ALAIDE BARBOSA MARTINS

**Desenvolvimento de uma metodologia para gestão de risco com
base no método CORAS e avaliação quantitativa para aplicação em
plantas de saneamento**

São Paulo

2014

ALAIDE BARBOSA MARTINS

**Desenvolvimento de uma metodologia para gestão de risco com
base no método coras e avaliação quantitativa para aplicação em
plantas de saneamento**

Tese apresentada à Escola
Politécnica da Universidade de São
Paulo para obtenção do título de
Doutora em Ciências.

Área de Concentração:
Sistemas Eletrônicos

Orientador:
Prof. Dr. Sergio Takeo Kofuji

São Paulo

2014

Este exemplar foi revisado e corrigido em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, 28 de janeiro de 2014.

Assinatura do autor _____

Assinatura do orientador _____

FICHA CATALOGRÁFICA

Martins, Alaide Barbosa

Desenvolvimento de metodologia para análise de risco com base no método CORAS e avaliação quantitativa para aplicação de plantas de saneamento / A.B. Martins. -- versão corr. -- São Paulo, 2014.

149 p.

Tese (Doutorado) - Escola Politécnica da Universidade de São Paulo. Departamento de Engenharia de Sistemas Eletrônicos.

1. Análise de risco I. Universidade de São Paulo. Escola Politécnica. Departamento de Engenharia de Sistemas Eletrônicos II. t.

Dedico este trabalho a Valmir Martins, meu esposo, pelo seu carinho e apoio, que sempre me auxilia a superar as barreiras mais difíceis; à Laila, minha querida filha, que é tão parecida comigo; à minha pequena Lara Judith, que é a minha alegria e uma fonte de sabedoria; e a todos que sempre me incentivaram para que eu atingisse todos os meus objetivos.

AGRADECIMENTOS

A Deus, que sempre está ao meu lado, me orientando e abrindo meus caminhos.

A toda a minha família, que por inúmeras vezes compreenderam minha ausência durante o período de elaboração deste trabalho.

Ao Prof. Dr. Sergio Takeo Kofuji, por sua orientação e disponibilidade, e aos demais colegas do LSI, especialmente Marcelo Teixeira de Azevedo, pela constante ajuda e apoio.

Aos amigos da Organização Odebrecht e da Faculdade Dom Pedro Segundo que apoiaram e colaboraram com a pesquisa.

Tudo quanto te vier à mão para fazer, faze-o
conforme as tuas forças.
(Eclesiastes 9:10)

RESUMO

Gradualmente a sociedade mundial tem se tornado mais dependente de sistemas automatizados, bem como, as diversas plantas de saneamento estão se modernizando e integrando as infraestruturas existentes de redes corporativas. Portanto, conforme o cenário de desenvolvimento tecnológico em que se encontra a área de segurança da informação (security) e da segurança do processo (safety) propôs-se nesta pesquisa uma metodologia em gestão de riscos com análise quantitativa, por meio da utilização do método Consultative Objective Risk Analysis System (CORAS) e função *Reliability*, utilizando a modelagem matemática de Markov, para a realização da gestão de risco em plantas de saneamento. Os resultados obtidos pela metodologia de gestão de risco foram validados por meio da aplicação em estudo de caso na planta de saneamento, especificamente uma elevatória de esgoto com a vazão de 2,3 m³/s localizada no município de Salvador na Bahia. Ao implantar a metodologia verificou-se que elevatória possui a confiabilidade de 98,78%, além de identificar e classificar os riscos existentes ao processo, contemplando a avaliação com uma visão sistêmica envolvendo a segurança do processo e da informação.

Palavras-chave: Análise de risco. Automação. Saneamento. Segurança.

ABSTRACT

Gradually the world society has become more dependent on automated systems, as well as the various plants sanitation are modernizing and integrating existing infrastructure of corporate networks. Therefore, depending on the scenario in which technological development is the area of information security and process safety proposed in this research methodology for risk management with quantitative analysis, by using the method Consultative Objective risk Analysis System (CORAS) Reliability and function, using mathematical modeling Markov for the realization of risk management in plant sanitation. The results obtained by the methodology of risk management were validated by applying on a case study on a wastewater treatment plant, particularly a pumping sewage with flow rate of $2.3 \text{ m}^3 / \text{s}$ located in the city of Salvador in Bahia. When deploying the methodology it was found that the lift has a 98.78% reliability, and identify and classify the existing process risks, contemplating the review with a systemic vision involving process safety and information.

Keywords: Risk analysis. Automated. Wastewater. Safety.

LISTA DE FIGURAS

Figura 1 – Princípio <i>As Low as Reasonably Possible</i> (ALARP).....	30
Figura 2 – Ciclo de Vida – IEC 61508.	35
Figura 3 – Curva da banheira.....	40
Figura 4 – Elementos básicos do FMEA.	43
Figura 5 – Etapas do FTA.	48
Figura 6 – Diagrama da ISO/IEC 31000.....	50
Figura 7 – Grafo de Estados - Markov.....	58
Figura 8 – Cenário sugerido pela ISA 99.....	66
Figura 9 – Padrões de Gestão de SGSI e Riscos.	73
Figura 10 – Sistema serial simples.....	78
Figura 11 – Ciclo da metodologia de gestão de risco.	82
Figura 12 – Diagrama de estados.	88
Figura 13 – <i>Software</i> CARMS – versão 1.1.....	90
Figura 14 – Cadeia de Markov para o sistema de bombeamento.....	91
Figura 15 – Gráfico da cadeia de Markov.	92
Figura 16 – Sistema de bombeamento no CORAS.	93
Figura 17 – CORAS Platform.	94
Figura 18 – Diagrama de ameaças.	97
Figura 19 – Gráfico da função densidade.....	98
Figura 20 – Gráfico função de risco.	99
Figura 21 – Gráfico função confiabilidade.	99
Figura 22 – Diagrama de risco.	100
Figura 23 – Passos para implantação do CORAS.....	102
Figura 24 – Conhecendo o ambiente.	104
Figura 25 – Diagrama de ameaças – CORAS.....	107
Figura 26 – Diagrama de ameaças com estimativas.	109
Figura 27 – Diagrama de tratamento de risco.	110
Figura 28 – Análise de risco.....	112

LISTA DE QUADROS

Quadro 1 – Níveis do SIL.	35
Quadro 2 – Fórmulas da função <i>reliability</i>	37
Quadro 3 – Escala de severidade.	45
Quadro 4 – Escala de ocorrência.	45
Quadro 5 – Escala de detecção.	46
Quadro 6 – Planilha de probabilidade de estado em 4 passos.....	59
Quadro 7 – Recomendações da ISA 99.	67

LISTA DE TABELAS

Tabela 1 – Planilha de cálculo da probabilidade do estado parado $P(0)$	59
Tabela 2 – Classificação do efeito.	76
Tabela 3 – Falhas dos componentes.	88
Tabela 4 – Tabela de transição de estado.	89
Tabela 5 – Matriz de transição dos estados.	92
Tabela 6 – Matriz de ativos.	95
Tabela 7 – Matriz de nível de risco.	95
Tabela 8 – Matriz de consequência.	96
Tabela 9 – Matriz de consequência x penalidades.	96
Tabela 10 – Matriz de probabilidade x frequência.	96
Tabela 11 – Matriz de referências para análise de risco.	96
Tabela 12 – Matriz de falhas.	98
Tabela 13 – Diagrama de ativo.	105
Tabela 14 – Escala de consequência.	105
Tabela 15 – Escala de consequência x penalidades.	106
Tabela 16 – Probabilidade x frequência.	106
Tabela 17 – Referências para análise de risco.	106
Tabela 18 – Análise de risco qualitativo.	109

LISTA DE ABREVIATURAS E SIGLAS

ALARP	<i>As Low as Reasonably Practicable</i>
ANSI	American National Standards Institute
API	<i>Application Programming Interface</i>
CARMS	<i>Computer-Aided Rate Modeling and Simulation</i>
CCM	Central de Controle de Motores
CCO	Centro de Controle de Operações
CLP	Controlador Lógico Programável
CORAS	<i>Consultative Objective Risk Analysis System</i>
CRAMM	<i>CCTA Risk Analysis and Management Method</i>
DFMEA	<i>Design Failure Modes and Effects Analysis</i>
DoS	<i>Denial of Service</i>
EEE	Estação Elevatória de Esgoto
FIPS	Federal Information Processing Standards
FMEA	Análise de Modos e Efeitos de Falhas
FMECA	<i>Failure Mode Effects and Criticality Analysis</i>
FTA	<i>Fault Tree Analysis</i> – Análise da Árvore de Falhas
HAZID	<i>Hazard Identification Studies</i>
HAZOP	<i>Hazard and Operability Study</i> – Estudo de Perigo e Operabilidade
HST	<i>Homeland Security Technologies</i>
IDMEF	<i>Intrusion Detection Messaging Exchange Format</i>
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISA	International Society of Automation
ISO	International Organization for Standardization
LOPA	<i>Layer Of Protection Analysis</i>
MTBF	<i>Mean Time Between Failure</i> – Tempo Médio entre Falhas
OMG	Object Management Group
PES	<i>Programmable Electronic Safety</i>
PFMEA	<i>Process Failure Modes and Effects Analysis</i>
PPP	Participação Pública-Privada
QID	Quadro Indicador de Desempenho
RRF	<i>Risk Reduction Factor</i> – Fator de Redução de Risco

SCADA	<i>Supervisory Control and Data Acquisition</i>
SIL	<i>Safety Integrity Levels</i>
SIS	Sistema de Segurança Instrumentado
SSPP	<i>System Safety Program Plan</i>
TBF	<i>Time Between Failure</i> – Tempo entre Falhas
TMF	Tempo Médio de Falha
TTF	<i>Time to Failure</i> – Tempo até a Falha
UML	<i>Unified Modeling Language</i>
UP	<i>Unified Process</i>
USEPA	US <i>Environmental Protection Agency</i>
VOCs	<i>Volatile Organic Compounds</i>
VPN	<i>Virtual Private Network</i>
XMI	<i>XML Metadata Exchange</i>
XML	<i>eXtensible Markup Language</i>

LISTA DE SÍMBOLOS

β	Parâmetro de forma da distribuição Weibull
$h(t)$	Função taxa de falhas
λ	Taxa de falhas
λ_s	Taxa de falhas sistema série
λ_p	Taxa de falhas sistema paralelo
$\lambda(i)$	Taxa de falha /ano
$r(i)$	Tempo de reparo
r_s	Tempo de reparo de componentes em série
r_p	Tempo de reparo de componentes em paralelo
$R(t)$	Função confiabilidade
T	Parâmetro de espaço (discreto ou contínuo)
t	Parâmetro de tempo (contínuo)
n	Janelas temporais ou passos do processo (de parâmetro discreto)
ij	Probabilidade de transição direta do estado i para o estado j
A	Matriz infinitesimal geradora da cadeia de Markov
$P(0)$	Condições iniciais do processo markoviano
T	Tempo de ciclo (de falha e reparação)
f	Frequência de visitas ou entrada num determinado estado

SUMÁRIO

1 INTRODUÇÃO	17
1.1 OBJETIVOS	22
1.1.1 Objetivo Geral	22
1.1.2 Objetivos Específicos	22
1.2 CONTRIBUIÇÕES	23
1.3 SOLUÇÃO PROPOSTA.....	24
1.4 JUSTIFICATIVAS	24
1.5 DESCRIÇÃO DO PROBLEMA.....	26
1.6 MATERIAIS E MÉTODOS.....	27
1.7 ORGANIZAÇÃO DO TEXTO.....	28
2 FUNDAMENTAÇÃO TEÓRICA.....	30
2.1 SEGURANÇA DO PROCESSO – SAFETY	31
2.1.1 Norma de Segurança do Processo - IEC 61508	32
2.1.2 Tempo Médio Entre Falhas - MTBF.....	36
2.1.3 O Padrão IEEE 493-2007 e Confiabilidade (Reliability)	36
2.1.4 Failure Mode and Effect Analysis (FMEA).....	41
2.1.5 Hazard and Operability Study (HAZOP).....	46
2.1.6 Fault Tree Analysis (FTA)	48
2.1.7 Consultative Objective Risk Analysis System (CORAS).....	49
2.1.7.1 Recursos do método CORAS.....	52
2.1.8 Processo Estocástico Markoviano	55
2.2 SEGURANÇA DA INFORMAÇÃO – SECURITY	63
3 ESTADO DA ARTE E TRABALHOS RELACIONADOS.....	68
3.1 TRABALHOS RELACIONADOS	69
3.2 ANÁLISE QUANTITATIVA DE RISCO E CONFIABILIDADE	74
4 METODOLOGIA PROPOSTA E VALIDAÇÃO POR ESTUDO DE CASO... 81	81
4.2 CENÁRIO DO ESTUDO DE CASO	86
4.3 APLICAÇÃO DA METODOLOGIA	93
4.4 DETALHAMENTO DO ESTUDO DE CASO COM CORAS	102

4.5 RESULTADOS	110
5 CONCLUSÃO	115
REFERÊNCIAS.....	119
APÊNDICES	123
APÊNDICE A – PUBLICAÇÕES	123
APÊNDICE B – FMEA	125
APÊNDICE C – HAZOP.....	127
APÊNDICE D – ESTIMATIVAS DOS RISCOS.....	129
APÊNDICE E – CENÁRIO DO ESTUDO DE CASO	136
APÊNDICE F – TRATAMENTO	143
ANEXO	146
ANEXO A – DIAGRAMAS FUNCIONAIS, INFRAESTRUTURA E UNIFILARES DO SDOJ	146
ANEXO B – RELATÓRIO DA AUDITORIA.....	149

1 INTRODUÇÃO

No contexto hodierno, gradualmente a sociedade mundial tem se tornado mais dependente de sistemas automatizados, bem como, as diversas plantas de saneamento estão se modernizando e integrando as infraestruturas existentes de redes corporativas. Nesse contexto, incidentes de segurança ocorrem diariamente na maioria das organizações, e os sistemas que nos rodeiam são vulneráveis a ataques.

Nessa conjuntura, a importância da análise de risco tem aumentado nas últimas décadas, devido a complexidade dos sistemas e as acentuadas implicações decorrentes, inclusive, de pequenas falhas. A segurança da informação não foi inicialmente uma prioridade no ambiente dos sistemas de controle, pois tradicionalmente esses sistemas eram constituídos de equipamentos isolados, não conectados à rede corporativa ou mesmo à internet, pois raramente necessitavam de integração com outros sistemas. Normalmente, a interconexão desses sistemas dava-se por meio de redes e protocolos proprietários, por isso, esses sistemas eram formados de tecnologias dedicadas, além de serem compostos de redes fechadas e sem nenhuma conectividade externa (KRUTZ, 2006).

Esse cenário tem sofrido grandes alterações nas duas últimas décadas, como a utilização do sistema operacional Microsoft Windows como base para os sistemas *Supervisory Control and Data Acquisition* (SCADA), que convergem para sistemas abertos e, em alguns casos, conectados à rede corporativa ou até mesmo à internet. Além das diversas soluções que são portadas para as *Applications Programming Interfaces* (APIs) da Microsoft, a adoção de padrões de rede, como a Ethernet e os protocolos de interconexão de mercado, trouxeram para os sistemas de controle uma condição mais “aberta” e “menos proprietária”, ou seja, heterogênea.

Da mesma forma, os ambientes de automação dos processos estão agregando as tecnologias de comunicação que permitem mobilidade e convergência, porém muitas vezes em detrimento da segurança, tornando essas redes suscetíveis a ataques.

Nessa conjuntura, existe a demanda de implantação de controle de segurança dos processos e análise de risco em unidades de serviços críticos, o que suscita a demanda de se avaliar riscos potenciais por questões materiais e problemas nas instalações, especialmente em plantas de saneamento.

Portanto, conforme o cenário de desenvolvimento tecnológico em que se encontra a área de segurança da informação (*security*) e da segurança do processo (*safety*), propôs-se nesta pesquisa uma metodologia em gestão de riscos que contempla a análise quantitativa, por meio da utilização do método *Consultative Objective Risk Analysis System* (CORAS) e *Reliability*, com a modelagem matemática de Markov, aplicada na realização de análise de risco em uma planta de saneamento.

Algumas das ferramentas e normas tradicionais de identificação e controle de risco do processo foram contempladas neste estudo, tais como: *Hazard and Operability Study* (HAZOP), *Fault Tree Analysis* (FTA), *Layer Of Protection Analysis* (LOPA), *Failure Mode Effects and Criticality Analysis* (FMECA), *International Electrotechnical Commission* (IEC) 61508, dentre outras. As empresas utilizam essas técnicas como base para o gerenciamento de segurança de processo, entretanto, em função da complexidade crescente dos sistemas e as severas implicações decorrentes das eventuais falhas no processo, torna-se cada vez mais relevante a utilização de combinações de técnicas para aperfeiçoar a análise de risco e verificar a confiabilidade do sistema.

Da mesma forma, os modernos sistemas de controle e automação industrial, em grande parte, são baseados em sistemas operacionais comerciais, implementações de protocolos e aplicações de comunicações desenvolvidas originalmente para o ambiente de tecnologia da informação. Sabe-se que muitos desses sistemas e implementações são vulneráveis aos ataques e, com as tecnologias abertas e padrões de internet, o conhecimento dessas vulnerabilidades podem ser facilmente utilizados por possíveis *hackers*. A conexão das plantas de processos críticos à internet ou a outras redes públicas expõe esses pontos vulneráveis aos possíveis invasores. Por isso, é preciso contemplar no processo de gestão de risco a análise dos riscos, a avaliação das falhas, além dos controles da segurança do processo (*safety*), e verificação das

vulnerabilidades da segurança da informação (*security*) nos sistemas de controle e automação industrial.

No âmbito dos sistemas de saneamento, os estudos citados durante o desenvolvimento desta pesquisa sobre o tema confirmam que o cenário de vulnerabilidade é o mesmo, pois, além de eventos físicos, estão sujeitas também à ataques cibernéticos que podem, por exemplo, interferir diretamente no sistema de dosagem de um determinado produto químico, contaminando a água ou mesmo levando à ocorrência de vazamentos de determinado produto, além da possibilidade de alteração de vazões de bombeamento de uma rede de distribuição e de transbordamento do efluente.

Conforme Kroll e King (2007), estudos da Força Aérea dos EUA, do *Corps of Engineers* e *Hach Homeland Security Technologies* (HST), calcularam que um ataque a sistemas de distribuição de água potável poderia ser montado com baixo investimento entre US\$ 0,05 e US\$ 5,00 por morte. Nesse exemplo, seriam utilizadas técnicas rudimentares com a capacidade de atingir milhares de pessoas em apenas poucas horas por meio de um método conhecido como ataque de refluxo, ou seja, uma técnica que utiliza o sistema de hidrante de incêndio e uma pequena bomba para injetar material contaminante no sistema, que seria rapidamente distribuído para as torneiras dos consumidores. Devido à vasta extensão da rede de distribuição, a garantia física do sistema de contra-ataque se tornaria impossível (KROLL; KING, 2007).

Não restam dúvidas de que as ameaças são diversas e podem vir de diversos modos, conforme se verifica no exemplo dos documentos que foram capturados no Afeganistão contendo textos que incluem os sistemas de tratamento de água como alvo de ataque do Al-Qaeda (KROLL, 2006); ou mesmo nas notícias veiculadas nos EUA no dia 6 de junho de 2011, que anunciavam a contaminação do sistema de abastecimento de água da cidade Somerset, Massachusetts, levando a proibição do consumo de água nas residências. A companhia de água teve o custo de aproximadamente US\$ 20 milhões para limpar a rede de distribuição, o que, embora fosse uma contaminação acidental, evidencia a fragilidade do sistema (FOX, 2011).

Muitos são os exemplos internacionalmente conhecidos de ações maliciosas e interrupções em redes de controle, veiculados em redes de noticiários e citados na Internet, tais como:

- 1997: adolescente invadiu a uma rede e interrompeu a comunicação terra-avião do Aeroporto de Worchester por seis horas;
- 1998: um garoto de 12 anos invadiu o sistema da barragem Roosevelt, assumindo o total controle do sistema SCADA de todas as comportas;
- 1998-2000: “Moonlight Maze” – por dois anos, *hackers* invadiram o Pentágono, NASA, DoE e laboratórios de pesquisa;
- Abril 2000: *hacker* acionou um sistema SCADA para extravasar milhões de litros de esgoto em pátios de um hotel, Hyatt Regency em Maroochydore, Queensland na Austrália;
- Abril 2000: *hackers* conseguiram assumir o controle da maior rede mundial de gasodutos (GAZPROM);
- Jan. 2003: o vírus, verme “Slammer”, infectou 300.000 computadores em quinze minutos, interrompendo o serviço 911 e linhas aéreas;
- Jan. 2003: o sistema de monitoramento de segurança da planta nuclear de Davis-Besse é derrubado por cinco horas pelo verme “Slammer”;
- Ago. 2003: CSX perde o controle da sinalização e expedição de 23 linhas férreas devido à contaminação por vírus;
- Ago. 2005: 175 companhias, incluindo grandes Organizações foram atacadas por verme Zotob;
- Ago. 2007: *hackers* derrubam os países mais conectados da Europa por duas semanas ;
- Set. 2007: vídeo do Laboratório Nacional de Idaho do DoE mostra a destruição remota de um amplo sistema SCADA;
- Nov. 2007: “Solar Sunrise” – três adolescentes invadem o sistema de logística da USAF em bases de apoio do Meio Leste;
- Jan. 2008: *hackers* desligam a iluminação em várias cidades e exigem pagamentos a título de extorsão;
- Mar. 2008: desligamento emergencial por dois dias da planta nuclear de Hatch devido a uma atualização de *software* de um computador.

A cada ano observa-se o crescimento de ocorrências de ataques a sistemas automatizados, conforme a revista Infoexame (2013):

A média diária mundial de ataques cibernéticos cresceu 42% em 2012 em relação a 2011, passando de 82 para 116. Sendo que o resultado contabiliza apenas ataques direcionados, ou seja, aqueles em que o invasor sabe a identidade da vítima - o que geralmente acontece em ações de espionagem industrial e de roubo de informações confidenciais. O setor mais afetado por esse tipo de crime foi o de manufatura, com 24%; em segundo lugar ficou a categoria que engloba os segmentos financeiro, de seguro e imobiliário, com 19%; serviços não tradicionais ficaram em terceiro, com 17%; o governo somou 12%; energia sofreu 10% dos ataques; e outros totalizaram 15%. (InfoExame, 2013).

Sabe-se, inclusive, que muitos incidentes não são reportados por razões de segurança nacional, ou mesmo em função da segurança das organizações. Além disso, muitos ataques podem não ter sido identificados em função da qualidade das ações, que podem ser indetectáveis ou mesmo não rastreáveis, conjugadas com a ineficácia das tecnologias de segurança que estão instaladas nos ambientes de automação.

Faz-se necessário também avaliar a interdependência dos sistemas críticos, pois situações como apagões no fornecimento de energia afetam outras infraestruturas fundamentais para a sociedade, tais como abastecimento de água, transporte e comunicação. Por isso, a ausência de informações sobre a integração das infraestruturas dos projetos de sistemas críticos dificulta a identificação e mensuração do risco (FLENTGE; BEYER, 2007). Por isso, emana a necessidade de uma melhor compreensão do impacto da mútua dependência no nível geral de risco de infraestruturas críticas, pois, quando os sistemas são mutuamente dependentes, uma ameaça para um sistema pode ser uma ameaça para todos os outros (RINALDI; PEERENBOOM; KELLY, 2001).

Rinaldi, Peerenboom e Kelly (2001) argumentam que as infraestruturas mutuamente dependentes devem ser consideradas de forma conjuntural. Entretanto, para a análise de risco muitas vezes não é possível analisar todos os sistemas possíveis que afetam o alvo de análise de uma só vez, portanto precisa-se de uma abordagem modular.

Observa-se a complexidade de se realizar a atividade de quantificar e qualificar a vulnerabilidade de uma planta, pois existem muitos métodos e

ferramentas disponíveis, mas não integradas, o que dificulta a análise de risco e de falhas no cenário de segurança da informação e segurança do processo. Entretanto, se torna importante o estudo de uma abordagem que contemple a gestão de risco das plantas de saneamento, pois, a demanda por sistemas mais confiáveis faz parte de um contexto de interesses conflitantes que envolvem a minimização de gastos e maximização de lucros. Portanto, a gestão de risco busca identificar o ponto de equilíbrio a ser alcançado, uma vez que a baixa confiabilidade pode acarretar perda de vidas, além de prejuízos ambientais e financeiros.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Desenvolver uma metodologia para a gestão de risco com base em critérios do método CORAS, proporcionando um aprimoramento desse método com modelagem matemática para análise quantitativa dos riscos e identificação de falhas em processos de plantas de saneamento.

1.1.2 Objetivos Específicos

- Quantificar os riscos de uma planta de saneamento utilizando o método CORAS com as melhorias propostas para avaliação das falhas.
- Desenvolver e validar uma metodologia de gestão de risco em uma planta de sistema crítico.
- Contemplar na gestão de risco as áreas de *safety* e *security*.

1.2 CONTRIBUIÇÕES

Este trabalho apresenta uma metodologia com análise quantitativa aplicada a gestão de risco e especifica os principais conceitos e seus relacionamentos em um modelo conceitual. A base conceitual se origina a partir do método CORAS, que é uma ferramenta que faz a compilação de diversas normas internacionais no âmbito da análise de segurança e de risco. Este trabalho apresenta algumas contribuições, tais como:

- Aprimoramento do método CORAS, com inclusão da análise quantitativa por Markov e MTBF.
- O desenvolvimento de estudos de *safety* e *security* em plantas de serviço críticos, especificamente em plantas de saneamento.
- A aplicação de uma metodologia de gestão de risco com a inclusão da análise quantitativa para análise de risco em um estudo de caso.

A metodologia proposta contempla a análise de segurança de sistemas de informação (*security*) e a análise de risco na visão da segurança do processo (*safety*). Este estudo amplia a análise realizada com CORAS, incluindo a verificação de confiabilidade por meio de Markov e MTBF.

Observa-se que, ao longo da elaboração desta pesquisa, que foram apresentados artigos em congressos, simpósios e revistas (Apêndice A) com o intuito de discutir entre especialistas a temática aqui proposta; o que trouxe grandes contribuições para a condução deste estudo.

1.3 SOLUÇÃO PROPOSTA

Na literatura há propostas que abordam gestão de risco utilizando ferramentas pontuais e com ênfase apenas na análise de risco, porém sabe-se que a gestão de risco é muito mais abrangente, pois envolve desde concepção e criação da cultura de risco na organização, além das etapas de análise, quantificação, tratamento, verificação e auditoria.

Parte-se, portanto, da hipótese de que as inúmeras vulnerabilidades existentes em uma planta de saneamento não foram devidamente identificadas e mensuradas. Sendo assim, este trabalho propõe o desenvolvimento de uma metodologia de gestão de risco que viabilizará um ambiente automatizado com ênfase em melhores práticas de segurança no processo e segurança da informação.

1.4 JUSTIFICATIVAS

Existe uma carência de pesquisa que contemple a segurança de processo (*safety*) e segurança da informação (*security*), principalmente em plantas de saneamento. Observa-se que o tema de ataques a sistemas de utilidades está em evidência em países de primeiro mundo em função de constantes ameaças de ataques ciberterroristas.

Durante o desenvolvimento deste trabalho, verificou-se a existência de uma vasta coleção de referências (artigos, normas, livros, dissertações e teses) tratando do tema de segurança da informação, ciberataques, ciberterrorismo e segurança de automação. Apesar dessa diversidade, são muito incipientes as pesquisas com ênfase em análise de risco para plantas de saneamento, com abordagem metodológica que contemple segurança do processo e segurança de informação.

Porém a justificativa mais relevante para o desenvolvimento desta pesquisa foi o fato da autora atuar na área de saneamento a mais de 15 anos e desenvolver diversos trabalhos de automatização das plantas e avaliar questões de segurança da informação, com pesquisa de mestrado e apresentação de artigos em fóruns específicos sobre o tema, além de nos últimos três anos exercendo a função de diretora executiva do contrato em estudo observar a grande fragilidade e riscos existentes na área, especialmente por falta de pesquisa no Brasil e em outros países.

Observa-se um maior investimento em automação das plantas de saneamento na última década no Brasil, principalmente com a entrada das empresas privadas no setor por meio de Participação Pública Privada (PPP).

Este novo cenário de investimento em automação possibilitou a integração da arquitetura dos sistemas SCADA com as redes corporativas, inclusive com acessos via tecnologia móvel.

O sistema SCADA e o CLP têm importância estratégica para o monitoramento de uma planta, e o ataque a tais sistemas pode colocar em risco uma cidade e prejudicar os serviços fornecidos para os seus cidadãos. Os alvos de ataque em uma ciberguerra são a rede e o computador, e os sistemas a eles interligados, como o CLP e seus instrumentos para a rede de automação. Observa-se que a exploração de vulnerabilidades das arquiteturas de sistemas de automação pode invalidar e até mesmo paralisar toda a infraestrutura (MARTINS et al., 2010).

A ausência de modelos referenciais para a realização da gestão de riscos em plantas de saneamento justifica a demanda por pesquisa que possa facilitar o dia a dia de gestores operacionais dessas plantas, possibilitando quantificar os riscos e a confiabilidade de seus processos.

A escolha de modelar informações contextuais utilizando o método CORAS justifica-se pela abrangência de atuação desse método e pela capacidade de otimizar as informações em uma única ferramenta documentando a análise de risco (BRAENDELAND; REFSDAL; STOLEN, 2010).

1.5 DESCRIÇÃO DO PROBLEMA

Há carência de pesquisa com ênfase em gestão de risco, principalmente aplicado a processo de saneamento, o que evidencia a falta de respostas para questionamentos, como:

- Como é possível avaliar os riscos e quantificar a confiabilidade dos processos em plantas de saneamento?
- Quais técnicas de análise de risco e modelagens matemáticas possibilitam quantificar os riscos dessas plantas e simular as falhas do processo?
- Qual a prioridade de atuação no desenvolvimento da gestão de risco em uma planta de tratamento de água ou esgoto?

Além do problema identificado, existe também a lacuna em função da falta de estudos em *safety* e *security* para plantas de utilidades com pesquisas sobre as análises dos riscos e falhas dessas unidades.

Dessa forma, esta proposta de pesquisa partiu da hipótese central (H^0) de que existe a demanda de desenvolvimento de uma metodologia para gestão de risco, que proponha uma identificação e quantificação dos riscos com a possibilidade de simulações para plantas de saneamento, possibilitando promover a otimização do processo de automação com consequente redução de riscos de ataques cibernéticos ou mesmo físicos ao sistema de controle operacional da planta. Essa hipótese central desdobra-se nas seguintes hipóteses secundárias:

- H^1 : aplicação do método CORAS para qualificar/quantificar os riscos e as falhas em uma planta de tratamento de água ou esgoto;
- H^2 : contribuição da criação de uma metodologia referencial para utilização em gestão de risco com modelagens de *safety* e *security*, na verificação de falha do processo, específica no tratamento de água ou esgoto;

- H³: aplicação da cadeia de Markov e MTBF para verificação da confiabilidade do processo.

As hipóteses desta pesquisa foram validadas após o desenvolvimento da metodologia de gestão de risco com a verificação da possibilidade de caracterização e quantificação das vulnerabilidades.

1.6 MATERIAIS E MÉTODOS

Foi utilizado o método hipotético-dedutivo de Karl Popper (1999), pois, a partir da hipótese central foram estabelecidos pressupostos testados através do estudo de caso, sendo que o resultado positivo viria a validar a metodologia.

O planejamento da pesquisa contemplou o estudo teórico e documental, e, por conseguinte, o estudo empírico com o desenvolvimento do estudo de caso em uma planta de tratamento de esgoto.

Inicialmente, no estudo teórico e documental ocorreu a análise dos diversos modelos, métodos, técnicas e ferramentas de análise de riscos e verificação de confiabilidade. Contemplou-se a pesquisa bibliográfica para a exploração das fontes, recomendada para estudos descritivos, ou seja, objetivando o entendimento amplo das condições atuais do contexto a ser estudado mediante a sua descrição ou delineamento. Assim, na pesquisa bibliográfica, foram coletados dados provenientes da leitura e análise de livros, artigos científicos, teses e estudos de caso correlatos com o tema da pesquisa, possibilitando o estabelecimento do marco teórico do trabalho. Trata-se de uma análise-síntese do estado da arte relativo ao cenário de segurança da informação (*security*) e segurança do processo (*safety*) em automação dos processos de saneamento.

Posteriormente, se contemplou a aplicação do método CORAS e a concepção de análise de risco quantitativo por modelagem, por meio da combinação das diversas técnicas selecionadas.

Já no estudo empírico, ocorreu a implementação da metodologia de gestão de risco em uma planta de tratamento de esgoto, viabilizando o processo de avaliação da metodologia utilizada.

Para implementar esta pesquisa, foram utilizados os seguintes recursos:

- CORAS *Application*;
- SCADA – Vijeo Citect;
- CLP – M340 Schneider;
- SO do CLP – Unity Pro;
- Banco de dados SQL;
- OPC Server;
- *Notebook* dual core de 1.67 GHz, RAM de 2 GB e HD de 200 GB;
- Instrumento ultrassônico para medição de variáveis no campo.
- CARMS versão 1.1;
- MAPLE 14;
- Excel 2007.

1.7 ORGANIZAÇÃO DO TEXTO

Para a produção deste texto, optou-se pela estruturação em cinco capítulos, descritos a seguir.

No capítulo 1, é apresentada a introdução e a contextualização da pesquisa, as motivações, caracterização do problema, solução proposta, os objetivos, justificativas, contribuições e a metodologia da pesquisa.

O capítulo 2 apresenta a fundamentação teórica da pesquisa, que contempla os conceitos elementares, uma introdução às técnicas de análise de falhas e de avaliação de risco de processo, além de detalhes sobre ferramentas de análise de segurança do processo e os conceitos básicos de segurança da informação. Este capítulo tem a função de facilitar a compreensão dos capítulos subsequentes e estabelecer padronização da notação a ser utilizada; além de apresentar e detalhar o método CORAS.

O capítulo 3 detalha o estado da arte e os trabalhos relacionados com a presente pesquisa. Aborda também os métodos estatísticos utilizados para quantificar a confiabilidade, os modelos matemáticos e os algoritmos necessários, além das diversas ferramentas e normas de segurança de processo, que serviram de base para o desenvolvimento desta pesquisa.

Já no capítulo 4 é apresentada a descrição do processo utilizado como estudo de caso na aplicação da metodologia proposta e os resultados obtidos. Apresenta as técnicas de análise utilizada neste estudo, além de ser justificado o detalhamento dos passos para conclusão da metodologia.

Finalmente, no capítulo 5, são apresentadas as conclusões e propostas de continuidade.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, apresentam-se conceitos elementares sobre segurança da informação (*security*) e segurança do processo (*safety*), com a função de facilitar a compreensão dos capítulos subsequentes e estabelecer a padronização da notação a ser utilizada.

Observa-se a importância de definir as duas áreas de atuação desta pesquisa – *security* e *safety* –, pois ambas são contempladas na análise de risco e verificação de falhas para melhorar a segurança de um processo.

Para melhor se definir os termos *security* e *safety*, deve-se inicialmente compreender o termo ‘risco’. Conforme relata Almeida Jr. (2003), e apresenta na Figura 1:

o risco pode ser visto como tendo relação direta com a frequência de possíveis eventos perigosos e com a severidade de suas consequências. Quanto maior a frequência de um evento perigoso, maior o risco e quanto maior a severidade de suas consequências, maior o risco assumido. ...qualquer sistema tem a si associados os riscos inerentes, sendo que o risco representado por um sistema pode ou não ser aceito pela sociedade, que em última análise, é quem define o conceito de risco aceitável. (p. 15).

Figura 1 – Princípio *As Low as Reasonably Possible* (ALARP).

Fonte: Almeida Jr. (2003).

Quanto às nomenclaturas dos termos *security* e *safety*, Almeida Jr. (2003) apresenta as seguintes definições:

Embora haja essa diferenciação de competências, na língua portuguesa essas duas atividades recebem a mesma denominação, ou seja, segurança, enquanto que na língua inglesa há dois termos distintos. O termo *safety* é utilizado para se fazer referência à segurança dos Sistemas Críticos, enquanto que o termo *security* é utilizado para referenciar a segurança dos Sistemas de Informação. (p.19).

Neste trabalho, o termo *security* é adotado para definições de procedimentos, estruturas e processos de melhoria das condições de segurança da informação, do dado e da arquitetura da rede de comunicação; enquanto que o termo *safety* refere-se ao estado que define uma condição de proteção a um sistema, pessoa, objeto, processo, e contempla os diversos tipos de erro, falha e problema. É diferenciado o termo de modo similar ao adotado por Almeida Jr. (2003) em sua pesquisa: *safety* para segurança do processo (segurança dos sistemas críticos) e *security* para segurança da informação (sistemas de informação).

2.1 SEGURANÇA DO PROCESSO – *SAFETY*

A segurança do processo relaciona qualidade, confiabilidade, manutenção e segurança das pessoas e do meio ambiente. O principal objetivo é conhecer e controlar os riscos.

A análise de risco significa o processo de compreender a natureza do risco e de determinar o nível de risco. Conforme Braendeland, Refsdal e Stolen (2010), define-se risco como a combinação da consequência e da probabilidade de um evento indesejado.

Conforme a norma CETESB P4.261(2003):

As recomendações e medidas resultantes do estudo de análise e avaliação de riscos para a redução das frequências e consequências de eventuais acidentes, devem ser consideradas como partes integrantes do processo de gerenciamento de riscos; entretanto, independentemente da adoção dessas medidas, uma instalação que

possua substâncias ou processos perigosos deve ser operada e mantida, ao longo de sua vida útil, dentro de padrões considerados toleráveis, razão pela qual um Programa de Gerenciamento de Riscos (PGR) deve ser implementado e considerado nas atividades, rotineiras ou não, de uma planta industrial.(p.34)

A necessidade por sistemas cada vez mais confiáveis está inserida em um contexto que demanda um ponto de equilíbrio a ser alcançado, uma vez que a baixa confiabilidade pode acarretar perda de vidas humanas e prejuízos materiais, porém a alta confiabilidade, por sua vez, pode inviabilizar financeiramente um projeto.

No desenvolvimento deste estudo são abordadas algumas das normas e técnicas de mensuração e análise de risco, tais como: IEC 61508, Confiabilidade, FMEA, CORAS, QSP 31000 (ISO/IEC 31000), CETESB P4.261 e outras.

2.1.1 Norma de Segurança do Processo - IEC 61508

A norma IEC 61508 é uma norma internacional para eletroeletrônicos e sistemas eletrônicos programáveis relacionados com a segurança do equipamento e do processo. Estabelece requisitos para garantir que os sistemas sejam projetados, implementados, operados e mantidos para prover o nível de integridade de segurança (*Safety Integrity Levels – SIL*), além de identificar os níveis de riscos inaceitáveis que podem promover danos físicos ao processo e à saúde das pessoas. O dano pode surgir para as pessoas diretamente, ou indiretamente, como resultado de prejuízos à propriedade ou ao meio ambiente. Essa norma é utilizada para estabelecer critérios de segurança para processos que têm funções críticas.

Essa norma enfoca, por meio de uma abordagem genérica, as atividades do ciclo de vida de segurança para os sistemas elétricos, eletrônicos e eletrônicos programáveis (E/E/PES) que são utilizados para desempenhar as funções de segurança. Nesse sentido, essa norma tem sido elaborada com o objetivo de desenvolver um policiamento técnico consistente para todos os sistemas elétrico-eletrônicos relacionados com a segurança, por meio de:

- Tratamento sistemático para todas as atividades do ciclo de vida de um sistema instrumentado de segurança;
- Habilitação para que os desenvolvimentos tecnológicos dos produtos se realizem em ambiente sistemático com segurança funcional;
- Potencialização de melhorias dos *Programmable Electronic Safety* (PES) nos aspectos de desempenho e de viabilidade econômica;
- Uniformização de conceitos para servir de base na elaboração de normas setoriais.

Embora a norma IEC 61508 esteja sendo direcionada para sistemas elétricos ou eletrônicos de segurança, sua orientação pode ser aproveitada em sistemas de segurança implementados por meio de outras tecnologias, como, por exemplo, mecânica, hidráulica ou pneumática. Essa norma está subdividida em 7 partes:

- Parte 1: Requisitos Gerais;
- Parte 2: Requisitos para Sistemas Elétricos, Eletrônicos e Eletrônicos Programáveis (E/E/PES);
- Parte 3: Requisitos de *Software*;
- Parte 4: Definições;
- Parte 5: Guia na Aplicação da Parte 1 (métodos de determinação dos níveis de integridade de segurança);
- Parte 6: Guia para a Aplicação das Partes 2 e 3;
- Parte 7: Bibliografia de Técnicas e Medidas.

As partes de 1 a 4 da IEC 61508 são publicações tratando de segurança básica, detalhadas na *IEC Guide 104 – The preparation of safety publications and the use of basic safety publications and group safety publications*, e *ISO/IEC Guide 51 – Safety aspects – Guidelines for their inclusion in standards* (IEC, 2010).

A norma IEC 61508 adota uma abordagem baseada em análise de risco, e trata o risco como uma combinação de probabilidades e consequências de

ocorrência. O termo utilizado, *safety*, abrange a característica de sistemas relacionados com a segurança do processo e, ao mesmo tempo, com a característica do equipamento, incluindo o sistema de controle associado que pode produzir o risco.

Os níveis de integridade de segurança representam medidas internas do sistema adequadas para lidar com o risco. Esse conceito direciona a padronização de duas classes de requisitos que devem ser especificados antes do início do processo de desenvolvimento do sistema de segurança. A primeira classe de requisitos diz respeito às funções de segurança, especificadas por meio do documento denominado *Especificação dos Requisitos Funcionais de Segurança*. A segunda classe de requisitos está relacionada com a integridade de segurança, documentada por meio do relatório *Especificação dos Requisitos de Integridade de Segurança*.

A IEC 61508 é a publicação básica que faz referência ao: padrão IEC 61513 (setor nuclear); padrão IEC 62061 (setor de máquinas) e IEC 61511 (setor de processos). Essa norma influencia o desenvolvimento de todos os sistemas relacionados com segurança de E/E/PES e normalmente é aplicada nas seguintes áreas: processos industriais (sistemas *shutdown* de emergência, sistemas contra incêndio e vazamento de gás, controle de fornos); indústrias de máquinas (robôs, máquinas) e de transporte (sinalização metroferroviária, sistemas de frenagem, elevadores); e, ainda, na medicina (aparelhagem de medição eletrônica, radiografia).

A estratégia adotada na norma IEC 61508 para o tratamento de sistemas críticos é dar ênfase aos seguintes aspectos (ver Figura 2):

- Gerenciamento da segurança funcional, relacionada com as atividades de segurança;
- Requisitos técnicos para todo o ciclo de vida de segurança;
- Competência das pessoas envolvidas nas atividades do ciclo de vida de segurança.

Figura 2 – Ciclo de Vida – IEC 61508.

Fonte: IEC (1998, p. 18, tradução nossa).

A IEC 61508 apresenta também os requisitos de segurança para o Sistema de Segurança Instrumentado (SIS) e fornece orientações para validação e verificação de tais sistemas. As três primeiras partes são normativas e lidam com a avaliação do risco de processo industrial e com o *hardware* dos instrumentos e a confiabilidade do *software*; e as quatro partes restantes tratam das definições.

Integridade e segurança são conceitos fundamentais na norma IEC 61508, com o objetivo de realizar satisfatoriamente as funções de segurança em um período de tempo; sendo que a segurança é especificada em quatro níveis, conhecidos como SIL. Os níveis do SIL definidos na IEC 61508-4 são os apresentados no Quadro 1:

Quadro 1 – Níveis do SIL.

SIL (nível)	PFD (Probabilidade de Falha sob Demanda)	RRF (Fator de Redução de Risco)
1	$\geq 10^{-2}$ a $< 10^{-1}$	10 – 100
2	$\geq 10^{-3}$ a $< 10^{-2}$	100 – 1000
3	$\geq 10^{-4}$ a $< 10^{-3}$	1000 – 10.000
4	$\geq 10^{-5}$ a $< 10^{-4}$	10.000 – 100.000

Fonte: IEC 61508-4 (1998, tradução nossa).

Conforme a IEC 61508, para a análise da probabilidade de ocorrência em situações críticas, é possível considerar a técnica acima com parâmetros β , que se referem ao número de uma ocorrência conhecida dentro de um período determinado no processo, sendo:

$\beta_c = \beta \cdot \text{PFD}$, a probabilidade que n situações críticas irão ocorrer no intervalo $(0, t)$ é $\Pr(N_c(t) = n) = \frac{(\beta \cdot \text{PFD} \cdot t)^n}{n!} e^{-\beta \cdot \text{PFD} \cdot t}$ para $n = 0, 1, 2, \dots$. Portanto, o tempo médio entre falhas (MTBF – *Mean Time Between Failure*) para essa situação será: $\text{MTBF} = \frac{1}{\beta \cdot \text{PFD}}$.

2.1.2 Tempo Médio Entre Falhas - MTBF

O tempo médio entre falhas (MTBF) é um parâmetro de confiabilidade de um componente, medido entre o instante inicial de funcionamento e o instante de ocorrência de uma incidência que ocasione uma parada no funcionamento regular desse sistema que leve a indisponibilidade. O valor normalmente é dado pelo fabricante da peça nas suas especificações técnicas e indica, de acordo com o procedimento de testes usado, qual é o tempo médio entre falhas daquele produto ocorrido nos laboratórios do fabricante.

Neste estudo, foi realizada a avaliação de probabilidade de falhas e tempo de indisponibilidade para o sistema em análise, considerando os dados fornecidos pelos fornecedores dos componentes e os parâmetros referenciados pelo padrão IEEE 493-2007.

Além de quantificar as probabilidades de falhas e o tempo de indisponibilidade, este estudo fez uso de ferramentas e metodologias de análise qualitativa e de gestão dos riscos, conforme descrito nas próximas seções.

2.1.3 O Padrão IEEE 493-2007 e Confiabilidade (*Reliability*)

O capítulo 2 do padrão IEEE 493-2007 descreve a função *reliability* como um método quantitativo de análise com as fórmulas do Quadro 2:

Quadro 2 – Fórmulas da função *reliability*.

Informação	Fórmula para o cálculo
Ai, Disponibilidade Inerente.	$A_i = \text{MTBF}/(\text{MTBF} + \text{MTTR})$
Ao, Disponibilidade Operacional.	$A_o = \text{MTBM}/(\text{MTBM} + \text{MDT})$
λ , taxa de falha (f/h) - hora	$\lambda = T_f/T_p$
λ , taxa de falha(f/y) - ano	$\lambda = T_F/T_p(8760)$
MDT, tempo de inatividade (h)	$\text{MDT} = (\text{Rdt} + \text{Rlt} + \text{Mdt})/T_{de}$
MTBF, tempo entre falhas (h)	$\text{MTBF} = T_p/T_f$
MTBM, tempo entre manutenção (h)	$\text{MTBM} = T_p/T_{de}$
MTTM, tempo para manutenção (h)	$\text{MTTM} = \text{Mdt}/T_{ma}$
MTTR, tempo para reparo (h)	$\text{MTTR} = r = \text{Rdt}/T_f$
R(t), Confiabilidade	$R(t) = e^{-\lambda t}$

Fonte: IEEE 493 (2007, tradução nossa).

A confiabilidade é centrada no estudo de falhas no decorrer do tempo. Conforme Carvalho (2008), desde a criação do conceito de confiabilidade, ocorreu ao longo dos anos o seu desmembramento em vários ramos de aplicação, como confiabilidade de equipamentos mecânicos, confiabilidade de *software*, confiabilidade humana, otimização da confiabilidade, crescimento da função confiabilidade (*reliability growth*), entre muitos outros.

Na tese de Carvalho (2008), é desenvolvido um aprimoramento do método convencional com o tratamento das incertezas, porém, neste estudo, como a função *reliability* é uma complementação para avaliação quantitativa, associada ao método CORAS, será adotada a abordagem convencional.

Em uma avaliação convencional de confiabilidade, os valores coletados dos sistemas e componentes são tratados como valores precisos. A análise clássica de confiabilidade normalmente não aborda a suscetibilidade a eventos externos ou ao erro humano em operação e manutenção. Sendo desejável considerar a contribuição relativa da incerteza para o risco total, mesmo os modelos mais sofisticados, precisos e bem construídos podem fornecer resultados incorretos se essa incerteza não for tratada de alguma forma.

Aspectos de confiabilidade (*reliability*) de sistemas de segurança devem ser projetados para serem ativados em situações de desvios de processo, para proteger as pessoas, o meio ambiente e os bens materiais. De acordo com

Rausand e Hoyland (2004), os sistemas de segurança possuem camadas de proteção, tais como:

- Sistema de desligamento dos motores da bomba de entrada de vazão, intertravado com sensores de nível, com inversores de frequência e sistema PID programado para desligamento automático de bombas;
- Sistema de descarga de pressão compreendendo válvulas multijato com alívio de pressão, e atuadores programados para fechamento automático da válvula;
- Comportas com atuadores para fechamento automático para evitar extravasamento.

Conforme IEC 61882, os instrumentos de campo (medidores de vazão, pressão, etc.), são instalados como meio de monitorar e criar as devidas camadas de proteção, em função da demanda potencial do processo, que é geralmente identificada pelos perigos e operabilidade conforme o estudo por HAZOP.

Demandas do processo podem ser classificadas de acordo com sua frequência de ocorrência. Algumas demandas do processo ocorrem com tanta frequência que o sistema de segurança é operado quase que continuamente, como é o caso da válvula multijato para controle de vazão de efluente enviada a um emissário, detalhada no capítulo do estudo de caso, ou mesmo o exemplo do freio de um carro, como citado por Rausand e Hoyland (2004). Em outro extremo, têm-se os processos que ocorrem muito raramente, portanto, em um estado passivo durante longos períodos de tempo. Um exemplo de tal sistema é o *airbag* em um carro: o sistema de *airbag* permanece passivo até que um “processo” de demanda ocorra, ou seja, é um sistema de segurança com um modo de baixa demanda de operação. Esse sistema de segurança pode falhar em estado passivo, e a falha pode permanecer escondida até que uma demanda ou processo ocorra ou até que o sistema seja testado. Para revelar falhas ocultas, sistemas de segurança com o modo de baixa demanda de operação são normalmente testados em intervalos regulares, como ocorre com as comportas de segurança do sistema de efluente.

Conforme Hines et al. (2012), considerando um instrumento que acaba de ser fabricado e que será operado a um “nível de estresse” estabelecido ou dentro de alguma faixa de estresse, como temperatura, choque e assim por diante, a variável aleatória T será definida como o tempo de falha e a confiabilidade do componente no tempo t é $R(t) = P[T > t]$. R é chamada de função de confiabilidade. O processo de falha é usualmente complexo, consistindo em pelo menos três tipos de falha: falhas iniciais, falhas de desgaste e falhas que ocorrem entre estas. Para uma distribuição mista, temos: $p(0) + \int_0^\infty g(t)dt = 1$.

Como para muitos componentes as falhas iniciais ou as falhas do instante zero são removidas durante os testes, a variável aleatória T é condicionada para o evento $T > 0$, de modo que a densidade de falha é $f(t) = \frac{g(t)}{1-p(0)}, t > 0$, caso contrário $= 0$. Logo, a função de confiabilidade R é $R(t) = 1 - F(t) = \int_t^\infty f(x)dx$.

O termo taxa de falha por intervalo denota a taxa de falha em um intervalo de tempo particular $[t_1, t_2]$, e os termos taxa de falha, taxa de falha instantânea e risco serão usados como sinônimos à maneira de uma forma-limite da taxa de falha por intervalo quando $t_2 \rightarrow t_1$. A taxa de falha por intervalo $FR(t_2, t_1)$ é $TF(t_1, t_2) = \left[\frac{R(t_1) - R(t_2)}{R(t_1)} \right] \cdot \left[\frac{1}{t_2 - t_1} \right]$. O primeiro termo entre colchetes representa $P\{\text{Falha em } [t_1, t_2] \mid \text{Sobreviveu até tempo } t_1\}$, enquanto que o segundo colchete representa a característica dimensional, de modo que se pode expressar a probabilidade condicional em base de tempo por unidade. Será avaliada também a taxa de falha instantânea (como a função de t), ou seja, $h(t)$ a função de risco, $h(t) = \lim_{\Delta t \rightarrow 0} \frac{R(t) - R(t + \Delta t)}{R(t)} \cdot \frac{1}{\Delta t} \Rightarrow - \lim_{\Delta t \rightarrow 0} \frac{R(t + \Delta t) - R(t)}{\Delta t} \cdot \frac{1}{R(t)}, h(t) = \frac{-R'(t)}{R(t)} = \frac{f(t)}{R(t)}$, uma vez que $R(t) = 1 - F(t)$ e $-R'(t) = f(t)$.

Uma função de risco típica é a “curva da banheira”, conforme Carvalho (2008), Figura 3, a $h(t).dt$ deve ser considerada na probabilidade instantânea de falha em t , dada a sobrevivência até t .

Figura 3 – Curva da banheira.

I – falhas de fabricação/projeto;

II – vida útil;

III – desgaste do equipamento.

Fonte: Carvalho (2008).

Um resultado útil é o de que a função de confiabilidade R pode ser facilmente expressa em termos de hora, como $R(t) = e^{-\int_0^t h(x)dx} = e^{-H(t)}$, onde $H(t) = \int_0^t h(x)dx$. Realizando a integração de ambos os membros das equações, temos:

$$\int_0^t h(x)dx = - \int_0^t \frac{R'(x)}{R(x)} dx = - \ln R(x) \Big|_0^t, \text{ de modo que } \int_0^t h(x)dx = - \ln R(t) +$$

$\ln R(0)$. Como $F(0) = 0$, temos $\ln R(0)=0$ e $e^{-\int_0^t h(x)dx} = e^{\ln R(t)} = R(t)$. Logo, o Tempo Médio de Falha (TMF) é $E[T] = \int_0^\infty t f(t)dt$.

A maioria das modelagens de sistemas complexos supõe que apenas as falhas aleatórias dos componentes precisam ser consideradas. Isso é equivalente a dizer que a distribuição do tempo de falha é exponencial, ou seja: $f(t) = \lambda e^{-\lambda t}$, $t \geq 0$, caso contrário $= 0$, de modo que $h(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{-\lambda t}}{e^{-\lambda t}} = \lambda$, será uma constante. Quando todas as falhas iniciais (falhas de fabricação/projeto) tiverem sido removidas por depuração e o tempo para a ocorrência de falhas de desgaste for muito grande (inclusive das partes eletrônicas), então essa hipótese será razoável.

Conforme Leemis (2009) a distribuição normal é mais usada para a modelagem de falhas de desgaste ou falhas de estresse (em que a variável aleatória em estudo é o nível de estresse). Em situações em que a maioria das falhas é devida ao desgaste, a distribuição normal pode ser bem apropriada. Observa-se que a distribuição lognormal tem sido considerada aplicável para a

descrição do tempo de falha para alguns tipos de componente, e a literatura parece indicar uma crescente utilização para esse propósito.

Conforme Rausand e Hoyland (2004) a distribuição de Weibull tem sido extensamente usada para representar o tempo de falha, principalmente quando um sistema é composto de um número determinado de componentes e a falha é devida a um grande número de defeitos ou possíveis defeitos.

Tem-se também o uso por distribuição gama, na modelagem de redundância em espera, em que os componentes têm uma distribuição exponencial para o tempo de falha, considerando-se apenas falha aleatória. As funções densidade, confiabilidade e de risco são dadas por:

$$f(t) = \lambda e^{-\lambda t}, t \geq 0, \text{ caso contrário} = 0.$$

$$R(t) = P[T > t] = e^{-\lambda t}, t \geq 0, \text{ caso contrário} = 0.$$

$$h(t) = \frac{f(t)}{R(t)} = \lambda, t \geq 0, \text{ caso contrário} = 0.$$

Nota-se que na fase II da curva da banheira (vida útil) a função de risco é constante, considerando que o processo de falha não tem memória, isto é:

$P\{t \leq T \leq t + \Delta t | T > t\} = \frac{e^{-\lambda t} - e^{-\lambda(t+\Delta t)}}{e^{-\lambda t}} = 1 - e^{-\lambda \Delta t}$. Portanto a vida útil restante tem a mesma probabilidade de falha, logo se um componente estiver funcionando no instante T é tem a mesma confiabilidade que um novo (CARVALHO, 2008).

2.1.4 Análise do Modo de Falha e Efeito - FMEA

A análise dos modos de falha e efeitos é definida por Palady (1997) como uma técnica que oferece três funções distintas:

1. Ferramenta para prognóstico de problemas.

2. Procedimento para desenvolvimento e execução de projetos, processos ou serviços.
3. Diário do projeto, processo ou serviço.

Como ferramenta, mostra-se eficiente para prevenção de problemas e soluções. Além disso, aplica procedimento que oferece uma abordagem estruturada para o desenvolvimento de projetos e processos. Finalmente, como diário, a FMEA inicia-se na concepção do projeto, processo ou serviço, e se mantém durante a vida de mercado do produto.

Uma importante característica da FMEA é ser proativa, o que implica a eliminação de problemas potenciais antes que eles sejam realmente criados em um protótipo, durante o processo ou em campo. Porém, sabe-se que a FMEA é altamente subjetiva e requer muita suposição em relação às possibilidades e à sua prevenção. Desse modo, o resultado da FMEA está diretamente ligado à capacidade, especialidade e experiência da equipe envolvida.

Nota-se durante a aplicação da FMEA que é relevante identificar todas as funções do projeto em análise, pois isso possibilitará uma lista completa dos modos de falha. Entretanto, nem todas as causas identificadas são relevantes ao modo de falha.

Atualmente, existem dois tipos de FMEA:

- FMEA de projeto (*Design Failure Modes and Effects Analysis* – DFMEA).
- FMEA de processo (*Process Failure Modes and Effects Analysis* – PFMEA).

FMEA deverá ser aplicado conforme o fluxo dos cinco elementos básicos (vide Figura 4). Caso um dos elementos não seja atendido, a qualidade e a confiabilidade poderão ser impactadas.

Figura 4 – Elementos básicos do FMEA.

Fonte: Palady (1997).

Os cinco elementos da Figura 4 são definidos por Palady (1997):

1. Selecionar o projeto/processo;
2. Perguntar e responder as três perguntas;
 - Como pode falhar?
 - Por que falha?
 - O que acontece quando falha?
3. Implementar um esquema para identificar os modos de falha mais importantes, com o objetivo de trabalhar neles e melhorá-los;
4. Priorizar os modos de falha que serão tratados em primeiro lugar;
5. Acompanhar se as intervenções realizadas atenderam aos objetivos, bem como realizar auditorias.

A norma militar americana do departamento de defesa 1629A (MIL-STD-1629A) abrange modos de falha e análise de efeitos (FMEA) e suas variantes, incluindo modos de danos e análise de efeitos (DFMEA) e efeitos de modos de falha e análise de criticidade (FMECA).

Essa norma define os seguintes processos para FMEA:

- Planejamento.

- Modelo de planilha para coleta de informações.
- Regras básicas e suposições.
- Sistema de codificação.
- Detalhamento de informações adicionais.
- Nível de estrutura (incluindo *hardware* e abordagens funcionais).
- Definição de fracasso.
- Identificação de modos de falha e efeitos.
- Métodos de detecção e as ações corretivas.
- Identificação de design corretivo.
- Classificação da gravidade.

FMEA é uma análise qualitativa, enquanto FMECA é uma extensão da FMEA, com ênfase nos parâmetros quantitativos, pois acrescenta probabilidade de ocorrência e gravidade para a análise. A norma que melhor detalha a FMECA é a IEEE Std. 352 (2006). Nesta pesquisa, são referenciadas ambas as análises como FMEA.

Para realizar a FMEA, o sistema deve ser dividido em subsistemas e diagrama de função com as devidas dependências, e o subsistema deve ser visto no nível de componente. Essa técnica também exige tarefas básicas, como:

- Montar a equipe.
- Estabelecer as regras básicas.
- Recolher e analisar informação relevante.
- Identificar os itens ou processos a serem analisados.
- Identificar as funções, falhas, efeitos, causas e controles para cada item ou processo para realizar a análise.
- Avaliar o risco associado com as questões identificadas pela análise.
- Priorizar e atribuir ações corretivas.
- Realizar ações corretivas e reavaliar o risco.
- Distribuir, revisar e atualizar a análise, conforme o caso.

O objetivo da FMEA é tomar ações na remoção ou redução de falhas, a começar pela de maior prioridade. Para isso, é utilizada uma planilha que irá ajudar na classificação da análise.

Na análise por FMEA, três parâmetros são quantitativos: severidade, ocorrência e detecção. Conforme os Quadros 3,4 e 5 são atribuídos os valores quantitativos na matriz de risco conforme for mais apropriado para a situação em análise.

Quadro 3 – Escala de severidade.

Grau	Descrição da Escala de Severidade
1	Efeito não percebido pelo cliente.
2	Efeito bastante insignificante, percebido pelo cliente, mas sem qualquer consequência.
3	Efeito insignificante, que perturba o cliente, mas sem consequência.
4	Efeito bastante insignificante, mas perturba o cliente e com consequência.
5	Efeito menor, inconveniente para o cliente, mas sem consequência.
6	Efeito menor, inconveniente para o cliente, com consequência.
7	Efeito moderado, que prejudica o desempenho do projeto levando a uma falha grave ou a uma falha que pode impedir a execução das funções do projeto.
8	Efeito significativo, resultando em falha grave; entretanto, não coloca a segurança do cliente em risco e não resulta em custo significativo da falha.
9	Efeito crítico que provoca a insatisfação do cliente, interrompe as funções do projeto, gera custo significativo da falha e impõe um leve risco de segurança (não ameaça a vida nem provoca incapacidade permanente) ao cliente.
10	Perigoso, ameaça a vida ou pode provocar incapacidade permanente ou outro custo significativo da falha que coloca em risco a continuidade operacional da organização.

Fonte: Palady (1997).

Quadro 4 – Escala de ocorrência.

Grau	Percentual	Avaliação de Ocorrência
1	Menos de 0,01%	Extremamente remoto; altamente improvável.
2	0,011 – 0,20	Remoto, improvável.
3	0,210 – 0,60	Pequena chance de ocorrência.
4	0,610 – 2,00	Pequeno número de ocorrências.
5	2,001 – 5,00	Espera-se um número ocasional de falhas.
6	5,001 – 10,00	Ocorrência moderada
7	10,001 – 15,00	Ocorrência frequente.
8	15,001 – 20,00	Ocorrência elevada.
9	20,001 – 25,00	Ocorrência muito elevada.
10	Mais de 25%	Ocorrência certa.

Fonte: Palady (1997).

Quadro 5 – Escala de detecção.

Grau	Descrição da Escala de Detecção
1	É quase certo que será detectado.
2	Probabilidade muito alta de detecção.
3	Alta probabilidade de detecção.
4	Chance moderada de detecção.
5	Chance média de detecção.
6	Alguma probabilidade de detecção.
7	Baixa probabilidade de detecção.
8	Probabilidade muito baixa de detecção.
9	Probabilidade remota de detecção.
10	Detecção quase impossível.

Fonte: Palady (1997).

Com base na severidade, na ocorrência e no grau de detecção, chega-se à matriz de risco, detalhado no Apêndice B.

Normalmente, a FMEA é demorada, pois estuda todos os componentes separadamente, como única falha e um evento independente. Porém, é extremamente eficaz quando utilizada em sistema simples com componente único. Um dos inconvenientes principais da FMEA é que normalmente todas as falhas dos componentes são analisadas e documentadas, o que inclui até mesmo aquelas falhas que têm consequências pequenas ou praticamente nulas. Isso cria grande quantidade desnecessária de documentação, principalmente se for um grande sistema a ser analisado.

Na presente pesquisa, foi aplicada para conhecimento do ambiente a análise com as referências da FMEA, conforme apresentado no Apêndice B desta tese.

2.1.5 Estudo da Operabilidade e dos Perigos - HAZOP

HAZOP é uma técnica de identificação de risco, que foi inicialmente desenvolvida para analisar os sistemas de processo químico, mas foi posteriormente contemplando outros tipos de sistema, até mesmo para operações complexas e de sistemas de *software*. O HAZOP é basicamente qualitativa e fundamenta-se num *brainstorming*, com objetivo de encontrar

formas de comportamento do sistema que pode desviar da intenção de projeto, sendo que esse desvio pode ser incidentes indesejados (riscos).

A entrada para a análise é a documentação do sistema e, além disso, o líder da análise deve ser especializado no processo para garantir que todos os aspectos sejam cobertos. O método faz uso de palavras-guias que levam as pessoas a pensarem em aspectos que não tenham pensado antes. Uma técnica similar que é comumente usada na análise de segurança é a Identificação de Perigos (*Hazard Identification Studies* – HAZID). Esta é basicamente uma versão simplificada do HAZOP que utiliza listas de verificação em vez de guias de palavras, e é muitas vezes usada no início da análise do processo ou para análises de risco menor.

O procedimento para usar a técnica HAZOP pode ser:

1. Dividir o sistema em partes (caixa de areia, reatores etc.);
2. Escolher um ponto de estudo (ou seja, bomba, válvula etc.);
3. Descrever a intenção do projeto;
4. Selecionar um parâmetro de processo (vazão, temperatura, nível etc.);
5. Aplicar uma palavra-guia (não, máximo etc.);
6. Determinar as causas;
7. Avaliar as consequências/problemas;
8. Recomendar ações: O quê? Quando? Quem?
9. Registrar as informações;
10. Repetir o procedimento (a partir do passo 2).

A execução de todos esses passos para cada ponto do processo torna o HAZOP bastante demorado, e é essencial ter acesso ao projeto detalhado e às informações operacionais, pois o HAZOP se concentra em descobrir uma determinada falha que pode levar a um específico acidente em estudo (vide Apêndice C).

Tabelas semelhantes ao FMEA/FMECA e também ao HAZOP são insatisfatórias para mostrar as relações entre os riscos identificados. Há claramente uma necessidade para ambos os métodos de documentação, em que se mantenham informações pormenorizadas sobre cada risco.

2.1.6 Análise da Árvore de Falha - FTA

A análise da árvore de falhas foi inicialmente utilizada em 1962 pelo Bell Telephone Laboratories para desenvolvimento de avaliação de segurança. É uma técnica bastante difundida e utilizada com sucesso em sistemas de estações nucleares, conforme norma NUREG-0492 (1981).

Limnios (2007) define FTA como sendo uma técnica que visa a melhorar a confiabilidade por meio de análise sistemática de possíveis falhas e consequências, adotando medidas corretivas ou preventivas. É baseada na construção de diagramas e pode utilizar abordagens diferentes para modelar, mas a forma mais comum e popular pode ser resumida em poucas etapas. A análise envolve cinco etapas, que estão ilustradas na Figura 5, conforme o método descrito pela IEC 61025 (1990).

Figura 5 – Etapas do FTA.

Fonte: Autora, conforme IEEE 61025 (1990).

- **Etapa 1:** as definições de eventos indesejados se constituem uma tarefa complexa e requer o envolvimento de pessoas qualificadas, tais como, engenheiros e analistas, para a definição do número de eventos e quais os eventos que devem ser estudados;
- **Etapa 2:** após a definição dos eventos, todas as causas com probabilidade de acontecer devem ser estudadas e analisadas;
- **Etapa 3:** definidos os eventos e analisado o sistema são descobertas as causas e efeitos de um evento indesejado e a sua probabilidade de acontecer. Dessa forma, é possível construir a árvore de falhas;
- **Etapa 4:** depois da montagem da árvore de falhas para um evento específico, ele então é analisado e avaliado para melhorias. A gestão de riscos ocorre nessa etapa e são encontradas melhorias para o sistema e também o controle dos riscos identificados;
- **Etapa 5:** após a identificação das vulnerabilidades, todos os métodos possíveis são levados em consideração para diminuir a probabilidade de ocorrência.

A utilização da técnica FTA facilita a identificação das falhas e suas relações. Essa técnica é uma das que foram integradas ao método CORAS, o principal meio de análise de risco utilizado nesta pesquisa.

2.1.7 Sistema de Análise de Risco Objetivo Consultivo - CORAS

CORAS é um método que integra diversas técnicas para avaliação de risco com base em *Unified Modeling Language* (UML). O projeto foi iniciado em 2001 por quatro países da União Europeia (Grécia, Alemanha, Noruega e Reino Unido), com apoio de empresas de TI (Intracom, Solinet e Telenor) e de sete institutos (CTI, FORTH, IFE, NCT, NR, RAL e Sintef), além da universidade QMUL, no Reino Unido. O desenvolvimento ocorreu em dois estágios: a principal tarefa da primeira fase (2001-2003) foi desenvolver uma plataforma de avaliação

de informações e o principal objetivo da segunda fase (2004-2007) foi de melhorar as funcionalidades do CORAS.

O CORAS segue os padrões regionais e internacionais, tais como Áustria Standard/Padrão da Nova Zelândia (AS/NZS) 4360:1999 e ISO/IEC 17799-1:2000. Mas a sua principal base é a norma de gerenciamento de risco que estabelece o padrão internacional, a ISO/IEC 31000:2009 – *General Guidelines for Principles and Implementation of Risk Management*, que por sua vez foi desenvolvida com base na norma AS/NZS 4360. O processo de gerenciamento de risco conforme a norma ISO/IEC 31000, possui o escopo apresentado na Figura 6, que contempla as etapas do CORAS.

Figura 6 – Diagrama da ISO/IEC 31000.

Fonte: ISO/IEC 31000 (2009).

- **Fase 1 – identificar o contexto:** busca caracterizar o alvo da análise, e qual é o foco e o escopo da análise de risco. Até que nível o risco é tolerável?
- **Fase 2 – identificar os riscos:** identificar ameaças e vulnerabilidades aos ativos;
- **Fase 3 – estimar o nível de risco, avaliar riscos:** nem todos os riscos podem ser eliminados, por isso há necessidade de decidir qual é o risco que precisa de tratamento;
- **Fase 4 – tratar os riscos:** identificar o tratamento de riscos indesejáveis. Avaliar e priorizar os diferentes tratamentos.

O CORAS utiliza ferramentas de identificação e análise de riscos oriundos da prevenção de acidentes em processo (*safety*), tais como:

1. Estudo de perigo e operabilidade (HAZOP);
2. Análise da árvore de falhas (FTA);
3. Modo falha efeito e análise de criticidade (FMECA);
4. Métodos de análise quantitativa de Markov;
5. CCTA análise de risco e gestão (CCTA *Risk Analysis and Management Method* – CRAMM).

O principal objetivo do CORAS é aperfeiçoar metodologias tradicionais de avaliação de risco para obter melhores resultados. O desenvolvimento de sua análise ocorre em oito passos:

Contexto	{	1. Preparação da análise (definição do escopo); 2. Definição das metas; 3. Detalhamento da origem (diagrama de ativos); 4. Aprovação do detalhamento do objetivo;
Avalia Risco	{	5. Identificação do risco (diagrama de ameaças); 6. Estimativa de risco (diagrama de ameaças); 7. Avaliação de risco (diagrama de risco); 8. Tratamento do risco (diagrama de tratamento).

O CORAS é um método de análise de risco que identifica, analisa e descreve o risco por meio de uma linguagem padronizada.

A estrutura do CORAS pode ser separada em três instrumentos diferentes:

1. **Linguagem de modelagem de risco:** a gráfica e a sintaxe textual;
2. **Método:** descrição do processo de análise de segurança e as diretrizes para criação dos diagramas CORAS;
3. **Ferramenta:** para documentação, manutenção e comunicação de resultados de análise de risco.

O *software* do CORAS é uma ferramenta para modelar análise de risco, desenvolvido pela Sintef e disponível sob a Licença Pública Geral (LGPL) – Versão 2.1 Beta 1, em 28 de março de 2006.

2.1.7.1 Recursos do método CORAS

- a) Tecnologia de código aberto (*open source solution*);
- b) Atualizações e software sem custo de licença (*free of charge*);
- c) Fornecido com cinco métodos de avaliação de risco: incluindo HAZOP, FMECA, análise de Markov e CRAMM;
- d) Portátil com XML padrão;
- e) Em módulos, que facilitam a inclusão de novas funcionalidades;
- f) Integrado com três principais modelos de dados *eXtensible Markup Language* (XML), incluindo:
 - i. XML *Metadata Exchange* (XMI) padronizado por Object Management Group (OMG);
 - ii. compatível com XML, dados formatados de indicadores de avaliação de risco;
 - iii. *Intrusion Detection Messaging Exchange Format* (IDMEF) pelo Internet Engineering Task Force (IETF).

Aplicam-se CORAS UML e *Unified Process* (UP) em avaliações de risco para segurança da informação e segurança do processo.

A linguagem CORAS é uma linguagem de modelagem gráfica para documentação, comunicação e análise de ameaça à segurança e cenários de risco no processo de análise de risco. Em análise de risco, é comum o uso de técnica de *brainstorming* estruturado em suas reuniões para levantamento das informações. Nessas sessões de *brainstorming*, a linguagem CORAS é aplicada para fazer modelos de cenários de ameaças e riscos. Uma das vantagens na utilização da linguagem CORAS nas sessões de *brainstorming* é promover a padronização em um ambiente bastante heterogêneo, em que muitas pessoas com conhecimentos específicos são envolvidas. A linguagem de CORAS melhora a eficiência do processo de análise, assim como a qualidade dos resultados obtidos. Conforme Lund, Solhaug e Stolen (2011), a padronização é facilitada principalmente pelo uso limitado de ícones para representar os ambientes, tais como:

- => Ativos – algo que é de valor para a parte interessada e requer proteção.

- => Ameaças internas – sem intenção – uma possível causa de um incidente indesejado.

- => Ameaças externas – com intenção.

- Threat (non-human) => Ameaça não humana.

- => Envolvidos (*stakeholder*) – pessoas ou organizações que podem ser afetadas, ou podem influenciar uma avaliação ou atividade sob o alvo da análise.

- => Vulnerabilidade – fraqueza que pode ser explorada por ameaças.

- => Cenário de ameaça – algo que pode ocorrer por causa de uma ameaça que explora alguma vulnerabilidade.

- => Incidente não desejado – algo que se deseja evitar, pois pode causar danos aos ativos.

- => Risco – a possibilidade de acontecer algo que vai impactar os ativos.

- => Cenário de tratamento – ferramentas e técnicas de correção das falhas.

O capítulo desta tese referente ao estudo de caso apresenta o detalhamento da aplicação desse método na análise de risco. Durante a pesquisa, foi necessário um aprimoramento da análise quantitativa da metodologia, utilizando o processo estocástico de Markov para situações com complexa análise de risco.

2.1.8 Processo Estocástico Markoviano

Um processo estocástico é considerado um processo markoviano se o estado futuro depender apenas do estado presente e não dos estados passados. Esse tipo de processo estocástico é também denominado de *memoryless process* (processo sem memória), uma vez que o passado é desprezado. Para melhor entendimento é necessário estabelecer algumas definições para o processo estocástico, pois o mesmo é definido como uma coleção indexada de variáveis aleatórias $\{X_t\}$, onde o índice t pertence a um dado conjunto T . O conjunto T é normalmente composto de números inteiros não negativos, e X_t representa uma característica mensurável de interesse num instante de tempo t . Formalmente, a notação indicada pela expressão é $\{X_t; t \in T\}$, que define um processo estocástico sobre um dado espaço de probabilidade. Os valores assumidos pela variável aleatória X_t são chamados estados, e o conjunto de todos os possíveis valores forma o espaço de estado do processo.

A análise de Markov é, entre outras técnicas, indicada para a realização da análise de risco pela ISO/IEC 61508, pois pode ser usada para analisar a confiabilidade dos sistemas que têm um elevado grau de dependências. Em contraste com a FTA, a análise de Markov não assume independência por completo. Uma análise de Markov considera o sistema como um número de estados, e as transições entre esses estados. Os estados são modelados graficamente e cálculos estatísticos são realizados para determinar a probabilidade de transição entre os estados.

De acordo com Alves e Menezes (2010), um processo markoviano é dito ser uma cadeia de Markov quando as variáveis randômicas X_t estão definidas

em um espaço de estados discretos. Portanto, quando o tempo é discreto, a cadeia de Markov será uma cadeia de Markov em tempo discreto. Uma cadeia de Markov pode ser uma sequência de variáveis aleatórias, exemplo: X_1, X_2, X_n . O escopo dessas variáveis, isto é, o conjunto de valores que elas podem assumir, é chamado de *espaço de estados*, onde X_n denota o estado do processo no tempo n . Se a distribuição de probabilidade condicional de X_{n+1} nos estados passados for uma função apenas de X_n , então: $\Pr(X_{n+1} = x | X_0, X_1, X_2, \dots, X_n) = \Pr(X_{n+1} = x | X_n)$, onde x é algum estado do processo. Esta identidade define a propriedade de Markov.

Os processos de Markov sempre envolvem a variável tempo, seja considerada na forma discreta onde o tempo varia em intervalos regulares, ou na forma contínua, podendo assumir valores reais. Nos processos de tempo discreto, em que o índice t assume apenas valores inteiros não negativos, ou seja, $t = \{0, 1, 2, \dots\}$; e nos processos nos quais a variável tempo é contínua, ou seja, $t \in [0, \infty)$. Em ambas as categorias, os estados são caracterizados por números inteiros não negativos, definidos a partir dos valores que a variável aleatória X pode assumir.

É fundamental no estudo de processos de Markov a noção de estado. Propriedades em comum entre indivíduos (ou objetos) caracterizam o que designamos por estados. No estudo de caso aqui apresentado, um exemplo de estado pode ser identificado, nas bombas da estação elevatória, cujos estados podem ser máquina funcionando, máquina parada e em reparo (ou máquina parada aguardando por reparo).

Um processo de Markov está completamente especificado se forem conhecidas as probabilidades de transição e a distribuição inicial de probabilidades dos estados. Toda vez que um estado suceder a outro, dizemos que o processo estocástico markoviano deu um passo. O passo pode representar um período de tempo que resulte em outro estado possível. Se o número de passos é zero, tal situação representa o presente, igual a um, estará representando um possível estado no próximo passo, e assim por diante.

A probabilidade de transição do estado i ao estado j , em um passo, pode ser simbolizada por P_{ij} , que é a probabilidade de um objeto que se encontra no estado i após um intervalo de tempo fixo predeterminado ser encontrado no estado j : $P(X_{t+1} = j | X_t = i)$, para todo $t = 0, 1, 2, \dots$. Para n passos à frente, é

possível escrever as probabilidades de transição para cada i e j , com $n = 0, 1, 2, \dots$, conforme a expressão: $P(X_{t+n} = j | X_t = i) = P(X_n = j | X_0 = i)$, para todo $t = 0, 1, 2, \dots$. Simplificando, tem-se: $P(X_1 = j | X_0 = i) = p_{ij}$; $P(X_n = j | X_0 = i) = p_{ij}(n)$.

De acordo com a referência de Alves e Menezes (2010), a notação $P_{ij}(n)$, citada anteriormente, implica que, para $n = 0$, $P_{ij}(0)$ é $P(X_0 = j | X_0 = i)$, sendo se $i = j$ igual a 1, senão será 0 (zero).

Uma maneira simples de visualizar um tipo específico de cadeia de Markov é por meio de uma máquina de estados finitos. Se o processo está no estado j no tempo n , então a probabilidade de que você se mova para o estado i no tempo $n+1$ não depende de n , e somente depende do estado atual j em que você está. Assim, em qualquer tempo n , uma cadeia de Markov finita pode ser caracterizada por uma matriz de probabilidades cujo elemento (i, j) é dado por $P_{ij} = \Pr(X_{n+1} = i | X_n = j)$ e é independente do tempo n . As integrações na probabilidade de transição de k passos são somatórias, e podem ser calculadas como a k -ésima potência da matriz de transição. Isto é, se P é a matriz de transição para um passo, então P^k é a matriz de transição para a transição de k passos. Esses tipos de cadeia de Markov finitas e discretas podem também ser descritas por meio de um grafo dirigido, que se compõe de nós, que são os estados, e arcos direcionados que simbolizam as transições entre estados. Esse grafo é denominado diagrama de transição.

Para melhor compreensão, será inicialmente exemplificada com apenas dois possíveis estados (parada e operando), sendo o espaço de estados $S = \{0, 1\}$. Considera-se que os estados parados e operando são representados pelos índices 0 e 1, respectivamente. A partir de observações históricas de manutenção, foram obtidas as probabilidades de transição supostas constantes, uma bomba em operação continuará em operação com probabilidade igual a $\frac{3}{4}$ e entrará em falha com probabilidade $\frac{1}{4}$ de parada. Bombas paradas continuarão paradas com probabilidades iguais a $\frac{1}{2}$, enquanto que a probabilidade de uma bomba parada suceder uma bomba em operação é de $\frac{1}{2}$.

O produto cartesiano, $S \times S$, é $\{(0,0), (0,1), (1,0), (1,1)\}$. A matriz de probabilidades de transição para um passo é a seguinte:

$$P = \begin{matrix} & p_{00} & p_{01} \\ p_{10} & p_{11} \end{matrix} \rightarrow P = \begin{bmatrix} 1/2 & 1/2 \\ 1/4 & 3/4 \end{bmatrix}.$$

A representação em grafo, Figura 7:

Figura 7 – Grafo de Estados - Markov.

Fonte: Elaborado pela autora, conforme modelagem no software CARMS.

Ainda buscando a solução para o exemplo mencionado, pode-se também fazer uso do diagrama em árvore partindo do estado 0 (vide Quadro 6), considerando apenas 4 passos, sabendo que os eventos são independentes e que é preciso multiplicar todas as probabilidades do percurso trilhado no diagrama que levam ao estado da probabilidade desejada Quadro 6.

Quadro 6 – Planilha de probabilidade de estado em 4 passos.

	1º passo	2º passo	3º passo	4º passo
Parado	Operando	Operando	Operando	Operando
				Parado
		Parado	Parado	Operando
				Parado
			Operando	Operando
				Parado
	Parado	Operando	Operando	Operando
				Parado
		Parado	Parado	Operando
				Parado
			Operando	Operando
				Parado

Fonte: Elaborado pela autora.

Tabela 1 – Planilha de cálculo da probabilidade do estado parado P(0).

Produtos de probabilidades de transição	Probabilidades parciais
P01P11P11P11 = 1/2.3/4.3/4.3.4	0,2109375
P01P11P11P10 = 1/2.3/4.3/4.1/4	0,0703125
P01P11P10P01 = 1/2.3/4.1/4.1/2	0,046875
P01P11P10P00 = 1/2.3/4.1/4.1/2	0,046875
P01P10P01P11 = 1/2.1/4.1/2.3/4	0,046875
P01P10P01P10 = 1/2.1/4.1/2.1/4	0,015625
P01P10P00P01 = 1/2.1/4.1/2.1/2	0,03125
P01P10P00P00 = 1/2.1/4.1/2.1/2	0,03125
P00P01P11P11 = 1/2.1/2.3/4.3.4	0,140625
P00P01P11P10 = 1/2.1/2.3/4.1/4	0,046875
P00P01P10P01 = 1/2.1/2.1/4.1/2	0,03125
P00P01P10P00 = 1/2.1/2.1/4.1/2	0,03125
P00P00P01P11 = 1/2.1/2.1/2.3/4	0,09375
P00P00P01P10 = 1/2.1/2.1/2.1/4	0,03125
P00P00P00P01 = 1/2.1/2.1/2.1/2	0,0625
P00P00P00P00 = 1/2.1/2.1/2.1/2	0,0625

Fonte: Elaborado pela autora.

Vemos que a probabilidade do equipamento encontrar-se no estado parado $P0(4) = 0,3359375$, enquanto que no estado operando $P1(4) = 0,6640625$. Se for considerado um período de um ano, tem-se 2.942 horas da máquina parada.

A análise de cadeias de Markov utilizando matriz de probabilidades de transição pode ser efetuada tomando-se certas precauções, tendo em vista que nem todos os processos de Markov de tempo discreto comportam-se de modo semelhante à medida que o número de passos aumenta. Os estados de um processo de Markov são divididos em transitório e recorrente. Essa classificação diz respeito à probabilidade do processo retornar a um dado estado inicial se o processo partiu desse estado.

De acordo com a referência de Alves e Menezes (2010), a melhor forma de representar probabilidade de transição para n passos é a forma de matriz, considerando que seja $S = \{0, 1, \dots, M\}$ o conjunto finito de estados e seja o par de estados $(i, j) \in S \times S$, se associarmos a cada par (i, j) um número real $P_{ij}(n)$, de modo que sejam satisfeitas as propriedades $0 \leq P_{ij}(n) \leq 1$ para $\forall (i, j) \in S \times S$ e $\sum_{j \in S} P_{ij}(n) = 1$ para $\forall i \in S$, define-se a matriz P^n :

$$P^n = \begin{bmatrix} P_{00}(n) & P_{01}(n) & \dots & P_{0M}(n) \\ P_{10}(n) & P_{11}(n) & \dots & P_{1M}(n) \\ \vdots & \vdots & \vdots & \vdots \\ P_{M0}(n) & P_{M1}(n) & \dots & P_{MM}(n) \end{bmatrix}$$

Portanto, nota-se que, se $n=0$, tem-se a própria matriz identidade, P^0 é $P_{ij}(0) = P(X_0 = j | X_0 = i)$, logo, tem-se: $P_{ij}(0) = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$, mas se $n > 0$, tomando como base o teorema da probabilidade total, $P_{ij}(n) = P(X_n = j | X_{n-1} = i)$, tem-se para o estado j em n passos: $P_j(n) = P(X_n = j) = \sum_i P_i(0) P_{ij}(n)$. Em resumo, $P(n) = P(0) P^n$. No estudo de caso desta pesquisa, os estados estabelecidos para os componentes em plantas de saneamentos são finitos (contáveis), desse modo é relativamente fácil a aplicação do processo de Markov, considerando o cálculo de P^n . Por exemplo, uma situação em que se tem o interesse em controlar os estados dos equipamentos dosadores com definição de estados finitos, em que, conforme o histórico, uma determinada unidade dosadora de hipoclorito que hoje está funcionando perfeitamente pode, amanhã, apresentar uma pequena avaria (que a permita continuar operando), com probabilidade de 30%, ou quebrar completamente, sem possibilidade de conserto, com probabilidade de 20%. Por outro lado, se a unidade apresenta

hoje uma pequena avaria, a probabilidade de que amanhã ela esteja totalmente quebrada é de 70%.

Suponha que o processo estocástico que descreve o estado da unidade (perfeita, levemente avariada ou completamente quebrada) seja uma cadeia de Markov homogênea. Se a unidade está perfeita em determinado dia, a probabilidade de que ela esteja completamente quebrada dois dias depois será avaliada conforme a tendência:

- **1° Dia:** pequena avaria (0,3) ou totalmente quebrada (0,2) ou funcionando (0,5);
- **2° Dia:** pequena avaria do 1° dia (0,3) e totalmente quebrada no 2° dia (0,7) ou totalmente quebrada no 1° dia (0,2) ou funcionando no 1° dia (0,5) e totalmente quebrada no 2° (0,2).

Logo, tem-se: $(0,3 * 0,7 + 0,2 + 0,5 * 0,2) = 0,21 + 0,2 + 0,1 = 0,51$. Portanto, para situações de baixa complexidade, uma análise rápida por Markov, tendo como referência os estados e históricos do equipamento, facilmente identificaria a probabilidade de falha da bomba dosadora após dois dias de uso. Porém, a modelagem matemática não é nada trivial para casos em que o espaço de estados tendem a infinito, ou seja, o comportamento é assintótico, $n \rightarrow \infty$, de $p(n)$ e P^n , como, por exemplo, situações em que se deseja utilizar Markov para controle de dosagem de produto químico no tratamento de água.

Em uma abordagem de Markov para analisar a segurança, considera-se um sistema de segurança que é testado periodicamente com intervalo de teste t . Quando uma falha é detectada durante um teste, o sistema é reparado. O tempo necessário para o teste e reparação é desprezado. A abordagem a seguir é baseada em Rausand e Hoyland (2004). Seja $X(t)$ o estado do sistema *Safety* no tempo t , e que $X = \{0, 1, \dots, r\}$, tem-se um conjunto finito de todos os estados possíveis. Suponha que podemos dividir o espaço de estado X em duas partes, um conjunto B de estado em funcionamento e um conjunto F de estado em falha, de tal forma que $F = X - B$. A probabilidade média de falha *on demand*, PFD (n), do sistema de teste de intervalo n é:

$$PFD(n) = \frac{1}{t} \int_{(n-1)t}^{nt} \Pr(X(t) \in F) dt$$

Para $n = 1, 2, \dots$, se uma demanda para a segurança ocorre no intervalo n , a probabilidade (média) de que o sistema de *Safety* seja capaz de acionar o equipamento (instrumento) e desliga-lo é $PFD(n)$.

Assume-se que $\{X(t)\}$ comporta-se como um processo de Markov homogêneo com matriz de transição A , enquanto o tempo é executado dentro de um intervalo de teste, isto é, dentro de intervalos $(n-1)t \leq t < nt$, para $n = 1, 2, \dots$. Seja $P_{jk}(t) = \Pr(X(t) = k | X(0) = j)$, indica a transição da probabilidade para $j, k \in X$, e seja $P(t)$, de modo que corresponde à matriz. Falhas detectadas por falhas de diagnóstico autoteste podem ocorrer e serem reparadas dentro do intervalo de testes.

Seja $Y_n = X(nt-)$, de modo que o estado do sistema imediatamente anterior ao tempo nt é imediatamente anterior ao teste n . Se o estado de falha de funcionamento é detectado durante o teste, uma ação de reparo é iniciada e mudanças do estado de Y_n para Z_n , sendo Z_n o estado do sistema após o teste n . Quando Y_n é conhecido, pode-se assumir que Z_n é independente das transições do sistema antes do tempo nt . Seja $\Pr(Z_n = j | Y_n = i) = R_{ij}$ para todo $i, j \in X$ a transição da probabilidade, e seja R o correspondente à matriz de transição. Se o estado do sistema é $Y_n = i$ antes do teste n , a matriz R apresenta a probabilidade de o sistema estar no estado $Z_n = j$, logo após o teste/reparo n . A matriz R depende da estratégia de reparo e também da qualidade das ações de reparo.

Em todas as áreas da atividade humana busca-se quantificar eventos que possuem certo grau de incerteza de ocorrência, isso implica em prever as possíveis ocorrências. Modelos matemáticos probabilísticos são concebidos para auxiliar o homem na tomada de decisão e nessa situação foi utilizado Markov para apoiar de modo quantitativo a análise de risco, porém nem sempre é o suficiente para o desenvolvimento quantitativo da análise.

A análise do risco envolve a segurança do processo (*safety*) está diretamente ligada à segurança das pessoas e do meio ambiente, e a segurança da informação (*security*) que se refere à segurança da tecnologia envolvida, seja

ela *software* ou *hardware*. Porém, em função do alto nível de automação dos processos, é difícil de traçar os limites de atuação entre as duas áreas *safety/security*.

2.2 SEGURANÇA DA INFORMAÇÃO – *SECURITY*

A segurança da informação tem uma ampla abrangência, como definido pela *Federal Information Processing Standards – FIPS 199* (2004), contendo sete categorias:

- **Confidencialidade:** o objetivo da confidencialidade trata de impedir a divulgação de informação a pessoas ou sistemas não autorizados. No caso dos sistemas de controle e automação, esse objetivo é relevante tanto em relação à informação específica de processos, por exemplo, as fórmulas de produtos ou os dados de planejamento e rendimento de uma planta, quanto em relação aos segredos específicos dos próprios mecanismos de segurança, por exemplo, senhas;
- **Integridade:** o objetivo da integridade é garantir a detecção das modificações de informações específicas feitas por pessoas ou sistemas não autorizados. No caso dos sistemas de automação, esse objetivo se aplica a informações como as fórmulas dos processos, os valores de sensores e comandos de controle. A violação da integridade pode criar problemas de segurança ao equipamento e consequentemente ao meio ambiente, e mesmo as pessoas podem sofrer danos;
- **Disponibilidade:** a disponibilidade significa garantir que as informações e sistemas estejam disponíveis quando necessárias. A indisponibilidade (*Denial of Service – DoS*) pode não apenas causar danos econômicos, mas também problemas de segurança, já que os operadores podem perder a capacidade de supervisionar e controlar o processo da planta;

- Controle de acesso: o objetivo é tornar dados, aplicações e comunicação disponíveis apenas para quem tem permissão para tal;
- Autenticação: a autenticação se refere a determinar a verdadeira identidade do usuário de um sistema e correlacionar essa identidade com um registro interno do sistema, sendo que o sistema reconhece esse usuário;
- Autorização: o objetivo da autorização é conceder aos usuários, programas ou processos o direito de controle limitado após a autenticação do mesmo;
- Auditabilidade: consiste em poder reconstruir a história completa do comportamento anterior do sistema a partir de registros de todas as ações relevantes executadas nele. Esse objetivo de segurança visa fundamentalmente a descobrir e averiguar as causas das falhas no funcionamento do sistema e estabelecer seu alcance ou as consequências de um incidente de segurança.

Nas empresas dos mais diversos segmentos, o uso de práticas de segurança da informação vem sendo estudado e utilizado para minimizar os riscos apresentados, porém esse universo digital está sujeito a diversos tipos de ataque, físicos ou virtuais, que comprometem as pessoas e os sistemas a eles interligados. As práticas adotadas podem resolver partes do problema da segurança, que devem contemplar todos os recursos: computacionais, infraestrutura e recursos humanos (MARCIANO, 2006). Diante disso, torna-se evidente o relacionamento entre o aspecto humano e computacional, para assim contribuir como um todo para a segurança da informação. Portanto, as práticas de segurança da informação devem considerar os aspectos tecnológicos e humanísticos, pois, dessa forma, o ambiente como um todo é tratado de forma segura (MARTINS; SANTOS, 2005).

A segurança da informação requer um trabalho contínuo de acompanhamento e análise crítica periódica dos riscos, dos controles implementados, dos eventos, das mudanças nos requisitos de negócio e suas prioridades, para que os controles aplicados continuem eficientes e adequados;

além do constante estudo de novas tecnologias, de novas táticas de defesa e de novos ataques que poderiam comprometer a segurança do sistema.

O conjunto de normas que trata especificamente de segurança da informação é ISO/IEC 27000, tendo por influência o padrão inglês BS 7799, que se tornou um código de boas práticas para a gestão de segurança da informação, oferecendo um modelo de controle para identificação de requisitos. A identificação dos requisitos decorre da seleção de controles adequados para reduzir os riscos para valores aceitáveis. Já a padronização de segurança para sistemas de automação é feita pelas normas International Society of Automation (ISA) 99. Verifica-se nesta pesquisa a relevância da utilização dos critérios de melhores práticas recomendados nas duas normas, seja ele especificamente de tecnologia da informação(TI) ou de tecnologia de automação(TA).

As normas da série ISA 99 (2007) abordam aplicações do conceito de segurança para obter os requisitos mínimos de segurança no processo, que envolvem:

- ISA 99.00.01 – *Part 1: Terminology, Concepts and Models*. Estabelece as terminologias, conceitos e modelos para o ambiente de automação;
- ISA 99.00.02 – *Part 2: Establishing an industrial Automation and Control System Security Program*. Descreve os elementos de gerenciamento seguro e provê orientação para as aplicações de automação industrial e sistemas de controle com segurança;
- ISA 99.00.03 – *Part 3: Operating an Industrial Automation and Control System Security Program*. Aborda como operar um ambiente de automação seguro após a concepção e implantação;
- ISA 99.00.04 – *Part 4: Technical Security Requirements for Industrial Automation and Control Systems*. Define características de automação industrial e sistemas de controle, e o que os diferencia de outros sistemas de tecnologia da informação, tendo por base o ponto de vista de segurança.

Adicionalmente, o comitê da ISA produziu dois relatórios técnicos:

- ANSI/ISA-TR 99.00.01-2007 – *Technologies for Protecting Manufacturing and Control Systems*. Descreve as tecnologias de segurança e o seu uso com a automação industrial e sistemas de controle;
- ANSI/ISA-TR 99.00.02-2004 – *Integrating Electronic Security into the Manufacturing and Control Systems Environment*. Descreve como equipamentos de segurança eletrônicos podem ser integrados com a automação industrial e os sistemas de controle;

Relacionamento entre tais normas.

Atualmente, a ISA 99 é a principal norma com recomendações que integra as áreas de tecnologia da informação e automação, pois apresenta arquitetura híbrida com a comunicação entre os dois ambientes, conforme se observa na Figura 8.

Figura 8 – Cenário sugerido pela ISA 99.

Fonte: ISA 99 (2007, grifo da autora).

Verifica-se que mesmo esta norma que abrange as duas áreas security/safety, possui inúmeras limitações quanto às vulnerabilidades na arquitetura de acesso ao sistema, pois a arquitetura proposta conforme Figura 9, apresenta modems e equipamentos sem fio conectados diretamente a rede de automação e apenas um firewall é sugerido na infraestrutura. Além da utilização

do servidor OPC que demanda inúmeras portas de acesso sem qualquer segregação na arquitetura.

A ISA 99 possui suas limitações, porém é uma das poucas normas que faz referência à tecnologia necessária para melhores práticas de segurança em redes de automação, tais como: segmentação da rede, utilização de firewall etc., além de identificar as possíveis vulnerabilidades dos ambientes, conforme síntese apresentada no Quadro 7:

Quadro 7 – Recomendações da ISA 99.

Tecnologia	Descrição	Vulnerabilidades corrigidas	Deficiências	Recomendações
<i>Virtual Networks (Vlan)</i>	Segmentação das redes físicas em redes lógicas.	Segregação de tráfego.	<i>Spoof Mac, Spanning tree protocols VLAN Hopping.</i>	Atualizações periódicas da versão; Segmentação da rede corporativa da industrial.
<i>Network Firewalls</i>	Mecanismo utilizado para controle de tráfego	Proteção das redes que passam pelo dispositivo.	Necessidade de trabalhar em conjunto com detectores de intrusão; Grande quantidade de <i>logs</i> ; Profissionais capacitados para as operações diárias.	Segmentação das redes em zonas; Criação de DMZ para tráfego na internet.
<i>Virtual Private Network (VPN)</i>	Acesso remoto com criptografia.	Acesso controlado a redes via autenticação.	Acesso de qualquer lugar (internet) à rede corporativa.	Método de autenticação forte.
Utilitários de <i>log</i> de auditoria	Ferramenta de apoio de <i>log</i> .	Checagem de autenticação e utilização.	Extensiva documentação e <i>backup</i> .	Planejamento estratégico junto a outras áreas.
<i>Biometric Authentication</i>	Autenticação biométrica.	Autenticação forte.	Pouco utilizado.	Utilização pontual em equipamentos restritos.
Tecnologia de Autenticação e Autorização	Permissão e níveis de acesso.	Acesso controlado a redes via autenticação.	Necessidade de sincronização com todos os ativos do ambiente.	Método de autenticação/autorização centralizada na rede.
Criptografia	Processo de cifragem e decifragem.	Criptografia em tráfego <i>clear text</i> .	Deve-se utilizar um método de criptografia que todos os equipamentos suportem.	Uso de criptografia em toda comunicação interna e externa.
Detectores de Intrusão	Utilitário para detecção de eventos não permitidos na rede.	Identificação de tráfego malicioso.	Requer atualização de assinaturas e excesso de falso positivo.	Utilização em segmentos.
Controle Físico	Acesso restrito aos equipamentos de campo.	Somente pessoas autorizadas podem manipular e realizar alterações físicas.	Se não utilizada com um método de biometria, pode se mostrar ineficaz.	Acesso controlado.

Fonte: Azevedo, Kofuji e Martins (2013).

3 ESTADO DA ARTE E TRABALHOS RELACIONADOS

Este capítulo descreve os principais trabalhos relacionados a esta pesquisa. Aborda artigos sobre avaliação de riscos para plantas de serviços críticos, e outros que apresentam as vulnerabilidades de sistemas de tratamento de água e ferramentas de monitoramento *online*. Portanto, apresentam-se o estado da arte e os trabalhos relacionados a esta proposta sobre o modelo referencial para análise de risco com base no método CORAS e aprimoramento por cadeia de Markov e MTBF para a avaliação de falhas.

Métodos tradicionais de análise de riscos são imprevisíveis para situações que envolvam *security* e *safety* inter-relacionados, devido à falta de modularidade. Dessa forma, os métodos de análise convencionais de risco são inadequados para enfrentar esses desafios. Conforme Lund, Solhaug e Stolen (2011), o CORAS foi desenvolvido para resolver situações como esta.

Dessa forma, o método base deste estudo é o CORAS, pois o mesmo já realiza uma integração de diversas técnicas de análise de risco. As principais contribuições desta pesquisa envolvem a metodologia para a gestão de risco em sete etapas e o aprimoramento do CORAS na avaliação quantitativa, baseado na modelagem por Markov para análise de falha em processo automatizado, que poderá ser usado para resolver diversos problemas, tais como:

- Análise de falha do ambiente;
- Avaliação e possíveis soluções para problemas operacionais;
- Preparação para eventos especiais;
- Análise das pressões da rede e verificação de refluxo;
- Análise da qualidade de medição;
- Investigações da qualidade da água;
- Impacto na continuidade das operações etc.

O resultado dessa tese é uma metodologia (*framework*) para gestão de risco, validada em um sistema de bombeamento de esgoto, com base em

diagramas de ameaça CORAS e os valores de confiabilidade gerados com MTBF e cadeias de Markov para calcular a probabilidade dos riscos.

As cadeias de Markov são muito utilizadas para fazer equações de probabilidade, e mostram como um estado pode afetar outro ou todo o sistema. Muitos métodos de análise levam a previsões otimistas para o sistema, porque eles assumem que os componentes são independentes. Enquanto que a análise de Markov olha a confiabilidade e disponibilidade do sistema, em que os componentes apresentam forte dependência. Com o diagrama de transição de estado, permite ver como o sistema reage se houver mudança em um de seus estados.

3.1 TRABALHOS RELACIONADOS

Diversos estudos foram avaliados, principalmente os que envolviam falhas em sistemas de saneamento. Análises pontuais dessas pesquisas possibilitaram o desenvolvimento com maior maturidade do estudo de caso para validação da metodologia proposta.

Um artigo que foi referência para esta pesquisa é o de Dominguez-Chicas e Srimshaw (2010), que aplicam técnicas de análise de modo de falha (FMEA) para avaliação de risco no processo de reuso de efluentes. Utilizam modelagem para investigar pontos e tempos de contaminação. Outro artigo de Wang e Zeng, apresentado na IEEE 2010 – 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), apresenta o estudo sobre o método de avaliação quantitativa de riscos de segurança da informação, utilizando AHP e matemática Fuzzy como modelos quantitativos e cita o CORAS apenas como qualitativo. Porém, verifica-se nesse estudo que o CORAS apresenta uma ampla modelagem qualitativa e em algumas situações abordagem quantitativa por Markov, contudo se verifica que com aprimoramento do método CORAS é possível torná-lo capaz de atender a diversas situações.

Os autores Ostfeld e Shamir (1993) desenvolveram um modelo de otimização da qualidade da água usando estado constante e estado dinâmico por um sistema geral de modelagem algébrica.

Já o estudo desenvolvido por Mays e Tung (1992) apresenta a limitação do número de reservatórios e do número de bombas, pois o aumento do número de discretizações e variáveis de estado, conseqüentemente, aumenta o tamanho do problema drasticamente, sendo necessário restringir a aplicação do método para pequenos sistemas.

Conforme Murphy (1991), a primeira aplicação de modelagem de qualidade da água para sistemas de distribuição foi o caso de Woburn, Massachusetts. O modelo foi usado para comprovar a contaminação que tinha acontecido anos antes, portanto várias versões diferentes do modelo foram necessárias para refletir a forma como o sistema evoluiu ao longo do tempo. A mesma modelagem também se aplica ao caso de contaminação em San Jose, Califórnia.

A Agência Americana de Proteção Ambiental (US *Environmental Protection Agency* – USEPA) aplicou a modelagem da qualidade da água para investigar a contaminação em Cabool, Missouri (*Escherichia coli* sorotipo 0157: H7) e Gideon, Missouri (*Salmonella typhimurium*). O surto de Cabool envolveu 243 casos e seis mortes e foi atribuído a duas quebras de linha de água (GELDREICH, 1996).

Em Gideon, a modelagem da qualidade da água foi utilizada para identificar a contaminação de um tanque por excrementos de pássaros como a provável fonte (CLARK; GRAYMAN, 1998). Algo similar ocorreu com o sistema de água contaminada em Walkerton, Ontario, Canadá.

Kramer et al. (1996) relatam que 26,7% dos surtos de doenças transmitidas pela água nos Estados Unidos em 1993-1994 foram devido à deficiência no sistema de distribuição de água e apresenta as vulnerabilidades do sistema.

Modelos de qualidade da água também têm sido utilizados em estudos forenses para identificar os responsáveis em litígio. Embora muitos estudos tenham sido realizados, poucos têm sido publicados por causa de questões legais que cercam tais aplicações. Dois casos de aplicações forenses de modelos de qualidade da água são documentados por Walski et al. (2001), um

em Phoenix e outro em Dover Township, Nova Jersey. Os autores relatam que as concentrações de contaminantes podem variar muito em um determinado local, em determinado horário ou em situações sazonais, devido a mudanças no funcionamento da bomba causadas por diferentes demandas.

Estudos forenses são diferentes da maioria dos modelos desenvolvidos para aplicações de análise de qualidade da água, pois, em vez de apenas executarem o modelo para um dia normal ou um dia de pico, esses modelos devem ser executados por um grande número de dias reais para reconstruir os acontecimentos históricos. Esse tipo de modelagem envolve uma grande quantidade de pesquisas sobre como o sistema estava sendo operado quando a contaminação ocorreu. Porque o sistema evoluiu ao longo de muitos anos, várias versões do modelo são necessárias para refletir topologias diferentes, instalações e carga da rede.

Enquanto na literatura são encontrados normalmente estudos de qualidade de água com ênfase em análise por contaminação de cloro (CLARK; GRAYMAN, 1998; ROSSMAN; CLARK; GRAYMAN, 1994), estudos forenses podem envolver uma variedade de contaminantes, incluindo *Volatile Organic Compounds* (VOCs), micróbios e produtos químicos inorgânicos. Os comportamentos de alguns produtos químicos são muitas vezes tratados nos modelos como únicos, contudo os produtos químicos podem sofrer uma variedade de transformações.

Mesmo quando não é possível modelar com precisão o comportamento de um produto químico ou de um microrganismo em um sistema de distribuição, modelos de qualidade da água podem fornecer um panorama de como a água se move no sistema e, portanto, quais partes do sistema estão expostas à água de fontes particulares, tanques, ou quebra da tubulação. Conforme Walski et al. (2001), outro controle importante na análise de vulnerabilidade de um sistema de tratamento de água é o da pressão dos hidrantes, pois um dos modelos de ataques envolve a abertura do hidrante e o sistema de refluxo para inserção de contaminante na rede, o que alteraria a pressão nesse ponto; em condição normal o hidrante deverá encontrar-se em ponto de pressão estática. O controle e os testes de hidrantes em uma rede de distribuição podem ser monitorados pelo CCO, se a concessionária possuir uma modelagem bem definida e calibrada, integrada com o modelo de análise de risco.

Uma abordagem relevante foi apresentada por Kominek e Byres (2011) em seu artigo sobre proteção de sistemas de controles industriais baseados em OPC Server, recurso similar ao estudo de caso desta pesquisa. Situação em que apenas o uso de firewalls tradicionais de TI para isolar os vários sistemas de controle, possibilita a existência de várias portas abertas em função da necessidade do uso dinâmico de portas do OPC. Assim como, a demanda de acesso remoto tornou muitos sistemas de controle acessível através de redes externas, aumentando a vulnerabilidade do ambiente automatizado.

Além da análise dos diversos trabalhos relacionados com as vulnerabilidades das plantas de saneamento foram vistos também artigos que tratam de gestão de risco, entretanto, verifica-se a existência de diversas pesquisas com ênfase na área financeira e com foco na visão estratégica, porém o mesmo não ocorre para área operacional, especialmente em saneamento.

A gestão de riscos ultrapassa a análise de vulnerabilidades e riscos de uma planta, produto ou protótipo. Define-se na ISO 2002 que a gestão de riscos baseia-se em atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. A mesma envolve um processo criterioso e recursivo de documentação, avaliação e decisão durante todas as fases do ciclo de vida do projeto.

Conforme Brandão e Fraga (2008) a gestão de riscos baseia-se em princípios e boas práticas de gerenciamento e segurança, para auxiliar na tomada de decisões. Entre as ferramentas metodológicas disponíveis para o desenvolvimento da gestão de riscos, destacamos a especificação SP800-30 - *Risk Management Guide for Information Technology Systems* (STONEBURNER et al., 2002) desenvolvida pelo NIST (National Institute of Standards and Technology), a especificação AS/NZ4360 (AS/NZS, 2004) desenvolvida pelos governos da Austrália e Nova Zelândia, a norma ISO/IEC 27005:2008 e a proposta de norma ISO 31000 (ISO/IEC 31000, 2009). Os principais padrões com recomendações na área de gestão de risco podem ser visto na Figura 10.

Dentre os principais padrões com as recomendações de gestão de risco/segurança apresentadas na Figura 9, a SP800-30 fornece a fundamentação para o desenvolvimento de um programa de gestão de risco, contendo as definições e as direções necessárias para avaliar e atenuar os riscos identificados em sistemas de Tecnologia da Informação – TI (*security*),

porém para aplicar em área de Tecnologia de Automação - TA, verifica-se a necessidade de revisão e ajustes nas propostas e recomendações já existentes para ampliar o escopo de atuação em tecnologias da área de automação em um ambiente que demande segurança do processo (safety).

Figura 9 – Padrões de Gestão de SGSI e Riscos.

Fonte: <http://dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/ceseg:2008-sbseg-mc1.pdf>

em 10 de outubro de 2013.

Além dos trabalhos já citados nesta pesquisa, há também uma relação de continuidade com a pesquisa desenvolvida pela autora durante Mestrado, pois amplia os estudos desenvolvidos em segurança da informação – security, o que possibilita o desenvolvimento de uma metodologia mais completa com ênfase na área de automação e com análise de riscos, confiabilidade e falhas em plantas operacionais, não contempladas na pesquisa do mestrado.

3.2 ANÁLISE QUANTITATIVA DE RISCO E CONFIABILIDADE

Para o desenvolvimento desta pesquisa, inicialmente foi realizado um extenso levantamento bibliográfico para conhecer o estado da arte das técnicas de análise risco e modelos já desenvolvidos. Esse levantamento mostrou, fundamentalmente, a existência de um grupo de pesquisas utilizando modelos e técnicas com a geração do método CORAS para análise e avaliação do risco, contemplando áreas de *security* e *safety*, porém carente na abordagem quantitativa e sem demonstrações de aplicação em área de plantas de saneamento.

A integração da cadeia de Markov ao modelo CORAS possibilita a avaliação de análise de falha quantitativa em várias situações, por exemplo:

Considere um sistema de recalque de esgoto com dois conjuntos de motor bomba idênticos. Seja X_n a variável aleatória tal que seu valor é o número de bombas em operação normal no passo n . Se uma das bombas falhar, ela poderá ser consertada, enquanto, se ambas falharem, o sistema irá parar, mas ainda haverá possibilidade de que uma das bombas seja consertada sendo esta a reigência do processo de Markov e não a transição para outro estado.

As probabilidades são as seguintes: se uma bomba que nunca passou por reparo é boa no tempo t_{n-1} , ela tem confiabilidade de 90% no tempo t_n ; porém, uma bomba que se estragou no tempo t_{n-1} , após reparada, é apenas 60% confiável no tempo t_n . Sabendo que as probabilidades são independentes e de tempo discreto, ou seja, modelo Binomial, pois a falha de uma bomba não

implica a falha da outra e cada bomba só pode ser encontrada em uma das duas condições. Os valores possíveis para a variável X são: 0, 1 e 2, sendo, respectivamente, duas bombas paradas, apenas uma operando e ambas operando. Então se tem:

1. Ambas em operação, $P(X_n = 2|X_{n-1} = 2) = P_{22} = 0,9 \times 0,9 = 0,81$;
2. Uma bomba em operação e a outra em falha, $P(X_n = 1|X_{n-1} = 2) = P_{21} = 0,9 \times 0,1 + 0,1 \times 0,9 = 0,18$;
3. Ambas em falha, $P(X_n = 0|X_{n-1} = 2) = P_{20} = 1 - P_{22} - P_{21} = 0,01$;
4. Uma em operação e a outra em operação após reparo, $P(X_n = 2|X_{n-1} = 1) = P_{12} = 0,9 \times 0,6 = 0,54$;
5. Nenhuma em operação, sendo que apenas uma estava boa, $P(X_n = 0|X_{n-1} = 1) = P_{10} = 0,1 \times 0,4 = 0,04$;
6. Uma em operação sendo que uma delas estava em falha, $P(X_n = 1|X_{n-1} = 1) = P_{11} = 1 - P_{12} - P_{10} = 0,42$.

O estado 0 é absorvente, uma vez que entrando nele não se pode abandoná-lo, exceto se o processo partir novamente, portanto, $P_{00} = 1$.

A matriz de probabilidades de transição para um passo será:

$$P = \begin{matrix} & \begin{matrix} 2 & 1 & 0 \end{matrix} \\ \begin{matrix} 2 \\ 1 \\ 0 \end{matrix} & \begin{bmatrix} 0,81 & 0,18 & 0,01 \\ 0,54 & 0,42 & 0,04 \\ 0 & 0 & 1 \end{bmatrix} \end{matrix}$$

A metodologia proposta neste trabalho também implementa a análise de FMEA conforme diversas normas, principalmente a IEC 61508 e outras normas, gerando hierarquia de blocos com as conexões lógicas entre os subsistemas e componentes que constituem o sistema de tratamento de água e/ou esgoto, com o objetivo de representar modos de falhas em vários níveis hierárquicos da planta. Possibilitando rastrear automaticamente efeitos de falha, os valores de gravidade e as causas de falha por meio da hierarquia do sistema. A modelagem calcula as taxas de falha e os valores de criticidade. Busca-se com o FMEA

identificar falhas detectáveis e não detectáveis e determina a relação entre a frequência de falhas e fracassos detectáveis.

A metodologia proposta também aplica uma abordagem quantitativa ao cálculo da criticidade ou à atribuição de uma probabilidade de ocorrência. O sistema deverá ser alimentado com entrada de dados por meio do preenchimento dos campos solicitados. O aprimoramento na modelagem poderá promover a integração com a base de informações históricas do banco de dados do SCADA, sob os quais são aplicados cálculos de probabilidade matemática.

Na análise, é necessário identificar a probabilidade de falha, que na fórmula é chamada de β . A probabilidade do efeito de falha resultará na classificação da criticidade. Os valores representam o julgamento do analista para a probabilidade de ocorrência da perda que poderá ser, conforme os valores apresentados na Tabela 2.

Tabela 2 – Classificação do efeito.

Efeito de Falha	Valor (β)
Perda Real	1,0
Perda Provável	> 0,10 a <1,00
Possível Perda	>0 a <= 0,10
Nenhum Efeito	=0

Fonte: MIL-HDBK-217 (1991).

A relação de modo de falha é a probabilidade expressa como uma fração decimal do equipamento/processo/ou item que falhará. Se todos os potenciais modos de falha de um processo são listados, a soma dos valores deverá ser igual a um.

A taxa de fração da falha no processo (λ_p) deverá ser encontrada a partir da previsão de confiabilidade, conforme o procedimento MIL-HDBK-217 (1991).

O tempo de operação (t) será a quantidade de horas conforme evento.

O cálculo da criticidade requer o uso de taxas de falhas específicas e de dados de configuração. Quando as configurações são conhecidas, as taxas de falhas podem ser obtidas a partir da previsão de segurança do sistema, de dados já conhecidos a partir de ambientes similares, ou por histórico de falhas no banco de dados, como mencionado na MIL-HDBK-217. Com taxas de falhas conhecidas, o número de criticidade de um item é o número de falhas de um tipo específico esperado por milhões de horas.

O cálculo do número crítico de modo de falha (C_m), para uma classificação de gravidade específica, dará o valor da classificação da falha, com base na fórmula descrita no padrão militar MIL-HDBK-217 (1991):

$$C_m = \beta \alpha \lambda_p t$$

Sendo:

C_m : O número de criticidade da falha.

β = Probabilidade condicional de perda do processo.

α = Razão do modo de falha.

λ_p = Taxa da parte da falha.

t = Tempo de duração da aplicação do processo normalmente em horas ou número de ciclos da operação.

O número de criticidade do item C_r , para uma classificação do grau de severidade e da gravidade, é então calculado pela soma dos C_m para cada modo de falha dessa mesma classificação de gravidade. Essa soma é dada pela expressão:

$$C_r = \sum_{n=1}^j (\beta \alpha \lambda_p t)_n \quad n = 1, 2, 3 \dots j$$

Sendo:

C_r = O número de criticidade de cada item do processo.

n = Os modos de falha nos itens que se enquadram uma classificação de criticidade particular.

j = O último modo de falha no item sobre a criticidade em classificação.

Esta pesquisa fez uso da matriz de criticidade como um meio de identificação e comparação de cada modo de falha com outras falhas do processo e sua relação com a gravidade. Fazem parte da matriz: o número de identificação, o item de identificação funcional, a função e os modos de falhas e causas, a fase operacional, além da classificação da gravidade. A matriz é gerada após os cálculos da criticidade, ou mesmo na atribuição de uma probabilidade de ocorrência. O resultado do cálculo da criticidade tem o papel de fornecer uma classificação relativa para as falhas ou fracassos e não como valor

absoluto, afinal as taxas de insucesso são geralmente definidas em termos de falhas por milhão de horas ($fx10^6$).

A matriz resultante mostra a distribuição de criticidade de modos de falha por item e possibilita a criação do diagrama de tratamento com a ferramenta para atribuir corretivas.

Para a análise quantitativa, foi utilizado também o modelo de cálculo do MTBF descrito na IEEE 493-2007, principalmente em situações como a apresentada no estudo de caso em que o medidor de nível do poço das bombas tem uma taxa de falha de $2,3 \times 10^{-8}$ por hora. No entanto, sob o estresse de vibração e cavitação das bombas, sabe-se que a taxa de falha passa para $1,5 \times 10^{-5}$ por hora. O tempo de falha é distribuído exponencialmente, de modo que se tem:

$$f(t) = (1,5 \times 10^{-5}) e^{-(1,5 \times 10^{-5})t}, t \geq 0, = 0 \text{ caso contrário},$$

$$R(t) = e^{-(1,5 \times 10^{-5})t}, t \geq 0, = 0 \text{ caso contrário},$$

$$h(t) = 1,5 \times 10^{-5}, t \geq 0, = 0, \text{ caso contrário}.$$

Para determinar a confiabilidade em $t=10^4$ e $t=10^5$, calcula-se $R(10^4)=0,86$ e $R(10^5)=0,223$.

Considerando um sistema serial simples (Figura 10), como, por exemplo, no estudo de caso analisado de um CCM que controla as bombas na estação elevatória, vê-se que, para que o sistema funcione, todos os componentes devem funcionar, e se supõe que os componentes funcionem independentemente, então em análise do tempo médio de falha (TMF), tendo T_j o tempo de falha para o componente c_j , $j=1,2,...,n$ e T o tempo de falha do sistema. O modelo de confiabilidade é, então, $R(t) = P[T > t] = P(T_1 > t, PT_2 > t, \dots, PT_n > t)$, ou $R_t = R_1 t \cdot R_2 t \cdot \dots \cdot R_n t$, em que $PT_j > t = R_j t$.

Figura 10 – Sistema serial simples.

Fonte: Elaborado pela autora.

Conforme Rausand e Hoyland (2004), para quantificar qual a confiabilidade do sistema, pode-se, por exemplo, considerar que nesse sistema serial simples há três componentes e que devem todos funcionar para que o sistema funcione, cujas variáveis aleatórias T_1, T_2 e T_3 , que representam os tempos de falhas para cada componente, são independentes, e com as seguintes distribuições:

$$T_1 \sim N(2 \times 10^3, 4 \times 10^4),$$

$$T_2 \sim \text{Weibull} \left(y = 0, \delta = 1, \beta = \frac{1}{7} \right),$$

$$T_3 \sim \text{lognormal} (\mu = 10, \sigma^2 = 4), \text{ segue que:}$$

$$R_1(t) = 1 - \Phi \left(\frac{t - 2 \times 10^3}{200} \right)$$

$$R_2(t) = e^{-t^{(1/7)}}$$

$$R_3(t) = 1 - \Phi \left(\frac{\ln t - 10}{2} \right),$$

de modo que,

$$R(t) = \left[1 - \Phi \left(\frac{t - 2 \times 10^3}{200} \right) \right] \cdot [e^{-t^{(1/7)}}] \cdot \left[1 - \Phi \left(\frac{\ln t - 10}{2} \right) \right]$$

Se no estudo de caso o tempo analisado foi $t=2187$ horas, conforme base do sistema SCADA, então:

$$R(2187) = [1 - \Phi(0,935)][e^{-3}][1 - \Phi(-1,154)] = [0,175][0,0498][0,876] \cong 0,0076$$

Sabe-se que em um sistema serial simples a confiabilidade do sistema pode ser calculada com o uso do produto das funções de confiabilidade dos componentes, conforme demonstrado, no entanto, quando todos os componentes têm uma distribuição exponencial, os cálculos são simplificados, pois $R(t) = e^{-\lambda_1 t} \cdot e^{-\lambda_2 t} \dots e^{-\lambda_n t} = e^{-(\lambda_1 + \lambda_2 + \dots + \lambda_n)t}$, ou $R(t) = e^{-\lambda_s t}$, ou $R(t) = e^{-\lambda_s t}$, em que $\lambda_s = \sum_{j=1}^n \lambda_j$ representa a taxa de falha do sistema. Então, a função de confiabilidade do sistema é da mesma forma que as funções de confiabilidade dos componentes. Portanto, a taxa de falha do sistema é simplesmente a soma

das taxas de falha dos componentes, conforme cálculo do MTBF descrito na IEEE 493-2007.

Além da utilização de modelo matemático para avaliação de risco e do desenvolvimento de ferramentas de TI/TA, algumas das análises para o estudo de caso incluem:

- Método CORAS;
- Sistema de plano de programa de segurança (*System Safety Program Plan* – SSPP);
- Análise de perigos (PHA, SHA, SSHA, OSHA etc.);
- Avaliação da segurança (quantitativa e qualitativa);
- Avaliação qualitativa e quantitativa de risco probabilístico;
- Gestão de avaliação de risco;
- Análise de árvore de eventos;
- Análise da árvore de falhas (FTA).

Conforme CETESB P4.261(2003), verifica-se ainda que no estudo de risco do processo é relevante avaliar o risco social, valor do risco de um determinado grupo de pessoas, PLL (Potential Loss of Life), definido como a média de mortes por ano, como consequência da realização de certa atividade. A sua expressão é o somatório dos produtos das frequências(f) de cada um dos acidentes possíveis pelo número(n) esperado de mortes em cada acidente. calculado por:

$$PLL = \sum (f * n)$$

Podendo ser representado:

- Pela curva f-N, que expressa o risco de grupo, representados pela frequência estimada (f) de acidentes que podem causar N ou mais mortos;
- Ou por valores de risco calculados, especialmente para a instalação em análise, podem ser comparados com valores de riscos absolutos (valores regulamentados pelos governos ou internos da organização). Se o valor calculado superar o valor tomado como referência, será necessária uma redução do risco.

4 METODOLOGIA PROPOSTA E VALIDAÇÃO POR ESTUDO DE CASO

Esta pesquisa propõe uma metodologia para a gestão de risco que tem como base principal o método CORAS. Durante o desenvolvimento desta pesquisa se observou que o CORAS não contemplava algumas etapas importantes para uma gestão de risco completa, especialmente quanto a estimativa de risco, método quantitativo, e a verificação com auditoria do sistema de gestão de risco do processo.

Esta pesquisa considera que a concessionária do estudo de caso já possui uma planta de saneamento automatizada e em operação, portanto será validada a metodologia para gestão dos riscos e falhas do processo nesse ambiente com ênfase em tecnologia da automação.

A análise convencional de falhas de sistemas reparáveis estabelece o estudo de duas variáveis aleatórias de interesse: tempo entre falhas (*Time Between Failure* – TBF) e o tempo de reparo (TR). Considera-se neste trabalho que após a ocorrência de uma falha ocorre o reparo imediato, e que essa manutenção é capaz de levar o item que falhou (componente ou sistema) novamente à sua condição original, tendo as mesmas características que um componente novo. Como consequência, a distribuição da variável aleatória tempo até a falha (*Time to Failure* – TTF) será considerada igual à distribuição da variável aleatória TBF.

A metodologia proposta realiza a análise de risco/falha com base na modelagem matemática por MTBF e na cadeia de Markov, utilizando o histórico da base existente no sistema SCADA.

O principal ponto na gestão de risco é descobrir qual é o problema, o diagnóstico do risco, onde os riscos ocorrem e como tratá-los, além de auditá-los, considerando todo o processo como um fluxo cíclico. A análise de risco começa com uma descrição da situação e indica que as ameaças poderiam ser a razão para que ele ocorra, quais as consequências e como ele poderia ser evitado. Considera-se nesta tese uma metodologia para gestão de risco desenvolvida em sete fases, que envolve estabelecimento do contexto, identificação de riscos, estimativa do risco, avaliação de risco, tratamento,

verificação dos resultados e auditorias de acompanhamentos periódicos, em um fluxo contínuo com base no PDCA (Figura 11)

Figura 11 – Ciclo da metodologia de gestão de risco.

Fonte: Elaborado pela autora.

O momento de concepção apresentado na metodologia consiste em caracterizar o processo descrevendo o ambiente ao qual está vinculado, a sua missão, questões culturais, os seus requisitos. Enquanto que a primeira fase (1ª Fase) é a etapa da definição do contexto, momento em que se definem os parâmetros básicos, por meio dos quais serão identificados os riscos que precisam ser geridos e qual será o escopo do restante do processo de gestão de riscos. Também são definidos os critérios os quais serão utilizados na identificação, avaliação, impacto e aceitação dos riscos. A definição do contexto

tem como entrada todas as informações relevantes sobre a organização, que sejam relevantes para a definição do contexto da gestão de riscos de segurança.

O passo principal para se obter o contexto está na aplicação correta de técnicas como a HAZOP, que possibilite a descrição dos objetivos, premissas, e critérios dos ambientes que serão usados na determinação dos riscos do processo. Estes critérios envolvem a determinação das consequências de segurança e os métodos usados para a análise e avaliação dos riscos.

O passo seguinte (2ª Fase), refere-se a identificação dos riscos, conforme Brandão e Fraga (2008) essa é uma das etapas mais críticas, pois os riscos não identificados não serão analisados nem tratados. O objetivo dessa etapa é determinar os eventos que possam causar perdas potenciais e deve deixar claro como, onde e por que a perda pode ocorrer. A identificação deve conter os riscos que estão e os que não estão sob controle do processo em estudo. Na prática, a identificação de riscos é bem mais complexa, pois as informações, quase sempre, são baseadas em experiências e critérios subjetivos dos próprios responsáveis pelo projeto. (BRANDÃO; FRAGA, 2008). A identificação dos riscos envolve a identificação das ameaças, dos controles existentes, das vulnerabilidades e das consequências. Foi nesta fase do projeto que o método CORAS mais contribuiu para o desenvolvimento da análise de risco, conforme descrito na seção 4.4 desta tese.

A terceira fase (3ª Fase) da metodologia refere-se a estimativas, nesta etapa, são produzidos dados que irão auxiliar na decisão sobre quais riscos serão tratados e as formas de tratamento que serão adotadas, levando-se em consideração a eficiência de custos. Portanto envolve considerações sobre a origem dos riscos, suas consequências e as probabilidades de ocorrência dos mesmos, além do estudo de confiabilidade e disponibilidade do processo. A estimativa pode ser qualitativa ou quantitativa, ou mesmo uma combinação de ambas.

A estimativa qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das potenciais consequências e a probabilidade destas consequências ocorrerem, e são bem representadas na ferramenta CORAS, enquanto que a estimativa quantitativa adota modelagem matemática para determinação dos riscos, com estimativas das falhas, da confiabilidade do processo e análise da disponibilidade dos componentes no processo. Adota-se

nessa pesquisa a combinação os dois tipos de estimativas. São registradas as saídas desta fase da metodologia de gestão de risco, por formulários FMEA, planilhas MTBF, modelagens por Markov e consolidação no CORAS, conforme detalhamento nas seções seguintes.

A quarta fase (4ª Fase) da metodologia refere-se a avaliação, o objetivo da avaliação de riscos é facilitar a tomada de decisões, baseadas nos resultados da análise de risco das fases 2 e 3 da metodologia. É necessário definir as prioridades e a real necessidade de tratamento dos riscos analisados. A avaliação envolve a comparação dos níveis de risco encontrados, com os critérios estabelecidos quando o contexto foi considerado. É relevante nesta fase avaliar a segurança empresarial, os impactos da decisão tomada na seleção dos riscos aceitos. Porém nada impede que a qualquer momento uma nova avaliação seja realizada e novos riscos sejam tratados, pois o processo de gestão de risco é dinâmico.

A quinta fase (5ª Fase) refere-se ao tratamento do risco, que contempla desde a identificação das opções de tratamento, avaliação das opções, custos até a preparação para implementação dos tratamentos no cenário em estudo. Esta etapa é equivalente à etapa de atenuação de riscos da especificação SP800-30 ou mesmo da ISO/IEC 31000. O tratamento é identificado no diagrama de tratamento no CORAS, associados aos possíveis cenários de incidentes que os provocam. A cada um dos riscos são relacionadas opções de tratamento. Há quatro opções possíveis para o tratamento do risco: redução, retenção, prevenção e transferência. Ao término do tratamento são identificados os riscos residuais. Se tais riscos não forem aceitáveis, os tratamentos podem ser refeitos ou, ainda, todo o processo de gestão de riscos pode ser revisto. (BRANDÃO; FRAGA, 2008). A implementação do tratamento pode envolver a aquisição de tecnologias, ou não, pode ser simplesmente a criação de padrões, capacitação de pessoas e desenvolvimento de normas internas a serem obdecidas.

A fase da verificação (6ª Fase) é o momento do monitoramento e de verificação do resultado, portanto é essencial para o processo da gestão de riscos, pois os riscos não são estáticos e devem ser monitorados a fim de verificar a eficácia das estratégias de implementação e o resultado dos mecanismos de gerenciamento utilizados no tratamento dos riscos. Portanto, o

processo de monitoramento deve ser contínuo e dinâmico. Além do monitoramento contínuo, mudanças organizacionais ou externas podem alterar o contexto da análise, levando a necessidade de uma revisão completa da gestão de riscos.

A última fase da metodologia (7ª Fase), refere-se a auditoria, a qual consideramos muito importante para garantir a atualização do processo e eficácia da gestão de risco. As auditorias podem ser iniciadas periodicamente por equipe interna ou realizadas por terceiros. As auditorias internas têm a finalidade de verificar, com base em evidências objetivas, se as seguintes condições ocorrem satisfatoriamente:

- Os procedimentos e instruções operacionais são adequados e eficazes;
- As áreas vêm atuando em concordância com os documentos normativos e as listas de verificação são preenchidas;
- Os relatórios de alarmes e log estão sendo avaliados.

As não conformidades (reais e potenciais) detectadas devem ser registradas de acordo com procedimento específico, incluindo ações para registro e tomada de ação para encerramento da mesma. É indicada uma análise crítica das não conformidades e, caso pertinente, é executada a investigação de suas causas, a definição e a implantação de ações corretivas e o registro das alterações em procedimentos. Após a implantação das ações corretivas, deve ser feita uma avaliação de sua eficácia antes de seu encerramento.

Portanto, as quatro primeiras fases são na verdade suficientes para determinar o impacto dos riscos, e são contempladas no método CORAS, ou mesmo fazendo uma analogia ao ciclo do PDCA de qualidade, referem-se à fase do planejamento, enquanto que as fases cinco e seis, execução, correspondem ao processo da implantação do tratamento, mitigação dos riscos e verificação do resultado, e na última fase indica-se a auditoria periódica que deverá ser realizada para garantir que o sistema de análise de risco esteja sempre atualizado e evidenciando a real situação do sistema em operação.

Cada estágio do processo de gestão de riscos deve ser documentado de forma apropriada. Suposições, métodos, origens de dados, análises, resultados e justificativas das decisões tomadas devem ser registradas. Os relatórios produzidos devem ser o mais sucinto e objetivo quanto possível. (BRANDÃO; FRAGA, 2008).

O ciclo que é sugerido neste trabalho, se implementado, levará verdadeiramente a uma gestão de risco, e não apenas a uma avaliação pontual do risco em um sistema. A diferença é que em uma avaliação pontual de risco, normalmente, apenas se identifica, estima-se o risco e considera sua existência, enquanto que na gestão de risco, além da identificação, o risco é tratado e busca-se evitar que ocorra. No Apêndice D e na próxima seção deste texto são apresentados os diversos momentos do desenvolvimento do estudo de caso com a implantação de cada uma das fases da análise até a consolidação final do resultado de gestão de risco.

4.2 CENÁRIO DO ESTUDO DE CASO

A definição do cenário para o desenvolvimento do estudo de caso ocorreu em função da autora trabalhar em uma unidade de saneamento que demanda gestão de risco em função da criticidade da planta, além da facilidade de conseguir um ambiente favorável para validar a pesquisa.

O estudo foi desenvolvido em uma planta de tratamento de esgoto, especificamente uma Estação Elevatória de Esgoto (EEE), responsável pelo recalque de 2.300 l/s de esgoto e tem como base de avaliação apenas dois estados: operando ou parado, pois o contrato de operação dessa estação estabelece que ela não pode ter seus serviços interrompidos e deve ser monitorada a cada cinco minutos, conforme o Quadro Indicador de Desempenho (QID) estabelecido no edital de licitação pelo cliente; sendo que o não cumprimento desses indicadores de desempenho impacta diretamente no faturamento da empresa responsável pela operação, além de elevado risco

ambiental. A metodologia desenvolvida nesta pesquisa foi validada nesse cenário.

Foi realizada análise quantitativa por modelagem matemática (Markov e MTBF) para estabelecer os nível de confiabilidade do sistema e, após o conhecimento desses números, as informações foram consolidadas com a análise qualitativa realizada no CORAS, servindo assim de referência para plantas de saneamento. Para desenvolver a modelagem, o estudo foi iniciado com o componente mais crítico desse sistema, o conjunto motor bomba da elevatória, que possui a seguinte especificação:

É alimentada por um transformador principal TSA1 de 2.500 kVA, tensão primária de 11,9 kV e tensão secundária de 0,46 kV, ligação delta/triângulo. O secundário desse transformador alimenta o barramento geral do quadro. A partir desse barramento, estão sendo alimentados quatro inversores de frequência DANFOSS do tipo VLT AQUA DRIVE FC-202 P560-460V. O barramento alimenta ainda o transformador TSA2 de 75 kVA e o transformador TR3 de 150 kVA. Para o caso de falta de energia, existem três geradores de emergência. Esse sistema é responsável pelo funcionamento das bombas de recalque do esgoto.

São quatro conjuntos de motor bomba do tipo centrífuga de eixo vertical de simples estágio, com sucção axial e descarga radial do tipo Black Pull Out unificada, da marca ABS/Scanpump, modelo FR 500/00=67 C3S, com o motor elétrico de indução com rotor tipo gaiola, com potência de 550 KW (747 HP/cv), tensão nominal 440 V, corrente nominal 906 A, VI polos, rotação nominal 1.190 rpm, trifásico, frequência de 60 Hz, IP55.

Foi definido como premissa que o conjunto de bombeamento sempre deverá estar em operação para perfeito funcionamento do sistema e que o conjunto parado implica não realizar o recalque do sistema, consequentemente haverá prejuízo financeiro e ambiental, em função do extravasamento do esgoto.

O conjunto de bombeamento é formado por diversos subcomponentes, tais como: inversor de frequência, CLP, medidor de nível, etc.

Para esse cenário em estudo, foi realizado um estudo por MTBF, considerando que há um CCM automatizado de controle das bombas com CLP, formado por um circuito eletrônico com três aparelhos de circuito integrado, 12 diodos de silicone, 8 capacitores cerâmicos e 15 resistores de composição.

Conforme o *databook*, tem-se a informação das taxas de falhas, que sob níveis de estresse de temperatura, choque e outros, cada componente atua na faixa de falha conforme a Tabela 3 e que as falhas dos componentes são independentes.

Tabela 3 – Falhas dos componentes.

Componente	Falhas por hora
Circuitos integrados	$1,3 \times 10^{-9}$
Diodos	$1,7 \times 10^{-7}$
Capacitores	$1,2 \times 10^{-7}$
Resistores	$6,1 \times 10^{-8}$

Fonte: Elaborado pela autora.

Portanto,

$$\lambda_s = 3(0,013 \times 10^{-7}) + 12(1,7 \times 10^{-7}) + 8(1,2 \times 10^{-7}) + 15(0,61 \times 10^{-7}) = 3,9189 \times 10^{-6},$$

$$R(t) = e^{-(3,9189 \times 10^{-6})t}$$

O tempo médio de falha do circuito é:

$$TMF = E[T] = \frac{1}{\lambda_s} = \frac{1}{3,9189} \times 10^6 = 2,55 \times 10^5 \text{ horas.}$$

Para avaliar a confiabilidade desse sistema no tempo de 10.000 horas, tem-se $R(10^4) = e^{-0,039189} \cong 0,96$.

Tendo como referência o *log* dos alarmes do sistema SCADA, além do histórico dos equipamentos, *databooks* dos equipamentos e considerando o plano de manutenção, pode-se afirmar que o sistema de recalque apresenta 96% de disponibilidade, e quando parado só irá permanecer nessa situação em 10%.

Portanto, foram adotados os seguintes parâmetros, conforme diagrama de estados (Figura 12).

Figura 12 – Diagrama de estados.

Fonte: Elaborado pela autora.

A cadeia de Markov aplicada a essa situação calcula a confiabilidade desse sistema de modo simples e poderá ser utilizado para calcular a confiabilidade de toda planta nesse sistema crítico. A modelagem desenvolvida foi inicialmente calculada para apenas quatro passos da cadeia de Markov, fazendo uma analogia de cada passo ao mês do ano, e definindo que o estado 1, refere-se ao componente funcionando e o estado zero(0), refere-se a parado, logo tem-se a probabilidade apresentada na Tabela 4.

Tabela 4 – Tabela de transição de estado.

Jan.	Fev.	Mar.	Abr.	Probabilidade	Estado
0,96	0,96	0,96	0,96	0,84934656	1
			0,04	0,03538944	0
		0,04	0,9	0,0331776	1
			0,1	0,0036864	0
		0,9	0,96	0,0331776	1
			0,04	0,0013824	0
		0,1	0,9	0,003456	1
			0,1	0,000384	0
0,04	0,04	0,96	0,96	0,0331776	1
			0,04	0,0013824	0
		0,04	0,9	0,001296	1
			0,1	0,000144	0
		0,9	0,96	0,003456	1
			0,04	0,000144	0
		0,1	0,9	0,00036	1
			0,1	0,00004	0

Fonte: Elaborado pela autora.

Assim, 95,74% do tempo o sistema estará em operação, enquanto que, aproximadamente 122 horas paradas para o período em análise. Em um estudo mais detalhado com um diagrama de estados dos componentes, é possível avaliar quanto dessas 122 horas refere-se exclusivamente à falha do equipamento.

Com o apoio do *software* Maple 14, foi realizada uma análise com um pouco mais de complexidade, como, por exemplo, em situações que é considerado crítico manter pelo menos duas bombas em operação, ou uma bomba em operação e as demais paradas, para calcular a cadeia de Markov. Considerando duas bombas em operação, ou uma em operação e outra em falha, tem-se como resultado da matriz (Apêndice D): a probabilidade de 79,58% das duas em operação, destas, 7,1% de apenas uma em operação e a outra entrar em falha e 6,2% das duas em falhas.

Este estudo desenvolveu também a simulação utilizando o *software* *Computer-Aided Rate Modeling and Simulation* (CARMS) (Figura 13), parametrizado para cadeia de Markov, e vários diagramas de estado foram gerados para etapas do processo em estudo, os quais são apresentados no Apêndice D desta tese.

Figura 13 – *Software* CARMS – versão 1.1.

Fonte: Print screen da aplicação CARMS pela autora.

Ao ser aplicada a cadeia de Markov com o uso do CARMS ao processo da EEE, especificamente ao sistema de bombeamento, área mais crítica do processo, tem-se o resultado apresentado na Figura 14. Em que vemos que a taxa de falhas de sistemas em série, composto por n componentes, é igual à soma das respectivas taxas de falha individuais (em número de falhas/hora):

Figura 14 – Cadeia de Markov para o sistema de bombeamento.

Fonte: Print screen da aplicação CARMS pela autora.

Com o software CARMS foram gerados os diagramas de estado e as matrizes de simulação das possíveis falhas do processo, que serviram de parâmetros para a análise de risco e verificação da confiabilidade da planta em análise. Cada diagrama de estado gerado possui sua matriz equivalente, conforme Tabela 5.

Tabela 5 – Matriz de transição dos estados.

Estados	Prob	1	2	3	4	5	6	7
1	1		0,093			0,048	0,045	
2	0	$1,7 \cdot 10^{-3}$		0,993		0,048	0,045	
3	0		$1,2 \cdot 10^{-3}$		0,993	0,010		
4	0			$5,8 \cdot 10^{-4}$				0,993
5	0	0,010	0,010				0,010	0,010
6	0	$1,3 \cdot 10^{-3}$				0,048		0,045
7	0						$6,7 \cdot 10^{-4}$	
8	$\sum P_{A, P5, P7}$				FALHA	FALHA		FALHA

Fonte: Desenvolvido pela autora.

A matriz de transição dos estados associa a probabilidade do estado ocorre, as condições iniciais e as taxas de transição, propriamente ditas. As colunas correspondem aos estados de origem e as linhas indicam os estados de destino.

As probabilidades de permanência equivalem à diferença entre os somatórios das probabilidades de entrada e saída em cada estado, ponderadas as devidas taxas de transição.

Figura 15 – Gráfico da cadeia de Markov.

Fonte: Print screen da aplicação CARMS pela autora.

Após ter sido executada uma simulação para um período de 52.000 horas, que equivalem a 50% do tempo total do contrato, ou seja, aos oito anos de exploração necessários para que todos os fatores de risco se manifestem pelo menos uma vez na planta, observa-se nessa situação que o regime estacionário (Figura 15) é alcançado ao fim de cerca de 3.000 horas, ou seja, basta simular somente um semestre para se obter o comportamento limite do processo de falhas para esse cenário.

O cenário do estudo de caso foi representado no CORAS, incluídas as taxas de falhas (Figura 16), conforme as fases de implantação da metodologia de gestão de risco, detalhadas nas próximas seções.

Figura 16 – Sistema de bombeamento no CORAS.

Fonte: Print screen da aplicação CORAS pela autora.

4.3 APLICAÇÃO DA METODOLOGIA

Primeiramente, é importante enfatizar que preparar uma metodologia que possa ser validado em uma planta de tratamento real e em plena operação é uma tarefa complexa, tanto no nível técnico quanto no gerencial. Assim sendo, foi delimitado o cenário e realizadas as análises por partes.

No desenvolvimento da primeira fase (1ª Fase) da metodologia foi delimitado o cenário da planta do estudo de caso para análise de risco com apoio de técnicas como FMEA e HAZOP (vide o Anexo A e o Apêndice E).

O Software CORAS (Figura 17) foi a principal ferramenta que consolidou o estudo, possibilitando documentar e avaliar o resultado:

Figura 17 – CORAS Platform.

Fonte: Print screen da aplicação CORAS pela autora.

Para realizar da segunda fase (2ª Fase) da metodologia proposta foi necessária antes uma ampla revisão bibliográfica sobre o assunto, incluindo os objetivos do projeto, análise do processo de tratamento de esgoto e suas vulnerabilidades. Algumas literaturas científicas sobre as questões de risco em saneamento foram levantadas, e manuais e *databooks* do projeto da planta foram avaliados. Ainda nesta fase do projeto foram realizadas consulta à comunidade científica, com submissão de trabalhos a congressos e periódicos, além de participação em fóruns e comunidades colaborativas da área de risco ou mesmo da área de saneamento. As questões levantadas na definição do contexto foram revistas e colocadas aos participantes interessados nas reuniões de discussão do tema.

Na segunda fase da metodologia proposta, foi desenvolvida a análise textual dos riscos identificados durante a primeira fase. Nesse momento foi

gerada a documentação com a padronização CORAS para o desenvolvimento da análise de risco, alguns exemplos são apresentados nas Tabelas 6, 7, 8, 9, 10 e 11 e no diagrama da Figura 18, dentre outros documentos não listadas nesse trabalho.

Tabela 6 – Matriz de ativos.

Ativo	Importância	Tipo
Valor Pago pelo Serviço – QID variável	1	Direto
A confiança do Cliente no Sistema – SDOJ	1	Indireto
A contaminação do Meio Ambiente	1	Indireto
Funcionamento do SCADA	2	Direto
Funcionamento da Bomba	1	Direto
Funcionamento da rede	3	Direto
Fornecimento de energia	2	Direto
Sistema de energia do Gerador	2	Direto
Funcionamento do CLP	2	Direto
Funcionamento dos Instrumentos	1	Direto
Funcionamento dos Inversores	1	Direto
Serviço de Recalque do Efluente	1	Indireto
Comunidade do Entorno	1	Indireto
Imagem da Empresa	1	Indireto

Fonte: Elaborado pela autora.

Tabela 7 – Matriz de nível de risco.

Quem/O que pode causar isto?	Como? Qual o incidente? Qual a ameaça?	Quais as vulnerabilidades que pode permitir isso?
Empregados	Dar comando errado no SCADA	Falta de validação do comando
Hacker	Alterar código ou dar comando errado	Falta de autenticação
Falha do Sistema	Sistema <i>down</i>	Falta de redundância
Curioso	Alterar parâmetro do sistema	Falta de validação do comando
Falha da Rede	Sistema inoperante	Falta de redundância

Fonte: Elaborado pela autora

Tabela 8 – Matriz de consequência.

Consequência	Componentes afetados	Tempo parado
Catastrófico	[50%,100%]	[1 semana,∞]
Rompimento da Linha de Recalque	100%	20 dias
Maior	[20%,50%]	[1 dia, 1 semana]
Queima do Transformador	40%	3 dias
Moderado	[10%,20%]	[1 hora, 1 dia]
Vírus no SCADA	15%	2 horas
Menor	[1%,10%]	[1 minuto, 1 hora]
Travamento do CLP	5%	15 min
Insignificante	[0%,1%]	[0,1 minuto]
Perda de Pacote	0,5%	30 seg

Fonte: Elaborado pela autora.

Tabela 9 – Matriz de consequência x penalidades.

Consequência	Penalidades
Catastrófico	O Diretor Estatutário é sentenciado legalmente por mais de um ano
Maior	O Diretor Estatutário é sentenciado legalmente por até um ano
Moderado	Terá que indenizar ou realizar compensação
Menor	Pagar multa
Insignificante	Tem que parar imediatamente por ser ilegal

Fonte: Elaborado pela autora.

Tabela 10 – Matriz de probabilidade x frequência.

Probabilidade	Frequência	Faixa
Certamente	5 vezes ou mais por ano	[50,∞):10y
Provavelmente	2 a 5 vezes por ano	[20,49]:10y
Possível	Uma vez por ano	[6,19]: 10y
Pouco Provável	Menos de uma vez por ano	[2,5]: 10y
Raramente	Menos de uma vez em 10 anos	[0,1]:10y

Fonte: Elaborado pela autora.

Tabela 11 – Matriz de referências para análise de risco.

Consequência	Descrição
Catastrófico	Acidente catastrófico
Maior	Manobra brusca necessária – agir rápido
Moderado	A recuperação é de grande proporção
Menor	Uma maior carga de trabalho aos operadores
Insignificante	Sem efeito perigoso para operação

Fonte: Elaborado pela autora.

Figura 18 – Diagrama de ameaças.

Fonte: Elaborado pela autora.

Na seção 4.4 desta tese foi detalhada a aplicação do método CORAS para 2ª Fase da metodologia de gestão de risco.

A terceira fase (3ª Fase) da metodologia proposta foca na estimativa quantitativa dos riscos. A modelagem matemática utilizada foi basicamente a cadeia de Markov e estudos de confiabilidade, que forneceu as informações quantitativas para o CORAS. As ferramentas utilizadas nessa fase foram as citadas abaixo, que estão apresentadas de forma detalhada no Apêndice D:

- Cálculo por MARKOV – Diagrama de Estados no Excel;
- Cálculo por MTBF – No Excel e Programa em C;
- Cálculo por MARKOV – Diagrama de Estados no CARMS;
- Simulação da Matriz Markov no MAPLE.

Um dos estudos desenvolvidos contempla a avaliação do equipamento PLC, que, conforme o levantamento de dados históricos do SCADA, para um

período de aproximadamente 10 meses, ou melhor, 7.000 horas, registrou as seguintes ocorrências de falhas no sistema:

Tabela 12 – Matriz de falhas.

Intervalo de tempo (h)	Quant. Falhas no intervalo
0-1000	94
1001-2000	33
2001-3000	17
3001-4000	13
4001-5000	9
5001-6000	7
6001-7000	4
Total	177

Fonte: Elaborado pela autora.

É importante notar que nesta situação específica foram utilizados os dados históricos dos primeiros dez meses do período de comissionamento da planta, momento em que o sistema ainda não era estável e que os equipamentos programáveis como o CLP estavam em constante ajuste para melhorar a configuração de sua lógica e do sistema de comunicação de dados.

Calculando a função densidade $f(t)$, (Figura 19):

$$F(t) = P(T \leq t) = \int_0^t f(u) du, t > 0; \quad f(t) = \frac{d}{dt} F(t)$$

Figura 19 – Gráfico da função densidade.

Fonte: Elaborado pela autora.

A função de risco é dada pela taxa instantânea de falha, para determiná-la, divide-se a taxa de falha por um intervalo de tempo e calcula-se o limite, Figura 20:

$$h(t) = f(t) \times \frac{1}{R(t)}$$

Figura 20 – Gráfico função de risco.

Fonte: Elaborado pela autora.

Logo, a função confiabilidade, ou seja, a probabilidade do CLP não falhar no intervalo (0,t], Figura 21:

$$R(t) = 1 - F(t) = 1 - P(T \leq t) = P(T > t), t > 0$$

Figura 21 – Gráfico função confiabilidade.

Fonte: Elaborado pela autora.

Conforme estudo da função confiabilidade verifica-se que $R(t)$ e $f(t)$ são basicamente determinados por $h(t)$, portanto a principal base de avaliação são as equações: $R(t) = \exp \left[- \int_0^t h(t) dt \right]$ e $f(t) = h(t) \exp \left[- \int_0^t h(t) dt \right]$.

Durante o estudo de caso foram utilizados softwares de apoio para realizar as estimativas e desenvolvida a análise de confiabilidade dos itens em estudo, os dados são transferidos para os diagramas no CORAS, Figura 22.

Figura 22 – Diagrama de risco.

Fonte: Elaborado pela autora.

Na quarta fase (4ª Fase) da metodologia foram definidas as prioridades e quais os riscos seriam considerados e receberiam o devido tratamento ou quais riscos seriam apenas reconhecidos, porém aceitos sem qualquer investimento para mitigá-los.

Para apoiar a decisão no processo de priorização dos riscos desenvolveu-se a avaliação, que no estudo de caso teve como base referencial o banco de dados com informações históricas do sistema SCADA, que permitiu conhecer a confiabilidade dos componentes envolvidos na planta em análise e possibilitou a melhoria de alguns itens, conforme as técnicas e modelagens aplicadas na fase anterior.

A fase da avaliação nos leva à reflexão da diferença entre qualidade e confiabilidade, pois não são sinônimos e nem sempre uma melhor qualidade

implica maior confiabilidade, porém, normalmente, uma maior confiabilidade leva a uma maior qualidade dos componentes envolvidos, por exemplo, os componentes eletrônicos utilizados em PC comum para fins domésticos não possuem a mesma confiabilidade que os componentes eletrônicos utilizados no *hardware* de servidor SCADA.

Ao término da avaliação é verificado se o resultado é satisfatório, caso não seja, uma nova rodada da análise de risco e com novas estimativas deve ser realizada, inclusive com possibilidade de uma redefinição do contexto.

Na quinta fase (5ª Fase) da metodologia desenvolveu-se a análise do tratamento com o objetivo de reduzir os riscos, a principal ferramenta utilizada é o diagrama de tratamento do CORAS e foi partir dele que as melhorias foram implementadas (vide exemplo no Apêndice F e detalhamento na seção 4.4).

A sexta fase (6ª Fase) correspondeu à verificação, que nada mais é do que regras de controles que são muitas vezes estabelecidas nas lógicas dos sistemas para identificar possíveis falhas e evitar vulnerabilidades. Esta é uma rotina realizada diariamente pelo próprio sistema de controle, seja ele manual ou automático com geração de alarmes quando necessário, além de registros nos relatórios e no banco de dado do historiador, possibilitando uma consolidação dos dados por meio de ferramentas como *business intelligence* (BI).

A última fase (7ª Fase) da metodologia refere-se à auditoria, que ocorre basicamente por três processos:

- Processo diário – realizado pela equipe de operação através da verificação de cada etapa da planta e preenchimento do *checklist* de operação;
- Processo periódico – realizado conforme cronograma específico sob a responsabilidade da equipe de manutenção, com realização de preditivas e documentação em sistema histórico de Ordem de Serviço;
- Processo pontual – com o foco em verificação e não manutenção, realizado por equipe externa, seja por demanda do cliente para fiscalização do contrato de operação ou sob a responsabilidade da equipe Matriz, com ênfase na segurança corporativa.

Entre os exemplos para o processo pontual, podemos citar o relatório da última vistoria com a classificação de risco da unidade empresarial em análise neste estudo de caso, que foi classificado como padrão conforme as taxa de risco das seguradoras (vide Anexo B).

4.4 DETALHAMENTO DO ESTUDO DE CASO COM CORAS

As fases segunda e quinta da metodologia de gestão de risco proposta nesta tese utilizam o método CORAS para o desenvolvimento da análise de risco e o tratamento, respectivamente.

Seguindo o roteiro de implantação do método CORAS, foram nomeadas as pessoas envolvidas no processo de contextualização e definição das diretrizes para a análise de risco. A ferramenta CORAS disponibiliza recursos para documentar todo o processo de análise de risco e estabelecer a relação entre as etapas de análise, conforme apresentado na Figura 23. O desenvolvimento da análise com CORAS ocorre em oito passos, como detalhado a seguir:

Figura 23 – Passos para implantação do CORAS.

Fonte: Elaborado pela autora.

➤ **1º Passo: Contextualização – Definição do Escopo (Cenário)**

Primeiramente é definido o escopo de atuação e detalhado o cenário. Portanto, o foco do estudo de caso foi uma estação elevatória de esgoto, e neste ponto foram descritas as características técnicas da estação elevatória, tais como: uma Central de Controle de Motores (CCM), que alimenta as quatro bombas (sendo uma reserva) de 550 HP, com inversores de frequência; um transformador a seco de 2.500 kVA, chaveado por um disjuntor de 4.000; e três geradores de 687/757 kVA, acionados por motor de potência prime 585 kW, potência *standby* de 644 kW. A EEE é automatizada com inversores de frequência, medidores de nível, vazão e pressão, controladores de odores, CLP e outros instrumentos de campo, todos controlados pelo Centro de Controle de Operações (CCO), que fica aproximadamente a 3 km de distância.

Devido à complexidade e amplitude desse exemplo, o método CORAS é recomendado para desenvolvimento da análise de risco, pois de modo geral demanda uma análise superior a 150 H/H de estudo para o desenvolvimento da análise de risco. Porém, durante o estudo verificou-se a necessidade de combinar outras metodologias para a análise de risco com o objetivo de complementar o estudo.

➤ **2º Passo: Identificando o Ambiente**

Neste passo, objetivou-se identificar os riscos e as falhas de confiabilidade (*reliability*), detalhadas no passo 6. Verificaram-se as vulnerabilidades desse sistema com o estabelecimento de parâmetros, tais como o MTBF, período médio entre falhas para os seus componentes, pois há exigências de operação contínua dessa estação, considerando-se que na prática a perda do sistema, irá provocar o extravasamento de efluente, poluindo o meio ambiente.

Foi nesta fase da análise que foi definida a equipe de trabalho e o papel/responsabilidade de cada envolvido e o cronograma com o planejamento da análise de risco.

➤ 3º Passo: Detalhamento da Origem com Diagrama de Ativo

Na terceira etapa do CORAS, desenvolveu-se o detalhamento das origens dos riscos, com a construção da tabela de ativos envolvidos no cenário em análise. Nesse passo, foram utilizadas técnicas similares a 5W1H e preenchidos no *software* CORAS os formulários (Figura 24).

Figura 24 – Conhecendo o ambiente.

O que Causa? Quem?	Como? Qual o cenário ou incidente? O que é prejudicado?	O que pode produzir esta possibilidade?
Falha no servidor SCADA. Pen Drive com Virus	O SCADA irá parar, sistema fica fora e não consegue operar ou dar comandos errados.	Pode extravasar o esgoto. Pode causar danos a pessoas e ao meio ambiente.

Fonte: Elaborado pela autora.

O objetivo principal desta etapa foi o de dar visibilidade e documentar os ativos, favorecendo a tomada de decisão para definição em quais componentes deve-se atuar prioritariamente para a análise dos riscos.

➤ 4º Passo: Homologação do Detalhamento

O objetivo principal da quarta etapa no método CORAS é concordar com a descrição dos ativos, verificando se o foco e o escopo do contexto estão corretos. Nesta etapa, são aprovadas as documentações com as devidas definições de todo o escopo, ativos envolvidos, ameaças, cenários possíveis, escalas para probabilidades, grau de importância, consequências, bem como critérios e decisão de priorização para a avaliação de risco. Esta é uma etapa paralela a todo o processo de desenvolvimento.

Para o estabelecimento do critério de importância para cada ativo foi relevante o envolvimento de pessoas das diversas áreas da empresa, pois são critérios muito subjetivos, que tiveram como base definições estabelecidas no CORAS. Foram utilizados os critérios da escala **1** para Muito Alta Importância, ou seja, crucial para o negócio da empresa, e **5** para Menor/Sem Importância, conforme apresentado na Tabela 13.

Tabela 13 – Diagrama de ativo.

Ativo	Importância	Tipo
Funcionamento do SCADA	2	Direto
Funcionamento da Bomba	1	Direto
Funcionamento da rede	3	Direto
Fornecimento de energia	2	Direto
Sistema de energia do Gerador	2	Direto
Funcionamento do CLP	2	Direto
Funcionamento dos Instrumentos	1	Direto
Funcionamento dos Inversores	1	Direto
Serviço de Recalque do Efluente	1	Indireto
Comunidade do Entorno	1	Indireto
Imagem da Empresa	1	Indireto

Fonte: Elaborado pela autora.

Tabelas com mais detalhes e diferentes critérios de importância foram geradas, tais como: tabela de ativos para os instrumentos de campo, tabela de ativos para o sistema de tratamento de odores, entre outras.

Os ativos classificados pelo grupo como direto foram tratados no quinto passo, enquanto que os indiretos foram vistos apenas no sétimo passo, conforme orientação do método CORAS.

Nesse passo também foram utilizadas as referências do CORAS para a escala de consequência (Tabela 14).

Tabela 14 – Escala de consequência.

Consequência	Componentes afetados	Tempo parado
Catastrófico	[50%,100%]	[1 semana,∞]
Maior	[20%,50%]	[1 dia, 1 semana]
Moderado	[10%,20%]	[1 hora, 1 dia]
Menor	[1%,10%]	[1 minuto, 1 hora]
Insignificante	[0%,1%]	[0,1 minuto]

Fonte: Lund; Solhaug e Stolen (2011, tradução nossa).

Foi utilizada também, nesta fase do trabalho, a classificação das consequências em função da gravidade dos eventos (Tabela 15).

Tabela 15 – Escala de consequência x penalidades.

Consequência	Penalidades
Catastrófico	O CEO é sentenciado legalmente por mais de um ano.
Maior	O CEO é sentenciado legalmente por até um ano.
Moderado	Terá que indenizar ou realizar compensação.
Menor	Pagar multa.
Insignificante	Tem que parar imediatamente por ser ilegal.

Fonte: Lund; Solhaug e Stolen (2011, tradução nossa)..

Para a análise quantitativa, foi utilizada a classificação pela probabilidade e/ou frequência da ocorrência (Tabela 16).

Tabela 16 – Probabilidade x frequência.

Probabilidade	Frequência	Faixa
Certamente	5 vezes ou mais por ano.	[50,∞]: 10y
Provavelmente	2 a 5 vezes por ano.	[20,49]: 10y
Possível	Uma vez por ano.	[6,19]: 10y
Pouco Provável	Menos de uma vez por ano.	[2,5]: 10y
Raramente	Menos de uma vez em 10 anos.	[0,1]: 10y

Fonte: Lund; Solhaug e Stolen (2011, tradução nossa).

➤ 5º Passo: Identificação do Risco (Diagrama de Ameaças)

Identificaram-se as ameaças, potenciais causas de incidentes, vulnerabilidades que podem ser exploradas por uma ou mais ameaças, incidentes indesejáveis e riscos conforme as referências das tabelas vistas no 4º passo e definidas na Tabela 17.

Tabela 17 – Referências para análise de risco.

Consequência	Descrição
Catastrófico	Acidente catastrófico.
Maior	Manobra brusca necessária – agir rápido.
Moderado	A recuperação é de grande proporção.
Menor	Uma maior carga de trabalho aos operadores.
Insignificante	Sem efeito perigoso para operação.

Fonte: Lund; Solhaug e Stolen (2011, tradução nossa).

Para garantir um processo de qualidade na identificação dos riscos é relevante o envolvimento de pessoas que conheçam o processo com expertise e interesse no assunto e com diferentes pontos de vista. Neste estudo de caso, foram realizadas reuniões estruturadas, fazendo uso de técnicas como *brainstorming*, com a presença de diversos especialistas e consultores que conheciam a planta da EEE.

Com domínio das informações, foi possível desenhar os diagramas de ameaça no sistema CORAS (Figura 25), estabelecendo as relações de impacto.

Figura 25 – Diagrama de ameaças – CORAS.

Fonte: Elaborado pela autora.

Para este estudo de caso, foram desenvolvidos mais de vinte diagramas de ameaças contemplando os ativos identificados no passo três, completando com esta etapa a documentação para a análise de risco.

➤ 6º Passo: Estimativa de Riscos com Diagrama das Ameaças

O objetivo deste passo foi o de calcular e estimar os valores quantitativos para os riscos, buscando estabelecer a severidade para os riscos identificados, possibilitando apoiar a análise qualitativa do cenário. Para calcular a estimativa dos riscos foram utilizadas as modelagens de confiabilidade e análise de falhas descritas nas seções anteriores deste texto na análise por Markov e MTBF, além de levar em consideração a modelagem matemática apresentada por Lund;

Solhaug e Stolen (2011), que calcula a estimativa de risco conforme a probabilidade e frequência de ocorrência do incidente no período t . Portanto, a análise quantitativa por função *reability* foi igual ao produto das confiabilidades dos componentes individuais que constituem o sistema, a qual é definida conforme Equação 1:

$$R(t) = 1 - F(t) \Rightarrow \Pr (T > t) \text{ para } t > 0 \quad \text{equação (1)}$$

A probabilidade de ocorrer os cenários/incidentes c para as ameaças a é igual à probabilidade com que a inicia c . Nessa situação em que a ameaça a e o cenário (incidente) c estão relacionados, teve-se (*initiates*):

$$a \rightarrow c / ((a \sqcap c). (p)) \quad \text{equação (2)}$$

Houve situações em que a possibilidade de ocorrência de c_2 a partir de c_1 foi igual para a probabilidade p de c_1 , multiplicada pela possibilidade da frequência f , de ocorrer conforme c_1 venha a gerar o incidente c_2 , toda vez que c_1 ocorrer. Nessa situação tem-se o *leads-to*, ou seja, $c_1 \sqcap c_2$, o cenário/incidente c_2 é precedido por c_1 :

$$(c_1(p).c_1 \rightarrow c_2) / (c_1 \sqcap c_2).(p.f) \quad \text{equação (3)}$$

Porém, teve-se a situação em que os cenários/incidentes eram mutuamente exclusivos, portanto a probabilidade foi calculada em paralelo. Se dois eventos são mutuamente exclusivos, a probabilidade da união deve ser igual à soma das respectivas probabilidades, sendo consideradas todas as instâncias, $c_1 \sqcup c_2$. Nessa regra, viu-se que c_1 ou c_2 ocorrem, mas não ambos, desde que eles sejam mutuamente exclusivos. Sendo que, conforme equação 4, se os dois eventos forem estatisticamente independentes, ou seja, não houver probabilidade de um ter relação na probabilidade do outro, a probabilidade da união dos dois eventos será igual à soma individual das probabilidades.

$$(c_1(p_1) \cdot c_2(p_2)) / ((c_1 \sqcup c_2).(p_1 + p_2)) \quad \text{equação (4)}$$

Enquanto que, na independência estatística com a probabilidade da interseção, o cálculo deverá ser subtraído de modo que os resultados sejam computados somente uma vez, conforme equação 5:

$$(c_1(p_1) \cdot c_2(p_2)) / ((c_1 \cap c_2) \cdot (p_1 + p_2 - p_1 \cdot p_2)) \quad \text{equação (5)}$$

As probabilidades foram inseridas no sistema do CORAS, Figura 26.

Figura 26 – Diagrama de ameaças com estimativas.

Fonte: Elaborado pela autora.

➤ 7º Passo: Avaliação de Riscos com Diagrama de Risco

A análise qualitativa foi fundamental para identificar qual era a característica do risco e se ele era aceitável ou não. Usou-se como referência a tabela de análise de risco, que deve ser preenchida com a identificação qualitativa do nível do risco.

Tabela 18 – Análise de risco qualitativo.

	Insignificante	Menor	Moderado	Maior	Catastrófico
Raro	R7	R10			R11
Pouco	R18		R12,R20	R13	R14
Provável					
Possível	R3	R1, R5	R1		
Provável	R4	R9, R8	R15	R2, R17	
Certamente	R8	R6,19	R7, R16		

Fonte: Elaborado pela autora.

➤ 8º Passo: Tratamento de Risco com Diagrama de Tratamento

O diagrama de tratamento baseou-se no diagrama de ameaças e no diagrama de risco. O objetivo de um diagrama de tratamento é proporcionar uma visão geral de alto nível dos tratamentos disponíveis (Figura 27).

Figura 27 – Diagrama de tratamento de risco.

Fonte: Elaborado pela autora.

O CORAS foi o principal método que permitiu desenvolver as etapas da metodologia proposta, porém ele por se só não seria suficiente para o desenvolvimento da gestão de risco.

4.5 RESULTADOS

Nos primeiros meses de desenvolvimento desta pesquisa, o objetivo era a utilização do método CORAS com simulações efetuadas pelo modelo de probabilidade clássica, para atender a carência de estudos no desenvolvimento de uma gestão de risco em uma planta de saneamento com foco na segurança do processo, na segurança da informação e na melhoria contínua. Mas,

verificou-se que a utilização apenas do método CORAS não era suficiente para o desenvolvimento da gestão de risco, pois o CORAS se limita a um diagnóstico de análise de risco e a documentação do tratamento, ou seja, é muito pontual, não permitindo o acompanhamento, verificação e auditoria da gestão de risco no ambiente.

Entretanto, na finalidade de diagnóstico do risco, o CORAS deu excelente resultado, permitiu reduzir o tempo de análise em função da facilidade do uso da ferramenta e da padronização disponibilizada na condução do processo. Além do que o CORAS permitiu consolidar em uma única ferramenta a documentação com uso de diversas técnicas.

O desenvolvimento de uma metodologia de gestão de risco em sete fases proporcionou a implantação de um programa de gestão de risco sem complicação, direcionado, objetivo e com continuidade. Além de facilitar a consolidação das diversas características das ferramentas já existentes.

A segurança (*safety*) e a eficiência operacional dos sistemas de saneamento são influenciadas fortemente por sua base de automação e consequentemente pela disponibilidade e vulnerabilidades dos seus equipamentos. Compreender a interface entre as tecnologias de informação (TI) e a tecnologia de automação (TA) foi relevante para alcançar as conclusões obtidas nesta pesquisa, pois a gestão de risco desenvolvida contemplou as diversas etapas do processo da planta, com análise *security* e *safety*.

Constatou-se que a partir de uma simples vulnerabilidade podem ocorrer prejuízos significativos para organização ou mesmo para a comunidade que vive no entorno da planta, porém, são riscos previsíveis e quantificáveis em um projeto de gestão de risco (Figura 28), durante uma das etapas da implantação da metodologia.

Figura 28 – Análise de risco.

Fonte: Elaborado pela autora.

A simulação da confiabilidade de diversos componentes da planta foi relevante para tomada de decisão, especialmente pela gerência de manutenção na decisão da lista de peças de reposição ou mesmo no processo de substituição da tecnologia, como no caso da troca do modelo do CLP, pois os estudos das falhas de desgaste e das falhas que ocorrem antes mesmo do desgaste apresentam uma modelagem matemática que quantifica em horas o tempo de indisponibilidade do equipamento.

A modelagem com a cadeia de Markov para identificação do estado dos componentes e do comportamento do processo, desenvolvida durante a validação da metodologia, apresentou resultados favoráveis, pois a flexibilidade em realizar a simulação incluindo novos estados, ou mesmo inserindo a interdependência entre os equipamentos da planta, favoreceu a compreensão e quantificação do intertravamento entre os instrumentos de campo e o sistema de bombeamento, inclusive no processo de quantificação do tempo e frequência de paradas, realizando as análises de probabilidade.

Constatou-se também o resultado positivo na utilização de ferramentas como o software Carms para simulação das cadeias de Markov, possibilitando o uso desta modelagem matemática mesmo em sistemas de maior complexidade, e com muitos estados, além de fornecer para a metodologia de gestão de risco a informação necessária sobre o período estacionário do ambiente em análise.

Já as etapas realizada com o FMEA e consolidado no CORAS, foram relevantes na verificação de itens subjetivos e na análise qualitativa do processo operacional da estação elevatório de esgoto.

Com a aplicação da metodologia de gestão de risco, facilmente se constatou nas simulações efetuadas pelas modelagens matemáticas que a realização de pequenos investimentos pode produzir retornos significativos, em grande parte devido a uma redução de custos com a indisponibilidade operacional ou mesmo redução do faturamento (que, nesse caso, em função da nota avaliativa do QID, possibilita altas penalidades financeiras ao contrato). Um dos resultados da implantação da metodologia de gestão de risco foi exatamente a melhoria dos indicadores de desempenho nos últimos 12 meses, pois registra-se uma considerável margem de progressão nesse indicador com aumento na média de 22% da disponibilidade dos equipamentos, resultante unicamente de um programa de melhorias definido pela gestão de risco.

Dentre os resultados verificados durante a validação da metodologia observa-se o fornecimento de informações quantitativas que auxiliam a tomada de decisão, como por exemplo, no estudo de caso houve a necessidade de avaliar as informações de tempo entre falha, criticidade e tempo de reparo para auxiliar a tomada de decisão, quanto a opção da arquitetura do sistema elétrico adotada na mitigação do risco de harmônicos no ambiente da estação elevatória. As estimativas realizadas durante a implantação da metodologia, conforme apresentado no Apêndice D, foram essenciais no processo de decisão para definir o tratamento apropriado, conforme diagramas unifilares (Anexo A), em que o tempo entre falhas analisados em função da arquitetura adotada, aumentava em até 50%, além da possibilidade da análise do parâmetro de tempo de reparo quantificada em cada cenário.

Outra atitude favorável percebida na gestão de risco foi a flexibilidade que a metodologia oferece para realizar a ênfase na fase de maior relevância conforme o perfil do cenário em estudo, além de contemplar a análise de risco social. Ressalto ainda que o fluxo da metodologia é contínuo, favorecendo revisões das políticas de manutenção, de segurança, da qualidade e do esforço de supervisão e controle, sem esquecer as vias motivacional e cultural, que como amplamente se reconhece induz a um potencial de melhoria contínua difícil de quantificar.

Portanto, o fluxo da gestão de risco desenvolvido ao longo desta pesquisa demonstra possuir igualmente uma condição apropriada para a avaliação dos sistemas dominados pela incerteza e escassez de dados de confiabilidade. Reconhece-se, ainda, uma janela de possibilidades para conduzir uma gestão de risco em plantas similares com aproveitamentos de códigos de análise, reutilização das modelagens definidas para os equipamentos e dos diagramas desenvolvidos no CARMS e no CORAS, facilitando o processo de análise de confiabilidade dos diversos processos em plantas de saneamento. Além da possibilidade de aplicação da metodologia, com pequenos ajustes, para demais sistemas críticos.

5 CONCLUSÃO

O presente trabalho de pesquisa emanou da necessidade de implantação de controle de segurança dos processos e análise de risco em unidades de serviços críticos, com vistas a avaliar riscos potenciais por questões materiais e problemas nas instalações, especificamente em plantas de saneamento, conforme o cenário de desenvolvimento tecnológico em que se encontra a área de segurança da informação (*security*) e da segurança do processo (*safety*),

Para tanto, foi realizado um estudo teórico e empírico para validar a aplicação de uma metodologia para gestão de riscos com análise quantitativa, por meio da utilização do método *Consultative Objective Risk Analysis System* (CORAS) e *reliability*, com aprimoramento utilizando a modelagem matemática de Markov, para a realização de análise de risco em plantas de saneamento. Dessa forma, com base nas abordagens teóricas e no estudo de caso realizado numa planta crítica de tratamento de esgoto, concluiu-se que o CORAS apresenta uma ampla modelagem qualitativa, sendo uma eficiente ferramenta de consolidação das informações no processo de análise de risco, porém não contempla as demais fases de um processo de gestão de risco.

Verificou-se também que um diagrama de Markov representa eventos dependentes e permite o cálculo da evolução temporal dos estados de um sistema, desde que as probabilidades de transição entre esses estados permaneçam constantes. Essa imposição é uma limitação significativa e implica no uso de distribuições de probabilidade exponenciais para modelagem das taxas de falha e de reparo. Embora o diagrama de Markov seja capaz de descrever relações dinâmicas entre modos de falhas, existe uma falta de flexibilidade considerável dependendo do contexto em que é aplicado.

Concluiu-se ainda que os modelos markovianos são adequados para representar os modos de operação de um sistema em que ocorre a transição para frente e para trás entre os estados, como por exemplo, na operação de um equipamento do processo, e sua integração entre os estados do equipamento e os instrumentos de controle em que possuem relações de intrelaçamento. Já em um ataque cibernético, que é mais provável que seja em um único sentido,

verifica-se que a utilização de diagrama de eventos apresenta melhores resultados na análise.

No entanto, descrevendo os modos de operação de um sistema que inclui os diferentes obstáculos, que devem impedir um ataque ou reduzir as suas consequências, a análise de Markov para essa finalidade pode ser uma ferramenta útil. Entretanto, para usar a análise Markov exige-se um sistema bem especificado, portanto não é adequado plenamente para uma análise de alto nível.

Pôde ser observado ainda que, dependendo do tamanho do sistema modelado, pode existir um número demasiadamente grande de estados possíveis, o que inviabiliza a análise do comportamento do sistema. Dessa forma, conclui-se que a modelagem quantitativa por Markov é mais adequada para a análise da confiabilidade de sistemas de pequeno porte ou recomenda-se a sua utilização híbrida com outras modelagens, como a FMEA. Nesse sentido, foi realizada no estudo de caso a combinação da análise por Markov e análise confiabilidade com verificação de falhas por MTBF, para auxiliar na tomada de decisão, fazendo uso do CORAS na consolidação das diversas técnicas e modelagem matemática.

A principal contribuição deste trabalho foi desenvolver uma metodologia sistêmica para a gestão de risco que pode ser aplicada em plantas de saneamento, possibilitando o processo de tomadas de decisão e conhecimento dos riscos envolvidos em um ambiente ainda totalmente desprovido de informações quantitativas confiáveis. Verificou-se o sucesso da implantação da metodologia, especialmente por utilizar o princípio do PDCA, conceito já comum nas organizações.

Destarte, com a utilização da metodologia de gestão de riscos foi possível identificar e implementar o tratamento da maioria das vulnerabilidades conhecidas e pertinentes às soluções adotadas em uma estação de tratamento de esgoto, contemplando aspectos de tecnologia da informações e tecnologias de automação. Isso sem dúvida auxilia no entendimento dos problemas de segurança que podem ser enfrentados, tendo como consequência a melhoria do processo como um todo. Infelizmente, não é possível garantir que a unidade esteja totalmente segura, contudo, pode-se afirmar que, com a realização de boas práticas de gestão de risco, são tomadas as medidas preventivas

necessárias à atenuação do impacto negativo que possíveis vulnerabilidades infringiriam ao projeto.

Constatou-se ainda que as situações de inexistência de dados experimentais ou de registro histórico das ocorrências requerem percepção mais nítida acerca das relações de interdependência entre as diversas etapas dos fatores de risco presentes na planta de saneamento. Com base nessa premissa, foi mais fácil delinear um programa de gestão de risco apropriado ao contexto empresarial e introduzir uma modelagem com um grau de confiança que contemple os valores mais admissíveis das características operacionais, com vistas à obtenção de respostas que mostrem um efetivo significado prático.

Observando-se as conclusões alcançadas e a validação da proposta de metodologia para gestão de riscos em plantas de saneamento, conclui-se que os resultados obtidos foram muito relevantes e promissores, apesar da quantidade de modos de falha e de riscos documentados, além do que o escopo de aplicação da gestão de risco incidir apenas numa parte mais restrita do processo.

Portanto, tendo em vista a amplitude e abrangência das validações e de suas aplicabilidades, considera-se que a eficácia da metodologia utilizada foi aprovada e que o escopo da análise de risco deverá ser ampliado para demais áreas do processo, com vistas a melhoria, otimização e ampliação de sua utilização.

Por fim, com base nas análises teóricas e empíricas desenvolvidas nesta pesquisa, se faz necessário apresentar algumas perspectivas finais para subsidiar eventuais trabalhos futuros, que possam ampliar as abordagens sobre o tema e otimizar as propostas de metodologia para gestão de riscos em plantas de saneamento:

- Ampliar a investigação para demais etapas do processo e principalmente gerar indicadores de referências de confiabilidade para sistemas de saneamento.
- Desenvolver tecnologia apropriada que possa atuar na infraestrutura da rede em integração com o SCADA, CLP, OPC e o Banco de Dados com o objetivo de identificar comportamentos indevidos no sistema e atuar preventivamente na falha.

- Desenvolver *software* com a implementação da metodologia aqui sugerida e inclusão da modelagem matemática discutida nesta pesquisa.

REFERÊNCIAS

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **27005**. Tecnologia da informação - Técnicas de segurança – Gestão de riscos de segurança da informação. Brasil: ABNT NBR ISO/IEC 27005, 2008.
- ALMEIDA JR., J. R. **Segurança em sistemas críticos e em sistemas de informação**: um estudo comparativo. 2003. Tese (Livre Docência) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2003.
- ALVES, C. B.; MENEZES, M. A. F. **Introdução à pesquisa operacional**. Goiânia: Editora da PUC Goiás, 2010.
- AS/NZS (2004a). **Risk Management - AS/NZS4360:2004**. Australian: New Zealand Standard, third edition.2004.
- AZEVEDO, M. T.; KOFUJI, S. T.; MARTINS, A. B. Utilização das normas ISA 99 para minimizar os riscos em plantas de tratamento de água. **Revista Controle & Instrumentação**, n. 189, 2013.
- BRAENDELAND, G.; REFSDAL, A.; STOLEN, K. Modular analysis and modelling of risk scenarios with dependencies. **Journal of Systems and Software**, v. 83, n. 10, 2010.
- BRANDÃO, J.E.M.S.; FRAGA,J.S. Gestão de risco.**SBSEG2008**.VIII Simpósio Brasileiro em Segurança da Informação de Sistemas Computacionais. DAS. UFSC: Santa Catarina. 2008.
- CARVALHO, L. A. **Análise de disponibilidade utilizando abordagem nebulosa**. 2008. Tese (Doutorado) – Escola de Engenharia, Universidade Federal de Minas Gerais, Belo Horizonte, 2008.
- CLARK, M.; GRAYMAN, W. **Modeling water quality in distribution systems**. Denver, Colorado: American Water Works Association, 1998.
- CETESB P4.261. **Manual de orientação para a elaboração de estudos de análise de riscos**. Companhia Ambiental do Estado de São Paulo. São Paulo: SP, 2003.
- DOMINGUEZ-CHICAS, A.; SCRIMSHAW, M.D. **Hazard and risk assessment for indirect potable reuse schemes**: an approach for use in developing Water Safety Plans. UK: Elsevier, 2010.
- FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION (FIPS). **PUB 199**: standards for security categorization of Federal Information and Information Systems. Gaithersburg: FIPS 199, 2004.
- FLENTGE, F.; BEYER, U. The ISE metamodel for critical infrastructures. In: GOETZ, E.; SHENOI, S. (Eds.). **Critical infrastructure protection**. Springer: Heidelberg, 2007.

FOX. Somerset residents rush to pick-up bottled water during advisory.

FOXProvidence, 1 June. 2011. Disponível em:

<http://www.foxprovidence.com/dpps/news/massachusetts/somerset-residents-rush-to-pick-up-bottled-water-during-advisory_3833828>. Acesso em: 22 set. 2011.

GELDREICH, E. **Microbial quality of water supply in distribution systems**.

Boca Raton, Florida: Lewis Publishers, 1996.

HINES, W. et al. **Probabilidade e estatística na engenharia**. Rio de Janeiro: LTC, 2012.

INFOEXAME. **Ataques cibernéticos cresceram 42% em 2012**. Disponível em:

<<http://info.abril.com.br/noticias/seguranca/ataques-ciberneticos-cresceram-42-em-2012-16042013-49.shl>>. Acesso em 01 jun. 2013.

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). **61025**: Fault Tree Analysis (FTA). Geneva: IEC, 1990.

_____. **61508**: functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: IEC, 1998.

_____. **61513**: nuclear power plants – instrumentation and control for systems important to safety – general requirements for systems. Geneva: IEC, 2001.

_____. **61511**: functional safety – safety instrumented systems for the process industry sector. Geneva: IEC, 2004.

_____. **62061**: safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems – general requirements for systems. Geneva: IEC, 2005.

_____. **61508**: functional safety of electrical/electronic/programmable electronic safety-related systems. 2nd ed. Geneva: IEC, 2010.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE). **493 IEEE Standard** Recommended practice for the design of reliable industrial and commercial power systems. United States of America: IEEE, 2007.

_____. **352: IEEE Standard** for Qualification of Safety-Related Actuators for Nuclear Power Generating Stations. United States of America: IEEE, 2006.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO); INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). **2002**: Risk management - Vocabulary - Guidelines for use in standards. Switzerland: ISO/IEC Guide 73, 2002.

_____. **17799**: tecnologia da informação - código de prática para a gestão da segurança da informação. Switzerland: ISO/IEC, 2000.

_____. **27000**: series standard covering information security risk management. Switzerland: ISO/IEC, 2008.

_____. **31000**: general guidelines for principles and implementation of risk management. Switzerland: ISO/IEC, 2009.

INTERNATIONAL SOCIETY OF AUTOMATION (ISA). **99**: security guidelines and user resources for industrial automation and control systems. 3rd ed. Research Triangle Park: ISA, 2007.

KIRKPATRICK, S.; GELATT, D.; VECCHI, P. Optimization by simulated annealing. **Science**, v. 220, n. 4598, 1983.

KOMINEK, D.; BYRES, E. **Protegendo Sistemas de Controle Industriais OPC – Soluções de Segurança em que você pode apostar**. MatrikonOPC. Tofino Security: 2011.

KRAMER, M. H. et al. Waterborne disease 1993 and 1994. **Journal of the American Water Works Association**, v. 88, 1996.

KROLL, D.; KING, K. Operational and laboratory verification testing of a heuristic on-line water monitoring system for security. **Int. J. Hi. Spe. Ele. Syst.**, v. 17, n. 631, 2007.

KROLL, D. **Securing our water supply**: protecting a vulnerable resource. Tulsa, Oklahoma: Pennwell, 2006.

KRUTZ, R. L. **Securing SCADA systems**. Indianapolis: Wiley, 2006.

LEEMIS, L.M. **Reliability Probabilistic Models and Statistical Methods**. 2nd ed. USA: 2009.

LIMNIOS, N. **Fault trees**: control systems, robotics & manufacturing series. Washington, DC: Wiley-ISTE, 2007.

LUND, M. S.; SOLHAUG, B.; STOLEN, K. **Model-driven risk analysis**. Springer: Heidelberg, 2011.

MARCIANO, J. L. P. **Segurança da informação**: uma abordagem social. Brasília: UnB, 2006.

MARTINS, A. et al. **Instrumentation SCADA, LIMS**: tools for efficient management the operational process of the water treatment. In: International Instrumentation Symposium, 56., 2010, Rochester. **Proceeding...** Rochester: ISA, 2010.

MARTINS, A.B.; SANTOS, C.A.S. Metodologia para Implantação do sistema de gestão da segurança da informação. **Revista de Gestão da Tecnologia e sistemas de Informação**, v.2,n.2,p.121-136,2005.

MAYS, L.; TUNG, Y. **Hydrosystems engineering and management**. New York: McGraw-Hill, 1992.

MIL-HDBK-217. **Military handbook reliability prediction of electronic equipment**. USA, 1991.

MURPHY, J. **Prediction and validation in water distribution modeling.**

Denver, Colorado: American Water Works Association, 1991.

NUREG-0492, Nuclear Regulatory Commission. **Fault tree handbook.** Systems and Reliability Research Office of Nuclear Regulatory Research. Washington, D. C. 1981.

OSTFELD, A.; SHAMIR, U. Optimal operation of multiquality networks: steady state-conditions. **Journal of Water Resources Planning and Management**, n. 119, 1993.

PALADY, P. **FMEA**: análise dos modos de falha e efeitos: prevendo e prevenindo problemas antes que ocorram. São Paulo: IMAM, 1997.

POPPER, Karl R. **A lógica da pesquisa científica.** 9. ed. São Paulo, Cultrix, 1999.

RAUSAND, M.; HOYLAND, M. **System reliability theory:** models, statistical methods, and application. 2nd ed. New Jersey: Wiley, 2004.

RINALDI, S. M.; PEERENBOOM, J. P.; KELLY, T. K. **Identifying, understanding and analyzing critical infrastructure interdependencies.** IEEE Control Systems magazine, December, 2001.

ROSSMAN, A.; CLARK, M.; GRAYMAN, M. **Modeling chlorine residuals in drinking water distribution systems.** Journal of Environmental Engineering, v. 120, 1994.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A.. **Risk management guide for information technology systems.** NIST Special Publication 800-30. 2002.

WALSKI, T. et al. **Advanced water distribution modeling and management.** Exton, PA: Bentley Institute Press, 2001.

WANG, Z.; ZENG, H. **Study on the risk assessment quantitative method of information security.** In: International Conference on Advanced Computer Theory and Engineering (ICACTE). Chengdu: IEEE, 2010.

APÊNDICES

Apêndice A – Publicações

Durante o período da elaboração desta pesquisa foram apresentadas as seguintes contribuições em conferências internacionais realizadas em: Portugal, Estados Unidos, Alemanha e no Brasil, relatando as pesquisas afins em desenvolvimento pelo grupo de pesquisa.

Publicação no ano de 2009

AZEVEDO, M. T.; KOFUJI, S. T.; MARTINS. Detecção de intrusões baseado em anomalias em sistemas de tratamento de água utilizando técnicas de inteligência artificial. In: Conferência Ibérica de Sistemas e Tecnologias de Informação – CISTI, 4., 2009, Póvoa de Varzim. Póvoa de Varzim: CISTI, 2009. (ISBN: 978-989-96247-1-9).

Publicações no ano de 2010

MARTINS, A. et al. Instrumentation SCADA, LIMS: tools for efficient management the operational process of the water treatment. In: International Instrumentation Symposium, 56., 2010, NY. Rochester: ISA, 2010. (ISBN: 978-193-60074-2-4).

AZEVEDO, M. T.; KOFUJI, S. T.; MARTINS. A simplified approach to intrusion detection based on anomalies in control and data acquisition systems. In: IADIS International Conference Intelligent Systems and Agents, 2010, Freiburg. Freiburg: IADIS, 2010. (ISBN: 978-972-8939-23-6)

Publicação no ano de 2012

AZEVEDO, M. T.; KOFUJI, S. T.; MARTINS. Utilização das normas ISA 99 para minimizar os riscos de segurança – estudo de caso: plantas de tratamento de

água. In: Congresso Brazil Automation, 2012, São Paulo. Anais... São Paulo: Brazil Automation, 2012. (ISBN: 978-193-60074-2-4).

Publicações no ano de 2013

MARTINS, A. B.; AZEVEDO, M. T.; KOFUJI, S. T. ISA99 - Security Standards in water treatment plants. In: ISA Water/Wastewater and Automatic Controls Symposium, 2013. Orlando: ISA, 2013.

MARTINS, A. B.; AZEVEDO, M. T.; KOFUJI, S. T. Utilização das normas ISA 99 para minimizar os riscos em plantas de tratamento de água. **Revista Controle & Instrumentação**, 2013. (ISSN 0101-0794).

MARTINS, A. B.; AZEVEDO, M. T.; KOFUJI, S. T. Análise de risco e confiabilidade em uma de planta de saneamento (estudo de caso). In: ABES – Associação Brasileira de Engenharia Sanitária e Ambiental, 2013, Goiânia. Goiânia: ABERS, 2013.

Apêndice B – FMEA

Durante a implantação da metodologia de gestão de risco diversos formulários do FMEA foram gerados, segue exemplo abaixo:

FMEA - ANÁLISE DOS MODOS DE FALHA E SEUS EFEITOS																
FMEA: PROCESSO	PROJETO: Engenharia de Operação				APROVAÇÃO: Alaide						ETAPA: 1		Página: 1/3			
	FOZ - UNIDADE JAGUARIBE															
EQUIPE: ALAIDE, FERNANDO, DANILO E JAYME				DATA 1ª ANÁLISE: 10/03/2012						DATA REVISÃO: 17/05/2013						
ITEM/NOME/FUNÇÃO DO PROJETO/PROCESSO	MODO DE FALHA POTENCIAL	EFEITO(S) DA FALHA EM POTENCIAL	SEVERIDADE	CAUSA(S) POTENCIAL DA FALHA	OCCORRÊNCIA	CONTROLE ATUAL DE PREVENÇÃO	CONTROLE ATUAL DE DETECÇÃO	DETECÇÃO	RISCO (RPN)	AÇÃO PREVENTIVA RECOMENDADA	ÁREA E PRAZO	AÇÃO TOMADA	SEVERIDADE	OCCORRÊNCIA	DETECÇÃO	RISCO (RPN)
INVERSOR DE FREQUENCIA	DESATIVA O EQUIPAMENTO	INTERROMPE O BOMBEAMENTO	7	FALTA DE ENERGIA	8	UTILIZA O GERADOR	ALARME SCADA	2	34	UTILIZAR O GERADOR + 2º TRANSFORMADOR	GERMAN - JUN/2013	REDUNDÂNCIA GERAÇÃO	8	2	2	24
			7	QUEIMA DE COMPONENTE	6	PREDITIVA	ALARME SCADA	2	70	ESTOQUE PEÇAS + REVISÃO PERIÓDICA	GERMAN - JUN/2013	TROCA DE PEÇAS ANTES DA QUEBRA	8	4	4	96
		BOMBEAMENTO DE VAZAO ERRADA	7	ERRO DE LÓGICA	3	REVISÃO DA LÓGICA	ALARME SCADA	2	42	ANÁLISE PELO FORNECEDOR	DANFOS - MAI/2013	VERIFICAÇÃO PONTUAL	8	4	8	144
GERADOR	NÃO FORNECE GERAÇÃO	PERDER O SINCRONISMO	7	HARMONICO	8	FILTRO DE HARMÔNICO	MEDIDAÇÃO	2	112	Verificação periódica do funcionamento dos filtros	Fernando => 03/2013	Aquisição e instalação de Filtros	7	2	2	28
		PARAR DE OPERAR OU NÃO ENTRAR EM OPERAÇÃO		DEFEITO COMPONENTE	8	PREDITIVA	OS	2	34	Realização da rotina de manutenção	Danilo => 03/2013	Nova rotina de manutenção	7	4	2	68
				FALTA COMBUSTIVEL	8				34	Verificação periódica	Danilo => 03/2013	Incluir na rotina operação	7	2	2	28
BOMBAS	NÃO RECALCA	NÃO ATENDER A VAZÃO DE 2,27 M³/s	7	FALHA NA BOMBA	7	OPERADOR NO CAMPO	ALARME SCADA	4	198	Realização Preditiva	Danilo => 04/2013	Nova rotina de manutenção	7	6	2	70
			7	FALHA NO LIT	6	PERDA DE DADOS	ALARME SCADA	3	106	Preditiva	Danilo => 04/2013		7	4	2	68
			7	FALHA NO SCADA	4	RTU COM VALOR DIFERENTE	VISUAL OPERADOR	4	112	Substituição	Alaide => 06/2013	Aquisição do VJeo	7	3	2	42
CLP	INOOPERANTE	PERDE CONEXÃO	8	FALHA NA REDE	8	TESTE DO LINK	TESTE DE REDE	4	144	ANÁLISE POR 8MNP	Bruno => 01/2013	Instalação de novo link	8	6	2	80
		EQUIP DESLIGADO OU COM ALARME	8	FALHA NO HARDWARE	3	ANÁLISE DOS ALARMES	ALARME	3	64	TESTE EM BANCADA	Danilo => 02/2013	Aquisição de CLP reserva	8	2	3	38
		TRAVANDO OU OPERAÇÃO ERRADA	8	FALHA NO SOFTWARE	4	BOOT E RELOAD	ATUALIZAÇÃO	3	72	ATUALIZAÇÃO DO SOFTWARE	Danilo => 02/2013	baixar driver	8	3	3	64

Fonte: Autora.

ITEM/NOME/ FUNÇÃO DO PROJETO/ PROCESSO	MODO DE FALHA POTENCIAL	CAUSA (S) POTENCIAL DA FALHA	RISCO antes (RPN)	RISCO depois (RPN)
INVERSOR DE FREQUENCIA	DESATIVA O EQUIPAMENTO	FALTA DE ENERGIA	84	24
		QUEIMA DE COMPONENTE	140	96
		ERRO DE LÓGICA	63	36
GERADOR	NÃO FORNECE GERAÇÃO	HARMONICO	112	28
		DEFEITO COMPONENTE	84	56
		FALTA COMBUSTIVEL	84	28
BOMBAS	NÃO RECALCA	FALHA NA BOMBA	196	70
		FALHA NO LIT	105	56
		FALHA NO SCADA	112	42
CLP	INOOPERANTE	FALHA NA REDE	144	60
		FALHA NO HARDWARE	54	36
		FALHA NO SOFTWARE	72	54

Estudo de Caso - FASE 1 - Output: FMEA
Índice dos Riscos Prioritários - EES

Fonte: Elaborado pela autora.

Fonte: Print screen da aplicação PowerPoint treinamento Hazop elaborado pela autora.

Verificação das causas e das consequências:

Fonte: Print screen da aplicação PowerPoint treinamento Hazop elaborado pela autora.

Apêndice D – Estimativas dos Riscos

Exemplo de umas das planilhas de validação dos cálculo por MTBF:

Análise MTBF EES			
Conjunto A					
Número do Componente	Componente	λ	r	Tempo indisponível por ano $\lambda \cdot r$	Tempo indisponível por ano $\lambda \cdot r$
		Taxa de falha	Tempo de reparo (horas)	(horas)	(anos)
1	Suprimento Energia*	1,956	3	5,868	6,69863014E-04
2	Seccionador fusível	0,0061	2,8	0,01708	1,94977169E-06
3	Pequeno trecho de cabo(*1)	0,00175	26	0,0455	5,19406393E-06
4	Terminações de média tensão(6)	0,0018	11,3	0,02034	2,32191781E-06
5	Sistema de proteção e	0,0006	5	0,003	3,42465753E-07
6	Disjuntor de média tensão	0,0036	168	0,6048	6,90410959E-05
7	Transformador	0,0059	297	1,7523	2,00034247E-04
8	Duto de barras de baixa tensão	0,000125	9,5	0,0011875	1,35559361E-07
9	Disjuntor de baixa tensão	0,003	5	0,015	1,71232877E-06
TOTAL conj A	Total até entrada do cub. BT	1,975875	522,6	8,3272075	9,50594463E-04
Conjunto B					
Número do Componente	Componente	λ	r	Tempo indisponível por	Tempo indisponível por ano $\lambda \cdot r$ (anos)
		Taxa de falha	Tempo de reparo (horas)		
12	Conjunto gerador motor	0,1691	478	80,8298	9,23E-03
11	Trecho cabo B.T.	0,00141	10,5	0,014805	1,69E-06
8	Duto de barra BT	0,000125	9,5	0,0011875	1,36E-07
9	Disjuntor de B. Tensão	0,003	5	0,015	1,71E-06
2	Seccionador (enclosed)	0,0061	2,8	0,01708	1,95E-06
10	Cubículo de BT	0,000802	27	0,021654	2,47E-06
Total		0,180537		80,8995265	9,24E-03
conjunto A		conjunto B	Serie A e B	Paralelo A e B	A e B Paralelo e Serie com C
λ	1,975875	0,180537	2,156412	3,60E-03	0,004398761
$\lambda \cdot p$	9,50594463E-04	9,24E-03			
rp					0,00086188
Para 2 componentes em série:				MTBF(anos)	227,34
$\lambda_s = \lambda_1 + \lambda_2$		2,15641200E+00			
Conjunto C					
Número do Componente	Componente	λ	r	Tempo indisponível por ano $\lambda \cdot r$ (horas)	Tempo indisponível por ano $\lambda \cdot r$ (anos)
		Taxa de falha	Tempo de reparo		
10	Cubículo de baixa tensão	0,000802	27	0,021654	2,47192E-06
Para 2 componentes em paralelo:					
$\lambda_p = [\lambda_1 \lambda_2 (r_1 + r_2)] / [(1 + \lambda_1 r_1)(1 + \lambda_2 r_2)]$					
$r_p = (r_1 r_2) / (r_1 + r_2)$					
A e B em paralelo e em série com C:					
$\lambda = 0,0041155$ (MTBF 242 anos)					
$r = 0.0004953$ anos ou seja 4.3388 horas					

Simulação de alguns cenários do estudo de caso e análise por Markov:

Fonte: Elaborado pela autora.

Simulação da Matriz Makov no MAPLE:

```

with(linalg) :
  BombaAopera := 0.99;
  BombaAfalha := 0.01;
  BombaBopera := 0.99;
  BombaBfalha := 0.01; BombaAeBfalha := 0.2; BombaAeBopera := 0.99; Bombaemfalharetorna
    := 0.8;
  size := 4;
  Q := array(sparse, 1..size, 1..size);
  e := array(sparse, 1..size);
  Q[1, 2] := BombaBfalha; Q[2, 1] := Bombaemfalharetoma;
  Q[1, 3] := BombaAfalha; Q[3, 1] := Bombaemfalharetoma;
  Q[2, 4] := BombaAfalha; Q[4, 1] := BombaAeBopera;
  Q[3, 4] := BombaBfalha; Q[4, 3] := Bombaemfalharetoma; Q[4, 2] := Bombaemfalharetoma;
  Q[1, 4] := BombaAeBfalha;
  for i to size do
    s := 0;
    for j to size do
      s := s + Q[i, j]
    od;
    Q[i, i] := -s
  od;
  Qt := transpose(Q);
  for i to size do Qt[size, i] := 1 od;
  e[size] := 1;
  p := linsolve(Qt, e);

```

```

0.99
0.01
0.99
0.01
0.2
0.99
0.8
4
array(sparse, 1..4, 1..4, [ ])
array(sparse, 1..4, [ ])
0.01
0.8
0.01
0.8
0.01
0.99
0.01
0.8
0.8
0.2

0
-0.22
0
-0.81
0
-0.81
0
-2.59

-0.22  0.8  0.8  0.99
0.01  -0.81  0  0.8
0.01   0  -0.81  0.8
0.2   0.01  0.01 -2.59

1
1
1
1
1

```

```

[ 0.7958637560 0.07106540766 0.07106540763 0.06200542832 ]

```

Simulação por MARKOV – Diagrama de Estados no Excel:

probabilidade	95,74474	4,255264	ano	horas paradas	%H para.	horas funcin.		
						operando	66,6	parado	33,4	2880	122,5516	5,106317	2757,448	
Estados	parado	operando											0,09375	9,375
parada	0,1	0,9	p00	p01									0,125	0,375
operando	0,04	0,96	p10	p11										

jan	fev	mar	abr	probabilidade	Estado
0,96	0,96	0,96	0,96	0,84934656	1
			0,04	0,03538944	0
		0,04	0,9	0,0331776	1
			0,1	0,0036864	0
	0,04	0,9	0,96	0,0331776	1
			0,04	0,0013824	0
		0,1	0,9	0,003456	1
			0,1	0,000384	0
0,04	0,9	0,96	0,96	0,0331776	1
			0,04	0,0013824	0
		0,04	0,9	0,001296	1
			0,1	0,000144	0
	0,1	0,9	0,96	0,003456	1
			0,04	0,000144	0
		0,1	0,9	0,00036	1
			0,1	0,00004	0

estado inicial	jan	fev	mar	abr
1	1	1	1	1
				0
		0	1	1
				0
	0	0	1	1
				0
		1	0	1
				0
0	1	1	1	1
				0
		0	1	1
				0
	0	1	1	1
				0
		0	1	1
				0

jan	fev	mar	abr
p11	p11	p11	p11
	p11	p11	p10
	p11	p11	p01
	p11	p11	p00
	p11	p10	p01
	p11	p10	p01
	p11	p10	p00
	p11	p10	p00
	p10	p01	p11
	p10	p01	p11
	p10	p01	p10
	p10	p01	p10
	p10	p00	p01
	p10	p00	p01
	p10	p00	p00
	p10	p00	p00
p10	p01	p11	p11
	p01	p11	p11
	p01	p11	p10
	p01	p11	p10
	p01	p10	p01
	p01	p10	p01
	p01	p10	p00
	p01	p10	p00
	p00	p01	p11
	p00	p01	p11
	p00	p01	p10
	p00	p01	p10
	p00	p00	p01
	p00	p00	p01
	p00	p00	p00
	p00	p00	p00

Código executado no Maple para duas bombas:

```

with linalg :
BombaAopera d 0.99;
BombaAfalha d 0.01;
BombaBopera d 0.99;
BombaBfalha d 0.01; BombaAeBfalhad0.2; BombaAeBoperad0.99;
Bombaemfalhareturna
d0.8;
size d 4;
Q d array sparse, 1 ..size, 1 ..size ;
e d array sparse, 1 ..size ;
Q 1, 2 d BombaBfalha; Q 2, 1 d Bombaemfalhareturna;
Q 1, 3 d BombaAfalha; Q 3, 1 d Bombaemfalhareturna;
Q 2, 4 d BombaAfalha; Q 4, 1 d BombaAeBopera;
Q 3, 4 d BombaBfalha; Q 4, 3 d Bombaemfalhareturna; Q 4, 2 d Bombaemfalhareturna;
Q 1, 4 d BombaAeBfalha;
for i to size do
s d 0 :
for j to size do
s d s C Q i, j
od;
Q i, i d Ks
od;
Qt d transpose Q ;
for i to size do Qt size, i d 1 od;
e size d 1;
p d linsolve Qt, e ;
0.99
0.01
0.99
0.01
0.2
0.99
0.8
4
array sparse, 1 ..4, 1 ..4,
array sparse, 1 ..4,
0.01
0.8
0.01
0.8
0.01
0.99
0.01
0.8
0.8

```

0.2
(1)
0
K0.22
0
K0.81
0
K0.81
0
K2.59
K0.22 0.8 0.8 0.99
0.01 K0.81 0 0.8
0.01 0 K0.81 0.8
0.2 0.01 0.01 K2.59
1
1
1
1
1
[0.7958637560 0.07106540766 0.07106540763 0.06200542832]

Simulação de Diagramas de Estado – MARKOV:

Fonte: Elaborado pela autora.

Apêndice E – Cenário do Estudo de Caso

O Estudo de caso foi desenvolvido na Empresa Foz de Jaguaribe, responsável por operar o sistema de disposição oceânica do Jaguaribe - SDOJ. Que recebe atualmente o volume de 2.300 litros/segundo de esgoto e atende uma população de aproximadamente 700 mil habitantes. O investimento total para a construção do SDOJ foi de aproximadamente R\$256 milhões e entrou em operação em junho de 2011.

O SDOJ é formado pela Estação de Condicionamento Prévio – ECP, Estação Elevatória de Esgoto – EES e o Emissário Submarino.

A ECP, localizada nas imediações da Av. Jorge Amado, bairro Boca do Rio, Salvador, em uma cota elevada de 39 m, foi concebida de modo a abrigar as instalações e unidades de tratamento preliminar dos esgotos domésticos de 12 bacias da região, cujo montante alcançará 5.903 l/s em 2030, para sua destinação final, através de emissários terrestre e submarino, ao mar. Sendo constituída de uma caixa de chegada, duas unidades de desarenação – Caixas de Areia prismáticas (seção quadrada), cinco Peneiras Escalares e uma unidade de medição – Calha Parshall.

O principal ponto deste projeto em análise é a Estação Elevatório de Esgoto - EEE, responsável por recalque do esgoto para a ECP, composta de quatro bombas centrifugas de 550Kw, uma grade mecanizada de 25 mm e uma caixa de área tipo pista, além de uma unidade de tratamento de odor projetada para 10 lavagens horárias dos gases coletados com uma eficiência final de 98% em relação à remoção de gás sulfídrico.

O esgoto bruto chega a EEE por dois tubos de 1.500 mm de diâmetro, pressurizados e mais um tubo de 200 mm de diâmetro, parcialmente cheio. A EEE possui sensores de vazão, instalados para medição da vazão do esgoto que chega a estação e que sai da mesma. Sendo um medidor de vazão eletromagnético no esgoto pré-tratado que sai da EEE para a ECP e outros dois sensores para a medição de vazão nos dois tubos extravasores que deságuam no Rio das Pedras.

Estação de condicionamento prévio:

Fonte: Autora.

Mapa de localização e bacias de contribuição:

Fonte: Autora.

- 17,5% EES
- 15% ECP
- 15% by pass
- 2,5% Emissário

- Plano de Manutenção + Situação dos equipamentos e inexistência de vazamentos, etc.

- 7,5 % Remoção de H₂S - Odores => 3,75 EES + 3,75 ECP
- 7,5 % Análise Laboratório.

Fonte: Print screen da aplicação PowerPoint elaborado pela autora.

Estuturação dos critérios de avaliação pela nota do QID:

[illegible]

Fonte: Autora

Fluxograma do processo e seus pontos de vulnerabilidades:

Caixa de recepção do esgoto na ETE, o esgoto chega até a estação elevatória parte por duto livre aprox. 800 l/s e por duto forçado mais 1.500 l/s. Todo esgoto que chega tem que ser bombeado para a estação de tratamento que fica em uma cota de aproximadamente 40 m de altura. O ponto crítico desta etapa é evitar que o esgoto in natura extravase para o Rio. Os instrumentos do processo e as comportas são componentes vulneráveis no processo.

Os instrumentos que monitoram a vazão e o nível do esgoto na ETE são críticos, pois estabelecem os parâmetros para o funcionamento eficiente do processo de retirada de areia.

A bomba de recalque é o ponto mais crítico na EEE, pois qualquer parada no equipamento leva a extravasamento do esgoto. Os medidores de nível estão intertravados com as bombas, se as informações dos LIT estiverem erradas o comportamento do bombeamento será alterado. AS informações destes instrumentos vão para o CLP local e via link (rádio e LP) e são transferidos para o CCO, outro ponto de vulnerabilidade.

O sistema de bombeamento da EEE é intetravado com o medidor de nível e vazão que ficam remoto na Estação de Tratamento.

Os medidores de pressão e abertura da válvula que ficam remotos na entrada do emissário, também são pontos críticos, pois o sistema não possui uma bacia de contenção e o funcionamento errado na válvula pode levar a danos no emissário submarino e terrestre.

Segue abaixo registros fotográficos do ambiente analisado no estudo caso:

Fonte: Autora.

Caixa de entrada do esgoto na EEE.
É importante verificar que equipamentos passivos como comportas estejam em pela condição de operação para realizar o controle da chegada do esgoto na estação.

Fonte: Autora.

Medidores de nível são sensores importantes, pois as demais etapas do processo são intertravadas com essa informação.

Fonte: Autora.

Acionadores automáticos das comportas devem está em pleno funcionamento e evitar ataques externos, pois são responsáveis pelo nível de esgoto dentro da estação.

Fonte: Autora.

A planta de tratamento de odores é responsável pela dosagem de produtos químicos e a tarefa de evitar dano ao meio ambiente.

Fonte: Autora.

O esgoto é conduzido por linhas que passam em área com elevado índice de habitantes.

Apêndice F – Tratamento

Durante a gestão de risco foram identificadas diversas vulnerabilidade referentes a integração entre TI e TA, e alguns ações de mitigação do risco foram indicados no diagrama de tratamento, tais como: implantação de lógica no firewall para evitar muitas portas abertas em função da demanda do OPC, revisão da lógica do CLP para incluir controles; criação de alarmes para o SCADA, dentre outras.

Exemplo de umas das telas de configuração do CLP via OPC:

Fonte: Autora.

Há também a demanda de verificação remota, em que as informações locais são enviadas ao CCO central, porém sabe-se que quanto maior a disponibilização das informações, maior a vulnerabilidade, porém no estudo de caso os riscos foram identificados e mitigados. Entretanto com a disponibilização das informações do SCADA no CCO central foi possível a realização de integração das informações a ferramenta de BI, o que possibilita o desenvolvimento de análise crítica de verificação do estado do sistema, veja uma das tela do sistema supervisorio no CCO central e da integração a ferramenta de BI:

Fonte: Autora.

Durante a implantação da metodologia foi identificada a necessidade de ajustes nos na lógica do SCADA e nos formulários manuais para coleta de dados, com o objetivo de possibilitar uma maior precisão em novas análises de confiabilidade do processo.

Exemplo de alguns dos formulários alterados para atender a demanda de mais informações e detalhamento dos estados:

OP.0001.QLD-R00	Página: 1/6
	CHECK LIST PARA PASSAGEM DE TURNO	

Verificação	Conformidade	Estado (Parado/Operando)	Tempo no Estado
1. Sistema Supervisório	☐ Conforme ☐ Não Conforme		
2. Medidores de Vazão	☐ Conforme ☐ Não Conforme		
3. Links de Comunicação	☐ Conforme ☐ Não Conforme		
4. Amperagem dos equipamentos	☐ Conforme ☐ Não Conforme		
5. Ruídos de operação dos equipamentos	☐ Conforme ☐ Não Conforme		
6. Vibração dos equipamentos	☐ Conforme ☐ Não Conforme		
7. Temperatura dos equipamentos	☐ Conforme ☐ Não Conforme		

Fonte: Autora.

Plano de Manutenção 2013

Item	Atividade Desenvolvida	Tipo de manutenção	Duração equip. parado horas	Freq.	JAN					FEV				
					1	2	3	4	5	1	2	3	4	5
1.0	Grade Mecanizada - EES													
1.1	Inspecionar o cabo de operação e o moto-freio	Preventiva		1t										
1.2	Verificar os dentes do rastelo, os rolamentos guias, engrenagem e as guias laterais	Preventiva		S										
1.3	Verificar o nível do óleo no motoredutor e Lubrificar	Preventiva	1	M										
1.4	Limpar as engrenagens	Corretiva		1t										
1.5	Apertar todos os parafusos	Preditiva		M										
2.0	Bombas - EES													
2.1	Verificar o nível do óleo	Preventiva	1	M										
2.2	Inspeção de Ruídos, Vibração	Preventiva		S										
				M										

Fonte: Autora.

ANEXO

Anexo A – Diagramas Funcionais, Infraestrutura e Unifilares do SDOJ

Layout da infraestrutura de comunicação da rede de rutomação do SDOJ:

Fonte: Autora.

Topologia do CLP:

Diagramas unifilares da EEE antes e depois das melhorias proposta com base na gestão de risco:

Sistema Atual

Sistema Proposta- Secundário seletivo

Fluxograma do processo do SDOJ:

Anexo B – Auditoria

Conforme metodologia de gestão de risco implantada, periodicamente ocorrem as auditorias do processo, sendo que as auditorias internas são conduzidas pela equipe de engenharia e registrada as não conformidades no plano de ação de melhorias. Enquanto que as auditorias externa ocorrem em dois formatos:

- Realizado pelo cliente, com a verificação *in loco* e a geração de relatório mensal do resultado da análise e da nota do QID;
- Realizado por auditores externos e pela área de risco da *holding*, com o objetivo de avaliar a segurança corporativa, diagnosticando os riscos e estabelecendo os referenciais corporativo.