, fabricação inteligente, redes inteligentes, cirurgia robótica, fabricação de automóveis autônomos, são todos bons exemplos de um ambiente industrial com uso de sistemas ciber-físicos capazes e em perfeitas condições de gerar resultados significativos (AAZAM *et al*., 2018).

Como discutido constantemente no decorrer do texto, é possível identificar inúmeras vulnerabilidades e ameaças advindas das tecnologias digitais da indústria 4.0, e, para alcançar os níveis desejados de segurança para essas tecnologias é necessário obter a característica de resiliência para os sistemas industriais. A resiliência pode ser assumida como sinônimo de confiabilidade, capacidade de sobrevivência ou capacidade de lidar com as ameaças. As propriedades básicas para se alcançar a resiliência são: a tolerância a falha (manter as condições normais ao tolerar a ocorrência de quaisquer falha), a sobrevivência (preservar os bens essenciais do sistema, apesar de catástrofes em larga escala), a segurança (preservar o comportamento correto mesmo em casos de ameaças e ataques maliciosos), e a escalabilidade (garantir a capacidade de bom desempenho, apesar de cargas de trabalho excessivas) (CINQUE *et al*., 2018).

Para apoiar a segurança, proteção e privacidade na indústria 4.0 em um ambiente industrial e alcançar a resiliência é necessário estudar novos mecanismos que garantam a fiabilidade dos sistemas. Esses mecanismos devem assegurar que as instalações de produção não ameacem as pessoas e o ambiente e que o uso indevido dos produtos, dos meios de produção e dos acessos não autorizado às instalações de produção sejam prevenidas (PILLONI, 2018).

No estudo apresentado por Tuptuk e Hailes (2018), foi advertido que tem havido tentativas de ataques com grande significância contra algumas das tecnologias facilitadoras da fabricação inteligente, mais notadamente a internet das coisas. Dessa forma, a quebra de segurança na tecnologia base dos sistemas industriais digitais pode causar danos como um todo no sistema. Para evitar danos e minimizar o perigo para as pessoas, os bens e o meio ambiente, ocorreram crescentes reconhecimentos da indústria de que a segurança e a proteção estão relacionadas e que a implantação da tecnologia em seus setores traz consigo oportunidades para os ganhos industriais, no entanto, conduz riscos que podem ser constatados por todas as áreas organizacionais (BOYES *et al*., 2018).

A avaliação e a gestão de riscos como campo científico pode ser considerada jovem, não mais de 50 anos de idade. Nesse período que são identificadas as primeiras revistas científicas, comunicações e conferências cobrindo ideias e princípios fundamentais em como avaliar e gerenciar os riscos de forma adequada. Em grande medida, essas ideias e princípios ainda formam a base para o campo ainda hoje, são métodos e ferramentas para a prática da avaliação e gestão de riscos que temos visto desde os anos 70 e 80. No entanto, o campo desenvolveu-se consideravelmente nos últimos 20 anos, novos e mais sofisticados métodos e técnicas de análise têm sido desenvolvidas, e as abordagens e métodos analíticos de risco agora são usados na maioria dos setores econômicos (AVEN, 2017).

Considerando esses aspectos, torna-se necessário a identificação de quais as principais ameaças emergentes para a indústria 4.0 e a discussão de quais as técnicas desenvolvidas nos últimos tempos para análise e gerenciamento de riscos e como estas podem solucionar os problemas de segurança digital.

2.3. Gerenciamento de riscos

As ferramentas de gestão de risco tidas como tradicionais são comumente baseadas em cadeias causais, análise de eventos, relatórios de falhas e avaliações de risco probabilísticas baseadas em dados históricos, estas abordagens tem fortes limitações na análise de sistemas

complexos, comuns no atual cenário mundial, com isso, dificilmente os sistemas podem ser tratados considerando componentes com interações lineares. A utilização de métodos como árvores de falhas, árvores de eventos e principalmente métodos com perspectivas de dados históricos geram problemas de falta de adequação do contexto. Estes problemas são abordados com a engenharia de resiliência, embora a resiliência seja um termo genérico que é mais utilizado no domínio da segurança, ela defende modelos e métodos mais adequados para sistemas complexos. Dessa forma, métodos alternativos têm sido desenvolvidos para lidar com ameaças contemporâneas (LEVESON, 2012; AVEN, 2016).

Como conceituada anteriormente, a engenharia de resiliência à primeira vista parece estar em conflito com a gestão de riscos, pois em alguns casos rejeita as avaliações tradicionais, mas tal conflito é desnecessário, a resiliência usa os conceitos de risco e dada a dimensão da aplicação é apenas parte integrante da gestão de risco, tornando-se um domínio mais apropriado na aplicação em sistemas complexos (AVEN, 2016).

Para entender melhor conceitualmente os novos e alternativos métodos para o gerenciamento de riscos, deve-se entender os processos de gestão de riscos tradicionais e mais experientes. Alguns autores, como Hale e Hovden (1998) e Waterson e outros (2015) em suas análises do desenvolvimento histórico do estudo científico da segurança, construíram a evolução da ciência do risco em três idades. A primeira, cobre o período do século XIX até a segunda guerra mundial, envolveu a utilização de medidas exclusivamente técnicas para evitar a ocorrência de explosões e colapsos estruturais (por exemplo, válvulas de segurança e proteções de máquinas). A segunda (era dos fatores humanos) foi caracterizada pela integração de fatores humanos com métodos estabelecidos para análise de risco e segurança, por exemplo, análise de risco probabilístico, desenvolvimento de métodos com análises da confiabilidade humana – HRA (SWAIN e GUTTMAN, 1983), estudo de riscos e operacionalidade (KLETZ, 1983) e modos e análises de falhas e efeitos - FMEA (KIRWAN e AINSWORTH, 1992).

No final do século 20, foram percebidos os desenvolvimentos de métodos com um foco maior na compreensão do papel da cognição na tomada de decisão humana, particularmente em domínios complexos e de alto risco, como usinas nucleares, aviação e comandos e controles militares (HOLLNAGEL e WOODS, 1983; RASMUSSEN, 1986; WOODS e HOLLNAGEL, 1987; WOODS e ROTH 1988). Nesse mesmo período a engenharia de sistemas cognitivos também obteve maior ênfase, com o estudo de decisões naturalistas, exigindo a consideração do contexto sociotécnico mais amplo nas análises de risco e segurança (KLEIN *et al*., 1993; WOODS e ROTH, 1988) incluindo o desenvolvimento de ferramentas de análise cognitiva do

trabalho como o (CWA) (RASMUSSEN, 1986; VICENTE, 1999; READ *et al*., 2014) e análise de tarefa cognitiva (CTA) (KLEIN, CALDERWOOD e MACGREGOR, 1989). Então, no início da década de 1990, e objetivando novas ações contra acidentes como os de Chernobyl (1986), Zeebrugge (1987) e Challenger (1986), novos conceitos e desenvolvimentos da área de riscos são discutidos, caracterizando a terceira idade da segurança, com foco crescente na compreensão das causas subjacentes das falhas dos grandes e complexos sistemas sociotécnicos, afastando-se de um enfoque exclusivo de erros, para obter uma melhor compreensão da gestão da segurança (HALE e HOVDEN, 1998).

O estudo de riscos tornou-se uma tarefa cada vez mais complexa. As organizações, por exemplo, buscam gerenciar adequadamente todos os riscos percebidos, sejam eles relevantes para a produção de bens ou serviços ou para a garantia de qualidade e atendimento do seu produto final aos requisitos legais, regulamentos e resoluções, bem como às expectativas da sociedade. No entanto, apesar das organizações se preocuparem com a identificação e o monitoramento de riscos, a disponibilidade restrita de recursos é um ponto crucial (DE ALMEIDA *et al*., 2015).

Outro problema recorrentemente visto no campo dos riscos industriais é a diversificação dos tipos de riscos, que aumentaram concomitantemente com o desenvolvimento industrial, ao tempo em que o limite de aceitação de risco da população diminuiu. Em resposta a esta preocupação as autoridades competentes e as autoridades industriais desenvolveram metodologias e ferramentas para a prevenção e proteção de riscos, bem como a gestão de crises (TIXIER *et al*., 2002).

Segundo Pinto e outros (2011) os métodos mais difundidos de gerenciamento de riscos são tipicamente baseados em informações, que estão sujeitas a incertezas, imprecisões ou são apenas incompletas. Muitos autores como: Andersson (1986); Cornell (1996); Pender (2001); Sii e outros (2001); Tixier e outros (2002); Nilsen e Aven (2003) e Leveson (2004) discutiram as limitações dos métodos de gerenciamento de riscos tradicionais e propuseram novos desenvolvimentos para a ciência do risco, mas cabe agora verificar esses métodos quanto a sua aplicação e uso nas tecnologias da indústria 4.0.

De acordo com Pasha e outros (2018) o gerenciamento de riscos pode ser fracionado em etapas, para facilitar sua aplicação. As principais categorias indicadas pelos autores são: identificação dos riscos, análise dos riscos, planejamento do gerenciamento dos riscos, rastreamento de riscos, controle de riscos e monitoramento de riscos. Os autores ainda indicam

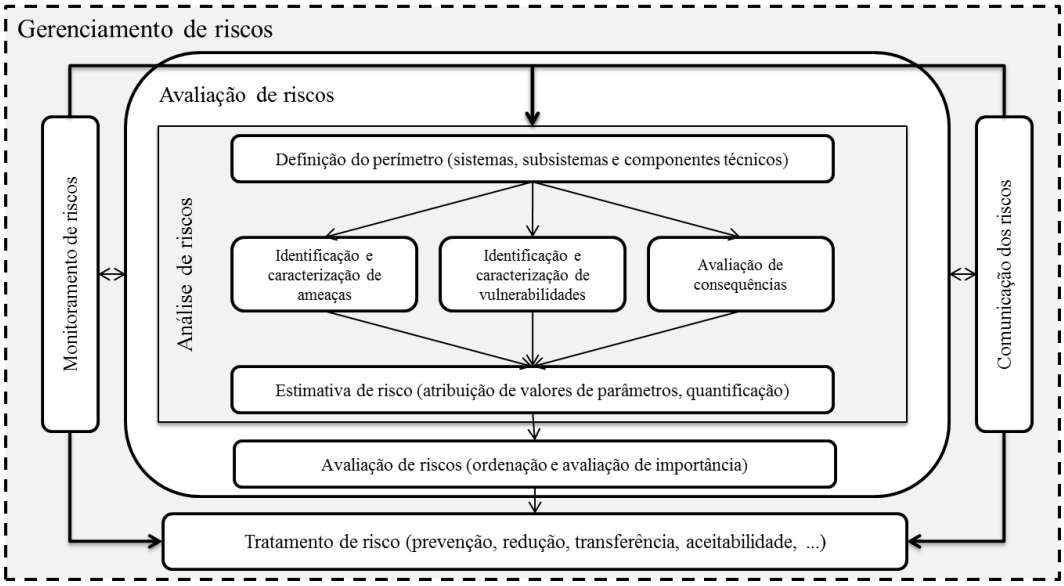
um *framework* para avaliação dos riscos, considerando oito atividades para o gerenciamento de risco bem-sucedido (PASHA *et al*., 2018).

Já o guia PMBOK 6ª edição (2017) considera que o gerenciamento de riscos pode ser tratado como um processo, e nesse processo algumas etapas devem ser seguidas para se alcançar um resultado satisfatório de segurança, são essas: planejamento do gerenciamento dos riscos, identificação dos riscos, análise qualitativa dos riscos, análise quantitativa dos riscos, respostas aos riscos, implementação de respostas aos riscos e o monitoramento dos riscos.

O conceito de riscos é entendido de diversas formas por diferentes áreas de conhecimento. Assim, de acordo com Oliveira e outros (2017) em um estudo sobre riscos logísticos, puderam ser identificadas cinco fases para o gerenciamento de riscos. A identificação dos riscos, a avaliação dos riscos, a gestão dos riscos, o monitoramento e controle dos riscos e a comunicação dos riscos. No estudo, foi possível verificar também que a avaliação de riscos foi o tópico mais discutido, indicando que a maioria dos estudos demonstra formas de classificar e avaliar riscos, mas que grande maioria dos artigos desenvolve conteúdo sem aplicação da teoria discutida, produzindo estudos fundamentados principalmente em dados estimados ou sem a aplicação real de estudos de caso.

Usando as classificações propostas, percebe-se que o escopo do gerenciamento de riscos pode incluir inúmeras atividades. Identificação, análise, avaliação, decisões de tratamento de riscos, tratamento de riscos, prevenção de risco, redução ou mitigação, aceitação do risco além de outras atividades de apoio, como o monitoramento dos riscos e a comunicação dos riscos. Mas a Figura 3 resume de forma gráfica como todas essas atividades podem ser estruturadas para lidar com riscos (PIETRE-CAMBACEDES e BOUISSOU, 2013).

Figura 3 - Estrutura básica de análise e gerenciamento de riscos



Fonte: Adaptado de Pietre-Cambacedes e Bouissou (2013)

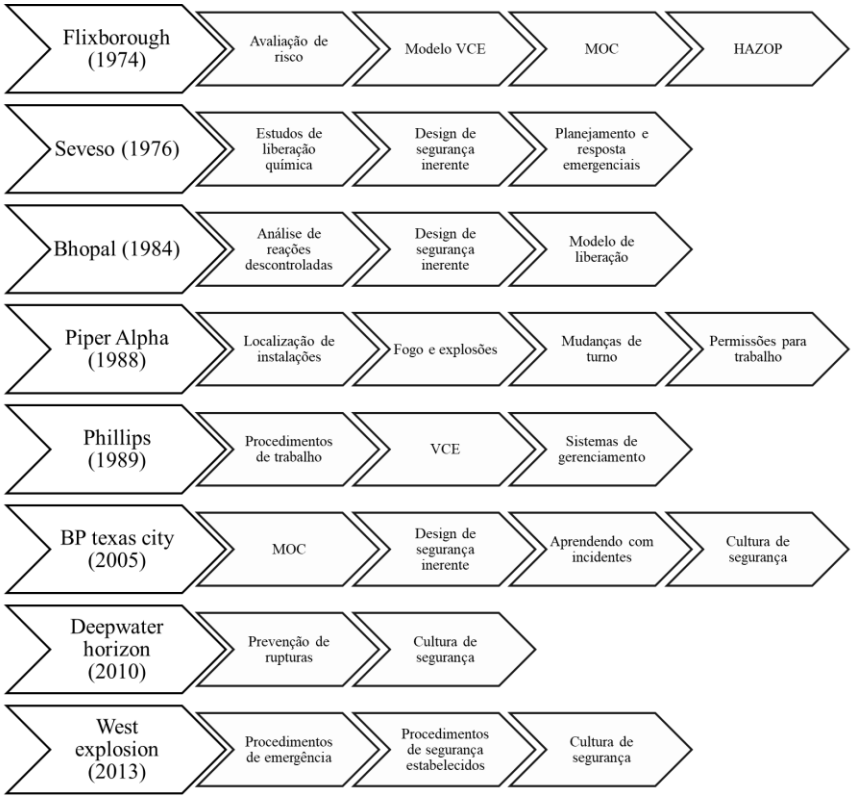
A maturidade organizacional apresenta total relação com as fases do processo de gerenciamento de risco. O nível de maturidade baixo implica em técnicas voltadas apenas para a identificação de riscos. No nível intermediário de maturidade indica que a organização não trabalha apenas a análise de risco, mas também com a resposta, o monitoramento e o controle dos riscos. Por fim, a organização com maior maturidade trabalha o processo completo de gerenciamento de riscos, desde a identificação até o monitoramento e controle, incluindo análises quantitativas de riscos. Além disso, o nível de maturidade mais alta indica que o processo de gerenciamento de riscos tem maior integração com as demais áreas organizacionais, podendo ser considerado uma tendência cultural e organizacional voltada a segurança (CAGLIANO *et al*., 2015).

A cultura de segurança são aquelas características reunidas nas atitudes das organizações e dos indivíduos que estabelecem como prioridade questões de proteção e segurança e tais questões recebem a maior atenção pelo seu significado em si. No entendimento comum, a cultura de segurança compartilha semelhanças significativas com um bom gerenciamento de riscos, onde o maior compromisso é visto na gestão sênior da organização, com uma política de treinamento proativo e com a responsabilização do papel de todos os participantes que desempenham atividades em termos de segurança, todos esses são vistos como componentes essenciais para a aplicação da cultura de segurança (PIETRE-CAMBACEDES e BOUISSOU, 2013).

Mas antes de chegar em um grau de maturidade organizacional alto, voltado para a cultura de segurança, diversos conceitos, ferramentas, tecnologias e metodologias devem ser aplicadas nas diversas áreas organizacionais do negócio, como: planejamento, design, desenvolvimento, integração de sistemas, prototipagem, infraestrutura física, gestão da confiabilidade, controle de qualidade e manutenção (MARHAVILAS *et al*., 2011). Para isso, a experiência com aplicações práticas do gerenciamento de risco é essencial, que no geral não é tarefa trivial. Os gerentes de segurança não podem tomar decisões objetivas apenas vendo os tipos de resultados na comparação de várias abordagens, essas devem ilustrar sua eficácia, prever cenários e indicar recomendações úteis das aplicações das ferramentas e da melhoria na segurança (MONTAGUE, 1990; DUNJO *et al*., 2010). Portanto, apresentar-se-á alguns dos principais influenciadores para o desenvolvimento de ferramentas tradicionais na gestão de riscos e da segurança dos processos.

A segurança do processo é um campo relativamente jovem, que cresceu lentamente desde os últimos 50 anos. E seus picos de atualização são identificados após cada novo desastre que ocorre nas empresas industriais. As principais áreas de desenvolvimento de segurança e risco ligadas a tecnologia industrial são influenciadas por incidentes, alguns desses descritos na Figura 4. Em geral, nos anos 1970 e no início dos anos 80, a maioria das pesquisas acadêmicas e industriais concentrou-se principalmente no aspecto de segurança técnica. No entanto, no final dos anos 80 e início dos anos 90, a importância dos fatores humanos na prevenção de incidentes de segurança de processo ganhou reconhecimento e, nos anos 90 e início dos anos 2000, os sistemas de gerenciamento de segurança começaram a ser incorporados aos regulamentos em todo o mundo. A visão atual em relação à segurança do processo pode ser dividida amplamente em três categorias: propriedades de substâncias, tecnologia de processo e segurança do sistema (MANNAN *et al*., 2016).

Figura 4 - Influência dos incidentes desastrosos e o desenvolvimento das ferramentas de segurança em risco



Fonte: adaptado de Mannan e outros (2016)

Anterior ao surgimento do conceito da indústria 4.0, o conceito de risco estava relacionado a perigos criados por seres humanos e pela natureza, e consequentemente a segurança constituía uma capacidade de reduzir ou eliminar a probabilidade de eventos perigosos ocorrerem. A segurança era relativa a um conceito que era considerado apenas na presença de algum perigo ou risco (GOBBO *et al*., 2018). Uma das principais formas de demonstrar os riscos visualmente era criando uma árvore de ocorrência, demonstrando um problema como a raiz e a fontes desse como as folhas. No entanto, essas abordagens de árvores demonstram fraquezas para análise dos riscos atuais, por não serem adequadas suficientemente para indicar os caminhos mais arriscados para o desenvolvimento dos riscos e consequentemente as contramedidas prioritárias para estes caminhos (KOBARA, 2016).

De acordo com Stringfellow e outros (2010), as técnicas tradicionais de análise de risco, como a árvore de eventos e falhas, foram desenvolvidas para sistemas mais elementares e de interações mais simples. O surgimento dos sistemas complexos é de conceitos mais desafiadores, que geralmente consistiam em múltiplos subsistemas e com interações não lineares, podiam causar resultados imprevisíveis e desastrosos, que as técnicas tradicionais de análise de riscos podiam não serem tão efetivas (SANTOS e ZHAO, 2017).

Dessa forma, para solucionar as limitações das técnicas de análise risco clássicas, surgiram ideais que tratam os riscos para sistemas complexos usando a teoria dos sistemas. Em meados dos anos 1940, desenvolvimentos tecnológicos (cibernética, teoria da informação, teoria de redes, teoria dos jogos, engenharia de sistemas e outros campos) resultaram no surgimento da teoria dos sistemas, estimulando e desenvolvendo uma multiplicidade de abordagens e tendências sobre o pensamento sistêmico (BÖRNER e BOYACK, 2010). Dois autores desenvolveram ideias semelhantes, Norbert Wiener com uma abordagem para o controle e engenharia de comunicações (WIENER, 1965) e Ludwig Von Bertalanffy utilizando princípios do pensamento sistêmico na biologia (BERTALANFFY, 1968).

As técnicas tradicionais de análise de riscos baseiam-se em muitos princípios, abordagens e métodos, mas ciência da análise de risco se estende para além desses princípios, pois estes não devem ser tratados como estáticos. O método científico tradicional de análise de risco, por exemplo, não é aplicável em muitos casos, tais como quando as incertezas são grandes e existem muitas premissas e dados estatísticos. Dessa forma, a avaliação de risco não tem qualquer poder explicativo em situações de previsões precisas, quando estas não podem ser feitas. No entanto, o método científico tradicional de análise de riscos ainda é considerado uma ferramenta extremamente útil em vários casos, em que pode ser justificado o uso de previsões, estatísticas, premissas e situações hipotéticas (AVEN, 2017).

O princípio básico do método científico da teoria de sistemas é dividir sistemas em partes distintas para que essas possam ser examinadas separadamente. Os sistemas são particionados em subsistemas ou até mesmo em parte menores (componentes), enquanto os procedimentos/tarefas dos subsistemas ou dos componentes são decompostos em eventos discretos ao longo do tempo (LEVESON, 2012). Então, utilizando os conceitos da teoria dos sistemas com o objetivo de analisar os riscos organizacionais e limitar os problemas relacionados à grande complexidade organizacional Nancy G. Leveson propôs um modelo de análise de riscos sistêmico, o STAMP (LEVESON, 2012).

O STAMP é apenas um exemplo das diversas técnicas que surgiram para solucionar limitações de abordagens clássicas de análise de risco, metodologias como FRAM, AcciMap, *Swiss Cheese*, HFACS, *Black Swan* e RiskSOAP tem grande influência nos comportamentos de segurança atuais.

2.4. Riscos emergentes na indústria 4.0

As novas formas de trabalho, as mudanças nas relações socioprofissionais, o interesse por novas competências e habilidades profissionais, o aumento do número de postos de trabalho mais complexos e com exigência de maiores qualificações são características do trabalho nos novos sistemas industriais. Mas entende-se que o aperfeiçoamento de competências e habilidades é uma necessidade e consequência lógica da quarta revolução industrial, indiferente do apresentado nas três primeiras. As novas tecnologias e as mudanças organizacionais provocam mudanças significativas nas condições do trabalho, no nível dos empregos e nas competências e habilidades requeridas, entretanto, todas essas são independentes da função exercida pelos trabalhadores e das peculiaridades de seus cargos (EDWARDS e RAMIREZ, 2016).

Na indústria 4.0 as novas interfaces homem-máquina devem ser confiáveis, fornecer informações transparentes sobre os status dos processos e permitir que os colaboradores interajam com as funcionalidades industriais e com o ambiente ao seu redor. Dessa forma, alguns problemas surgem com o grande número de interações entre ferramentas e operadores. A mobilidade dos componentes de tecnologia, a maior interação com os usuários, a elevada gama de componentes tecnológicos de automação, o aumento da complexidade dos sistemas, a necessidade de detecção de posições de componentes e trabalhadores, a melhora da mobilidade dos trabalhadores – que surge como um solucionador de problemas na indústria, mas se apresenta como um complicador para detecção de posições no sistema – todas essas são ameaças ao sucesso dos processos industrias digitais modernos (GORECKY *et al*., 2014).

Todavia, não apenas ameaças internas ao ambiente industrial devem ser avaliadas. Com o uso da tecnologia nos processos industriais novas ameaças foram detectadas e no geral essas podem partir de fontes ilimitadas e por inúmeros canais de comunicação entre o ambiente interno e externo. Tuptuk e Hailes (2018) caracterizaram os ataques às tecnologias digitais da indústria 4.0 mais comuns e os identificaram como: ataques de negação de serviço, ataques de espionagem, ataques *Man-in-the-middle*, ataques de falsa injeção de dados, ataques de tempo de atraso, ataques de adulteração de dados, ataques de repetição, ataques *Spoofing*, ataques de canal lateral, ataques de *covert-canal*, ataques *zero-day*, ataques físicos e até mesmo ataques contra aprendizado de máquina e contra a análise de dados.

Considerando isso, surgiram alguns estudos com o intuito de avaliar como esses tipos de ataques podem interferir nas redes corporativas e industriais, mas todos com características

teóricas, os estudos aplicados sobre as ameaças e ataques de *hackers* ainda são escassos. No presente, as atividades mais marcantes para reduzir a ocorrência de ataques externos são programas de sensibilização e formação técnica para os colaboradores, no entanto, os métodos de engenharia social e ataques de *malwares* ainda continuam a fazer vítimas. A ciência ainda carece de estudos empíricos para observar os fatores humanos que influenciam a gestão de segurança no nível de plantas fabris e industriais e a importância desses estudos tendem a crescer com o aumento das ocorrências (TUPTUK e HAILES, 2018).

Como descrito anteriormente, os ciber-ataques podem vir principalmente de fontes externas, mas sem excluir a possibilidade de fontes internas serem causadoras de danos. Portanto, na literatura, os responsáveis por ataques cibernéticos podem ser descritos de acordo com três classes, os ativos, os passivos e os maliciosos. Os ciber-ataques podem partir de uma fonte externa como canais de comunicação com o exterior, por transmissões sem fio ou por intrusos, sejam esses internos ou externos. O objetivo de um ataque cibernético em um sistema industrial pode ser diverso, destruir ativos físicos, prejudicar ativos cibernéticos ou tomar o controle de componentes industriais. Então, o homem, como agente primordial para a segurança, tem influência em três lugares contra ciber-ataques, no planejamento do sistema (desenvolvendo formas de mitigar as ameaças), na realização do ataque (aplicando ataques aos sistemas por meio de dispositivos ou intenções maliciosas) e como objetivo final do ciber-ataque (visto como alvo principal à ser prejudicado pelo atacante malicioso) (RAYA e HUBAUX, 2007; KHALID *et al*., 2018).

Diferente das ameaças caracterizadas por atacantes externos (ou internos) maliciosos, Varghese e Tandur (2014) e Preuveneers e Ilie-Zudor (2017) são autores que discutem outros desafios que a indústria 4.0 enfrenta, principalmente relacionados a problemas com conexão de internet e comunicação entre dispositivos. As altas latências da rede, a longevidade da bateria, a escala de conectividade, a confiabilidade de comunicação M2M, as altas taxas de dados e as falhas de conectividade são bons exemplos de outros problemas que as tecnologias industriais enfrentam e todos esses de extrema importância para o futuro da I4.0. Em particular, os autores investigam até que ponto o padrão de comunicação pode atender aos requisitos industriais e geralmente concluem que os atuais padrões de internet e comunicação sem fio não serão capazes de atender a todos os requisitos da era 4.0 e que apenas uma combinação de várias tecnologias será capaz de obter resultados eficientes para a rede de conexão industrial.

Outros autores confirmam a ocorrência de alguns tipos de ataques já discutidos, mas de forma diferente da análise por tipo de ataques, classificação essas ameaças por tipo de

responsável pelo ataque. Os ataques por ameaças externas incluem atividades de *hackers*, ataques APT e ataques de *hardware* alvo, enquanto as ameaças internas podem ser geradas intencionalmente por um empregado ou servidor externo com acesso direto aos sistemas fabris digitais (JIANG e YIN, 2018).

Os ataques maliciosos sobre as tecnologias da indústria 4.0 podem derivar de uma variedade de locais e ainda serem dedicados a ferramentas especificas das organizações, como os descritos na Quadro 3.

Quadro 3 - Tipos de ataques aplicados à sistemas da indústria 4.0

Aplicação	**Tipo de ataque**
Sistemas de supervisão de dados	Ataques Modbus TCP Ataques de DoS Acesso e modificação não autorizados Vulnerabilidades de segurança comuns e de exposições (CVE) Detecções críticas de estado (ataques *zero-day*) Negação de serviço, acesso não autorizado, sondagem Ataques Profinet IO DoS e ataques de integridade Ataques de sequência (explorando eventos válidos) Ataques passivos e adulterações Ataques específicos do SCADA, ataques de rede, ataques de desligamento
Sistemas *Wireless* de controle de processo	Ataque contra a rede sem fio
Sistemas de controle embarcados	*Malware* (sequestro de kernel)
Redes de sensores industriais *Wireless*	Atolamento de pacotes, representação, modificação de inundação, escutas
Sistema de transmissão de energia	Repetição de falha, injeção de comando, ataques *zero-day*
Rede inteligente	Negação de serviço, acesso não autorizado, sondagem
Sistema de fluxo de fluido	Desvios do fluxo de pacotes esperado
Automação de subestações elétricas	Ataques de quebra de senha, ataques DoS e ataques do protocolo de resolução de endereços forjados

Fonte: Adaptado de Tuptuk e Hailes (2018)

Alguns outros autores ampliam ainda mais as classificações dos ataques cibernéticos, classificando os incidentes por tipos de ataques, setor alvo do ataque, intenção, impacto e categorias da ocorrência. Essa análise mais robusta foi realizada por Al-mhiqani e outros (2018), em seu estudo os autores indicaram que muitos incidentes em sistemas produtivos surgem de diferentes fontes. Ataques como Stuxnet (2010), onde um *Worm* chamado Stuxnet infectou as instalações nucleares iranianas de Natanz utilizando quatro vulnerabilidades *zero-day*, o ataque objetivou sistemas operacionais do *software* Windows que executavam

programas maliciosos para dar acesso não autorizado. Pode ser citado também o ataque as instalações da Saudi Aramco, um vírus originário de fonte externa infectou cerca de 30.000 estações de trabalho. No estudo foi considerado ainda o ciber-ataque que sofreu o aeroporto de Istambul, especificamente o sistema de controle de passaporte na área de embarque internacional, desligando o sistema de controle de passaportes e causando o adiamento e atrasos de diversos voos e fazendo diversos passageiros esperar horas em conexões e aeroportos. De forma resumida, pode ser visto na Quadro 4 os diversos ataques identificados pelos autores e suas principais características.

Quadro 4 - Incidentes de ciber-ataques a empresas e outras organizações

Ano	País	Título	Tipo de Ataque	Setor alvo
2010	Irã	Stuxnet	*Worm*	Militar – indústria nuclear
2011	Irã	Infraestrutura de comunicação e empresas iranianas	Desconhecido	Governo – empresas de infraestrutura
2011	Irã	Sequestro do US drone no Irã	*Spoofing*	Militar – setor aérea americano
2012	Irã	Terminal de petróleo iraniano '*off-line*'	Vírus	Governo – empresa petrolífera
2012	Arábia	Saudi Aramco	Vírus	Governo – empresa de óleo
2012	Egito	Setor de transportes marítimos	DDoS	Governo – empresas de transporte
2012	Síria	Ministério sírio dos negócios estrangeiros	Desconhecido	Governo – ministério das relações exteriores
2012	Síria	E-mails pessoais do líder da Assad	*Whistleblowing*	Individual
2012	Catar	Ataque a RasGas no Qatar	Vírus	Companhia privada de óleo
2013	Arábia	Rompimento de segurança do sistema do ministério de defesa da Arábia	*Hijacking*	Governo – setor militar
2014	Síria	Ataques de Hackers ao RAT da Síria	Desconhecido	Individual
2015	Turquia	Ataque ao sistema de controle de passaportes de Istambul	Vírus	Governo – aeroporto
2015	Oriente médio	Ataques por Trojan as empresas de energia	Trojan	Governo – empresas de energia
2016	Turquia	Vazamento de dados da polícia turca	*Hijacking*	Governo – dados da polícia
2016	Arábia	Malware Shamoon 2	*Malware*	Governo – empresas industriais
2016	Arábia	Operação Ghoul nos Emidados Árabes Unidos	Ataque direcionado	Empresas industriais e de engenharia
2017	Turquia	Corte generalizado na rede de energia elétrica de Istambul	Desconhecido	Governo – empresas de transmissão de eletricidade
2017	Catar	Ataque Hacker a Agência de notícias do Qatar	*Hijacking*	Governo – website governamental

Fonte: Adaptado de Al-mhiqani e outros (2018)

Entendendo melhor como as ameaças aos sistemas industriais digitais podem surgir, pode-se planejar com maior riqueza de informação os tratamentos adequados para tais vulnerabilidades. Mas antes se faz necessário definir melhor o conceito de risco, ameaça, perigo e vulnerabilidade. O conceito de risco é abordado de forma diferente por vários autores e em todos os campos que está inserido, seja o gerenciamento de finanças, engenharia, segurança, saúde, transporte, proteção ou cadeia de suprimentos (ALTHAUS, 2005). O seu significado é um tema discutido de forma abrangente em todas as áreas (AVEN, 2016). O que em geral causa grande divergência, principalmente por estar ligado a diversas áreas e setores industriais e cada um desses tratá-lo de forma adaptada à suas necessidades. Aven (2016) elencou em seu trabalho algumas definições qualitativas globais de riscos, descritas como:

- A possibilidade de uma ocorrência lamentável;
- O potencial para a realização de consequências indesejadas e negativas de um evento;
- Exposição a uma proposição (por exemplo, a ocorrência de uma perda) ou evento incerto;
- As consequências da atividade e incertezas associadas;
- Incerteza sobre e gravidade das consequências de uma atividade, principalmente quando relacionadas ao valor dos seres humanos;
- Incertezas;
- O desvio do caminho de um valor de referência e as incertezas associadas a este.

Ainda assim, algumas áreas parecem ter encontrado a resposta há muito tempo, por exemplo, a indústria nuclear, que usa uma definição estipulada por Kaplan e Garrick (1981), identificando os riscos como o tripleto - probabilidade, incerteza e consequência, e essa durando mais de três décadas. Outros autores reconhecem a necessidade de novos desenvolvimentos, tais como no domínio da cadeia de fornecimento, como discutido por Heckmann e outros (2015), apontando para a falta de clareza na compreensão do que significa o conceito de risco da cadeia de suprimentos e procurando soluções para tal em suas publicações.

Em finanças, negócios e pesquisa operacional há um trabalho considerável relacionado a métricas de risco. Na área de finanças, a pesquisa sobre riscos abrange trabalhos exemplares, principalmente quando analisados os estudos quantitativos sobre funções e equações para cálculo do risco, como é o caso das funções de perda esperada e perda quadrada esperada, da *Valueat-Risco* (VAR) e Condicional *Valueat-Risco* (CVaR) (AVEN, 2016).

As diferentes perspectivas de análise e gestão de risco causam uma tensão inapropriada para a área, pois o principal objetivo deveria ser o de trazer aspectos de pensamentos integrativo entre a análise de risco tradicional e a análise de risco baseada na resiliência, alcançando uma base forte para a área e proporcionando em um futuro próximo estruturas mais robustas de gestão de risco e incorporação de todos esses elementos benéficos para o desenvolvimento do conhecimento em riscos (AVEN, 2016).

Por isso que o conceito de risco emergente tem ganhado cada vez mais atenção nos últimos anos e é preciso desenvolver avaliações de risco que sejam capazes de capturar esses desafios ligados à dimensão do conhecimento e da dinâmica de tempo. A abordagem probabilística pura, por exemplo, e uma análise Bayesiana não seriam viáveis como modelos para avaliação de tecnologias digitais. Há uma necessidade de equilibrar diferentes estratégias de gestão de risco de forma adaptativa, incluindo estratégias de precaução e atenção aos sinais e advertências, que é bem-vinda e necessária para enfrentar os desafios que o campo de gestão de riscos passa, relacionando problemas sociais, riscos tecnológicos e perigos emergentes complexos (FLAGE e AVEN, 2015; AVEN, 2016).

Assim, a conceituação de risco (em sua forma mais abrangente e generalista) e da resiliência para o estudo se torna desnecessária, avaliando que o conceito é entendível mesmo que não seja descrito para o estudo em questão. Portanto, o uso dos termos risco, ameaças, perigos e vulnerabilidades poderão ser entendidos como um único termo com sentido semelhante.

Os conceitos referentes a indústria 4.0 são geralmente abstratos e gerais, que ainda não ficaram claros o suficiente como aplicá-los diretamente a uma empresa específica (ZHENG *et al*., 2018). Mas isso não justifica que o controle, a análise e o gerenciamento dos riscos nesse campo, ainda em desenvolvimento, devam ser abastecidos por ferramentas inadequadas para a manutenção da segurança de seus processos. Devem possuir técnicas de identificação e análise de perigos atuais, desenvolver ferramentas de análise de risco adequadas, aplicar medidas de controle de risco e promover técnicas de verificação e validação, se utilizando do panorama de desenvolvimento industrial baseado na indústria 4.0, na internet das coisas e nos CPS para o gerenciamento de seus processos seguros (PUISA *et al*., 2018).

As medidas proativas e reativas de segurança são inclinadas fortemente para ações preventivas nos tempos atuais, onde o contexto principal é o de preservar a segurança e detectar intrusões nos ICS de forma rápida e objetiva. No entanto, alguns métodos para tal ainda

precisam ser melhor desenvolvidos, para se tornarem aceitáveis para a segurança digital (SHIN *et al*., 2010; FAIRLEY, 2016; DIEBER *et al*., 2017). Com isso em mente, buscou-se uma metodologia atual, com a aplicação de uma ferramenta que obedece aos requisitos previstos para os sistemas digitais, ser adaptativa e de fácil compreensão e que seja genérica, ao ponto de servir para a aplicação do gerenciamento de riscos sejam esses naturais, ambientais, físicos, químicos, terroristas, ocupacionais, de atividades industriais, financeiros e até mesmo digitais. São essas o método STAMP e a técnica STPA.

2.5. STAMP - STPA

A avaliação e a gestão de riscos devem fornecer importantes contribuições para apoiar o processo de tomada de decisão. Portanto, o conjunto de princípios e métodos desenvolvidos para avaliar e gerenciar riscos, ameaças, perigos e vulnerabilidades devem ser trabalhadas nas operações fabris e usadas da melhor forma possível para influenciar a segurança (AVEN, 2016; GOBBO *et al*., 2018). Com o passar do tempo e das eras industriais as ferramentas de gerenciamento de riscos sofreram inúmeras modificações na sua concepção, fugindo dos métodos tradicionais de identificação de riscos e partindo para métodos que identificassem perigos e falhas não probabilísticas, como é o caso dos métodos sistêmicos de análise de riscos (BOLBOT, *et al*., 2018).

Durante o design de um projeto industrial algumas fragilidades potenciais dos sistemas devem ser analisadas e seus potenciais riscos devem ser identificados. Essa aplicação se estende a sistemas mais complexos, e, por conseguinte, a segurança na concepção inicial tem que se demonstrar muito consistente e indicar processos de analises seguros. Por conta disso surgiram algumas ferramentas com o intuito de melhorar a forma de mitigar ameaças e perigos em sistemas complexos.

2.5.1. STAMP

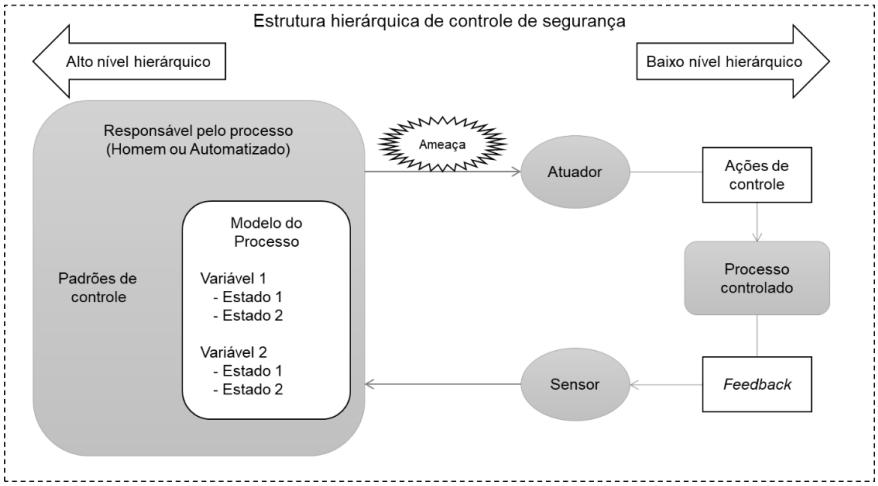
Segundo Leveson e Thomas (2018) o STAMP (*System-Theoretic Accident Model and Processes*) é um modelo de causalidade de acidentes baseado na teoria de sistemas que também pode ser considerado como um conjunto de suposições sobre como os acidentes ocorrem. O modelo STAMP foi idealizado por Nancy G. Leveson em 2004, tendo como hipótese principal que a teoria dos sistemas é uma maneira útil de analisar acidentes, particularmente acidentes em sistemas (LEVESON, 2004).

A grande diferença identificada entre o STAMP e outros modelos de causalidade é que o método vai além de simplesmente culpar a falha de componentes por acidentes, é necessário identificar as razões dessas falhas, incluindo desde fatores sistêmicos que levaram a um acidente até a identificação dos por quês dos controles instituídos não impedirem essas falhas ou simplesmente não minimizarem seu impacto. Além de buscar mais a fundo a identificação da causalidade de falhas o modelo inclui outros tipos de análises, procurando entender em como os acidentes são provocados ou causados pelas interações entre componentes e mais frequentes como a introdução de novas tecnologias e novas funções para os seres humanos no controle do sistema interferem nas ameaças sistêmicas (LEVESON, 2012).

Diferentemente dos métodos tradicionais de análise de riscos, que se concentram na confiabilidade de componentes individuais, o STAMP intensifica sua atenção nas propriedades emergentes de sistemas de manufatura, engenharia e segurança, tornando-se um meio eficaz para analisar de maneira holística sistemas complexos (PLACKE, 2012).

Segundo Barnatt e Jack (2018) o STAMP inicia sua análise com uma visão macroestrutural, partindo de uma análise de processos regulatórios e políticos do governo (quando necessário), e reduz seu escopo de análise, passando pelos processos estratégicos e gerenciais da organização, chegando finalmente aos níveis operacionais. No STAMP, os sistemas não são tratados como processos estáticos, mas dinâmicos e adaptativos, que evoluem continuamente e transformam-se para reagir a mudanças do ambiente em que está inserido (LEVESON, 2012). Essa ação adaptativa do comportamento do STAMP pode ser vista na Figura 5.

Figura 5 - Loop básico de controle do STAMP



Fonte: Adaptado de Meng e outros (2018)

A análise de riscos baseada no método STAMP considera que os eventos danosos tem seu início quando os requisitos de segurança não são atendidos adequadamente. Dessa forma, a falha no processo de segurança do sistema o compromete completamente, causando então controles inseguros e provocando grandes perdas aos componentes dos sistemas. Mortes, prejuízos corporativos, que incluem a reputação da empresa, perda de equipamentos, perda de financiamentos e outros benefícios governamentais e a perda de informações, atualmente o ativo mais valioso do mercado na era digital (LEVESON, 2012). O método STAMP baseia-se em três principais conceitos. As restrições de segurança, as estruturas hierárquicas de controle de segurança e os modelos do processo.

A restrição de segurança é o conceito mais básico do STAMP, ela pode ser entendida como o modo preventivo de um acidente, perigo ou ameaça. São ações de controle que o responsável de nível superior impõe ao processo, dentro de uma estrutura de controle de segurança. Perdas, lesões e danos podem ser eliminados ou mitigados ao impor restrições de segurança (MENG *et al*., 2018).

Em geral, eventos que levam à perigos ou ameaças ocorrem porque as restrições de segurança não foram aplicadas com êxito. Assim, para aplicar restrições, faz-se necessário entender os tipos de controles que podem ser aplicados aos sistemas (controles passivos e ativos). Os controles passivos são aqueles que mantêm a segurança por sua presença, caso um sistema apresente uma falha ou um estado não seguro, um sistema de seguraça simples é usado para limitar as interações entre os componentes do sistema e as ações inseguras (por exemplo: capacetes, cercas e grades de proteção, etc.) Os controles ativos, no geral, exigem algumas ações para fornecer a devida proteção aos atores dos processos, seja a detecção de um evento perigoso (monitoramento), a medição e interpretação de variáveis importantes do processo (diagnóstico) ou a resposta as ameaças e ações inseguras (procedimentos ou ações de recuperação de falhas). Todas essas ações devem ser realizadas antes dos acontecimentos de uma perda ou falha e geralmente são implementadas por um sistema de controle por meio computacional (LEVESON, 2012).

O segundo conceito essencial para se desenvolver no STAMP são as estruturas hierárquicas de controle de segurança, elas são processos de controle que operam entre níveis em uma determinada hierarquia, são regidas pelas restrições de segurança e controlam de um nível hierárquico mais alto o comportamento dos níveis inferiores. Os acidentes normalmente ocorrem quando esses processos de segurança fornecem controles inadequados e as restrições de segurança são violadas em níveis inferiores da estrutura (LEVESON, 2012).

Em uma dada estrutura hierárquica, o controle inadequado pode resultar da falta de restrições, comandos inadequados de controle de segurança, comandos que não foram executados corretamente em um nível inferior, falta de *feedback* de níveis hierárquicos mais baixos, comunicação inexistente ou inadequada e imposições de restrição sem fundamento técnico. Dessa forma, há a necessidade de que as estruturas hierárquicas de controle sempre mudem ao longo do tempo, principalmente aquelas que incluem seres humanos e componentes organizacionais. Os aspectos sociais e humanos da segurança nos modelos de causalidade de acidentes do STAMP devem incluir o conceito de mudança e são necessárias garantias de que a estrutura de controle de segurança permaneça sempre eficaz na imposição de restrições ao longo do tempo e que sejam sempre respeitadas (LEVESON, 2012).

Os modelos do processo são o terceiro conceito do STAMP, são registros que definem valores de controle para o sistema. O responsável pelo processo determina quais tipos de ações de controle de segurança devem ser escolhidas e quando a ação de controle deve ser aplicada para se manter a segurança nos sistemas. Modelos de processos exatos são essenciais em todos os níveis da estrutura hierárquica de controle, para atender aos requisitos de segurança durante a operação do sistema (MENG *et al*., 2018).

De acordo com Leveson (2012) o controle de um modelo de processo é necessário não apenas para que os níveis físicos inferiores da estrutura de controle hierárquico estejam atuantes, mas para que todos os níveis da estrutura o possam ser. Por isso, o uso do modelo de processo não é visto apenas durante as operações dos sistemas, mas também durante todas as atividades de desenvolvimento, desenho e melhorias. Em resumo, estes desempenham um papel importante para a compreensão da ocorrência dos acidentes e dos motivos que levam os seres humanos a fornecem controles inadequados sobre sistemas críticos de segurança, auxiliando assim a criar designs de sistemas mais seguros e completos.

O método STAMP frequentemente é aplicado em conjunto com uma técnica de análise da segurança de sistemas, a STPA. A STPA é especialmente adotada no controle e análise de segurança de sistemas complexos modernos e tem sido aplicada com sucesso em muitos domínios, como: aeroespacial, defesa, energia, química, saúde e sistema de transporte (HU *et al*., 2018). No presente estudo a técnica STPA será incorporada no desenvolvimento de um *framework* com o intuito de auxiliar os decisores fabris nos controles de riscos e ameaças das tecnologias da indústria 4.0.

2.5.2. STPA

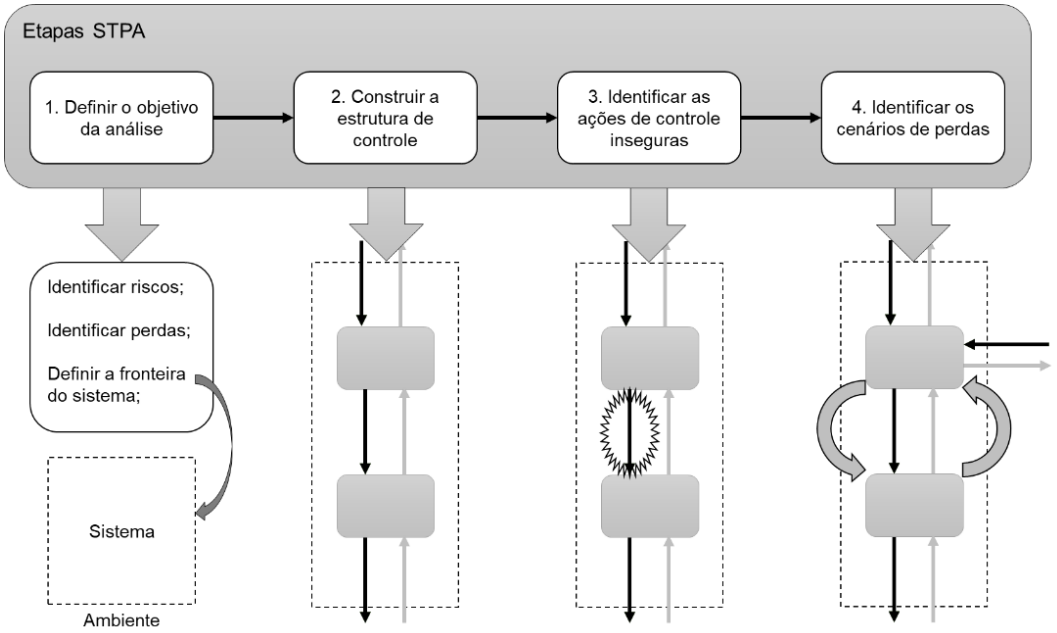
A técnica STPA (*Systems Theoretic Process Analysis*) foi apresentada pelos autores Margaret V. Stringfellow, Nancy G. Leveson e Brandon D. Owens em um artigo publicado em 2010. Esta surgiu para ampliar o modelo de casualidade de acidentes em softwares (STRINGFELLOW *et al*., 2010). A STPA é uma técnica baseada na teoria dos sistemas e foi projetada para tratar interações inseguras entre os componentes operacionais dos sistemas. A aplicação da STPA resulta na identificação de um superconjunto de causas de falhas, que poderiam ser identificadas por outras técnicas, mas grande parte dessas causas adicionais estão relacionadas com novos tipos de tecnologia, como computadores, sistemas digitais, processos avançados de manufatura, robôs e com níveis mais altos de complexidade nos sistemas (LEVESON, 2013).

A análise de árvore de falhas, análise de árvore de eventos, HAZOP e algumas outras técnicas variantes que combinam aspectos dessas três, como análise de causa-consequência e análise *bow-tie*, são amplamente utilizadas para a análise de riscos. Assim como a análise com base na ferramenta FMEA em diversas vezes é utilizada como uma técnica de análise de risco em sistemas tecnológicos, mas em seu cerne, tem aplicabilidade muito limitada para análise de segurança. Por isso, alguns fatores motivaram o desenvolvimento do STPA.

Os novos fatores causais de falhas – erros de projeto, falhas de software, acidentes por falhas na interação de componentes, erros cognitivamente complexos na tomada de decisão humana, fatores sociais que impactam nos sentidos e causam estresse no trabalho e outros aspectos organizacionais e de gestão que contribuem para acidentes – identificados no STAMP, em grande parte dos casos, não são tratados adequadamente pelas técnicas de gerenciamento de riscos mais antigas, mas descobriu-se que com a aplicação da STPA alguns novos riscos poderiam ser identificados e propostas soluções (LEVESON, 2012).

A aplicação da STPA pode ser dividida em 4 etapas. Inicialmente é definido o objetivo da análise, em seguida constrói-se o modelo do sistema, chamado estrutura de controle, posteriormente são identificadas as ações de controle inseguras na estrutura de controle do sistema, e por fim, são identificados os cenários de perdas e motivos causadores de controles inseguros no sistema (LEVESON e THOMAS, 2018). As etapas são exemplificadas em forma de diagrama na Figura 6, onde pode ser verificada sua relação com o método STAMP apresentado anteriormente.

Figura 6 - Etapas básicas da técnica STPA



Fonte: Adaptado de Leveson e Thomas (2018)

O primeiro passo na aplicação do STPA é o de definir os objetivos e a finalidade da análise. A definição dos objetivos pode ser dividida ainda em quatro microetapas, que facilitará a execução de todos os processos como demanda a aplicação da técnica. As quatro etapas para a definição dos objetivos são: identificar riscos, identificar perdas, identificar as restrições em nível de sistema e refinar os perigos identificados nos passos anteriores (LEVESON e THOMAS, 2018).

Como segundo passo para a construção da modelo sistêmico dos processos com base no STPA, tem-se uma tarefa complexa, o desenvolvimento da estrutura de controle hierárquico, no qual requer que todos os subsistemas tenham seu nível de controle adequado e que o modelo completo do sistema seja controlado por circuitos de realimentação (existindo processos e ações de controle e o *feedback* dos acionados). Uma estrutura de controle eficaz impõe restrições sobre o comportamento adequado de todo o sistema. No geral, uma estrutura de controle adequada pode fornecer ações de controle dos processos e impor restrições sobre o comportamento desses. Naturalmente, a maioria dos sistemas têm vários circuitos de controle, que se sobrepõem e que interagem, por conta de tal, as estruturas hierárquicas de controle têm, habitualmente, pelo menos cinco tipos de elementos, os controladores, as ações de controle, os *feedbacks*, as outras entradas e saídas dos componentes e os processos controlados (LEVESON e THOMAS, 2018).

A natureza da aplicação da STPA pode ser entendida quando se chega a terceira etapa do seu processo. A identificação das ações de controle inseguras é idealmente realizada quando são identificadas, evitadas e tomadas ações para eliminar a possibilidade de ocorrência de ameaças e perigos. Decisões de design do sistema podem prevenir ou mitigar as ações inseguras, principalmente quando é possível identificar prontamente alguma das quatro maneiras que uma ação de controle pode se tornar perigosa. Uma dessas maneiras é não fornecer uma ação de controle, a segunda ação potencial de risco é proporcionar uma ação de controle inadequada para alguma das partes interessadas, existe também a possibilidade de fornecer uma ação de controle potencialmente segura, no entanto, esta pode ocorrer muito cedo, muito tarde, ou na ordem errada e, por fim, quando ocorre o atraso ou adiantamento da ação de controle levando a um perigo potencial. As ações de controle inseguro são ocorrência que saem do controle em um contexto particular, mas que no pior dos casos, irá conduzir a um perigo (LEVESON e THOMAS, 2018).

Por fim, temos a identificação dos cenários de perda, ameaças, falhas, perigos ou vulnerabilidades dos sistemas. A premissa básica para a identificação de cenários de perda é que as ações de controle não seguras tenham sido identificadas. Os cenários de perda descrevem de maneira fácil quais fatores causais podem levar a ações de controle inseguras e perigos. Assim, para identificar os cenários de perda dos sistemas devem ser consideradas crenças sobre os estados ou modos atuais, os estados anteriores, as capacidades e limitações do sistema e como esse se comporta em meio dinâmico, ações e comportamentos anteriores, previsões de estados ou comportamentos futuros, atuação de sensores e atuadores ou outros aspectos relevantes do sistema ou meio ambiente (LEVESON e THOMAS, 2018).

Entendendo melhor os conceitos da pesquisa, conceituação e histórico da indústria 4.0, identificação de suas tecnologias digitais facilitadoras, descrição de ameaças e vulnerabilidades encontradas nas tecnologias digitais, descrição dos processos de gerenciamento de riscos e, por fim, a caracterização das técnicas de análise sistêmica de riscos e seus processos de aplicação, agora se deve aplicar a teoria descrita até o momento e construir metodologicamente o *framework* planejado no início do estudo, utilizando a estrutura metodológica da revisão sistemática da literatura, descrita mais profundamente no próximo capítulo.

3. REVISÃO SISTEMÁTICA DA LITERATURA

A metodologia de pesquisa aplicada no estudo foi puramente caracterizada como revisão sistemática da literatura, optou-se por tal metodologia por ser extensamente utilizada nos estudos teóricos de pesquisa bibliográfica e por ser amplamente aceita por diversas revistas, jornais e periódicos científicos.

O capítulo contará com cinco tópicos de discussão, inicialmente serão apresentados os conceitos teóricos da metodologia de revisão sistemática da literatura, assim como apresentadas as atividades que serão executas no estudo. No tópico dois mostrar-se-á a aplicação da fase inicial da revisão sistemática para as duas revisões planejadas no trabalho, as vulnerabilidades e ameaças das ferramentas tecnológicas da indústria 4.0 e o estudo sobre o contexto e a aplicação das ferramentas de análise sistêmica de risco STAMP e STPA.

No terceiro e quarto tópico serão apresentadas a segunda fase do estudo de revisão para ambas as pesquisas, explicitando como foi desenvolvida a fase de análise da revisão da literatura realizada no tópico anterior. Outros dados encontrados nas revisões serão mostrados, e, de acordo com suas análises, possibilitará a proposição do *framework* planejado inicialmente. O tópico cinco buscará discutir como os resultados da pesquisa poderão ser agrupados para se chegar ao objetivo geral do estudo.

3.1. Apresentação da metodologia

De acordo Kitchenham e Charter (2007) a revisão sistemática da literatura é uma forma de estudo secundário da ciência que utiliza uma metodologia bem definida para identificar, analisar e interpretar todas as evidências disponíveis relacionadas com uma questão de pesquisa específica e de forma que possa ser imparcial e na maioria das situações repetível.

Brereton e outros (2007) indica que para se realizar um estudo de revisão sistemática adequado deve-se executar e estabelecer um protocolo confiável para o estudo, ainda durante a fase de planejamento. O protocolo de aplicação de uma revisão visa minimizar o viés do estudo, definindo de antemão como a revisão sistemática deve ser conduzida. O protocolo indica o plano detalhado para a revisão, especificando o processo a ser seguido e todas as condições para seleção dos estudos primários.

Já para Gupta e outros (2018), para que um estudo de revisão bibliográfica seja considerado verdadeiramente sistemático, devem-se especificar ainda no seu início as questões

da pesquisa e aplicar um protocolo explícito e completo. A metodologia de revisão sistemática reduz o viés do autor e permite identificar e discutir melhores as provas, contradições, descobertas e lacunas da literatura.

O processo de revisão sistemático quando aplicado fielmente à sua literatura básica deve conter três etapas. A etapa de planejamento da revisão, a etapa de aplicação da revisão, onde é realizada a aplicação do protocolo da revisão e por fim a etapa de análise e reporte da revisão. Cada uma dessas etapas foi dividida em atividades menores para simplificar o processo. A etapa de planejamento engloba as atividades de identificação dos objetivos da revisão, especificação as questões da pesquisa e desenvolvimento do protocolo de revisão. A etapa de aplicação da pesquisa poderá ser fragmentada em atividades de identificação e seleção da pesquisa primária, avaliando a qualidade do estudo e extraindo, selecionando e sintetizando os dados, para se obter ao fim dessa fase os estudos melhores qualificados para análise e avaliação. A fase final da aplicação de pesquisa de revisão sistemática é composta por atividades de análise de dados, formatação e síntese da análise e discussão e divulgação dos dados descobertos (KITCHENHAM e CHARTER, 2007).

Na aplicação da revisão sistemática da literatura do estudo duas pesquisas foram realizadas em paralelo, uma delas refere-se à análise das aplicações da metodologia STAMP e da técnica STPA nas diversas áreas de estudo científico. A segunda aplicação foi realizada para identificar os principais riscos, ameaças, perigos e vulnerabilidades das tecnologias digitais da indústria 4.0.

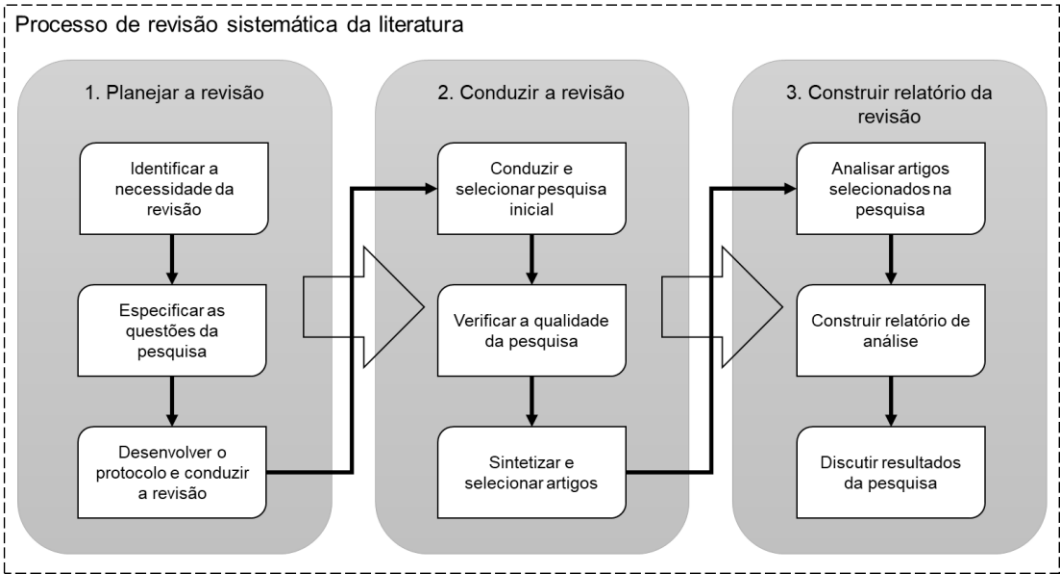
A aplicação da pesquisa seguiu os critérios metódicos definidos pela metodologia científica de revisão sistemática da literatura. Construíram-se dois estudos de revisão de forma semelhantes, mas buscando objetivos, parâmetros e análises distintas. No estudo de revisão sobre as ameaças, riscos, perigos e vulnerabilidades das tecnologias da indústria 4.0, objetivou-se como propósito primordial analisar as ameaças que as tecnologias digitais incorporaram aos processos industriais, não foi visto como objetivo desse primeiro estudo analisar quais os principais autores do tema, quais os estudos mais relevantes, qual a quantidade de citações e co-citações ou demais informações quantitativas sobre os trabalhos escolhidos, mas sim, identificar quais os perigos estudados e analisados pelos autores sobre as tecnologias digitais da indústria 4.0 nos últimos dez anos, com o intuito de avaliar ameaças comuns e potenciais e desenvolver ações para sanar as problemáticas identificadas.

O segundo estudo bibliográfico teve como objetivo principal avaliar a aplicação do método STAMP e da técnica STPA na última década e verificar a aplicação dessas ferramentas em determinadas áreas de estudo de forma mais quantitativa, analisando os principais autores por campo de estudo, as principais citações sobre o assunto e quais as derivações dos estudos, com a análise de co-citações e outras. A análise neste segundo estudo foi realizada de forma mais abrangente e com isso pode-se entender toda a complexidade das aplicações dessas ferramentas nos últimos anos. Haja vista que os conceitos metodológicos de revisão sistemática foram discutidos e os principais objetivos em relação as revisões a serem aplicadas foram explanados cabe-se explicitar as tarefas de aplicação da pesquisa.

3.2. Metodologia de revisão sistemática da literatura aplicada no estudo

O processo visualizado na Figura 7 descreve a revisão sistemática da literatura aplicada nas duas revisões realizadas no trabalho. Esse processo foi desenvolvido com três macroetapas e está de acordo com o procedimento padrão de revisão sistemática da literatura. Para melhor exemplificar as macroetapas do processo, este foi fragmentado em nove atividades que serão realizadas de forma sequencial para alcançar ao fim, o resultado planejado.

Figura 7 – Processo de revisão sistemática da literatura



Fonte: Neto e Alencar (2019)

Inicialmente, em ambos os estudos foram planejados e definidos seus objetivos. A revisão sobre ameaças das tecnologias da indústria 4.0 teve como objetivo principal conhecer quais as principais ameaças, riscos, perigos e vulnerabilidades encontradas no processo de

digitalização industrial, considerando que as ameaças analisadas são advindas das tecnologias digitais facilitadoras da nova revolução industrial corrente, a indústria 4.0.

Para a revisão aplicada às ferramentas de análise sistêmica de riscos STAMP e STPA, o objetivo do estudo foi analisar as aplicações do método STAMP e da técnica sistêmica de análise de risco STPA, reunindo os estudos dos últimos 10 anos sobre o tema e identificando a possibilidade de aplicação desses para a mitigação dos riscos nas tecnologias da indústria 4.0. Em ambas as situações descritas anteriormente, foi aplicado o protocolo de revisão sistemática da literatura descrito na Figura 7, assim como nos dois casos o processo de revisão executado foi semelhante, achar-se-á descrito no decorrer dos próximos parágrafos.

A segunda atividade da etapa de planejamento da revisão indica que devem ser especificados questionamentos sobre os resultados planejados com o estudo. Os questionamentos idealizados que a pesquisa sobre ameaças das tecnologias da indústria 4.0 deve responder estão descritos no Quadro 5. Esses, quando respondidos, serão suficientes para alcançar o objetivo primordialmente definido, possibilitando um maior conhecimento sobre as ameaças presentes nas tecnologias digitais da indústria 4.0 e complementando esse conhecimento com possíveis formas de promover a segurança e mitigar tais ameaças.

Quadro 5 - Questionamentos pesquisa 1 – ameaças das tecnologias digitais

P1Q1: Quais as principais tecnologias facilitadoras da indústria 4.0?
P1Q2: Quais as principais ameaças, riscos, perigos e vulnerabilidades apresentadas pelas tecnologias facilitadoras da indústria 4.0?
P1Q3: Qual a relação numérica entre ameaças e tecnologias facilitadoras da indústria 4.0?
P1Q4: Quais as principais formas de mitigar as ameaças encontradas no estudo?

Fonte: Esta pesquisa (2019)

A execução da segunda atividade da etapa de planejamento da revisão foi executada de forma semelhante para a pesquisa sobre as ferramentas STAMP e STPA. Foram definidos questionamentos que irão auxiliar no alcance do objetivo desse estudo ao fim do trabalho, questionamentos estes que foram desenvolvidos com um olhar mais quantitativo sobre os dados, pois devem demonstrar quais áreas de aplicação as ferramentas são mais utilizadas e devem proporcionar melhor entendimento sobre as ferramentas. Os questionamentos que deverão ser respondidos ao fim do estudo estão descritos no Quadro 6 e assim possibilitará o alcance do objetivo geral do trabalho.

Quadro 6 - Questionamentos pesquisa 2 - modelo STAMP e técnica STPA

P2Q1 – Como as ferramentas de análise sistêmica de riscos STAMP e STPA evoluíram nos últimos 10 anos, em termos do número de artigos publicados e número de citações?
P2Q2 – Quais as áreas de pesquisa e aplicações de campo fizeram uso das ferramentas de análise sistêmica de riscos nos últimos 10 anos?
P2Q3 – Quais os principais autores da área e qual a evolução de suas pesquisas na última década?
P2Q4 – Quais os autores mais citados nas publicações?
P2Q5 – Quais países se destacaram nas pesquisas de métodos e técnicas de análise sistêmica de riscos nos últimos 10 anos?
P2Q6 – Que outras técnicas são combinadas com o método STAMP?
P2Q7 – Qual a tendência das pesquisas do método STAMP e a técnica STPA?

Fonte: Neto e Alencar (2019)

Concluídas as atividades de criação de objetivos para os estudos e desenvolvimento de questionamentos que servirão de guias para a execução da pesquisa, faz necessário construir um grupo de palavras-chave que atendam as premissas do estudo, no Quadro 7 está descrito as palavras-chave utilizadas na aplicação do estudo sobre ameaças às tecnologias da indústria 4.0, foram utilizados também alguns operadores combinatórios de palavras que auxiliam na qualidade e quantidade de artigos incorporados à pesquisa.

Quadro 7 – Palavras-chave e combinação de termos para pesquisa sobre riscos às tecnologias da indústria 4.0

Grupo	**Palavras-chave e operadores**
Termos do primeiro grupo	*"INDUSTRY 4.0"*
	and
Termos do segundo grupo	*"ARTIFICIAL INTELLIGENCE" OR "INTERNET OF THINGS" OR "CLOUD COMPUTING" OR "CYBER-PHYSICAL SYSTEM" OR "ROBOT*" OR "ADDITIVE MANUFACT*" OR "BIG DATA"*
	and
Termos do terceiro grupo	*"RISK" OR "SAFETY" OR "SECURITY" OR "HAZARD" OR "THREAT*" OR "LOSS*" OR "FAILUR*" OR "DANGER" OR "VULNERABILIT*" OR "RELIABILITY" OR "UNCERTAINTY" OR "MAINTENA*" OR "DEFAULT" OR "DAMAGE" OR "CONSEQUENCE" OR "EFFECT"*

Fonte: Esta pesquisa (2019)

De forma semelhante, a organização do grupo de palavras-chave do estudo da metodologia STAMP e técnica STPA contou com algumas características específicas. No grupo foram incorporadas palavras representativas sobre o tema, foi composto por um número pequeno, mas adequado de palavras e contêm palavras com expressividade significante para o estudo.

As palavras-chave escolhidas para a pesquisa foram idealizadas segundo o conhecimento prévio do autor sobre o tema e de acordo com o *benchmark* realizado em outros estudos semelhantes, assim, o grupo de termos foi dividido em dois. O primeiro grupo de palavras é formado pelos termos principais da área em estudo. O segundo grupo definido é formado por palavras adequadas às características necessárias para a pesquisa. Vale ressaltar que a combinação entre os termos dos grupos foi feita com o operador de pesquisa "*or*". Já a combinação entre os grupos foi realizada pelo operador de pesquisa "*and*", seguindo a mesma linha de execução da pesquisa sobre ameaças à indústria 4.0. Para exemplificar, está descrito no Quadro 8 o agrupamento de palavras que foi usado na pesquisa sobre ferramentas sistêmicas de análise de riscos.

Quadro 8 – Grupos de palavras-chave e combinação de termos da pesquisa sobre STAMP e STPA

Grupo	**Palavras-chave e operadores**
Termos do primeiro grupo	"STPA" *or* "STAMP"
	and
Termos do segundo grupo	*"SYSTEM" or "THEORETIC*" or "ANALYSIS*" or "PROCESS*" or "ACCIDENT MODEL*" or "HAZARD" or "RISK" or "SAFETY" or "SECURITY"*

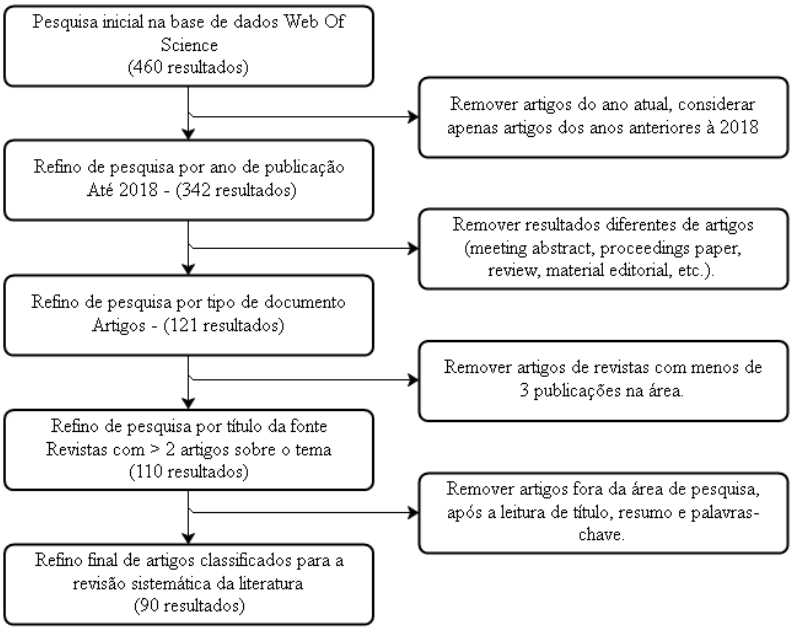
Fonte: Neto e Alencar (2019)

Para encerrar as atividades de planejamento da revisão, e concluir o planejamento do protocolo do estudo escolheu-se a base de dados da plataforma *Web of Science*, uma base de dados com serviço de indexação de citações científicas *on-line*, mantida pela Thomson Reuters e reconhecida mundialmente pela excelente qualidade de publicações e pelo seu grande acervo, atendendo as necessidades do estudo.

A etapa de condução da pesquisa foi iniciada aplicando-se as palavras-chave idealizadas no planejamento na plataforma *Web of Science.* A pesquisa sobre vulnerabilidades da indústria 4.0 foi aplicada no dia 02 de agosto de 2019, sendo realizada como uma pesquisa básica por

tópico e obteve o resultado inicial de 460 (quatrocentos e sessenta) artigos. Após o resultado inicial alguns filtros foram aplicados idealizando garantir a consistência adequada dos artigos analisados para o estudo, esses filtros aplicados podem ser melhor entendidos com a descrição do Fluxograma 2. Os filtros foram aplicados respeitando o rigor metodológico necessário para estudos científicos e tiveram o intuito principal de aprimorar os resultados das análises.

Fluxograma 2 - Etapas do processo de refino da pesquisa indústria 4.0

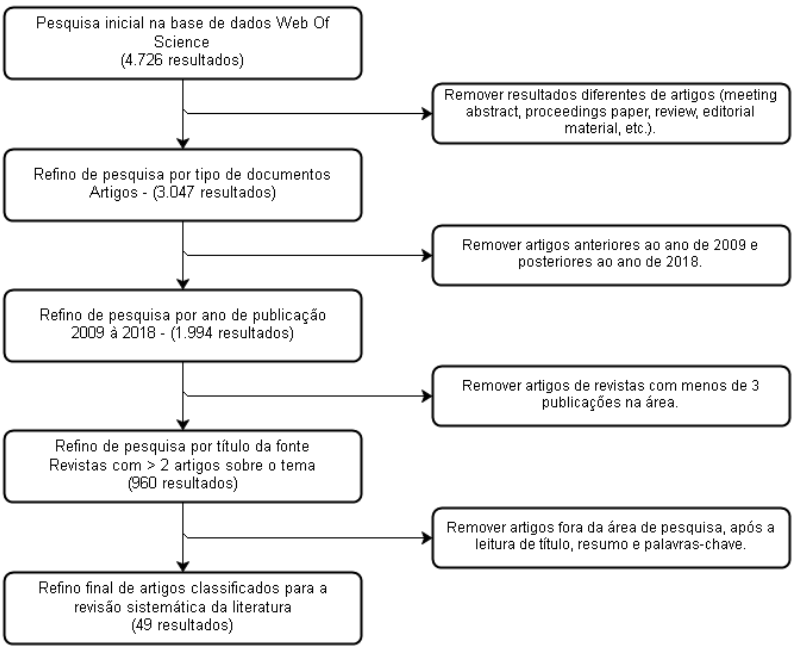


Fonte: Esta pesquisa (2019)

Inicialmente, foram removidos do estudo os artigos que não foram publicados entre os anos de 2009 e 2018, com o intuito de melhorar a reprodutibilidade do trabalho. Na segunda etapa de refino foram removidos do estudo documentos diferentes de artigos, por não conter o rigor científico apropriado de revisão por pares e segurança nas informações descritas. Foram removidos na terceira etapa de filtragem os artigos de revistas com menor expressividade na área, entendendo-se que estas devem conter mais de três publicações sobre o tema proposto, para garantir o aprimoramento de suas informações compartilhadas. Por fim, foi realizada a leitura dos títulos, resumos e palavras-chave dos 110 títulos que restaram nessa penúltima etapa de refino, finalizando todas as etapas de filtro, com o intuito de garantir a qualidade do estudo, os 90 artigos considerados para a revisão final foram lidos por completo e sua adequação aos objetivos primordiais foi verificada em parte desses (47 artigos).

A aplicação da pesquisa sobre as ferramentas de análise sistêmica de riscos STAMP e STPA foi realizada de forma semelhante, ocorreu a execução de filtros e a seleção prévia dos artigos que foram utilizados no estudo, refinando-os a partir dos títulos e resumos das publicações. A pesquisa foi executada como uma pesquisa básica por tópico e contou com a seleção inicial de 4.726 (quatro mil setecentos e vinte e seis) resultados. Identificada a quantidade inicial dos documentos, aplicou-se os filtros necessários e sintetizou-se o número de artigos para melhorar a qualidade do estudo. A aplicação dos filtros e o número de publicações selecionadas podem ser vistos no Fluxograma 3, seguindo a ordem de filtros por tipo de documento, ano da publicação, número de publicações do periódico na área e finalmente leitura de título e resumo dos estudos.

Fluxograma 3 - Etapas do processo de refino da pesquisa STAMP - STPA



Fonte: Neto e Alencar (2019)

Concluída a fase de pesquisa e seleção de artigos inicia-se a etapa de leitura e análise, com os 49 títulos que restaram ao fim da aplicação dos filtros. Os trabalhos selecionados foram analisados considerando as informações importantes para a revisão sistemática da literatura, classificando-os com propósito de alcançar os objetivos definidos anteriormente.

Com o fim da leitura completa dos textos em ambas as pesquisas, 47 artigos foram considerados relevantes para os objetivos da revisão sistemática da literatura sobre ameaças as tecnologias da indústria 4.0 e 49 trabalhos foram considerados úteis para os objetivos definidos

no estudo da metodologia STAMP e STPA. Assim, conclui-se a fase de condução e revisão sistemática da literatura com 96 textos, que devem ser analisados na terceira fase e de acordo com os questionamentos construídos anteriormente devem sanar as dúvidas sobre os assuntos.

O relatório final da revisão sistemática da literatura para os dois estudos será dividido em dois tópicos, para facilitar o entendimento sobre os textos e melhorar a visualização dos objetivos definidos com os estudos e seus resultados finais.

3.3. Relatório da revisão - Análise dos resultados da pesquisa sobre ameaças às tecnologias da indústria 4.0

Ao fim das etapas descritas anteriormente de pesquisa e refino dos textos, inicia-se a etapa de leitura e análise das publicações. Os textos foram lidos de forma completa e analisados minuciosamente com a intenção de investigar os principais riscos, ameaças, perigos e vulnerabilidades descritas sobre as tecnologias facilitadoras da quarta revolução industrial.

Na aplicação da metodologia de revisão da literatura foi possível identificar alguns pontos ainda incertos quanto aos riscos e perigos da indústria 4.0. Respondendo ao primeiro questionamento da pesquisa um, dentre as tecnologias pesquisadas, cinco delas tiveram mais destaque nos estudos revisados, são estas: sistemas ciber-físicos - CPS, *big data*, internet das coisas - IoT, computação em nuvem e robôs, sejam esses autônomos ou com capacidade de trabalho interativo com humanos.

Outras tecnologias de grande importância para a industrialização digital como a impressão 3D e inteligência artificial – AI, não foram alvos de tantos estudos sobre seus riscos e perigos. Dessa forma, pretende-se focar os estudos nas tecnologias com mais expressividade, buscando construir um *framework* de decisão que auxiliará aos gestores e engenheiros na digitalização de fábricas e indústrias e na preparação de seus projetos de transição industrial, tornando-os mais robustos e atualizados com as possíveis anomalias e barreiras no decorrer do processo de digitalização.

Assim, será definido como possíveis estudos futuros as ameaças e riscos das duas tecnologias com menor expressividade no estudo (*3D Printing* e *Artificial Intelligence*) e considerou efetivamente na análise apenas as cinco tecnologias com maior expressividade na pesquisa, que ao fim foram levadas em consideração para a construção do *framework*.

Algumas ameaças tiveram destaque entre os vários estudos analisados na pesquisa sobre ameaças da indústria 4.0, e receberam inúmeras citações de riscos potenciais para a

industrialização digital. Foi o caso dos ataques cibernéticos realizados por *hackers*, a possível falta de integração entre as diversas linguagens e tecnologias da indústria 4.0 e os riscos internos gerados pelos próprios operadores por medo de perderem seus postos de trabalho com o avanço tecnológico, todos esses descritos no Quadro 9. As ameaças identificadas nos artigos analisados no estudo foram estruturadas em forma de lista numa sequência decrescente de contagem por tipo de ameaça, das mais citadas para as menos citadas, todas relacionadas à perigos presentes na indústria 4.0, o quadro em questão responde também ao segundo questionamento referente a pesquisa um.

Quadro 9 – Riscos, ameaças e vulnerabilidades da indústria 4.0

Principais riscos, ameaças e vulnerabilidades da indústria 4.0	**Quantidade de citações por tipo de ameaça**
Ataques maliciosos	66
Problemas de conexão e instabilidade nas redes de comunicação	22
Falta de integridade e confiabilidade nos dados	20
Vazamentos e divulgação de informações sigilosas	15
Espionagem, sequestro e chantagem cibernética	14
Sabotagens, erros humanos e interrupções no sistema	13
Problemas com latência de conexão	11
Acesso não autorizado a sistemas	10
Complexidade de carga cognitiva das tecnologias	7
Falta de padrão uniforme para interoperabilidade	7
Ineficiência por danos físicos ou ambientais (ataques, poeira, vibração, umidade, etc.)	7
Sobrecarga de sistemas, lentidão e capacidade de memória limitada	6
Riscos de interação homem-máquina para movimentações e execução de processos	5
Incerteza dos resultados e custos elevados de implantação	4
Limitações tecnológicas em escala industriais	3
Falha em equipamentos ou dispositivos de base/servidores	3
Danos a operadores como consequência de ataques cibernéticos	2
Falha em sensores de detecção de movimento na interação homem-máquina	2
Trabalho na condição *offline*	2
Falta de entendimento comum das tecnologias	1
Emissão de gases e materiais poluentes aos seres humanos e ao meio ambiente	1

Fonte: Esta pesquisa 2019

Seguindo o mesmo tom da análise inicial, foi possível identificar também no estudo quais as tecnologias que foram alvos da maior quantidade de estudos na área de riscos, como é o caso da internet das coisas, que foi a tecnologia emergente da indústria 4.0 que teve o maior número de estudos em riscos, ameaças, perigos e vulnerabilidades dentre os artigos analisados

na pesquisa. Foi então possível montar uma tabela que identifica de forma decrescente quais as tecnologias com maior número de citações sobre riscos e perigos emergentes da industrialização digital, que pode ser visto no Quadro 10.

Quadro 10 – Número de ameaças por tecnologia facilitadora da indústria 4.0

Tecnologias 4.0	**Citações de ameaças por tecnologia 4.0**
Internet das coisas (*Internet of Things* - IoT)	113
Sistemas ciber-físicos (*Cyber Phisical System*)	58
Computação em nuvem (*Cloud Computing*)	32
Robôs (*Robot*)	24
Big Data	12
Impressão 3D ou manufatura aditiva (*3D Printing/Aditive Manufacturing*)	7
Inteligência artificial (*Artificial Intelligence* - AI)	5

Fonte: Esta pesquisa 2019

Consequentemente, é possível confrontar os Quadros 9 e 10 e encontrar uma interseção entre os riscos potencias na indústria 4.0 e as suas tecnologias para responder ao terceiro questionamento da pesquisa um. Estas informações estão dispostas no Quadro 11 e podem oferecer grande auxílio para a delimitação do *framework* que será proposto no estudo, auxiliará também na identificação de medidas para a eliminação dessas ameaças em cada uma das tecnologias, buscando melhor adaptação para sua aplicação ainda na fase de digitalização industrial.

Quadro 11 – Relação entre ameaças e tecnologias da indústria 4.0

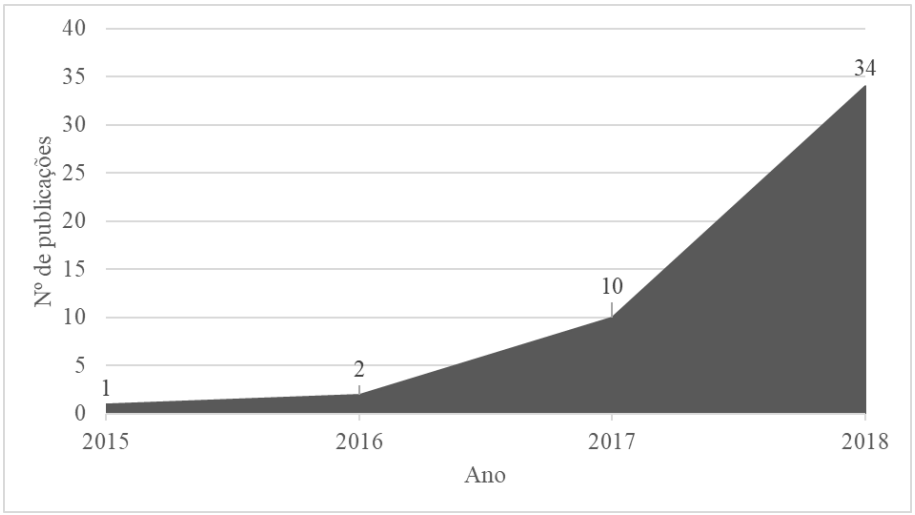
Riscos, perigos, ameaças e vulnerabilidades das tecnologias da indústria 4.0	AI	CN	BD	CPS	IoT	Robôs	3D
Complexidade de carga cognitiva das tecnologias	2	2	2	4	3	4	2
Incerteza dos resultados e custos elevados de implantação	1	1	1	1	3	2	1
Falta de entendimento comum das tecnologias	1	1	1	1	1	1	1
Falta de padrão uniforme para interoperabilidade	1	2	1	1	5	2	1
Ataques maliciosos		3	1	23	37	2	
Problemas de conexão e instabilidade nas redes de comunicação		4	1	4	13		
Ineficiência por danos físicos ou ambientais (ataques, poeira, vibração, umidade, etc.)				1	5	1	
Problemas com latência de conexão		1		1	9		
Sabotagens, erros humanos e interrupções no sistema		2		3	5	3	
Espionagem, sequestro e chantagem cibernética				3	10	1	
Vazamentos e divulgação de informações sigilosas		7		4	4		
Falta de integridade e confiabilidade nos dados		4	3	4	8	1	
Danos a operadores como consequência de ataques cibernéticos					2		
Limitações tecnológicas em escala industriais					2		1
Acesso não autorizado a sistemas				3	6	1	
Riscos de interação homem-máquina para movimentações e execução de processos						5	
Falha em sensores de detecção de movimento na interação homem-máquina				1		1	
Sobrecarga de sistemas, lentidão e capacidade de memória limitada		3	1	2			
Trabalho na condição *offline*		1	1				
Falha em equipamentos ou dispositivos de base/servidores		1		2			
Emissão de gases e materiais poluentes aos seres humanos e ao meio ambiente							1

Fonte: Esta pesquisa 2019

Com tal informação podemos perceber que a internet das coisas é a tecnologia digital mais afetada por três principais ameaças, os ataques maliciosos, que pode ocorrer de diversas fontes e por inúmeros canais, os problemas relacionados à conexão com os sinais de internet e comunicação, que não conseguem suprir as necessidades da grande quantidade de dados e informações transmitidas e a espionagem, sequestro e chantagem cibernética, que está muito relacionada com ataques maliciosos, mas pode ser tida com uma classificação a parte, por conter objetivos diferentes, como não apenas o possível vazamento ou divulgação de informações, mas com o objetivo de alcançar recursos financeiros das vítimas.

A grande maioria dos ataques observados no estudo foram publicadas por estudos mais recentes, partindo desde o ano de 2015, com apenas uma das publicações analisadas, alcançando 34 publicações discutindo sobre o tema segurança e riscos nas tecnologias da indústria 4.0 no ano de 2018. Isso pode ser percebido no Gráfico 1, demonstrando que as tecnologias da indústria 4.0 tem sofrido acréscimo acentuado na quantidade de ataques maliciosos.

Gráfico 1 - Número de publicações sobre ataques hackers nas tecnologias da indústria 4.0 por ano



Fonte: Esta pesquisa (2019)

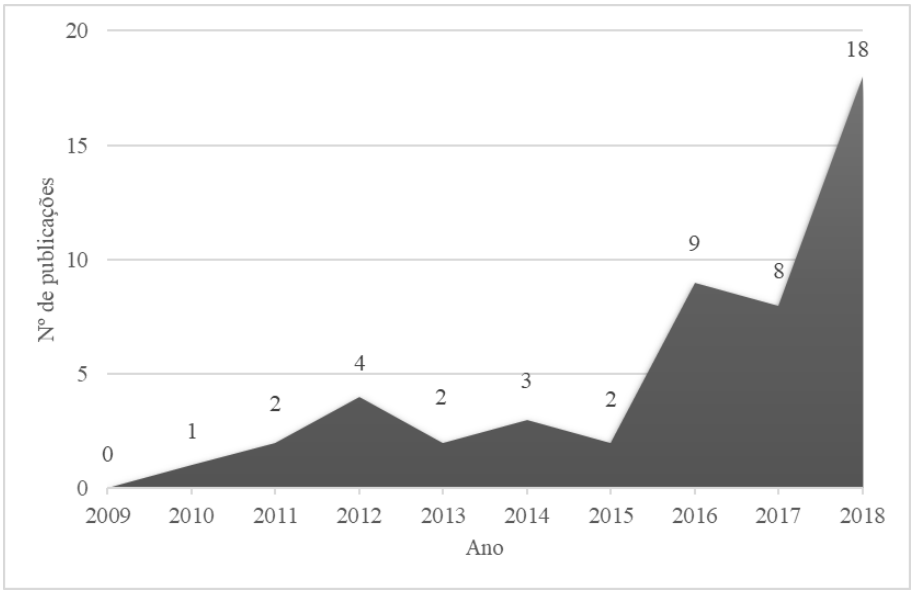
Alcançado quase todos os questionamentos definidos no início da pesquisa, resta agora analisar o resultado da segunda pesquisa realizada, optou-se por responder uma das questões construídas no início do planejamento da revisão ao fim do próximo capítulo, fazendo assim com que haja maior ligação entre a pesquisa realizada e os resultados obtidos com o trabalho.

3.4. Análise dos resultados – metodologia STAMP e técnica STPA

De forma semelhante ao tópico anterior, após concluir a fase de pesquisa e seleção de artigos, inicia-se a etapa de leitura e análise. Os trabalhos selecionados foram analisados considerando as informações importantes para a revisão sistemática da literatura, classificando-os com propósito de alcançar os objetivos definidos anteriormente.

Para análise e classificação dos artigos nessa segunda pesquisa utilizou-se o software RStudio, com aplicação do pacote Bibliometrix para análise das publicações. O software tem funcionalidades desenvolvidas exclusivamente para exploração de informações de estudo bibliométricos quantitativos e qualitativos (ARIA e CUCCURULLO, 2017). Inicialmente, os artigos sobre o método STAMP e a técnica STPA foram analisados em relação a sua evolução histórica de publicações, esses, apresentaram uma evolução significativa nos últimos anos quanto ao número de trabalhos publicados, que pode ser visto no Gráfico 2, respondendo o questionamento inicial da pesquisa dois.

Gráfico 2 – Número de publicações relacionadas aos STAMP e a STPA por ano



Fonte: Neto e Alencar (2019)

No ano de 2018 foram encontradas dezoito publicações científicas na área de análise sistêmica de riscos, considerando a estrutura de revisão sistemática da literatura desenvolvida no estudo. Esse número pode não parecer elevado quando visto isoladamente, mas indica um acréscimo representativo nos trabalhos de análise de riscos sistêmicos. As publicações do ano de 2018 representam 36,7% do número total de artigos classificados para análise no estudo,

além de que, quando comparado aos anos anteriores, cresceu percentualmente 125% em relação ao ano de 2017 e 100% em relação ao ano de 2016. Esse acréscimo percentual no número de publicações é ainda maior quando comparada a relação entre o ano de 2016 e os anos anteriores, que pode chegar a 350% de aumento.

Para justificar o aumento no número de publicações da análise sistêmica de riscos algumas hipóteses podem ser feitas, como: a mudança na natureza dos riscos, dada a maior complexidade dos sistemas produtivos e a nova interface homem-máquina, com uso de sistemas ciber-físicos e interações virtuais entre atores dos processos de manufatura; o desenvolvimento de novas técnicas de análise sistêmica de riscos, observados que muitos trabalhos discutiam comparações de métodos e técnicas de análise e gerenciamento de riscos, além de trabalhos de análise de acidentes ocorridos em décadas passadas com o uso de novas técnicas de análise.

Após a análise numérica da evolução do tema nos últimos anos, faz-se necessário investigar seu emprego quanto à área de pesquisa e ao domínio de aplicação. Todas as publicações analisadas têm sua classificação relacionada à área de estudo sobre segurança, dessa forma, há necessidade de avaliar minuciosamente apenas seu domínio de aplicação.

O setor de aviação tem grande destaque nas publicações com utilização das ferramentas de análise sistêmica de riscos. Dentre os estudos analisados, 20% deles trouxeram análises de riscos e propostas de mitigação destes no setor de aviação, fazendo assim, sugestões para melhoria da segurança nos processos de decolagem e pouso de aeronaves e no transporte aéreo de passageiros.

O setor de transporte no geral mostrou-se em evidência nas publicações em análise. Além do setor de transporte aéreo, os domínios do transporte ferroviário e marítimo foram frequentemente vistos nos estudos, com trabalhos relativos à análise e desenvolvimento de sistemas de segurança para os setores. Ademais, os domínios de aplicação que estiveram mais presente foram: o setor de petróleo e gás, com aplicações na análise de riscos de acidentes no transporte dutoviário; o setor de saúde, com análises de riscos nas práticas de atividades físicas e administração de medicamentos; e o setor de construção civil, com pesquisas relacionadas à avaliação de segurança na estrutura de túneis.

Os demais estudos foram agrupados na classe “outros”. Cerca de 35% dos estudos classificados para a análise da literatura foram reunidos em uma única categoria, com aplicações em diferentes domínios, como no setor aeroespacial, de segurança pública, de energia nuclear,

de tratamento de água, etc. Todos esses podem ser identificados no Quadro 12 e conclui a resposta para o segundo questionamento da pesquisa dois.

Quadro 12 - Domínio de aplicação do estudo de revisão sistemática das ferramentas STAMP e STPA

ÁREA DE ESTUDO	DOMÍNIO DA APLICAÇÃO	AUTORES E ANO DA PUBLICAÇÃO
SEGURANÇA	AVIAÇÃO	SCHMID D.; VOLLRATH M.; STANTON N.A., (2018)
		SCHMID D.; STANTON N.A., (2018)
		LOWER M.; MAGOTT J.; SKORUPSKI J., (2018)
		DAKWAT A.L.; VILLANI E., (2018)
		MOGLES N.; PADGET J.; BOSSE T., (2018)
		CASTILHO D.S.; URBINA L.M.S.; DE ANDRADE D., (2018)
		SPAN M.; MAILLOUX L.O.; MILLS R.F.; YOUNG W., (2018)
		ALLISON C.K.; REVELL K.M.; SEARS R.; STANTON N.A., (2017)
		LU Y.; ZHANG S.G.; TANG P.; GONG L., (2015)
		KONTOGIANNIS T.; MALAKIS S., (2012)
SEGURANÇA	TRANSPORTE FERROVIÁRIO	SALMON P.M.; READ G.J.M.; WALKER G.H.; GOODE N.; GRANT E.; DALLAT C.; CARDEN T.; NAWEED A.; STANTON N.A., (2018)
		BARNATT N.; JACK A., (2018)
		LEE S.; MOH Y.B.; TABIBZADEH M.; MESHKATI N., (2017)
		WANG R.; ZHENG W.; LIANG C.; TANG T., (2016)
		UNDERWOOD P.; WATERSON P., (2014)
		OUYANG M.; HONG L.; YU M.H.; FEI Q., (2010)
SEGURANÇA	TRANSPORTE MARÍTIMO	PUISA R.; LIN L.; BOLBOT V.; VASSALOS D.. (2018)
		BANDA O.A.V.; GOERLANDT F., (2018)
		WROBEL K.; MONTEWKA J.; KUJALA P., (2018)
		ROKSETH B.; UTNE I.B.; VINNEM J.E., (2018)
		KIM T.; NAZIR S.; OVERGARD K.I., (2016)
SEGURANÇA	PETRÓLEO E GÁS	GONG Y.; LI Y., (2018)
		LI W.; ZHANG L.; LIANG W., (2017)
		RODRIGUEZ M.; DIAZ I., (2016)
		ALTABBAKH H.; ALKAZIMI M.A.; MURRAY S.; GRANTHAM K., (2014)
SEGURANÇA	SAÚDE	CANHAM A.; JUN G.T.; WATERSON P.; KHALID S., (2018)
		FAIELLA G.; PARAND A.; FRANKLIN B.D.; CHANA P.; CESARELLI M.; STANTON N.A.; SEVDALIS N., (2018)
		HULME A.; SALMON P.M.; NIELSEN R.O.; READ G.J.M.; FINCH C.F., (2017)
		SALMON P.M.; GOODE N.; TAYLOR N.; LENNE M.G.; DALLAT C.E.; FINCH C.F., (2017)
SEGURANÇA	CONSTRUÇÃO CÍVIL	CHATZIMICHAILIDOU M.M.; DOKAS I.M., (2016)
		KAZARAS K.; KONTOGIANNIS T.; KIRYTOPOULOS K., (2014)
		KAZARAS K.; KIRYTOPOULOS K.; RENTIZELAS A., (2012)
SEGURANÇA	OUTROS (AEROESPACIAL, MINERAÇÃO, PERFURAÇÃO, SEGURANÇA PÚBLICA, SUBSTÂNCIAS QUÍMICAS PERIGOSAS, TRANSPORTE RODOVIÁRIO, TRATAMENTO DE ÁGUA, ENERGIA NUCLEAR)	DUZGUN H.S.; LEVESON N. G., (2018)
		MENG X.; CHEN G.; SHI J.; ZHU G.; ZHU Y., (2018)
		LEVESON N.G., (2017)
		FABIANO B.; VIANELLO C.; REVERBERI A.P.; LUNGHI E.; MASCHIO G., (2017)
		MAHAJAN H.S.; BRADLEY T.; PASRICHA S., (2017)
		AURISICCHIO M.; BRACEWELL R.; HOOEY B.L., (2016)
		BJERGA T.; AVEN T.; ZIO E., (2016)
		UNDERWOOD P.; WATERSON P.; BRAITHWAITE G., (2016)
		SALMON P.M.; READ G.J.M.; STEVENS N.J., (2016)
		YOOD Y.S.; HAM D.H.; YOON W.C., (2016)
		LEVESON N.G., (2015)
		UNDERWOOD P.; WATERSON P., (2013)
		DOKAS I.M.; FEEHAN J.; IMRAN S., (2013)
		SALMON P.M.; CORNELISSEN M.; TROTTER M.J., (2012)
		FERJENCIK M., (2012)
		FERJENCIK M., (2011)
		FERJENCIK M., (2011)

Fonte: Neto e Alencar (2019)

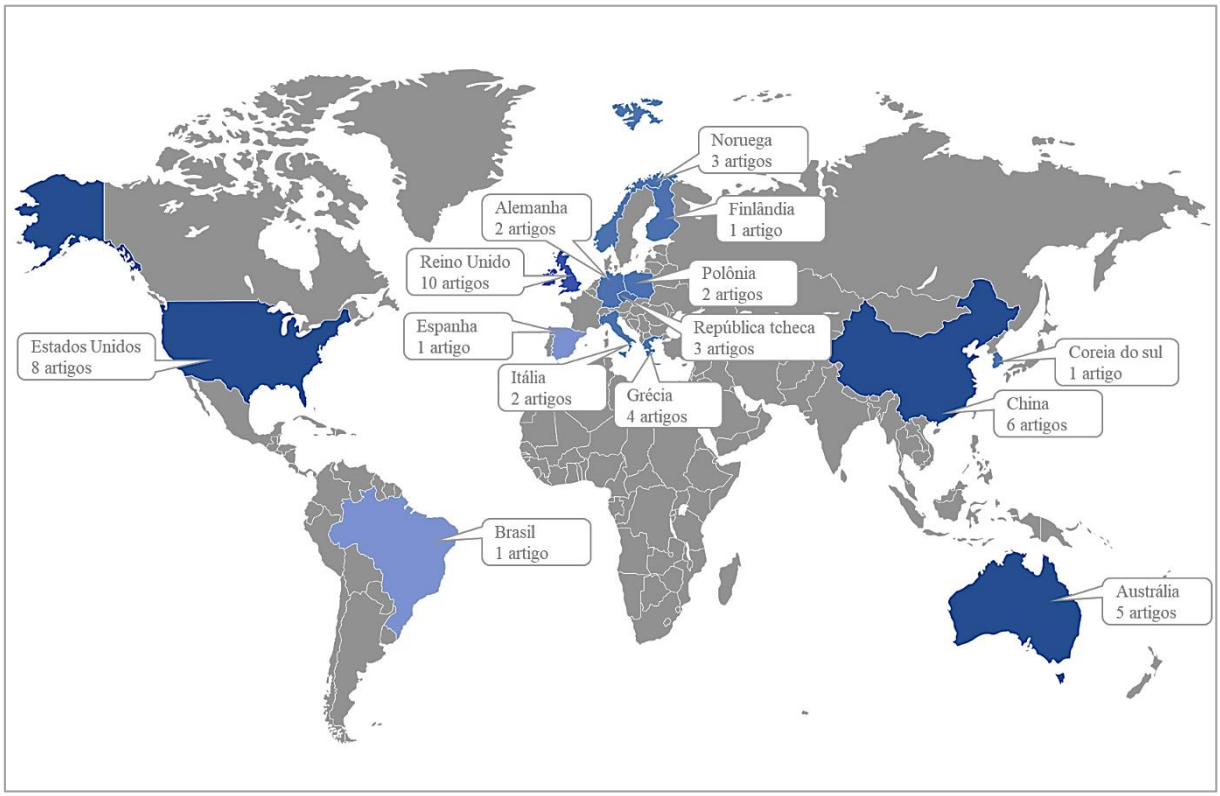
Após a análise do histórico e dos principais domínios de atuação das publicações referentes ao estudo sistemático, faz-se necessário analisar os principais autores e a evolução dos seus estudos com o passar dos anos.

Dos 120 (cento e vinte) autores analisados nos artigos da revisão sistemática sobre o método STAMP e a técnica STPA, seis deles merecem grande destaque, pois são responsáveis por 32% das publicações presentes no estudo. Atenção especial deve ser dada para Paul Salmon e Neville Stanton. O primeiro por conta de seu amplo trabalho de pesquisa sobre as ferramentas de análise sistêmica de riscos que vem desenvolvendo desde o ano 2012, com cinco publicações sobre o tema. O segundo por desenvolver trabalhos mais recentes, mas com grande expressividade, onde apenas no ano de 2018 participou de quatro publicações na área de análise sistêmica de riscos.

O autor Paul Salmon desenvolve trabalhos relacionados com o gerenciamento da segurança no transporte ferroviário, o gerenciamento de riscos na prática de esportes, a segurança pública e a análise de tragédias com uso de métodos de análise sistêmica de riscos. Neville Stanton realiza estudos de identificação de riscos e desenvolvimento de contramedidas para comportamentos inseguros na aviação, além de desenvolver estudos ligados à análise de falha nos processos farmacoterapêuticos e ao gerenciamento de segurança no transporte ferroviário. E, os autores Patrick Waterson, Milos Ferjencik, Gemma Read e Peter Underwood também receberam destaque na análise, pois todos desenvolveram mais de três estudos na última década sobre a análise sistêmica de riscos. Assim conclui-se a análise necessária para responder ao terceiro e quarto questionamento da pesquisa dois.

A realização das pesquisas científicas decorre de lacunas científicas encontradas por pesquisadores, no entanto, esses dependem de diversas variáveis para a execução dos estudos. Uma dessas variáveis pode ser analisada considerando a nacionalidade dos estudos, visto que, há distinção entre os objetivos científicos dos países, das empresas e dos órgãos governamentais, principais patrocinadores das pesquisas científicas em todo o mundo. As publicações em análise no estudo sistemático sobre método STAMP e técnica STPA tiveram origem em 14 países, que estão posicionados no mapa-múndi apresentado na Figura 8.

Figura 8 – Número de publicações por país



Fonte: Neto e Alencar (2019)

Os países responsáveis pelas publicações na área de análise sistêmica de riscos presentes no estudo são: Reino unido (10 publicações), Estados unidos (8 publicações), China (6 publicações), Austrália (5 publicações), Grécia (4 publicações), República tcheca e Noruega (3 publicações), Alemanha, Itália e Polônia (2 publicações) e demais países (Brasil, Espanha, Finlândia e Coreia do sul) com uma publicação cada.

Tal resultado não pode ser estendido para analisar outros temas, que apresentem correlação com o estudo, mas é o suficiente para responder ao questionamento cinco da segunda pesquisa e ainda é possível realizar algumas suposições para identificar a motivação dos estudos em ferramentas de análise sistêmica de riscos nos países citados anteriormente. As hipóteses para justificar o estudo do tema nesses países podem surgir em diversos ramos de exploração, como: o grau de desenvolvimento socioeconômico do país, as leis de segurança do trabalho de cada nação, o grau de desenvolvimento industrial do país, etc.

Em alguns dos estudos analisados, o método STAMP foi aplicado em conjunto com outras técnicas diferentes da STPA. Respondendo ao questionamento seis da segunda pesquisa, os estudos que se destacaram com esse tipo de aplicação são: Salmon e outros (2012) com aplicação da técnica EAST (*Event Analysis of Systemic Teamwork*) em conjunto com o método

STAMP; Duzgun e Leveson (2018) analisando a aplicabilidade do CAST (*Causal Analysis Based on Systems Theory*) em conjunto com o método STAMP; Puisa e outros (2018) aplicando o método STAMP agregado a técnica CAST; Dokas e outros (2013) verificando a aplicação das técnicas STPA e EWASAP unidas ao método STAMP.

Para responder ao sétimo questionamento e concluir a discussão sobre a pesquisa em questão, verifica-se que o método STAMP pode ser usado em diversos campos de estudos e ser adaptado de diversas formas e ainda pode ter seu leque de aplicação ampliado de acordo com as adaptações necessárias para cada natureza de estudo que se constrói, sendo encontrado em diversas utilidades práticas para o gerenciamento da segurança de sistemas, assim é impossível definir com precisão qual o futuro da aplicação do método, mas é possível identificar que sua tendência é evoluir constantemente combinado com outras técnicas de análise, possibilitando a criação de melhores ferramentas para o tratamento de riscos.

3.5. Relação entre pesquisas: a solução para as vulnerabilidades da indústria 4.0

Concluído os estudos de revisão em duas frentes, foi possível então construir a análise final, identificando a interseção das informações obtidas sobre ameaças das tecnologias da indústria 4.0 e a aplicação das ferramentas STAMP e STPA para promover a segurança e mitigar ameaças. A aplicação da técnica STPA e o método STAMP culminaram na identificação das ameaças potenciais das tecnologias digitais consideradas no estudo e indicou soluções viáveis para as vulnerabilidades encontradas nas ferramentas para toda a fase de digitalização da indústria 4.0. Como resultado, foi possível construir o *framework* idealizado.

Para agrupar as duas pesquisas realizadas nos temas desenvolveu-se um processo de decisão, que auxiliará nas decisões de análise e gerenciamento de riscos na indústria 4.0. Além desse objetivo, tem-se o intuito de facilitar as decisões gerenciais de seleção de técnicas e ações para a gestão de riscos na indústria 4.0.

O *framework* antes de sua apresentação requer a explicação de algumas premissas básicas, que serão identificadas posteriormente como limitações do estudo. A primeira dessas premissas com a análise que deve ser construída para uma quantidade limitada de tecnologias digitais. No estudo em questão, cinco ferramentas tecnológicas tidas como as principais da indústria 4.0 foram analisadas no trabalho (IoT, *big data*, computação em nuvem, IA e robôs). Outra premissa que deve ser respeitada é a relação do nível industrial tecnológico que a organização ou sistema em análise está inserido, recomendando-se que a avaliação com base

no *framework* seja feito em um estágio mais imaturo de industrialização digital entendendo-se que processo de decisão terá melhor aplicação em um patamar que as organizações tenham maior inexperiência sobre o tema e seja necessária uma maior atenção aos processos e decisões gerenciais sobre segurança e riscos. Mas não se elimina a possibilidade de aplicação do *framework* proposto em casos mais avançados de maturidade digital industrial.

Considerando que as soluções de segurança existentes atualmente para sistemas de produção podem ser divididas em duas categorias principais: a defesa estática e a defesa dinâmica. Será utilizado o como base o método STAMP para desenvolver a defesa estática para o *framework* que será proposto aos sistemas industriais digitais, buscando-se alcançar todos os níveis hierárquicos presentes na cadeia produtiva. Já a proposição feita para a estrutura de defesa dinâmica terá como base a técnica STPA, pois está adequa-se ao dinamismo dos processos industriais digitais e suas características de mudanças e evoluções exponenciais.

Agora que os conceitos metodológicos foram mais bem alinhados, a revisão sistemática foi estruturada, realizada e apresentada e os conceitos do STAMP e da STPA foram ajustados para sanar as problemáticas presentes nas tecnologias da indústria 4.0, pode-se apresentar o *framework* planejado para mitigar ameaças e vulnerabilidades das tecnologias da indústria 4.0.

4. FRAMEWORK PROPOSTO PARA APOIO AO GERENCIAMENTO DE RISCOS NA INDÚSTRIA 4.0

Concluídas as revisões bibliográficas planejadas e analisados os principais dados dos estudos pode-se agora propor um *framework* que se adeque as necessidades dos problemas propostos e dos dados encontrados nas pesquisas. O conhecimento obtido com os estudos auxiliará na construção do processo de decisão adequado para lidar com os riscos presentes nas tecnologias da indústria 4.0 e a metodologia STAMP e a técnica STPA serão utilizadas como base metodológica para sanar tais ameaças e vulnerabilidades.

Inicialmente será apresentado o problema que o *framework* buscará auxiliar na resolução. Em seguida, uma discussão sobre as restrições no uso da estrutura será realizada, indicando qual a melhor situação para sua aplicação e quais os principais pontos para atenção no seu uso. Por fim, no terceiro subtópico será apresentado o processo proposto, com aplicação dos conceitos do STAMP e da STPA para estruturação dos riscos e das ações de segurança recomendadas para seu tratamento.

4.1. Apresentação geral do problema

A quantidade de vulnerabilidades de segurança cibernética potenciais são mais elevadas do que a quantidade de usuários mal-intencionados que poderiam tirar proveito. Há uma variedade de ameaças e vulnerabilidades para serem exploradas pelos utilizadores maliciosos, então, diversos estudos e metodologias buscam desenvolver formas particulares de gerir tais situações e estabelecer ações de comportamento seguro. No entanto, o estabelecimento de ações para cada categoria de comportamento torna-se um desafio, em conjunto com a seleção dos mecanismos eficazes e com as diferentes estratégias de raciocínio sob diferentes categorias de comportamentos, reforçando ainda mais o desafio do raciocínio voltado para a incerteza (MOZZAQUATRO *et al*., 2018).

O estudo mostrou que há inúmeras formas de atacantes maliciosos alcançar seus resultados usando ataques cibernéticos para com as tecnologias digitais da indústria 4.0. Assim, devem ser desenvolvidas maneiras de reduzir a ocorrência de tais ameaças e atenuar seus impactos em toda a cadeia produtiva. O processo mais apropriado para tal é desenvolver um *framework* conceitual que abranja os riscos e ameaças potenciais à essas tecnologias digitais e buscar propor processos seguros e soluções para limitar a ocorrência de eventos danosos. No

entanto, faz-se necessário inicialmente limitar o estudo para atender ao escopo adequado de aplicação.

4.2. Status de digitalização industrial

Existem algumas etapas que definem a maturidade das empresas que planejam incorporar os princípios da indústria 4.0, essas etapas, como especificadas anteriormente, tem dois principais macro status, o status de digitalização, onde são observados os primeiros passos para a implantação da indústria digital e o status de indústria 4.0, onde são observados estágios mais avançados de conectividade e digitalização.

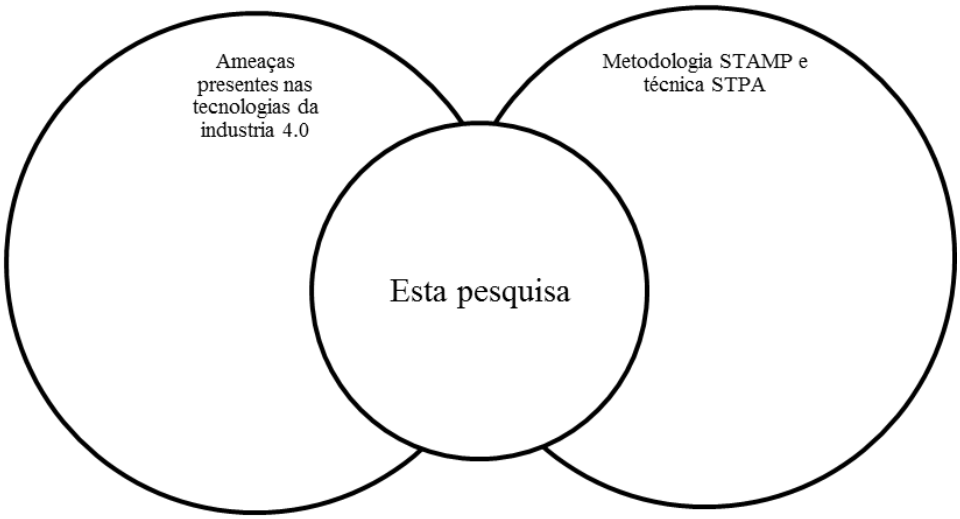
O status de digitalização é dividido em duas etapas, a informatização e a conectividade. A informatização tem como objetivo principal digitalizar os dados gerados nos processos industriais e adequar as máquinas e equipamentos, assim, na etapa posterior a adaptação dos dispositivos e sua conexão com a rede de internet compartilhada é necessária e essencial. Na etapa de conectividade, as máquinas e equipamentos estão aptas a se comunicar e compartilhar informações sobre os processos, esta etapa é a porta de entrada para a indústria 4.0, as etapas posteriores serão de melhorias e de aperfeiçoamento dos processos digitais.

Considerando que alguns preceitos devam ser indicados para a melhor adequação da estrutura às problemáticas mencionadas, recomenda-se que o *framework* proposto seja aplicado ainda na etapa de digitalização industrial, pois, pressupõe-se que no momento ao qual uma organização alcança o status de indústria 4.0, várias das problemáticas abordadas no processo já foram tratadas e eliminadas com a experiência adquirida. Mas, as considerações não garantem que as ameaças foram tratadas antes do alcance do status de indústria 4.0, por isso, indica-se que mesmo com um grau de desenvolvimento digital elevado, o *framework* conceitual deva ser utilizado, para validar seus processos e garantir que a segurança se encontra em alto nível.

4.3. Apresentação do *framework* proposto e desenvolvimento dos resultados

O estudo propôs construir um processo conceitual para auxiliar na tomada de decisão relacionada a riscos e segurança das tecnologias digitais da indústria 4.0. Assim, para exemplificar de forma mais efetiva como a atual pesquisa pode ser entendida, desenvolveu-se um diagrama de Venn na Figura 9, relacionando o atual cenário das tecnologias da indústria 4.0, as suas ameaças, riscos, perigos e vulnerabilidades e os modelos STAMP e STPA para o controle efetivo dessas ameaças.

Figura 9 - Diagrama de Venn para relação entre campos de aplicação do estudo



Fonte: Adaptado de Sisinni e outros 2018

Vale a ressalva ante a apresentação do *framework*, de que, dentre todas as tecnologias digitais facilitadoras da indústria 4.0 escolheu-se cinco dessas para a construção do estudo (internet das coisas, *big data*, sistemas ciber-físicos, inteligência artificial e robótica). Essa escolha teve como principal critério a quantidade de informações sobre cada tecnologia analisada. As tecnologias de manufatura aditiva e inteligência artificial não apresentaram dados suficientes ao ponto de gerar informações relevantes para tratamento de ameaças e vulnerabilidades na prática.

Portanto, com os dados encontrados no estudo pode-se propor o *framework* planejado, que auxiliará na tomada de decisão gerencial e na proposição de soluções adequadas para mitigar ou eliminar os riscos e ameaças das tecnologias da indústria 4.0, e ainda preparar os sistemas produtivos atuais para novas e emergentes ameaças que podem surgir com a maior aplicação prática da industrialização digital.

Inicialmente, será utilizada como base conceitual a técnica STPA para construir processos seguros com requisitos e restrições de segurança adequados a cada sistema e subsistema identificados nos processos e nas tecnologias digitais. Posteriormente será desenvolvido um modelo generalista para todas as ameaças identificadas no estudo de acordo com as ferramentas da indústria 4.0 consideradas no texto.

Cada etapa da estrutura proposta demandou uma análise mais aprofundada sobre o tema nos artigos da revisão sistemática, com essa análise foi possível construir modelos de processo

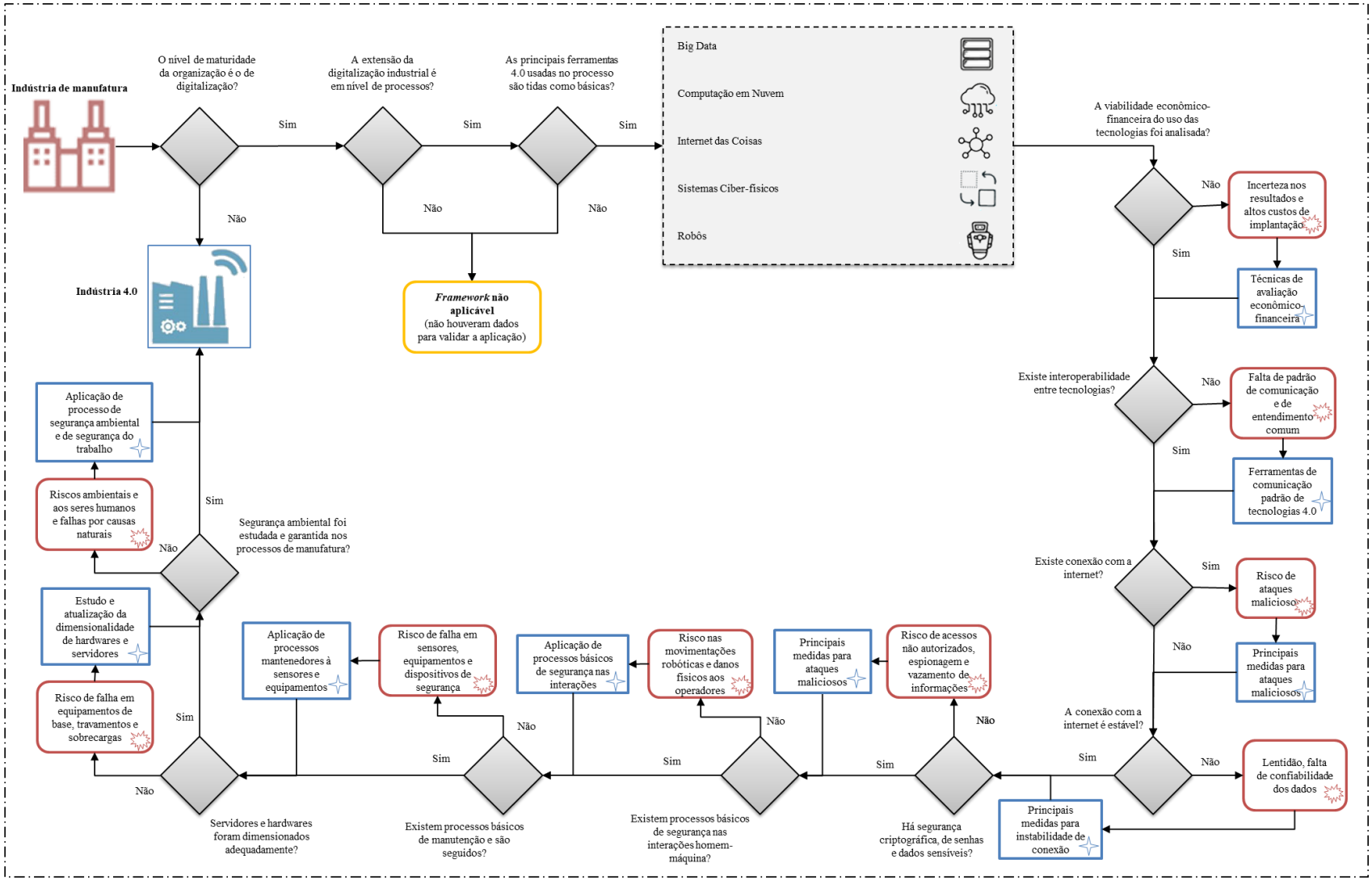
seguros, considerando as indicações do STAMP e da STPA para o desenvolvimento da estrutura hierárquica adequada. Dessa forma, indicaram-se os modelos de processos adequados para corrigir comportamentos inseguros, quais as ações de controle mais apropriada para cada tipo de ameaça existente e quais as estruturas hierárquicas de controle de segurança mais adequadas para manter os processos sistêmicos seguros.

O *framework* proposto contou com três questionamentos iniciais para identificar a sua perfeita aplicação nas organizações industriais que utilizam a indústria 4.0 ou planejam a ação para desenvolvimento futuro. O passo inicial é o de classificar o nível de maturidade digital que a organização em análise se encontra, levando em consideração as fases de maturidade da indústria 4.0. Caso a avaliação pelo analista seja por considerar que a organização encontra-se em um nível baixo de maturidade, ainda no status de digitalização, por exemplo, recomenda-se a aplicação do modelo, mas não elimina-se a possibilidade de aplicação em estágios mais avançados, por não se ter garantias de que todos os processos de análise de segurança propostos no *framework* foram seguidos anteriormente.

No segundo passo, deve-se avaliar qual a extensão do processo de digitalização da organização e em qual nível organizacional a aplicação do *framework* será realizada, em um nível de processo ou ao nível organizacional, englobando todos os processos do negócio. Recomenda-se que o nível adequado de aplicação da estrutura seja o nível de processo, sendo possível analisar mais detalhadamente todas as interações e as ameaças serem detectadas mais facilmente. Em um nível de digitalização organizacional o processo de análise poderá demandar um nível de organização e dedicação extremamente superior, por ser necessário avaliar todas as interações e todos os possíveis riscos digitais em nível organizacional, mas recomenda-se que caso a aplicação seja para nível organizacional, estratificar seus processos e analisar individualmente cada um desses.

O terceiro pré-requisito ou questionamento de validação para aplicação da estrutura é referente a quantidade ou tipo de tecnologias que serão incorporados aos processos da organização. Como indicado anteriormente, cinco tecnologias foram incluídas na avaliação do *framework*, entendidas como mais relevantes para a indústria 4.0 e avaliação de vulnerabilidades. No entanto, diversas ameaças identificadas no estudo são de origens comuns a todas as tecnologias digitais, então a depender de qual tecnologia será avaliada pode ser considerada a aplicação, avaliando todas as adaptações relevantes. Concluída a apresentação dos pré-requisitos de aplicação do *framework*, demonstra-se no Fluxograma 4 o processo de decisão desenvolvido para análise de riscos das tecnologias da indústria 4.0

Fluxograma 4 – Framework para análise de riscos e decisões gerenciais de segurança em organizações industriais digitais



Fonte: Esta pesquisa (2019)

Após avaliar os três pré-requisitos básicos para aplicação do *framework*, inicia-se a avaliação dos processos e das ameaças organizacionais, primeiramente indaga-se sobre a viabilidade econômico-financeira da aplicação da tecnologia, se esse processo foi efetuado no momento da escolha da tecnologia e qual seu impacto para o avanço digital tecnológico da organização. Caso todas essas indagações tenham sido respondidas e atendidas adequadamente, prossegue-se com a análise.

O segundo passo para avaliar os riscos organizacionais das tecnologias digitais refere-se à interoperabilidade entre tecnologias, esse fator é de extrema relevância para a avaliação das tecnologias digitais na indústria 4.0, e constantemente foi indicado nos estudos analisados como um fator problemático para a aplicação e a segurança nas organizações. Com a aplicação da técnica STPA (que será apresentada posteriormente) as restrições e medidas de segurança adequadas foram tomadas e o processo de análise pode prosseguir para a avaliação da conexão com a rede de internet que as tecnologias apresentam.

A análise do terceiro questionamento da estrutura faz referência ao tópico percebido como principal gerador de problemas para as tecnologias digitais, mas ao mesmo tempo é o fator que proporciona seu desenvolvimento. Indaga-se ao analista se existe conexão global de internet entre as tecnologias industriais digitais e ainda avalia-se qual a ocorrência de ataques maliciosos advindos da rede. Os riscos de ataques cibernéticos foram as ameaças de maior ocorrência no estudo, principalmente para as tecnologias CPS - sistemas ciber-físicos e IoT - internet das coisas, com a aplicação das restrições de segurança adequadas e os modelos de processos seguros, há grande possibilidade de eliminar as principais ocorrência advinda de ataques cibernéticos, restando as restrições impossíveis, como os ataques *zero-day*, que nunca foram previstos, mas devem ser criadas ações de segurança para identificar principalmente quando ataques estão ocorrendo.

A instabilidade de conexão com a internet é um fator de grande relevância também para as análises, por isso foi considerado como um dos passos. Em diversas situações foram apresentados estudo na revisão sobre quais as vulnerabilidades criadas pelo sinal falho de conexão com a internet, com isso abre-se a possibilidade de análise dos modelos de processos adequados para eliminar tais ocorrências e melhorar a conectividade com a rede, indispensável na aplicação da indústria 4.0.

Alguns perigos internos das organizações também foram levados em consideração na análise de vulnerabilidades. São os casos de acessos não autorizados ao ambiente fabril,

espionagem e vazamento de informações confidenciais, identificado essas ameaças devem ser criadas restrições de segurança adequadas para mitigar os perigos e ações de controle para serem aplicadas quando identificadas ameaças reais nas organizações.

Recomenda-se como sexto passo para analisar conceitualmente as ameaças das tecnologias digitais na organização avaliar o risco que as movimentações de máquinas, equipamentos e robôs industriais provocam aos seres humanos participantes dos processos. Restrições de segurança serão indicadas posteriormente com o uso da STPA e ações de controle serão previstas para eliminar as ocorrências indesejadas.

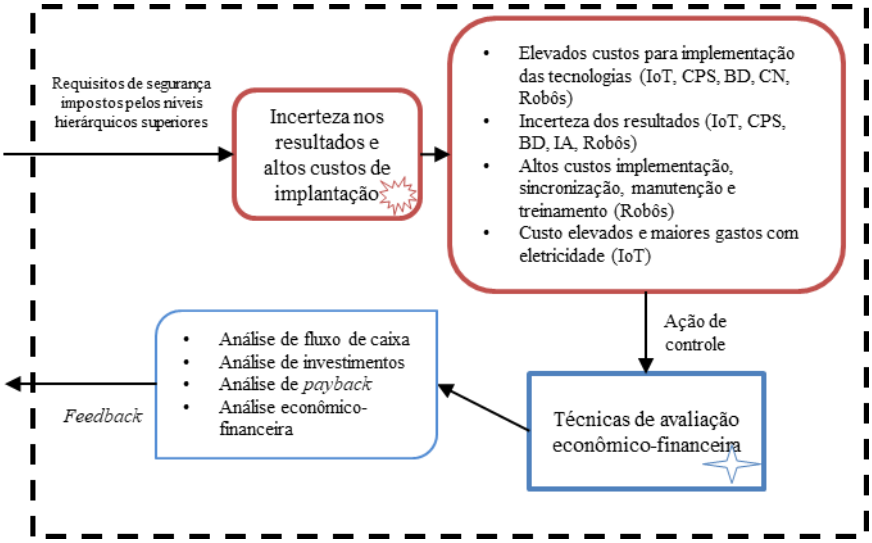
A sétima etapa para avaliação do processo fabril segundo o *framework* proposto visa identificar quais as possibilidades de falha nos sensores, atuadores, equipamentos e outros dispositivos de segurança, que podem influenciar na ocorrência de acidentes ou ameaças aos agentes do processo, indagando se técnicas de reparo são aplicadas adequadamente para manutenção do bom estado desses sensores. Depois de identificadas as principais falhas de acordo com a revisão sistemática da literatura, ações de controle seguro e padrões de segurança são desenvolvidos e os riscos reduzidos, mas nunca totalmente eliminados.

A oitava análise a ser realizada nos processos industriais digitais não diz respeito as tecnologias digitais, mas as demais tecnologias, materiais, equipamentos e máquinas que apoiam a indústria 4.0, fazem sua estrutura de base. A atualização de *softwares* e *hardwares*, as atividades de manutenção tradicional e todos os demais processos externos devem ser tratadas como possíveis perigos para o processo digital, as ações de controle e os níveis hierárquicos devem ser analisados e indicados, para manter os processos seguros da organização.

Por fim, a última etapa considerada para avaliação das ameaças tecnológicas que as ferramentas digitais da indústria 4.0 trouxeram, será analisar qual o impacto da adoção de tecnologias digitais nos processos de manufatura que influenciam no meio ambiente, quais os riscos de emissão de gases e materiais poluentes ao meio ambiente e qual a ameaça de contaminação dos colaboradores e de outros *stakeholders*.

Para descrever quais as ações de controle adequadas para cada uma das ameaças identificadas na revisão sistemática da literatura, formataram-se estruturas menores para análise das ameaças e proposição das soluções encontradas também na revisão. Assim, sistemas foram criados e estão exemplificados de melhor forma na Figura 10.

Figura 10 - Sistema de controle de ameaças para incertezas de custos da digitalização industrial

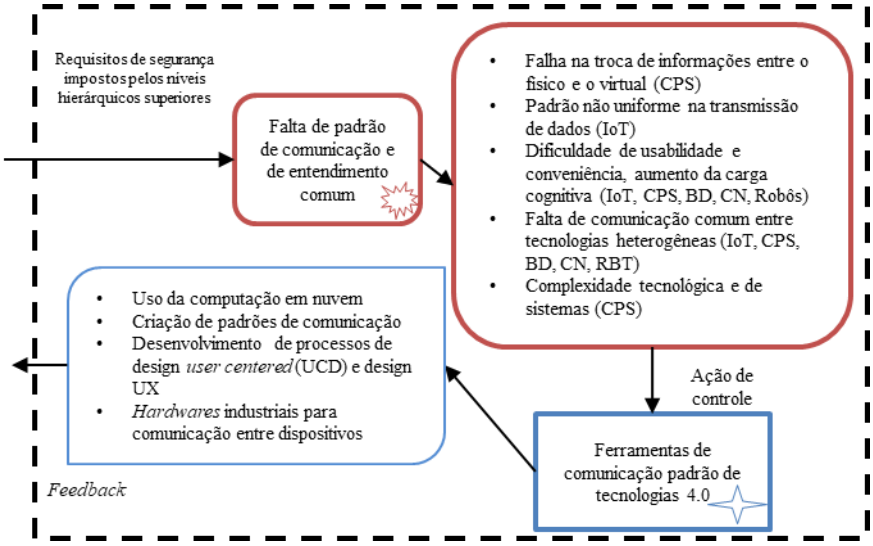


Fonte: Esta pesquisa (2019)

A incerteza nos resultados futuros e os altos custos de implantação das tecnologias da indústria 4.0 direcionam perigos ao projeto de digitalização, dessa forma, alguns riscos puderam ser identificados. Segundo os dados recolhidos pela revisão aplicada, todas as tecnologias digitais em análise apresentam ameaças econômico-financeiras ao sucesso da indústria 4.0, mas algumas ações de controle podem ser executas para eliminar ou mitigar essas vulnerabilidades, a ação recomendada pelos níveis hierárquicos superiores é a de analisar, de acordo com as técnicas de avaliação econômico-financeira, o fluxo de caixa projetado para a organização, verificar a perspectiva futura dos investimentos realizados, analisar o *payback* (simples ou descontado) e demais análises econômicas, para assegurar que as proposições incluídas ao projeto de digitalização industrial tenham bons resultados e o *feedback* apropriado seja aplicado e aprimorado.

Para a redução das vulnerabilidades relacionadas a falta de padrões entre tecnologias digitais e sobre o entendimento dessas também foi proposto um sistema de análise com base no STPA. Os principais causadores identificados no estudo estão relacionados com o aumento da demanda cognitiva que deve ser dedicada pelos operadores aos sistemas. Sabendo disso, podem ser aplicadas ações para eliminar tais ocorrências, estas podendo ser visualizadas na Figura 11.

Figura 11 – Sistema de controle de ameaças para vulnerabilidades de falta de padrão entre tecnologias



Fonte: Esta pesquisa (2019)

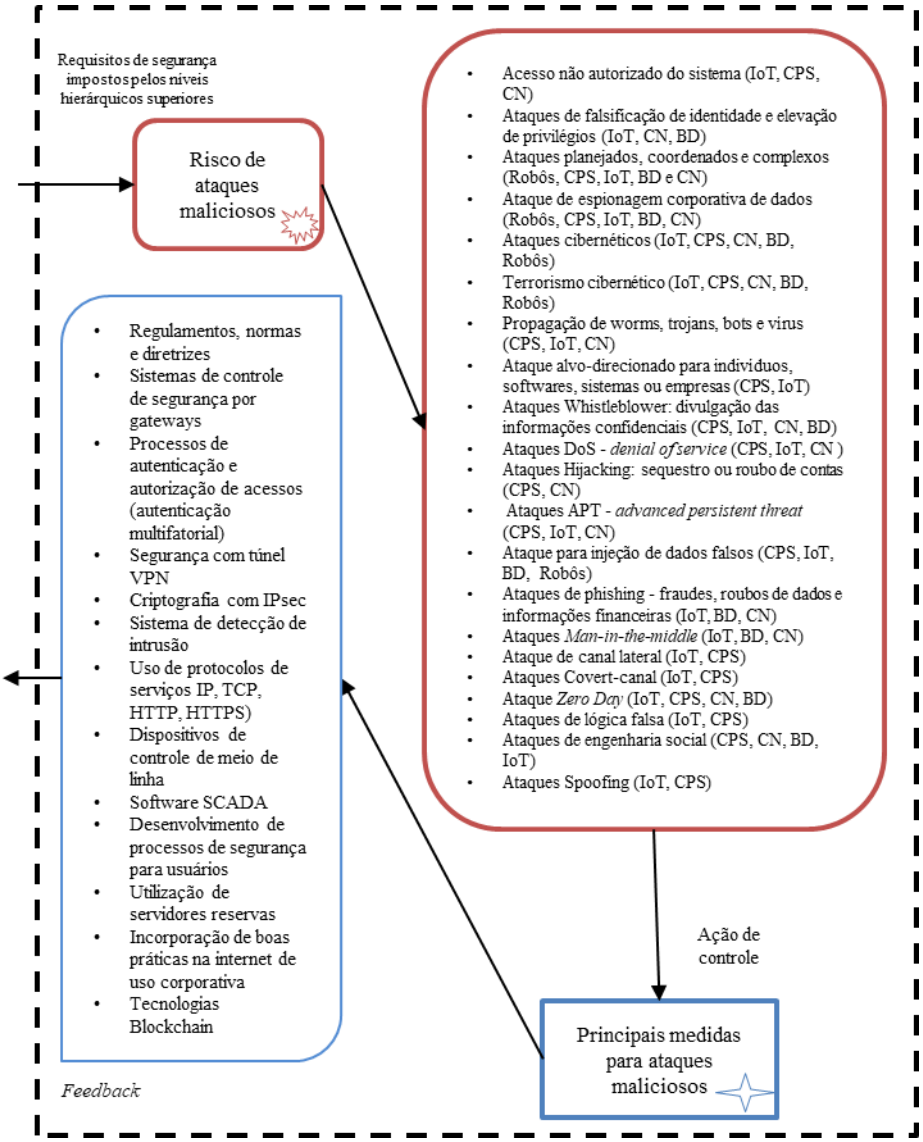
A falha na troca de informações entre tecnologias pode ser entendido por duas perspectivas de acordo com os dados analisados no estudo, a primeira relaciona-se com a comunicação entre o mundo virtual e físico, que demanda grande capacidade de armazenamento e de conexão, a segunda está relacionada com a falha de comunicação e não padronização de informações entre as tecnologias interlocutoras, levando a ocorrência do não entendimento de comandos e falha na interoperabilidade. Nessas situações especificadas puderam ser encontradas diversas formas de eliminar tais problemáticas, inicialmente com o uso do *big data* e da computação em nuvem possibilitando maior velocidade de leitura e armazenamento de informações. Podem ser usadas estratégias de desenvolvimento de padrões de comunicação, para mitigar as problemáticas de não heterogeneidade de comunicação entre dispositivos, por fim, pode ser proposta a utilização de hardwares de comunicação, que facilitaram a interconexão entre tecnologias digitais industriais.

A vulnerabilidade relacionada ao aumento da carga cognitiva em sistemas fabris industriais pode ser eliminada com o trabalho de design UX (*user experience*) ou com a aplicação de técnicas de UCD (*user centered design*), essas voltadas para o desenvolvimento da experiência do usuário e com o objetivo de facilitar a usabilidade e reduzir a carga cognitiva necessária para a tomada de decisões, tornando a interação entre homens e dispositivos simples e intuitiva.

Invariavelmente a indústria 4.0 ganhou escala e projetou seus expressivos resultados com o uso da internet para se sobressair as demais tecnologias industriais tradicionais, com isso,

faz-se necessário avaliar as ameaças que a conexão com a internet traz para as organizações, sistemas e processos de produção. O *framework* proposto analisa como a conexão com a internet frutifica os riscos de ataques maliciosos e danosos aos sistemas organizacionais. Assim, a Figura 12 indica quais as principais vulnerabilidades encontradas no estudo que a conexão com a internet gera para as tecnologias digitais e para todos os sistemas da empresa.

Figura 12 - Modelo de controle de ameaças e ataques maliciosos advindas da rede de internet mundial



Fonte: Esta pesquisa (2019)

Algumas das principais ameaças cibernéticas encontradas com o uso da internet foram descritas como ataques maliciosos, todos os tipos de perigos descritos foram encontrados nos estudos escolhidos para a revisão, mas o estudo não busca exaurir todas as ameaças e métodos

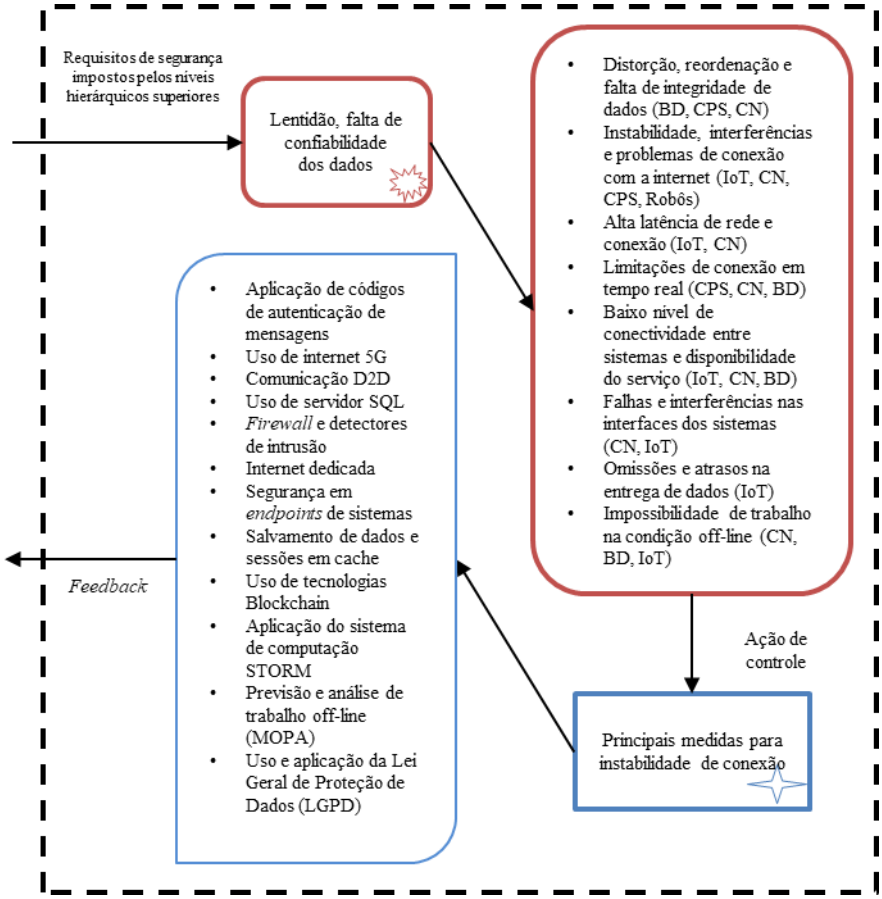
de mitigar essas vulnerabilidades e limitou toda a análise aos artigos finais escolhidos para a revisão sistemática da literatura.

Algumas das ameaças visualizadas foram encontradas em todas as tecnologias digitais em análise, como os ataques maliciosos planejados, coordenados e complexos, a espionagem corporativa, os ataques *hackers* e o terrorismo cibernético. Algumas outras ameaças identificadas tem grande influência na propagação dos perigos, como são os casos dos ataques de engenharia social, a pratica de *pishing* e os ataques DoS – negação de serviço ou acesso as informações.

Para limitar tais ataques também foram verificadas quais as aplicações mais usuais. Avalia-se que dentre todas as indicações, os processos básicos de segurança se sobressaem diante de outras técnicas, como são os casos de uso dos protocolos básicos de segurança digital como o VPN, IP, senhas, criptografia, HTTP, HTTPS, etc. Ainda verificou-se que os próprios usuários internos ao sistema tem grande responsabilidade pela ocorrência de ataques maliciosos, assim, vale a consideração de que o desenvolvimento de procedimentos padrões de segurança cibernética e a incorporação de boas práticas de uso da internet corporativa são essenciais para desenvolver a cultura de segurança contra ataques maliciosos externos e limitar eventualmente tais incidentes.

A transmissão de dados é um processo de grande influência para o sucesso da indústria 4.0, principalmente por conta do *big data* e da computação em nuvem serem atrelados exclusivamente a conexão com a internet. Dessa forma, a lentidão e falta de confiabilidade na transmissão desses dados tem um impacto significativo nos comportamentos inseguros que os sistemas digitais podem apresentar, considerando, desde mau rendimento a distorções e interferência nos dados. A Figura 13 indica quais os principais causadores de ameaças relacionados à lentidão e falta de confiabilidade de dados e indica também como essas ações maliciosas podem ser eliminadas e quais seus respectivos *feedbacks* para controle adequado dos requisitos de segurança.

Figura 13 – Sistema de controle de vulnerabilidades para falta de confiabilidade na transmissão de informações



Fonte: Esta pesquisa (2019)

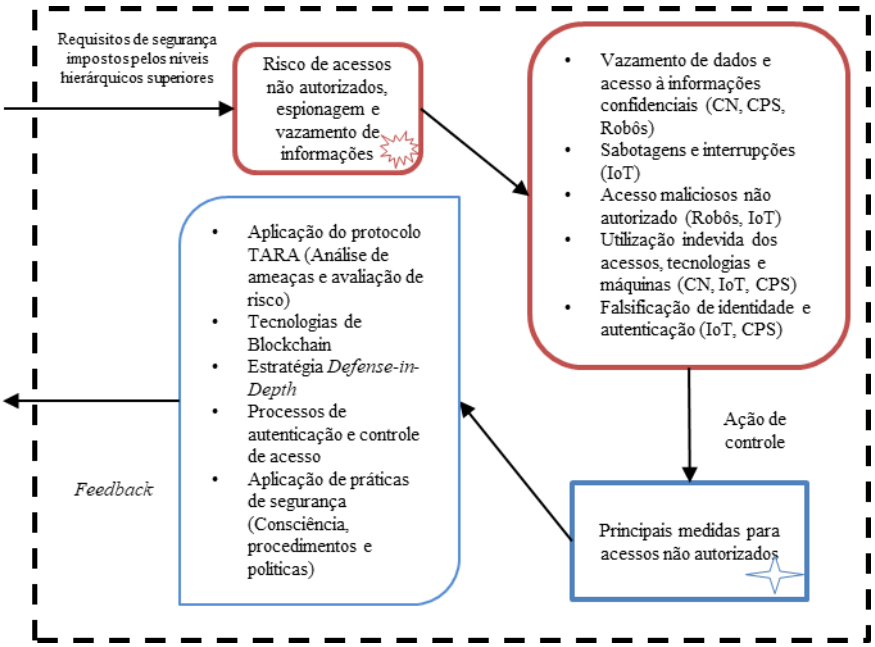
As principais ocorrências identificadas na falta de confiabilidade de dados estão relacionadas com a distorção, reordenação e falta de integridade dos dados que são transmitidos entre dispositivos, os problemas com a conexão com a internet, visualizando-se alta latência de rede e transmissão, a baixa disponibilidade do serviço de internet e entre os dispositivos na troca de dados e informações, e principalmente, a falta de conectividade, havendo a necessidade de trabalhos na condição *off-line*, sendo que a conexão com a internet é essencial para a comunicação entre dispositivos digitais.

Por conta de tais problemáticas, algumas soluções foram estudadas e indicadas para mitigar a falta de integridade da transmissão de dados e os problemas com a instabilidade de conexão. Como são indicados o uso de salvamento de dados em cache, o uso de servidores SQL e principalmente para solucionar problemas de conexão a aplicação de internet dedicada aos sistemas mais importantes ou o uso de tecnologias 5G, para melhorar os sinais de internet e facilitar a comunicação entre dispositivos, ainda para eliminar possíveis ameaças de interferências e falta de confiabilidade de dados podem ser usados códigos de autenticação de

mensagens, para garantir que esses não foram reordenados ou distorcidos e ainda com o uso de tecnologias de *Blockchain* para garantir a autenticidade das informações transmitidas.

A espionagem, o vazamento de dados e os acessos não autorizados são aspectos que merecem atenção especial, relacionadas à segurança na indústria 4.0. Essas ameaças foram identificadas e analisadas na Figura 14, e alguns processos de segurança foram propostos para eliminar a possibilidade de ocorrência de tais acontecimentos.

Figura 14 – Sistema de controle de riscos para acessos não autorizados e vazamento de informações



Fonte: Esta pesquisa (2019)

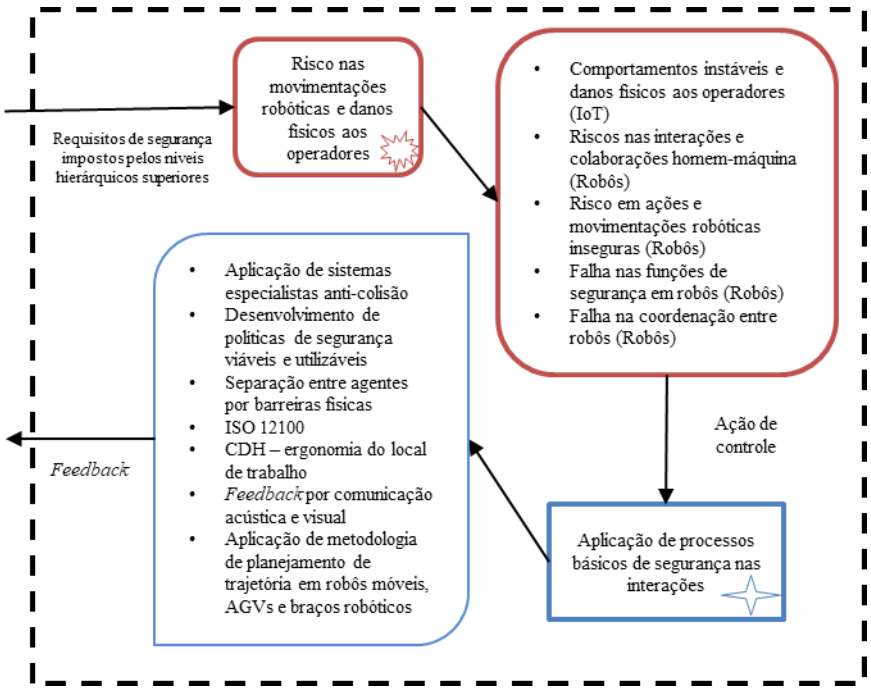
As principais problemáticas advindas com os acessos não autorizados à sistemas, são a espionagem e o vazamento de informações confidenciais. Essas vulnerabilidades são relacionadas com a utilização indevida de acessos e tecnologias, possibilitando que atacantes coletem e distribuam informações entre a comunidade em geral, esses podem usar falsa identidade e falsa autenticação para acessar locais indevidos, e consequentemente sabotar ou interromper os processos, sejam esses processos de segurança ou processos de fabricação, causando perigos ainda maiores aos utilizadores do sistema.

Buscando limitar a ocorrência de tais ameaças algumas medidas de segurança podem ser indicadas, como a aplicação das tecnologias de *blockchain*, para garantir a autenticidade de informações fornecidas no acesso ao sistema, o uso de protocolos de avaliação de ameaças adequado, a utilização de estratégias de segurança convenientes e a aplicação de práticas de

segurança digital apropriadas, de acordo com as políticas e os procedimentos indicados pelos altos níveis hierárquicos.

Assim como deverão ser criados requisitos de controle de segurança para o vazamento de informações, para a espionagem e para o risco de acesso não autorizados, há necessidade de desenvolver requisitos para mitigar os perigos relacionados a movimentações robóticas e nas interações homem-máquina. Alguns comportamentos inseguros foram determinados com o estudo, indicando a possibilidade de ameaças à segurança dos trabalhadores, como danos físicos aos operadores ou parceiros de trabalho das máquinas, movimentações robóticas que poderiam causar ferimentos, apresentação de falhas de segurança dos equipamentos sensores e falha na coordenação do trabalho entre humanos e robôs. A Figura 15 indica quais as ameaças encontradas e como essas poderiam ser eliminadas com aplicações de processos básicos de segurança.

Figura 15 – Sistema de controle de riscos para movimentações robóticas inseguras



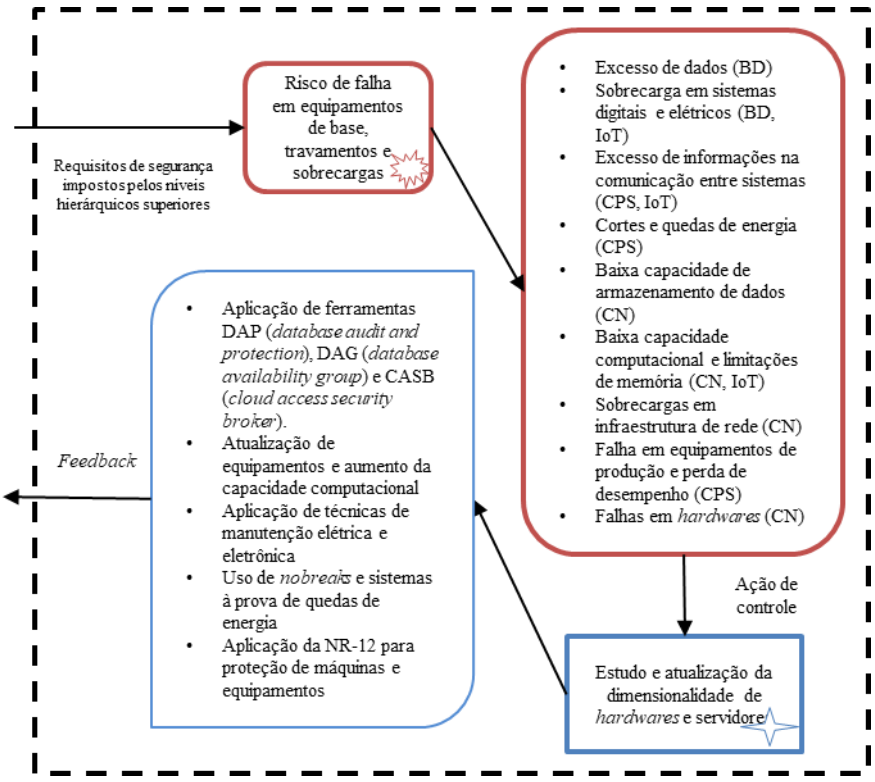
Fonte: Esta pesquisa (2019)

O desenvolvimento de algumas atividades essenciais de segurança podem eliminar os riscos e ameaças encontradas nesse sistema descrito acima, como é o caso da aplicação de políticas de segurança interna na organização, que sejam viáveis e aplicáveis para todos os processos interativos, a separação dos agentes por barreiras físicas, quando houver a possibilidade para tal, a aplicação da ISO 12100 para o desenvolvimento de máquinas seguras

e o controle ergonômico do ambiente de trabalho e o desenvolvimento de processos ergonômicos para as interações, que garantam a segurança dos operadores, da produção e dos equipamentos fabris.

Além das preocupações básicas com as tecnologias primárias da indústria 4.0, outros controles devem ser adequados para eliminar as ameaças de falha em equipamentos de base (servidores, *hardwares* e equipamentos físicos de apoio), mas outras vulnerabilidades atreladas a essas falhas ainda podem ser identificadas, como os riscos de sobrecargas e travamentos. Em diversos casos, vulnerabilidades como a sobrecarga dos sistemas elétricos e eletrônicos, o excesso de dados, a baixa capacidade computacional e de armazenamento foi discutida pelos autores dos artigos em análise, assim como foram detectadas que falhas em *hardwares* e quedas e cortes de energia poderiam influenciar na confiabilidade dos sistemas industriais digitais, gerando ameaças ao processo. Com base nessas informações a Figura 16 foi desenvolvido, buscando indicar quais os principais perigos potenciais e como esses poderiam ser reduzidas pelas ações de controle indicadas.

Figura 16 – Sistema de controle para eliminar ameaças de mal dimensionamento de equipamentos

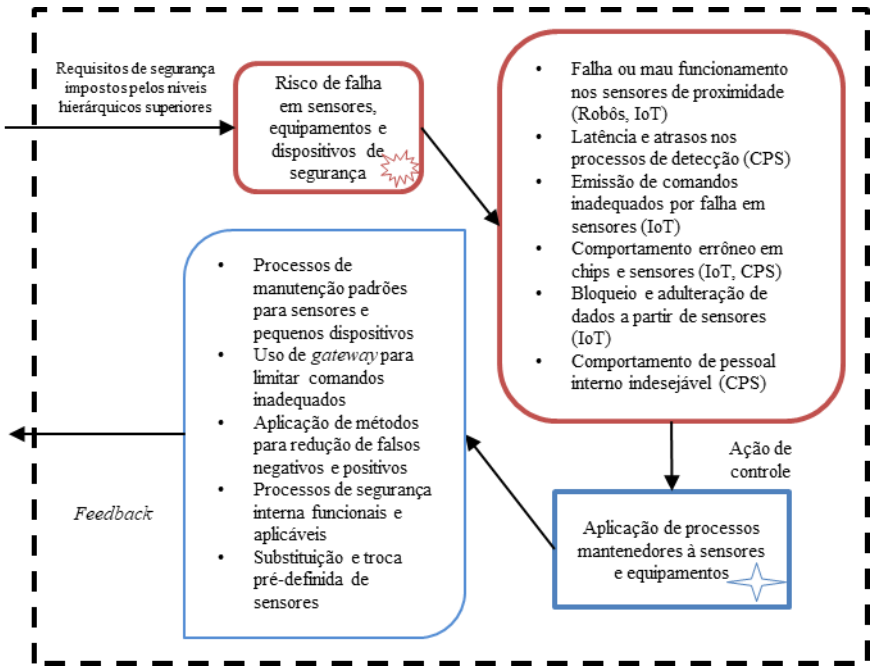


Fonte: Esta pesquisa (2019)

As principais ações de controle indicadas pelos próprios estudos em análise estão relacionadas com a aplicação de melhores projetos de dimensionamento, como é o caso da indicação da ação de controle para atualização de equipamentos com melhor capacidade computacional, os sistemas digitais sofrem atualizações há uma velocidade exponencial, com isso, há a necessidade de se desenvolver projetos de dimensionamento de equipamentos que garantam o uso desses por um período de tempo adequado nos sistemas. O uso de *nobreaks*, técnicas de manutenção elétrica e eletrônica, sistemas a prova de quedas de energia são também algumas das atividades de controle adequadas aos sistemas que apresentam risco quanto a falhas por sobrecarga ou travamentos.

Os sensores, atuadores, chips e outros dispositivos dessa classe podem ser vistos como o elo mais sensível dos sistemas industriais. Dessa forma, alguns requisitos de segurança devem ser impostos no *framework* com relação à manutenção da segurança desses dispositivos. Foram analisados em determinados casos que os sensores apresentaram comportamentos inadequados, como mal funcionamento, erros de comportamento (falsos positivos ou negativos), atrasos nos processos de detecção ou até mesmo adulteração de dados por meio desses sensores ou chips de controle, assim, a Figura 17 busca estruturar etapas para o planejamento de ações de controle que possam eliminar as ameaças advindas desses dispositivos.

Figura 17 – Sistema de controle para eliminar falhas em sensores e dispositivos de monitoramento

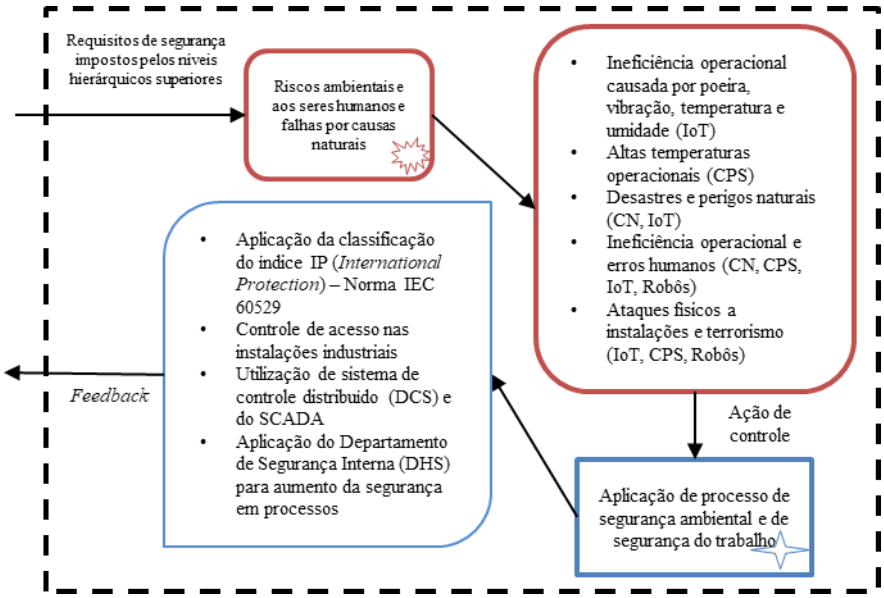


Fonte: Esta pesquisa (2019)

Seguindo a estrutura, algumas ações de controle são indicadas para eliminar as ameaças provenientes da falha de sensores, atuadores ou chips de controle de processos industriais. São essas: o desenvolvimento e aplicação de técnicas e processos adequados para manutenção desse tipo de equipamento, como as técnicas tradicionais de análise de riscos como o FMEA, as técnicas de árvore (falha ou evento), entre outras. São ainda indicadas como ações de controle a aplicação de mecanismo para detecção de falsos positivos ou negativos, a aplicação de manutenções preventivas para reposição antecipada à falha e o uso de *gateways* para limitar acessos e prevenir que dados errôneos sejam incorporados e inseridos nas leituras.

Os perigos ambientais são preocupações recorrentes em todo o mundo, e em textos analisados no estudo foram discutidas ameaças relacionadas a perigos ambientais ou por causas naturais. Mesmo que grande parte poderia está pouco correlacionada com as atividades e os processos industriais, mas que devem ser considerados na estrutura proposta por incorrer perigos aos humanos e aos processos, além de que devem ser apresentadas ações de controle para garantir a segurança ou reduzir os impactos da ocorrência desses. A Figura 18 revela essas indicações de requisitos de segurança e ações de controle adequadas para os riscos ambientais ou naturais.

Figura 18 – Sistema de controle para limitar o impacto dos riscos naturais ou ambientais



Fonte: Esta pesquisa (2019)

O requisitos de segurança para tais perigos são extrapolados principalmente quando ocorrem algumas situações anormais nos sistemas, como é o caso da ineficiência operacional causado por poeira, vibração, temperatura ou umidade, outros casos também foram encontrados

na análise dos textos, como a ocorrência de desastres naturais, como tempestades, furacões, inundações, ataques terroristas físicos ou até mesmo a ineficiência operacional humana, que em algumas situações, não são intencionais, mas apenas da natureza do ser, por não ser capaz de alcançar a capacidade de processamento de máquinas e equipamentos.

Para limitar o impacto da ocorrência dessas ameaças citadas, algumas ações de controle foram indicadas nos estudos analisados na revisão, como a recomendação de aplicação da norma NBR IEC 60529, que aponta qual o índice IP adequado para garantir que os limites de poeira, temperatura e umidade não sejam ultrapassados pelos dispositivos e pelo ambiente industrial. Foram indicados também o desenvolvimento de departamentos e sistemas de segurança, para desenvolver ações adequadas ao combate das ameaças naturais e controlar de forma remota e distribuída todos os sistemas, melhorando consequentemente a predição de perigos e a tomada de decisões rápidas, quando problemas naturais e ambientais ocorrerem.

Como visto anteriormente, construiu-se um *framework* com a visão de auxiliar a redução de ameaças e vulnerabilidades das tecnologias da indústria 4.0, no decorrer desses processos foram aplicados conceitos do método STAMP e da técnica STPA, ferramentas essas que são adequadas ao tratamento de riscos novos e emergentes, principalmente por serem metodologias de análise sistêmica de risco, solucionando diversas problemáticas encontradas nas aplicações de outras ferramentas de risco, tidas como tradicionais. O principal objetivo do *framework* proposto foi o de poder reduzir consideravelmente o descuido com a segurança, que em diversas situações é deixada em segundo plano, mas acredita-se que o processo conceitual proposto irá auxiliar aos tomadores de decisão comportar-se de forma mais adequada ao tratamento de riscos, ou todos sofreram com as ameaças cibernéticas que a tecnologia carrega em sua companhia.

Concluída a apresentação e discussão do *framework* proposto e indicada suas restrições e premissas para aplicação têm-se posteriormente as conclusões do estudo, indicando quais objetivos foram alcançados ao longo do texto, quais as limitações da pesquisa e qual o futuro das análises, planejando possibilidades de melhorias para tal e indicando passos que possam ser realizados posteriormente, para evoluir a discussão e promover a segurança digital na indústria 4.0.

5. CONCLUSÕES E TRABALHOS FUTUROS

5.1. Conclusões

Ainda não é possível que máquinas e produtos inteligentes consigam interagir entre si sem qualquer intervenção humana, o que na verdade é considerado um passo pequeno, visto que a tecnologia de desenvolve de forma exponencial. Então, no mundo digital contemporâneo não se pode considerar que as fábricas digitais atuais sejam totalmente inteligentes, uma vez que as tecnologias digitais de alto nível só foram usadas em determinadas linhas de produtos e em setores específicos da indústria e não é possível encontrar plantas industriais totalmente livres da intervenção humana.

Essas afirmações puderam ser comprovadas com o estudo, visto que a análise das publicações ajudou a identificar inúmeras características das ferramentas estudadas, verificando sob a ótica do passado quais as possíveis realizações futuras para o setor em análise. Foi possível identificar também o expressivo crescimento quanto ao número de publicações sobre a área de estudo sistemático de riscos, considerando que o desenvolvimento tecnológico tem tendência crescente ao uso desse tipo de ferramenta.

As análises demostraram que grande parte dos estudos são relacionados com atividades produtivas complexas. Inúmeros atores, complexas interações entre partes, pessoas submetidas a riscos mais graves, importância e relevância para a economia (aviação, transporte ferroviário, indústria de petróleo e gás, setor automotivo e outros), etc. Todas essas características fazem com que seja necessário tomar providências de segurança no projeto do processo, não sendo possível esperar que falhas ocorram para se analisar a probabilidade de nova ocorrência. Os acidentes são inaceitáveis e em função disso, a tendência de crescimento no uso de análise sistêmica de riscos em organizações produtivas é elevada.

Foi possível identificar no estudo o grau de participação do Brasil no desenvolvimento da indústria 4.0 e no uso de abordagens sistêmicas para análise de riscos. Sem grande expressividade no cenário mundial no estudo desse tipo de ferramenta, o país ainda carece de grandes investimentos e apoio governamental ao desenvolvimento das pesquisas nesse âmbito, desconsiderando ainda o baixo grau de interesse dos pesquisadores sobre o tema, podendo ser reunidos em poucos pares os nomes relevantes para a ciência dos riscos no país. Isso também é comprovado visto o número de publicações desenvolvidas por brasileiros que foram analisadas na pesquisa.

Assim, o estudo mostrou-se de grande relevância, por identificar as lacunas existentes nas áreas de análise, além de alcançar os objetivos traçados logo no início da pesquisa e conseguir responder os questionamentos relativos à revisão sistemática da literatura.

O objetivo geral do trabalho foi alcançado na etapa 5.3, onde se encontra o *framework* proposto para análise de vulnerabilidades das tecnologias digitais da indústria 4.0. Os objetivos específicos do trabalho foram alcançados no decorrer da pesquisa, contribuindo de forma crucial para a conquista do objetivo geral do estudo. Foram também identificadas quais as tecnologias digitais que mais tiveram suas vulnerabilidades exploradas, e ainda, foram identificadas, analisadas e propostas soluções adequadas para o tratamento de tais ameaças.

Com relação as revisões sistemáticas propostas, todas as questões definidas no início de cada uma das pesquisas foram respondidas com a finalização do *framework* proposto. Entregando uma discussão aprofundada sobre o domínio da segurança sistêmica, suas principais aplicações e os principais autores das publicações referentes ao tema na última década. Além de tal, foram identificadas quais as ameaças mais representativas para as tecnologias digitais e consequentemente a indústria 4.0 e quais dessas tecnologias eram mais afetadas.

Na construção do *framework* e em sua explicação foram aplicados conceitos das ferramentas STAMP e STPA. A aplicação dessas ferramentas permitiu que todo o processo de análise fosse planejado de maneira sistêmica, um dos principais requisitos para a solução de problemas da manufatura digital e que diversas ameaças e soluções fossem propostas para auxiliar decisões futuras. Ao todo foram apresentadas 67 possíveis vulnerabilidades nos processos industriais digitais e consequentemente diversas formas de tratar, mitigar ou eliminar essas ameaças.

O caminho para se produzir um estudo mais robusto sobre riscos na indústria 4.0 ainda é longo, pois as informações apresentadas no trabalho de longe não podem ser consideradas exaustivas, quanto a variedade de riscos e ameaças presentes nesse campo. A área de estudo ainda carece de maiores e melhores aplicações práticas, revisões e reaplicações em todos os campos, áreas e processos que as tecnologias se desenvolvem, mas um grande pontapé inicial foi dado.

Com a conclusão do trabalho foi possível encontrar também alguns pontos de limitação. Em geral, as análises de risco e vulnerabilidades da indústria 4.0 não contam com informações precisas, pois tais informações trazem consigo algumas características ímpares, como por

exemplo a perda de reputação e credibilidade para as empresas que são vítimas, quando suas vulnerabilidades são expostas. Como descrito anteriormente, não foi possível encontrar dados suficientes sobre riscos, ameaças e vulnerabilidades para demais tecnologias digitais e no estudo, apenas cinco delas foram analisadas. Representando pequena parte das tecnologias presentes na indústria 4.0, por motivo principal de insuficiência de estudos para se estruturar uma análise mais robusta. Hoje, se estima que podem ser encontradas na literatura cerca de 60 tecnologias digitais disruptivas.

5.2. Limitações do estudo

No decorrer do desenvolvimento do estudo algumas limitações foram encontradas para a sua aplicação de forma completa. Como discutido anteriormente, a limitação quanto a maturidade organizacional foi a de maior peso, considerando que uma organização com maturidade de indústria 4.0 já se preparou inicialmente para todos os riscos, ameaças e vulnerabilidades discutidas no estudo. No entanto, tal limitação não exclui a possibilidade de aplicação do *framework* por empresas em um nível tecnológico mais avançado, possibilitando a validação por parte da organização dos atendimentos aos requisitos de segurança impostos pela estrutura proposta.

O estudo limitou a maturidade organizacional de acordo com a avaliação dos autores Rodseth e outros (2017), incluindo apenas o nível de digitalização para avaliação da segurança da organização, entendendo que nessa etapa os processos básicos de segurança devem ser garantidos para só então ser alcançado o status de indústria 4.0, ampliando as atividades da etapa inicial. Informatização e conectividade.

Em geral, indica-se como limitação o tipo de pesquisa utilizado, revisão sistemática da literatura, principalmente porque os dados em análise foram encontrados em um grupo limitado de artigos e não representam de forma total todas as vulnerabilidades, ameaças e riscos encontrados na indústria 4.0 e nas tecnologias digitais. Mas avalia-se que para superar essa limitação o estudo deva ser um norteador do processo decisivo, auxiliando na tomada de decisão dos gerentes e analistas de segurança para incorporação de técnicas e aplicações que podem mitigar e controlar os riscos digitais.

5.3. Estudos futuros

Como discutido em diversos tópicos do texto, as tecnologias digitais estão em evolução constante e se desenvolvem de forma exponencial, buscou-se limitar o estudo dos artigos com publicação até o final do ano de 2018, mas entende-se que diversas análises e estudos foram realizadas e incorporadas as bases científicas no de 2019 e 2020 e que podem ser de grande influência para a segurança digital. Assim, é válido tratar como uma tarefa ou estudo futuro a atualização do *framework* proposto, melhorando as pesquisas, refinando melhor os dados e evoluindo a proposta inicial.

Outras metodologias também podem ser incorporadas ao *framework* proposto, como exemplo o uso de modelos multicritérios para solucionar problemáticas de decisão de investimento de recursos, identificação de vulnerabilidades de maior gravidade e melhorias no processo proposto, indicando melhor reordenação de questionamentos e de etapas da estrutura.

A pesquisa bibliográfica inicial incorporou sete tecnologias digitais, mas na construção do *framework* conceitual apenas cinco destas foram consideradas por falta de dados ou informações relevantes sobre as demais. Então, define-se como possibilidade para estudos futuros a análise das tecnologias digitais não consideradas, a manufatura aditiva e a inteligência artificial.

O trabalho também pode evoluir de outras formas, buscando alcançar outros resultados diferentes da análise de ameaças da indústria 4.0. Como estudo futuro pode ser indicado que o *framework* proposto posso ser melhorado para avaliar o nível de maturidade organizacional das empresas que buscam incorporar a indústria 4.0 nos seus processos, avaliando o nível de maturidade das tecnologias digitais já aplicadas ou que podem ser incorporadas nas organizações em avaliação.

REFERÊNCIAS

AAZAM, M.; ZEADALLY, S.; HARRAS, K. A. Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*. 2018.

AL-MHIQANI, M. N.; AHMAD, R.; YASSIN, W.; HASSAN, A.; ABIDIN, Z. Z.; ALI, N. S.; ABDULKAREEM, K. H. Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems. *International Journal of Advanced Computer Science and Applications*. v. 9, n. 1, 2018

ALTHAUS, C. E. A disciplinary perspective on the epistemological status of risk. *Risk Analysis*. v. 25, n. 3, p. 567-88, 2005.

ANCILLOTI, E.; BRUNO, R.; CONTI, M. The role of communication systems in smart grids: Architectures, technical solutions and research challenges. *Comput. Commun*. v. 36, p. 1665–1697, 2013.

ANDERSSON, L. A new method based on the theory of fuzzy sets to obtaining na indication of risk. *Civil Engineering and Environmental Systems.* v. 3, n. 3, p. 164-174, 1986.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: a survey. *Comp. Networking*. v. 54, n. 15, p. 2787-2805, 2010.

AVEN T. What defines us as professionals in the field of risk analysis? *Risk Analysis*. v. 37, n. 5, p. 854-860, 2016.

AVEN, T. An Emerging New Risk Analysis Science: Foundations and Implications. *Risk Analysis*. 2017.

BAHRIN, M. A.K.; OTHMAN, F.; AZLI, N. H. N.; TALIB, M. F. Industry 4.0: A review on industrial automation and robotic. *Journal Teknologi*. v. 78, n. 6-13, p. 137–143, 2016.

BARNATT, N.; JACK, A. Safety analysis in a modern railway setting. *Safety Science*. v. 110, p. 177-182, 2018.

BERGER, R. A game changer for the manufacturing industry? Additive manufacturing. Strategic Consultants, Munich, 2013.

BERTALANFFY, L. *General Systems Theory: Foundations, Development, Applications*. New york: braziller, 1968.

BOLBOT, V.; THEOTOLATOS, G.; BUJORIANO, M. L.; BOULOUGOURIS, E.; VASSALOS, D. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review, *Reliability Engineering and System Safety*, 2018.

BORGIA, E. The Internet of Things vision: key features, applications and open issues. *Computer Communications*, v. 54, p. 1-31, 2014.

BOYES, H.; HALLAQ, B.; CUNNINGHAM, J.; WATSON, T. The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*. Coventry. v. 101, p. 1-12, 2018.

BRERETON, P.; KITCHENHAM, B. A.; BUDGEN, D.; TURNER, M.; KHALIL, M. Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software.* v. 80, p. 571-583, 2007.

BRESSANELLI, G.; ADRODEGARI, F.; PERONA, M.; SACCANI, N. Exploring How Usage-Focused Business Models Enable Circular Economy through Digital Technologies. *Sustainability*. v. 10, 2018.

BROCAL, F.; GONZÁLEZ, C.; SEBASTIÁN, M. A. Technique to identify and characterize new and emerging risks: A new tool for application in manufacturing processes. *Safety Science*. Espanha, v. 109, p. 144–156, 2018.

BROCAL, F.; SEBASTIAN, M. A. Identification and analysis of advanced manufacturing processes susceptible of generating new and emerging occupational risks. *MESIC Manufacturing Engineering Society International Conference*, Espanha, v. 132, p. 887–894, 2015.

CAGLIANO, A. C.; GRIMALDI, S.; RAFELE, C. Choosing project risk management techniques. A theoretical framework. *Journal of Risk Research*, v. 18, n. 2, p. 232-248, 2015.

CAMERON, I.; MANNAN, S.; NEMETH, E.; PARK, S.; PASMAN, H.; ROGERS, W.; SELIGMANNC, B. Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better? *Process Safety and Environmental Protection*. Austrália, v. 110, p. 53-70, 2017.

CARUSO, L. Digital innovation and the fourth industrial revolution: epochalsocial changes? AI & Society: Knowledge, Culture and Communication. Londres, v. 33, n. 3, p. 379-392, 2017.

CHAO, H.; CHEN, Y.; WU, J. Power saving for machine to machine communications in cellular networks. IEEE GLOBECOM Workshops (GC Wkshps). p. 389-393, 2011.

CHEN, M.; MAO, S.; LIU, Y. Big data: A survey. *Mobile Netw. Appl*. v. 19, n. 2, p. 171-209, 2014.

CHEN, M.; WAN, J.; LI, F. Machine-to-Machine Communications: Architectures, Standards and Applications. *KSII Transactions on Internet and Information Systems*. v. 6, n. 2, p. 480-495, 2012.

CHIDAMBARAM, P. Perspectives on human factors in a shifting operational environment. *Jornal of Loss Prevention Process Industries*. v. 44, p. 112–118, 2016.

CHONG, S.; PAN, G.; CHIN, J.; SHOW, P. L.; YANG, T. C. K.; HUANG, C. Integration of 3D Printing and Industry 4.0 into Engineering Teaching. *Sustainability*. v. 10, 2018.

CINQUE, M.; RUSSO, S.; ESPOSITO, C.; CHOO, K.-K. R.; FREE-NELSON, F.; KAMHOUA, C. A. Cloud Reliability: Possible Sources of Security and Legal Issues? *IEEE Cloud Computing*, 2018.

CORBO, G.; FOGLIETTA, C.; PALAZZO, C.; PANZIERI, S. Smart Behavioural Filter for Industrial Internet of Things - A Security Extension for PLC. *Science* + Business Media, 2017

CORNELL, M. E. P. Uncertainties in risk analysis: six levels of treatment. *Reliability Engineering and System Safety*. v. 54, p. 95-111, 1996.

DE ALMEIDA, A. T.; ALENCAR M. H.; GARCEZ T. V.; FERREIRA, R. J. P. A systematic literature review of multicriteria and multi-objective models applied in risk management, *IMA Journal of Management Mathematics*, 1–32, 2017.

DE ALMEIDA, A. T.; CAVALCANTE, C. A. V.; ALENCAR, M. H.; FERREIRA, R. J. P.; DE ALMEIDA-FILHO, A. T.; GARCEZ, T. V. *Multicriteria and Multiobjective Models for Risk, Reliability and Maintenance Decision Analysis.* International Series in Operations Research & Management Science 231, ISBN: 978-3-319-17968-1. Springer International Publishing Switzerland, 2015.

DIEBER, B.; BREILING, B.; TAURER, S.; KACIANKA, S.; RASS, S.; SCHARTNER, P. Security for the Robot Operating System. *Robotics and Autonomous Systems*, 2017.

DOKAS, I. M.; FEEHAN, J., IMRAN, S. EWaSAP: An early warning sign identification approach based on a systemic hazard analysis. *Safety Science*, v. 58, p. 11-26, 2013.

DU, G.; LONG, S.; LI, F.; HUANG, X. Active Collision Avoidance for Human-Robot Interaction With UKF, Expert System, and Artificial Potential Field Method. *Frontiers in Robotics and AI*. v. 5, n. 125, 2018.

DUDA, T.; RAGHAVAN, L. V. 3D Metal Printing Technology. *IFAC-PapersOnLine*, v. 49, n. 29, p. 103-110, 2016.

DUNJO, J.; FTHENAKIS, V.; VILCHEZ, J. A.; ARNALDOS, J. Hazard and operability (HAZOP) analysis. A literature review. *Journal of Hazardous Materials*. v. 173, p. 19-32, 2010.

DUZGUN, H. S.; LEVESON, N. Analysis of soma mine disaster using causal analysis based on systems theory (CAST). *Safety Science*, v. 110, p. 37-57, 2018.

EDWARDS, P.; RAMIREZ, P. When should workers embrace or resist newtechnology? *New technology, work and employment*, v. 31, n. 2, p. 99-113, 2016.

ERDEI E.; POP J.; OLAH J. Comparison of time-oriented methods to check manufacturing activities and na examination of their efficiency. *LogForum*. v. 14, n. 3, p. 371-386, 2018.

FAIRLEY, P. Cybersecurity at u.s. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory. *IEEE Spectrum*. v. 53, n. 5p. 11-13, 2016.

FLAGE, R.; AVEN, T. Emerging risk - conceptual definition and a relation to black swan types of events. *Reliability Engineering and System Safety*, v. 144, p. 61-67, 2015.

FLEISCH, E.; WEINBERGER, M.; WORTMANN, F. Geschäftsmodelle im Internet der Dinge. *HMD Praxis der Wirtschaftsinformatik*. v. 51, n. 6, p. 812-826, 2014.

GANDOMI, A.; HAIDER, M. Beyond the hype: Big data concepts, methods, and analytics. *Int. J. Inf. Manage*. v. 35, n. 2, p. 137-144, 2015

GANTZ, J.; REINSEL, D. Extracting value from chaos. *IDC iview*. v. 1142, n. 2011, p. 1-12, 2011.

GAO, W.; YU, W.; LIANG, F.; HATCHER, W. G.; LU, C. Privacy-preserving auction for big data trading using homomorphic encryption. *IEEE Transactions on Network Science and Engineering*. p. 1-1, 2018.

GARRIDO-HIDALGO, C.; HORTELANO, D.; RODA-SANCHEZ, L.; OLIVARES, T.; RUIZ, M. C.; LOPEZ, V. IoT Heterogeneous Mesh Network Deployment for Human-in-the-Loop Challenges Towards a Social and Sustainable Industry 4.0. *IEEE Access*. v. 6, 2018.

GASPAR, R.; GIGER, J.-C. Emerging technologies, Emerging Risks: Current Approaches on the Future Risks of Human Enhancement Technologies. *Hum Behav & Emerg Tech*. v. 1, p. 6768, 2019.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4ª ed. São Paulo: Editora Atlas, 2002.

GOBBO, J. A. J.; BUSSO, C. M.; GOBBO, S. C. O.; CARREÃO, H. Making the links among environmental protection, process safety, and industry 4.0. *Process Safety and Environmental Protection*. Bauru-SP, n. 117, p. 372-382, 2018.

GORECKY, D.; SHIMITT, M.; LOSKYLL, M.; ZUHLKE, D. Human-Machine-Interaction in the Industry 4.0 Era. *IEEE*, 2014.

GRAETZ, G.; MICHAELS, G. Robots at Work: CEP Discussion Papers. *Centre for Economic Performance*. London. n. 1335, 2015.

GUBBI, J.; BUYYA, R.; MARUSIC, S.; PALANISWAMI, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* v. 29, p. 1645-1660, 2013.

GUNES, V.; PETER, S.; GIVARGIS, T.; VAHID, F. A survey on concepts, applicationsand challenges in Cyber-Physical Systems. *KSII Trans. Internet Inf. Syst*. v. 8, n. 12, p. 4242-4268, 2014.

GUPTA, S.; RAJIAH, P.; MIDDLEBROOKS, E. H.; BARUAH, D. CARTER, B. W.; BURTON, K. R.; CHATTERJEE, A. R.; MILLER, M. M. Systematic Review of the Literature: Best Practices. *Academic Radiology*, v. 25, n. 11, p. 1481-1490, 2018.

HALE, A. R.; HOVDEN, J. Management and Culture: The Third Age of Safety. A Review of Approaches to Organisational Aspects of Safety, Health and Environment. In Occupational Injury. *Risk, Prevention and Intervention*, P. 129-166, 1998.

HECKMANN, I.; COMES, T.; NICHEL, S. A critical review on supply chain risk - Definition, measure and modeling. *Omega*, v. 52, p. 119-132, 2015.

HIRSCH-KREINSEN, H. Digitization of industrial work: development paths and prospects. *J Labour Market Res*. v. 49, p. 1-14, 2016.

HOLLNAGEL, E.; WOODS, D. D. Cognitive Systems Engineering: New Wine in New Bottles. International Journal of Man - Machine Studies. v. 18, n. 6, p. 583-600, 1983.

HOUTMAN, I.; DOUWES, M.; ZONDERVAN, E.; JONGEN, M. Monitoramento dos riscos novos e emergentes.

HSIEH, H. C.; CHANG, K. D.; WANG, L. F.; CHEN, J. L.; CHAO, H. C. ScriptIoT: A Script Framework for and Internet-of-Things Applications. *IEEE Internet of Things Journal*. v. 3, n. 4, p. 628-636, 2016.

HU J.; ZHENG L.; XU S. Safety analysis of wheel brake system based on STAMP/STPA and Monte Carlo simulation. *Journal of Systems Engineering and Electronics*. v. 29, p. 1327- 1339, 2018.

HUNG-LIN, T.; CHI-LEE, C.; HAO-CHANG, C. WSN Integrated Authentication Schemes Based on Internet of Things. *Journal of Internet Technology*. v. 19, n. 4, p. 1043-1053, 2018.

ISAKSSON, A. J.; HARJUNKOSKIB, L.; SANDD, G. The impact of digitalization on the future of control and operations. *Computers and Chemical Engineering*. Suiça. v. 114, p. 122-129, 2018.

JIANG, Y.; YIN, S. Recursive total principle component regression based fault detection and its application to Vehicular Cyber-Physical Systems. *IEEE Trans. Ind. Inf.* v. 4, p. 1415-1423, 2018.

KAMBLE, S. S.; GUNASEKARAN, A.; GAWANKAR, S. A. Sustainable industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives. Process Safety Environment Protection. v. 117, p. 408-425, 2018.

KAMP, B.; PARRY, G. Servitization and advanced business services as levers for competitiveness. *Ind. Mark. Manag*. v. 60, p. 11-16, 2017

KAPLAN, S.; GARRICK, B. J. On the quantitative definition of risk. *Risk Analysis*. v. 1, p. 11-27, 1981.

KHALID, A.; KIRISCI, P.; KHAN, Z. H.; GHRAIRI, Z.; THOBEN, K.-D.; PANNEK, J. Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*. v. 97, p. 132-145, 2018;

KIRWAN, B.; AINSWORTH, L. *A Guide to Task Analysis.* London: Taylor & Francis. 1992.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing Systematic Literature Reviews in Software Engineering. 2.3 ed. UK: Keele University and Durham University: *EBSE Technical Report*, 2007. v. 2

KLEIN, G. A.; CALDERWOOD, R.; MACGREGOR, D. Critical Decision Method for Eliciting Knowledge. *IEEE Transactions on Systems, Man, and Cybernetics*. v. 19, n. 3, p. 462-472, 1989.

KLEIN, G. A.; ORASANU, J.; CALDERWOOD, R.; ZSAMBOK, C. E. Decision Making in Action: Models and Methods. Norwood, NJ: Ablex. 1993.

KLETZ, T. A. HAZOP and HAZAN: *Notes on the Identification and Assessment of Hazards*. Rugby: Institute of Chemical Engineers. 1983.

KOBARA, K. Cyber Physical Security for Industrial Control Systems and IoT. *IEICE Trans. Inf. & Syst*. v. E99-D, n. 4, p. 787-795 2016.

KUMAR, S.; MOOKERJEE, V.; SHUBHAM, A. Research in Operations Management and Information Systems Interface. *Production and Operations Management*. v. 27, n. 11, p. 1893-1905, 2018.

LASI, H.; FETTKE, P.; KEMPER, H. G.; FELD, T.; HOFFMANN, M. "Industry 4.0," *Business & Information Systems Engineering*. v. 6, n. 4, p. 239-242, 2014.

LAWLESS, W. F.; MITTU, R.; SOFGE, D.; RUSSEL, S. *Autonomy and Artificial Intelligence: A Threat or savior?* Springer, 2017.

LEE, I.; LEE, K. The Internet of Things (IoT) Applications, investments and challenges for enterprises. *Bussiness Horiz.* v. 58, p. 431-440, 2015.

LEE, J.; BAGHERI, B.; KAO, H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*. v. 3, p. 18-23, 2015.

LEE, J.; KAO, H.; YANG, S. Service innovation and smart analytics for Industry 4.0 and big data environment. *Proceedings of the 6th CIRP Conference on Industrial Product-Service Systems*. v. 16, p. 3-8, 2014.

LEVESON, N. A new accident model for engineering safer systems. *Safety Science*. v. 42, p. 237-270, 2004.

LEVESON, N. G. *An STPA Primer*. 2013.

LEVESON, N. G. *Engineering a Safer World: Systems Thinking Applied to Safety*. Londres: Editora Board, 2012.

LEVESON, N. G.; THOMAS, J. P. *STPA Handbook*. 2018.

LIANG, F.; YU, W.; NA, D.; YANG, Q.; FU, X.; ZHAO, W. A survey on big data market: Pricing, trading and protection. *IEEE Access*. v. 6, p. 15132-15154, 2018.

LU, Y. Industry 4.0: a survey on technologies, applications and open research issues. *Journal of Industrial Information Integration*, v. 6, p. 1-10, 2017.

LUKAC, D. The fourth ICT-based industrial revolution, 23rd Telecommunications Forum Telfor, IEEE. p. 835-838, 2015.

MANNAN, M. S.; REYES-VALDES, O.; JAIN, P.; TAMIM, N.; AHAMMAD, M. The Evolution of Process Safety: Current Status and Future Direction. *Annu. Rev. Chem. Biomol. Eng*. v. 7, n. 5, p. 1-28, 2016.

MANOGARAN; GUNASEKARAN; VARATHARAJAN, R.; LOPEZ, D.; THOTA, C. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. *Future Generation Computer Systems.* v. 82, p. 375-387, 2018.

MARHAVILAS, P.K.; KOULOURIOTIS, D.; GEMENI, V. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000 e 2009. *Journal of Loss Prevention in the Process Industries*. v. 24, p. 477-523, 2011.

MARYSKA, M.; DOUCEK, P.; NEDOMOVA, L.; SLADEK, P. The Energy Industry in the Czech Republic: On the Way to the Internet of Things. *Economies*. v. 6, n. 36, 2018.

MATTERN, F.; FLOERKEMEIER, C. Vom Internet der Computer zum Internet der Dinge. *Informatik-Spektrum*. v. 33, n. 2, p. 107-121, 2010.

MELL, P.; GRANCE, T. The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. Special Publication v. 800, n. 145, 2011.

MENG, X.; CHEN, G.; SHI, J.; ZHU, G.; ZHU, Y. STAMP-based analysis of deepwater well control safety, *Journal of Loss Prevention in the Process Industries*. 2018.

MOKTADIR, M. A.; ALI, S. M.; KUSI-SARPONG, S.; SHAIKH, M. A. A. Assessing challenges for implementing industry 4.0: Implications for process safety and environmental protection. *Process Safety Environment Protection.* v. 117, p. 730-741, 2018.

MOLANO, J. I. R.; LOVELLE, J. M. C.; MONTENEGRO, C. E.; GRANADOS, J. J. R.; CRESPO, R. G. Metamodel for integration of Internet of Things, Social Networks, the Cloud and Industry 4.0. *Journal Ambient Intell Human Comput*. 2017

MONGEON, P.; PAUL-HUS, A. The journal coverage of Web of Science and Scopus:a comparative analysis. *Scientometrics*, v. 106, p. 213–228, 2016.

MONOSTORI, L. Cyber-physical production systems: Roots, expectations and R&D challenges. *Procedia CIRP*. v. 17, p. 9–13, 2014.

MONTAGUE, D. F. Process risk evaluation—what method to use? *Reliability Engineering & System Safety*. v. 29, n. 1, p. 27-53, 1990.

MORRAR, R.; ARMAN, H.; MOUSA, S. The Fourth Industrial Revolution (Industry 4.0): A Social Innovation Perspective. 2017.

MOURTZIS, D.; VLACHOU, E. A cloud-based cyber-physical system for adaptive shop-floor scheduling and condition-based maintenance. *Journal of Manufacturing Systems*. Patras, v. 47, p. 179–198, 2018.

MOURTZIS, D.; VLACHOU, E.; MILAS, N. Industrial big data as a result of IoT adoption in manufacturing. *Procedia CIRP*. v. 55, p. 290-295, 2016.

MOZZAQUATRO, B. A.; AGOSTINHO, C.; GONCALVES, D.; MARTINS, J.; JARDIM-GONCALVES, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors*, v. 18, 2018.

MULLER, C.; GRUNEWALD, M.; SPENGLER, T. S. Redundant Configuration of Automated Flow Lines Based on 'Industry 4.0'-Technologies. *Journal of Business Economics*. v. 87, n. 7, p. 877-898, 2017b.

MULLER, C.; GRUNEWALD, M.; SPENGLER, T. S. Redundant configuration of robotic assembly lines with stochastic failures. *International Journal of Production Research*, 2017a.

NAGY, J.; OLAH, J.; ERDEI, E.; MATE, D.; POPP, J. The Role and Impact of Industry 4.0 and the Internet of Things on the Business Strategy of the Value Chain - The Case of Hungary. *Sustainability*. Budapeste, v. 10, 2018.

NETO, G. A. A.; ALENCAR, M. H. Estudo do método STAMP e técnica STPA para análise sistêmica de riscos: uma revisão sistemática da literatura. *XXXIX Encontro Nacional de Engenharia de Producao*, Santos: SP, 2019.

NILSEN, T.; AVEN, T. Models and model uncertainty in the context of risk analysis. *Reliability Engineering and System Safety*. v. 79, p. 309-317, 2003.

NILSSON, N. J. *Principles of artificial intelligence*. Stanford university. 2014.

OLIVEIRA, U. R.; MARINS, F. A. S.; ROCHA, H. M.; SALOMON, V. A. P. The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production*, 2017.

PASHA, M.; QAISER, G.; PASHA, U. A Critical Analysis of Software Risk Management Techniques in Large Scale Systems. *IEEE Access*, 2018.

PENDER, S. Managing incomplete knowledge: why risk management is not sufficient. *International Journal of Project Management*, v. 19, p. 79-87, 2001.

PFOHL, H. Ch.; YAHSI, B.; KURNAZ, T. The impact of Industry 4.0 on the supply chain. *Proceedins of the Hamburg International Conference of Logistics (HICL)*. p. 29-58, 2015.

PIETRE-CAMBACEDES, L.; BOUISSOU, M. Cross-fertilization between safety and security engineering. *Reliability Engineering and System Safety*. v. 110, p. 110-126, 2013.

PILLONI, V. How DataWill Transform Industrial Processes: Crowdsensing, Crowdsourcing and Big Data as Pillars of Industry 4.0. *Future Internet*. Cagliari, v. 10, n. 24, 2018.

PINTO, A.; NUNES, I. L.; RIBEIRO, R. A. Occupational risk assessment in construction industry - Overview and reflection. *Safety Science*. v. 49, p. 616-624, 2011.

PIRVU, B.-C.; ZAMFIRESCU, C.-B.; GORECKY, D. Engineering insights from na anthropocentric cyber-physical system: a case study for an assembly station. *Mechatronics*. v. 34, p. 147-159, 2016.

PLACKE, M. S. Application of stpa to the integration of multiple control systems: a case study and new approach. 2012.

PMI. Um guia do conhecimento em gerenciamento de projetos. Guia PMBOK® 6a. ed. EUA: Project Management Institute, 2017.

POPP, J.; EREDEI, E.; OLAH, J. A precíziós gazdálkodás kilátásai Magyarországon. *International Journal Engineering Management Science*. v. 3, p. 133-147, 2018.

PORTER, M. E.; HEPPELMAN, J. E. How smart, connected products are transforming competition. *Harvard Business Review*. v. 92, p. 64-88, 2014

PREUVENEERS, D.; ILIE-ZUDOR, E. The intelligent industry of the future: A survey on emerging trends, research challenges and opportunities in Industry 4.0. *Journal of Ambient Intelligence and Smart Environments*. v. 1, p. 1-12, 2017.

PUISA, R.; LIN, L.; BOLBOT, V.; VASSALOS, D. Unravelling causal factors of maritime incidents and accidents. *Safety Science*. v. 110, p. 124-141, 2018.

QI, Q.; TAO, F. Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison. *IEEE ACCESS*. v. 6, p. 3585-3593, 2018

QIN, J.; LIU, Y.; GROSVENOR, R. A Categorical Framework of Manufacturing for Industry 4.0 and Beyond. *Procedia CIRP*. v. 52, p. 173-178, 2016.

RASMUSSEN, J. *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*. New York: North-Holland. 1986.

RASMUSSEN, J. Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*, v. 27, p. 183-213, 1997.

RAYA, M.; HUBAUX, J.-P. Securing vehicular ad hoc networks, *Journal Computing Security*. v. 15, p. 39-68, 2007.

READ, G. J. M.; SALMON, P. M.; LENNE, M. G.; STANTON, N. A. Designing Sociotechnical Systems with Cognitive Work Analysis: Putting Theory Back into Practice. *Ergonomics*, v. 19, p. 1-30, 2014.

REINHART, G.; ENGELHARDT, P.; GEIGER, F.; PHILIPP, T. R.; WAHLSTER, W.; ZUHLKE, D.; SCHLICK, J.; BECKER, T.; LOCKLT, M.; PIRVU, B.; et al. CYBER physical Production-Systeme: Enhancement of Productivity and Flexibility by Networking of Intelligent Systems in the Factor. p. 84-89, 2013.

REIS, M. S.; KENETT, R. Assessing the Value of Information of Data-Centric Activities in the Chemical Processing Industry 4.0. *AIChE Journal*. Nova Iorque, v. 64, n. 11, p. 3868-3881, 2018.

RODA-SANCHEZ, L.; GARRIDA-HIDALGO, C.; HORTELANO, D.; OLIVARES, T.; RUIZ, M. C. OperaBLE: An IoT-Based Wearable to Improve Efficiency and Smart Worker Care Services in Industry 4.0. *Journal of Sensors*. 2018.

RODSETH, H.; SCHJOLBERG, P.; MARHAUG, A. Deep digital maintenance. *Advanced Manufacturing*. v. 5, p. 299-310, 2017.

ROSSMANN, M.; KHADIKAR, A.; LE FRANC, P.; PEREA, L.; SCHNEIDER-MAUL, R.; BUVAT, J.; GHOSH, A. Smart Factories: How can manufacturers realize the potential of digital industrial revolution. CAPGEMINI CONSULTING. 2017

RUBMANN, M.; LORENZ, M.; GERBERT, P.; WALDNER, M.; JUSTUS, J.; ENGEL, P.; HARNISCH, M. Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries. *Boston Consulting Group*. Boston, p. 1-14, 2015.

RYMASZEWSKA, A.; HELO, P.; GUNASEKARAN, A. IoT powered servitization of manufacturing - An exploratory case study. *Int. J. Prod. Econ*. v. 192, p. 92-105, 2017.

SALMON, P. M.; CORNELISSEN, M.; TROTTER, M. J. Systems-based accident analysis methods: A comparison of Accimap, HFACS, and STAMP. *Safety Science*, v. 50, p. 1158-1170, 2012.

SANTOS JR, E.; ZHAO Y. Automatic Emergence Detection in Complex Systems. Hindawi - Complexity. 2017.

SCHWAB, K. *A quarta revolução industrial*. São Paulo: Editora Edipro, 2016.

SEVERINO, A. J. *Metodologia do trabalho científico*. 2. ed. São Paulo: Editora Cortez, 2017.

SHIN, S.; KWON, T.; JO, G.-Y.; PARK, Y.; RHY, H. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. *Industrial Informatics*. v. 6, n. 4, p. 744-757, 2010.

SII, H.S.; WANG, J.; RUXTON, T. Novel risk assessment techniques for maritime safety management system. *International Journal of Quality and Reliability Management*. v. 18, n. 8, p. 982-999, 2001.

SILVA, E. L.; MENEZES, E. M. *Metodologia da pesquisa e elaboração de dissertação*. 4. ed. rev. atual. Florianópolis: UFSC. 138p, 2005.

SILVA, M.; VIEIRA, E.; SIGNORETTI, G.; SILVA, I.; SILVA, D.; FERRARI, P. A Customer Feedback Platform for Vehicle Manufacturing Compliant with Industry 4.0 Vision. *Sensors*. v. 18, 2018.

SISSINI, E.; SAIFULLAH, A.; HAN, S.; JENNEHAG, U.; GILLUND, M. Industrial Internet of Things: Challenges, Opportunities, and Directions. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, v. 10, n. 10, 2018.

SLUSARCZYK, B. Industry 4.0 - Are we ready? Pol. *Journal Management Study*. v. 17, 2018.

STANKAVIC, J. A. Research directions for the internet of things. *IEEE Internet Things journal*. v. 1, p. 3-9, 2014.

STORTI, E.; CATTANEO, L.; POLENGHI, A.; FUMAGALLI, L. Customized Knowledge Discovery in Databases methodology for the Control of Assembly Systems. *Machines*. v. 6, 2018

STRINGFELLOW M. V.; LEVESON N. G.; OWENS B. D. Safety-Driven Design for Software-Intensive Aerospace and Automotive Systems. *Proceedings of the IEEE*, v. 98. n. 4, 2010.

SZOZDA, N. Industry 4.0 and its impact on the functioning of supply chains. LogForum - *Scientific Journal of Logistics*. v. 13, n. 4, p. 401-414, 2017.

TAO, F.; ZHANG, M. Digital Twin Shop-Floor: A New Shop-Floor Paradigm Towards Smart Manufacturing. *IEEE Access*. v. 5, 2017.

TIXIER, J.; DUSSERRE, G.; SALVI, O.; GASTON, D. Review of 62 risk analysis methodologies of industrial plants. *Journal of Loss Prevention in the Process Industries*. v. 15, p. 291-303, 2002.

TORO, C.; BARANDIARAN, I.; POSADA, J. A perspective on Knowledge Based and Intelligent systems implementation in Industrie 4.0. *Procedia Comput. Sci*. v. 60, p. 362-370, 2015.

TUPTUK, N.; HAILES, S. Security of smart manufacturing systems. *Journal of Manufacturing Systems*. Londres, v. 47, p. 93–106, 2018.

VARGHESE, A.; TANDUR, D. Wireless requirements and challenges in Industry 4.0. *International Conference on Contemporary Computing and Informatics*. P. 634-638, 2014.

VICENTE, K. J. *Cognitive Work Analysis: Toward Safe, Productive, and Healthy Computer-Based Work*. Mahwah, NJ: Lawrence Erlbaum. 1999.

WAN, J.; YANG, J.; WANG, Z.; HUA, Q. Artificial Intelligence for Cloud-assisted Smart Factory. IEEE *Access*. Guangzhou. 2018

WATERSON, P.; ROBERTSON, M. M.; COOKE, N. J.; MILITELLO, L.; ROTH, E.; STANTON, N. A. Defining the methodological challenges and opportunities or an effective science of sociotechnical systems and safety, *Ergonomics*, v. 58, n. 4, p. 565-599, 2015.

WEINBERGER, M.; BILGERI, D.; FLEISCH, E. IoT business models in an industrial context. *Automatisierungstechnik*. v. 64, n. 9, p. 699-706, 2016.

WIENER, N. Cybernetics: *Or the control and communication in the animal and the machine*. 2 Ed. Cambridge: MIT Press, 1965.

WOODS, D. D.; HOLLNAGEL, E. Mapping Cognitive Demands in Complex Problem-Solving Worlds. *International Journal of Man - Machine Studies*. v. 26, n. 2, p. 257-275, 1987.

WOODS, D. D.; ROTH, E. M. Cognitive Engineering: Human Problem Solving with Tools. *Human Factors*. v. 30, n. 4, p. 15-430, 1988.

XU, H.; YU, W.; GRIFFITHY, D.; GOLMIEY, N. A Survey on Industrial Internet of Things: A Cyber-Physical *Systems Perspective*. 2018.

YAMADA, V. Y.; MARTINS L. M. INDÚSTRIA 4.0: UM COMPARATIVO DA INDÚSTRIA BRASILEIRA PERANTE O MUNDO. *Revista Terra & Cultura: Cadernos de Ensino e Pesquisa*. v. 34, n. especial, 2018

YAN, J.; MENG, Y.; LU, L.; LI, L. Industrial Big Data in an Industry 4.0 Environment: Challenges, Schemes and Applications for Predictive Maintenance. *IEEE Access*. v. 10, 2017.

YU, X.; NGUYEN, B.; CHEN, Y. Internet of things capability and alliance: entrepreneurial orientation, market orientation and product and process innovation. *Internet Research*, v. 26, n. 2, p. 402-434, 2016.

ZHENG, P.; SANG, Z.; ZHONG, R. Y.; LIU, Y.; LIU, C.; MUBAROK, K.; YU, S.; XU, X. Smart manufacturing systems for industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering*, p. 1–14, 2018.