VI-201 - ANÁLISE DE RISCO E CONFIABILIDADE EM UMA DE PLANTA DE SANEAMENTO (ESTUDO DE CASO)

Alaide B. Martins[(1)]
Graduada em Computação, Administração e Química e em Engenharia Sanitária. Mestre em Ciência da Computação (Automação de Processo e Segurança) pela Universidade de Salvador. Diretora de Operações na Foz do Brasil. Doutoranda em Engenharia Elétrica na Politécnica EEE/USP.
Sergio Takeo Kofuji[(2)]
Mestre e Doutor em Engenharia Elétrica. Professor titular e responsável pelo grupo de pesquisa do LSI na Escola Politécnica da Universidade de São Paulo
Marcelo Teixeira de Azevedo[(3)]
Graduado em Computação. Mestre em Engenharia Elétrica na Politécnica EEE/USP. Analista de Sistemas na ATT. Doutorando em Engenharia Elétrica na Politécnica EEE/USP.

Endereço[(1)]**:** Av. Jorge Amado, nº 1234 (Foz de Jaguaribe) - Boca do Rio - Salvador - BA - CEP: 40000-000 - Brasil - Tel: (71) 3555-9666 - e-mail: alaide@foz.com.br / alaide@usp.br

RESUMO

Gradualmente nos tornamos mais e mais dependentes de sistemas automatizados e as diversas plantas de saneamento estão cada vez mais se modernizando e integrando as infraestruturas existentes de redes coorporativas. Incidentes de segurança ocorrem diariamente dentro da maioria das empresas, e os sistemas que nos rodeiam são vulneráveis a ataques. Partindo deste problema e com o atual desenvolvimento tecnológico em que se encontra a área de segurança da informação (security) e da segurança do processo (safety), é proposta uma contribuição em análise de riscos com análise quantitativa, através da utilização do método CORAS e Reliability, com aprimoramento utilizando a modelagem matemática de Markov, para realização de análise de risco em plantas de saneamento. Os resultados obtidos pelo método CORAS com a modelagem proposta são validados através da aplicação em estudo de caso em uma Estação Elevatória de Esgoto.

PALAVRAS-CHAVE: Safety, Análise de Risco, CORAS, MARKOV, Reliability.

INTRODUÇÃO

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 destes sistemas e implementações são vulneráveis aos ataques e, com as tecnologias abertas e padrões de Internet, a perícia e o conhecimento destas vulnerabilidades podem ser facilmente utilizadas por possíveis atacantes. A conexão das plantas industriais à Internet ou a outras redes públicas expõe estes pontos vulneráveis a possíveis atacantes. Portanto, é preciso abordar também os problemas de segurança da informação (*security*) nos sistemas de controle e automação industrial, consequentemente a análise de risco e avaliação de falha (*safety*) deverá também contemplar toda a arquitetura e o processo.

Este trabalho apresentar uma nova abordagem com análise quantitativa em análise 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 compilação de diversas normas internacionais no âmbito de análise de segurança e risco. Este trabalho apresenta algumas contribuições, tais como:

- O desenvolvimento de estudos de safety e security em plantas de serviço críticos, especificamente em plantas de saneamento.

- A aplicação do método CORAS para análise de risco em um estudo de caso real em unidade de saneamento.

- Aprimoramento do método CORAS, com inclusão da análise quantitativa por funções de Reliability e Markov.

Neste documento é utilizado uma seção de "Revisão de Estudos Anteriores" com a síntese de apenas alguns dos diversos estudos avaliados para apresentar a necessidade da utilização de métodos matemáticos no desenvolvimento da análise de risco com o aprimoramento ao CORAS.

O presente trabalho foi executado em duas etapas. Na primeira, realizou-se uma revisão bibliográfica de técnicas existentes que viabilizasse a análise de risco em plantas de saneamento, e com base neste estudo modelamos um ciclo de gestão de risco para realização de análise de risco em diversos processos. A segunda etapa, validamos deste ciclo com a aplicação em um estudo de caso em uma Estação Elevatória de Esgoto, que faz parte do Sistema de Disposição Oceânica do Jaguaribe, em Salvador/Bahia.

MATERIAIS E MÉTODOS

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. A metodologia utilizada neste trabalho foi o método científico da inferência com a coleta de dados através de pesquisas bibliográficas, utilização de normas e principalmente artigos científicos, conceitos encontrados em livros, dissertações e teses, além de pesquisas na internet sobre informações pertinentes ao tema. O planejamento da pesquisa contempla duas etapas interligadas: o estudo teórico e documental, e o estudo empírico com desenvolvimento do estudo de caso em uma estação elevatória de esgoto.

Na primeira etapa ocorreu a análise dos diversos modelos, métodos, técnicas e ferramentas de análise de riscos e verificação de confiabilidade. A segunda etapa contempla a aplicação do método CORAS e a concepção de análise de risco quantitativa por modelagem matemática para realização da análise quantitativa, através da combinação das diversas técnicas selecionadas e sua validação na análise de risco e a avaliação da confiabilidade da estação elevatória.

O material utilizado contempla os equipamentos instalados na Estação Elevatório de Esgoto (EEE), tais como:

- Um CCM (Central de Controle de Motores), em que o sistema elétrico que foi projetado é com barra única, a qual alimenta as quatro bombas (sendo uma reserva). Cuja aalimentação da barra principal é feita a partir de um transformador a seco de 2500 kVA, com o secundário ligado em estrela não aterrado. O transformador tem ligação Dy1, impedância de 6%, tensão secundária 460/266V. A saída do transformador é protegida e chaveada por um disjuntor de 4000A, capacidade de interrupção simétrica de 75 kA.

- Além da barra principal, o sistema da EEE incorpora uma barra de geração, à qual estão ligados três geradores de 687/757 kVA, acionados por motor de potência "prime" 585 kW, potência "stand by" de 644 kW.

- Essa EEE é automatizada com inversores de frequência, medidores de nível, vazão e pressão, controladores de odores, PLC e outros instrumentos de campo, todos controlados pelo Centro de Controle de Operações – CCO, que fica aproximadamente a 3 km de distância.

A EEE faz parte de um sistema de disposição oceânica, emissário submarino, e possui a capacidade de recalque da vazão de 2.300 L/s de esgoto.

REVISÃO DE ESTUDOS ANTERIORES

A análise de risco significa o processo de compreender a natureza do risco e determinação do nível de risco, conforme Braendeland at.al (2010) define-se risco como a combinação da consequência e probabilidade de um evento indesejado.

Existem duas abordagens para segurança e análise de risco, as baseadas em ativos e as baseadas em cenários. A análise baseada em ativos reflete o pensamento de segurança tradicional de proteger os itens com valor. A

abordagem baseada em cenário reflete o pensamento tradicional de engenharia de processo, na proteção contra ataques específicos. É semelhante ao método de cenários proposto pela metodologia de análise de riscos denominada Process Hazard Analysis (PHA). Outra técnica também conhecida é o estudo de perigo e operabilidade – Hazard and Operability Studies (HAZOP) –, usada para proteger contra acidentes e ajudar a garantir a segurança. Ambas as abordagens de segurança, baseadas em ativos e baseadas em cenários, procuram vulnerabilidades ou fragilidades no sistema que permitem ataques bem-sucedidos.

O artigo de Wang e Zeng (2010), apresentado na IEEE 2010 - 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), mostra um estudo sobre o método de avaliação quantitativa de riscos de segurança da informação, utilizando AHP (Analytic Hierarchy Process) e matemática Fuzzy como modelo quantitativo e cita o CORAS apenas como método qualitativo. Verifica-se neste estudo que o CORAS apresenta uma ampla modelagem qualitativa e restrições para situações com abordagem quantitativa. Contudo com aprimoramento da modelagem e inclusão da teoria de confiabilidade para a análise quantitativa ao método CORAS, poderá tornar-se um modelo que atenda a diversas situações na análise de risco, e foi exatamente nesta demanda que desenvolvemos nossa pesquisa apresentada neste trabalho.

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 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 desenvolvida um aprimoramento ao método convencional com o tratamento das incertezas, porém em nossos estudos como a função reliability é uma complementação para avaliação quantitativa à metodologia CORAS iremos realizar apenas uma abordagem convencional.

Dente as diversas ferramentas disponíveis para realização da análise dos cenários e avaliação dos riscos, priorizamos nosso estudo em quatro delas:

- Análise dos modos de falhas e efeitos – *Failure Mode and Effects Analysis* (FMEA).
- Análise da árvore de falhas – *Fault Tree Analysis* (FTA).
- *Sneak Path Analysis* (SPA).
- Análise de Risco com CORAS.

FMEA

A análise dos modos de falha e efeitos é definida por Palady (2007) como uma técnica que oferece três funções distintas:

- Ferramenta para prognóstico de problemas.
- Procedimento para desenvolvimento e execução de projetos, processos ou serviços.
- Diário do projeto, processo ou serviço.

Como ferramenta mostra-se eficiente para prevenção de problemas e soluções. Como procedimento, oferece uma abordagem estruturada para o desenvolvimento de projetos e processos. Finalmente, como diário, o FMEA inicia-se na concepção do projeto, processo ou serviço, e se mantém através do ciclo de desenvolvimento do produto ou serviço.

Atualmente existem dois tipos de FMEA: FMEA de projeto (*Design Failure Modes and Effects Analysis* – DFMEA) e FMEA de processo (*Process Failure Modes and Effects* Analysis – PFMEA). A diferença entre as duas está nos objetivos, e ambas podem ser caracterizadas através de duas perguntas:

- Como esse projeto/processo pode deixar de fazer o que deve fazer?

- O que devemos fazer para prevenir essas falhas potenciais de projeto/processo?

Na utilização do método, cinco elementos básicos devem ser incluídos para garantir o sucesso, e, caso um dos elementos não seja atendido, a qualidade e a confiabilidade serão impactadas. Na figura 1 podem ser observados os elementos básicos.

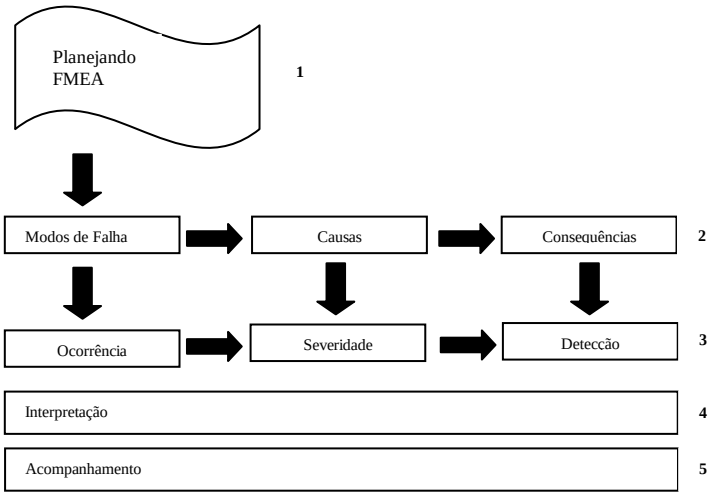


Figura 1: Elementos básicos do FMEA.

Os cinco elementos da figura 01 são definidos por (PALADY, 2007):

1. Selecionar o projeto/processo;
2. Perguntar e responder aos três questionamentos?
   - 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. Acompanhamento se as intervenções realizadas atenderam aos objetivos, bem como realização de auditorias.

FTA

Análise da árvore de falhas, a definição de Limnios (2007) de FTA é uma técnica que visa melhorar a confiabilidade através de análise sistemática de possíveis falhas e consequências, adotando medidas corretivas ou preventivas. É baseado 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 2.

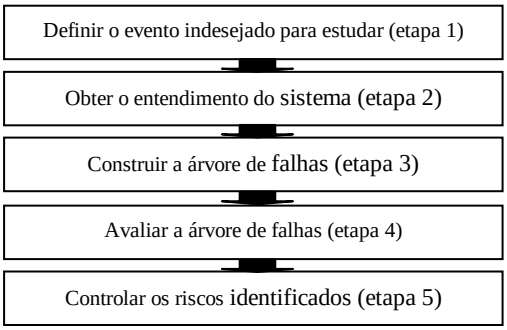


Figura 2: Etapas do FTA.

Etapa 1: As definições de eventos indesejados é 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.

SPA

Segundo Baybutt (2004), o Sneak Path Analysis (SPA), também conhecido como Sneak Circuit Analysis (SCA), tem por principal objetivo identificar caminhos inesperados ou fluxos lógicos em sistemas eletrônicos que sob certas condições podem produzir resultados indesejados ou impedir o funcionamento do sistema. Alterações do sistema podem erroneamente transparecer um problema sem importância ou com impacto local e, com isso, os operadores podem utilizar procedimentos operacionais impróprios.

Assim, pode ocorrer no hardware, software ou em ações do usuário e em alguns casos com a combinação desses três fatores. A falha no sistema é causada por situações incomuns que são disparadas independentemente dos componentes. Portanto, o SPA é diferente de outras técnicas de análise, como a FMEA, que analisam as falhas dos componentes do sistema.

Ainda conforme Baybutt (2004) existe um paralelo para aplicação de SPA para o processo de segurança, especialmente em cibersegurança, situação em que plantas podem ser manipuladas remotamente por suas redes de automação. Nesse contexto, são considerados os terroristas ou funcionários descontentes que têm por objetivo alcançar e manipular os ativos de processos: hardware, software e dados, além de informações sensíveis, como: firewall, senhas, criptografia, entre outros.

O ponto-chave para a análise de segurança cibernética é identificar formas ou caminhos ao longo do qual os atacantes podem penetrar os sistemas de acesso e os meios que podem utilizar para causar algum tipo de prejuízo. Alguns desses caminhos podem existir como falhas de projeto e corresponder às condições latentes de SPA convencional. Outras exigem o rompimento dos controles existentes do SPA, através da análise de barreira descrita na figura 3.

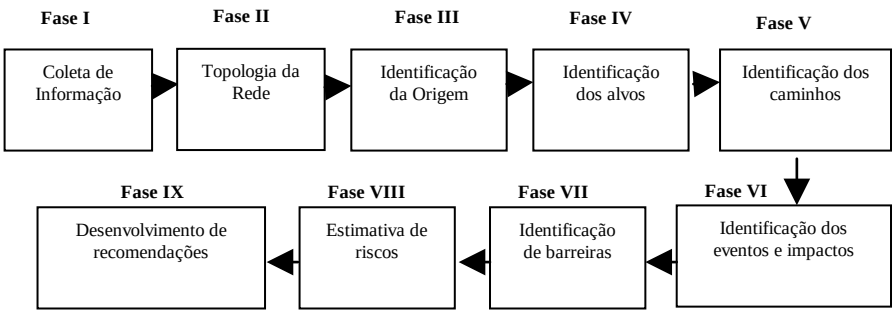


Figura 3: Passos para análise do SPA.

Fase 1: Refere-se à coleta das informações necessárias para o levantamento de contramedidas para cibersegurança. Nessa fase são incluídas informações de arquitetura, configuração de rede e interfaces (interna e externa), sistemas operacionais, desenhos lógicos e físicos. O autor menciona ser necessário pensar como um terrorista, um funcionário insatisfeito ou até mesmo como um invasor externo.

Fase 2: Com o conhecimento adquirido do ambiente monta-se uma topologia representando de forma gráfica os componentes e as suas conexões.

Fase 3: Com as informações da fase 1, identifica-se os potenciais invasores que podem comprometer o ambiente. Nessa fase são considerados os possíveis invasores, sendo eles internos ou externos.

Fase 4: Da mesma forma da fase 3, os possíveis alvos e os impactos são identificados nessa fase. Podendo incluir: hardware, software, pessoas e dados.

Fase 5: Através da topologia e diagramas construídos são identificados os caminhos e combinações de alvos que podem ocasionar um problema. Em todas as análises o fluxo de caminhos possíveis deve ser considerado.

Fase 6: Nessa fase é determinado o impacto dos riscos, ou seja, a identificação dos eventos e impactos e as suas consequências. Os impactos identificados nessa fase podem ser tantos lógicos como físicos.

Fase 7: As ações são propostas com base nas análises, medidas para reduzir ou eliminar as vulnerabilidades identificadas. Assim que identificadas, as recomendações são realizadas ou são feitas sugestões de melhoria.

Fase 8: A estimativa do risco é realizada nessa fase, criando um critério de impacto e importância.

Fase 9: Nessa fase é realizado o desenvolvimento das recomendações. A necessidade de novas contramedidas ou modificações é baseada nos possíveis impactos para que as ameaças sejam reduzidas para um nível tolerável ou aceitável.

ANÁLISE DE RISCO

Em nossa pesquisa de análise de risco em plantas de saneamento observa-se que além dos eventos físicos de falha no processo podem ocorrer também ataques cibernéticos, 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 em uma estação elevatória ou operar indevidamente uma comporta e levar a transbordamento de esgoto.

Diante deste cenário fica claro que uma nova abordagem deve ser estudada, para garantir a segurança de plantas de serviços críticos, como saneamento. Análise da vulnerabilidade de plantas de saneamento tende cada vez mais a fazer parte da preocupação da sociedade, porém observa-se que realizar esta atividade de quantificar e qualificar quão vulnerável encontra-se uma planta não é uma tarefa tão fácil, pois existem muitos métodos e ferramentas disponíveis, mas nada muito simples e integrado que possibilite quantificar a análise de risco e de falhas no cenário de segurança da informação e segurança do processo.

Vemos, portanto que os métodos tradicionais de análise de riscos são imprevisíveis para situações que envolvam security e safety inter-relacionados, devido a falta de modularidade, portanto os métodos de análise convencionais de risco são inadequadas para enfrentar esses desafios. Conforme Brændeland e Stolen (2010), o método CORAS surgir para resolver situações como estas.

A escolha de modelar informações contextuais utilizando método CORAS, justifica-se pela abrangência de atuação deste método e pela capacidade de otimizar as informações com a capacidade de quantificar os riscos. (BRAENDELAND, G., STOLEN, K., 2010).

Tomamos com base para nossa análise de risco o método CORAS, pois o mesmo já realiza uma integração de diversas técnicas de análise de risco. Realizamos o aprimoramento deste método para realizar avaliações quantitativas com base na modelagem por Markov, para análise de falha no processo automatizado, que poderá

em outras plantas, 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.

A Cadeias de Markov são bem conhecidas no mundo matemático para fazer equações de probabilidade, e mostra como um estado pode afetar o outro estado, ou todo o sistema. Muitos métodos de analise levar a previsões otimistas para o sistema, porque eles assumem que os componentes são independentes. Enquanto que a análise 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 ocorrer houver mudança em um dos estados do sistema.

O principal ponto na análise de risco é descobrir qual é o problema, onde os riscos ocorrem, e como tratá-los. Análise de risco começa com uma descrição da situação e indica que as ameaças poderiam ser a razão para que eles ocorram, e quais as consequências e como eles poderiam ser evitados. Iremos considerar em nosso estudo sete fases em uma análise de risco: Estabelecimento contexto, identificação de riscos, estimativa do risco, avaliação de risco, tratamento, verificação dos resultados e auditorias de acompanhamentos periódicos.

Com o objetivo de simplificar e coordenar atividades de avaliação de risco, desenvolvemos um ciclo de gestão de risco, tomando como referência o ciclo do PDCA, em cada uma das fases estipuladas temos um output que irá favorecer o acompanhamento do processo e documentar a análise de risco, vide figura 4.

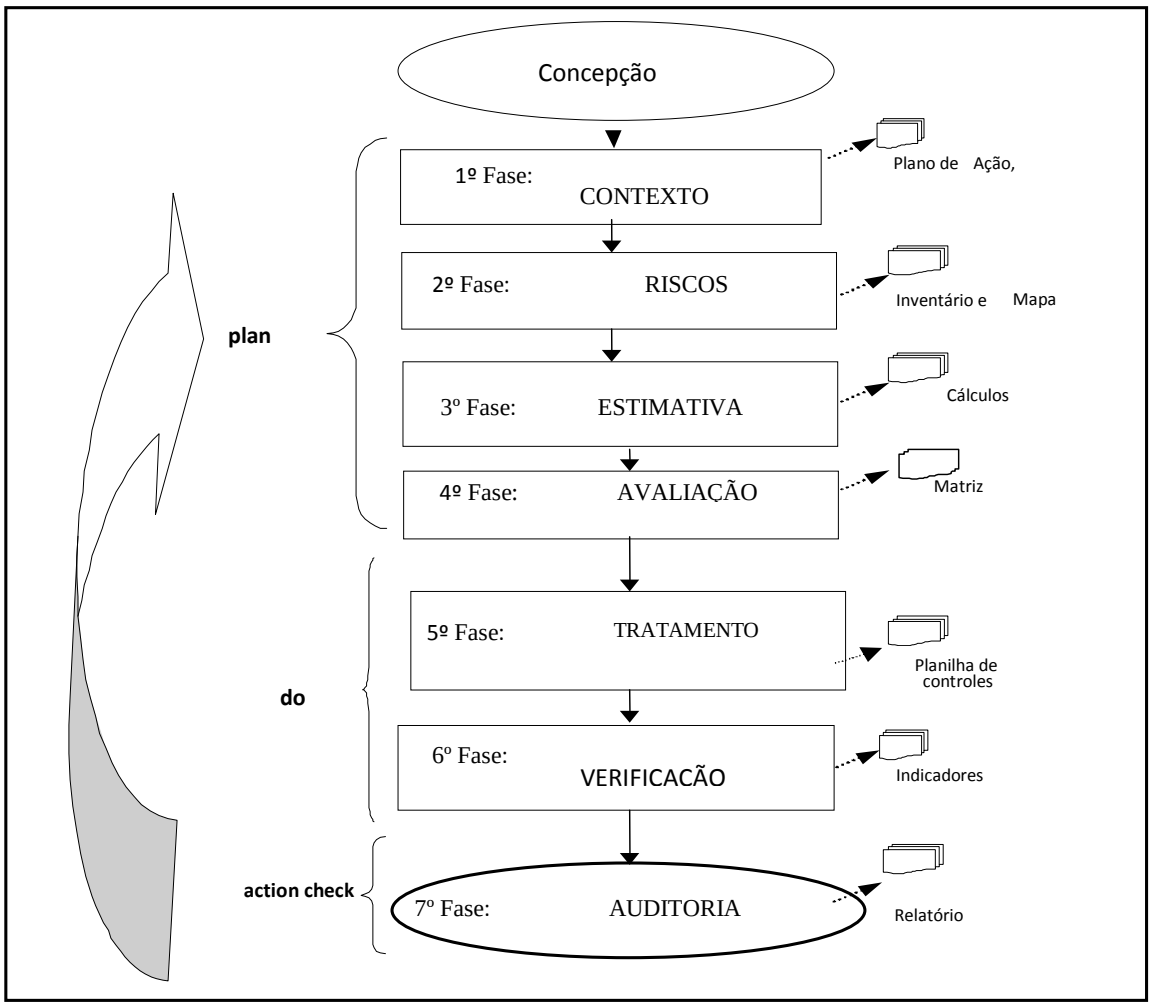


Figura 4: Ciclo de Gestão de Risco com referência do PDCA

As quatro primeiras fases são na verdade suficiente para determinar o impacto dos riscos, que fazendo uma analogia ao ciclo PDCA de qualidade, refere-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 indicamos 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.

O ciclo que sugerimos neste trabalho se implementando 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 identifica-se, 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.

ANÁLISE DE SAFETY E SECURITY COM O CORAS

O estudo de caso foi realizado em uma concessionária que já possui um planta de saneamento automatizada e em operação. Verificamos também a existência de boas práticas de segurança da informação, em conformidade com a ISO 27001, já sendo praticadas na rede de Tecnologia da Informação (T.I.) – *security*.

O método base utilizado para o desenvolvimento das fases da gestão de risco foi o CORAS e as teorias de confiabilidade (*reliability*).

O CORAS utiliza ferramentas de identificação e análise de riscos oriundos da prevenção de acidentes em processo (safety), tais como o Hazard and Operability study (HazOp), Fault Tree Analysis (FTA), Failure Mode, Effect and Criticality Analysis (FMECA), Markov analysis e Event Tree Analysis (ETA). O CORAS disponibiliza uma software gratuito com telas e formularios que possibilita o desenvolvimento da documentação da gestão de risco, ao longo de oito etapas de desenvolvimento do método, o risco é descrito usando Unified Modeling Language (UML). O CORAS é uma metodologia de análise de risco baseado no paradigma da modelagem uniformizada, em que pretende-se identificar, analisar e descrever o risco através de uma linguagem padronizada, única, idependente do processo.

O CORAS tem como base a norma de gerenciamento de risco que estabelece o padrão internacinal, a ISO/IEC 31000:2009 – *General guidelines for principles and implementation of risk management*, e 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 5, que contempla as etapas do CORAS.

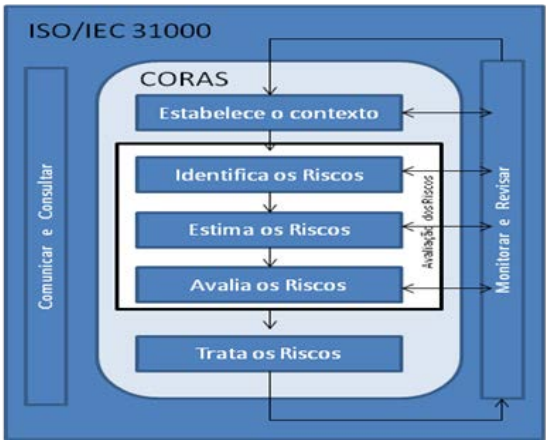


Figura 5: Diagrama da ISO/IEC 31000.

Conforme método de análise de risco CORAS sugere se o desenvolvimento 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).

DESENVOLVENDO A ANÁLISE DE RISCO UTILIZANDO O CORAS

Seguindo o roteiro de implantação da metodologia CORAS, devemos inicialmente definir as pessoas envolvidas no processo de contextualização e definição das diretrizes para a análise de risco. O software do CORAS disponibiliza recursos para documentar todo o processo de análise de risco e estabelecer a relação entre as etapas de análise. O desenvolvimento da análise com CORAS ocorre em oito passos, como veremos a seguir:

1º Passo: *Contextualização – Definição do escopo(cenário)*

Primeiramente definimos o escopo de atuação e detalhamos o cenário, portanto nosso foco do estudo de caso é uma Estação Elevatório de Esgoto – EEE, e neste ponto descrevemos as características técnicas da estação elevatória, tais como: Um CCM (Central de Controle de Motores), que alimenta as quatro bombas (sendo uma reserva) de 550 HP, com inversores de frequencia; um transformador a seco de 2500 kVA, chaveado por um disjuntor de 4000; três geradores de 687/757 kVA, acionados por motor de potência "prime" 585 kW, potência "stand by" de 644 kW. A EEE é automatizada com inversores de frequência, medidores de nível, vazão e pressão, controladores de odores, PLC 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 e desenvolvimento da análise de risco. Porém durante o estudo verifica-se a necessidade de combinar outras metodologias para a análise de risco com objetivo de complementar o estudo.

2º Passo: *Identificando o Ambiente*

Neste passo, objetiva-se identificar os riscos e as falhas de confiabilidade (r*eliability*), detalhada no passo 6. Verificam-se as vulnerabilidades deste sistema com o estabelecimento de parâmetros, tais como o de MTBF (*Mean Time Between Failures*), período médio entre falhas para os seus componentes, pois há exigências de operação contínua desta estação, considerando-se que na prática a perda do sistema, irá provocar o extravasamento de efluente, poluindo o meio ambiente.

É nesta fase da análise que definimos 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 estudo desenvolveu-se o detalhamento das origens dos riscos, com a construção da tabela de ativos envolvidos no cenário em análise. Nessa etapa utilizamos técnicas similares a 5W1H, e preenchemos no software do CORAS os formulários, conforme modelo da figura 6.

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.

Figura 6: Conhecendo o Ambiente

O objetivo principal desta etapa é da visibilidade e documentar os ativos, favorecendo a tomada de decisão para definição em quais componentes devemos atual 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. Essa é uma etapa paralela a todo o processo de desenvolvimento.

Para estabelecimento do critério de importância para cada ativo foi relevante o envolvimento de pessoas das diversas áreas da empresa, pois são critérios muitos subjetivos, que teve como base definições estabelecidas no CORAS, utilizamos 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 1.

Tabela 1: 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

Outras tabelas com maiores 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 outros.

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

Nesse passo também utilizamos as referências da metodologia CORAS para escala de consequência, conforme critérios da tabela 2.

Tabela 2: 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]

Utilizamos também nesta fase do trabalho a classificação das consequências em função da gravidade dos eventos, conforme a tabela 3.

Tabela 3: 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

Para análise quantitativa utilizamos a classificação pela probabilidade e/ou frequência da ocorrência, conforme tabela 4.

Tabela 4: 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

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

Identifica-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.

Tabela 5: 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

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. Nesse estudo de caso realizamos reuniões estruturadas fazendo uso de técnicas como *brainstorming* com a presença de diversos especialistas e consultores que conhecem a planta da EEE.

Com domínio das informações foi possível desenhar os diagramas de ameaça no sistema CORAS, vide figura 7, estabelecendo as relações de impacto.

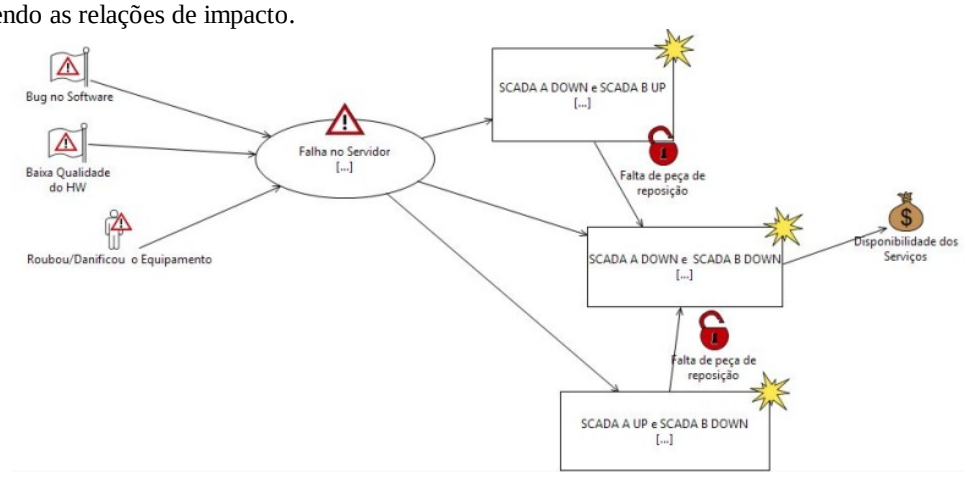


Figura 7 - Diagrama de Ameaças – CORAS.

Para este estudo de caso foram desenvolvidos dez 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 é calcular e estimar os valores quantitativos para os riscos, buscando estabelecer a severidade para os riscos identificados, possibilitando apoiar a análise qualitativa do cenário.

A estimativa de risco é calculada conforme a probabilidade e frequência de ocorrência do incidente no período t.

Portanto a análise quantitativa por função *reability*, é igual ao produto das confiabilidades dos componentes individuais, que constituem o sistema definida conforme equação 1:

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

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, temos *(Initiates),vide equação 2:*

$a \rightarrow c \,/\, ((a \prod c).\,(p))$ equação (2)

Em situações em que a possibilidade de ocorrência de c_2 a partir de c_1 é igual para a probabilidade p de c_1 multiplicada com a possibilidade da frequência f em que c_1 irá gerar o incidente c_2 quando c_1 ocorrer. Quando $c_1 \prod c_2$, vemos que o cenário/incidente c_2 é precedido por c_1. Logo temos (*Leads-to*), vide equação 3:

$(c_1(p).c_1 \rightarrow c_2) \,/\, (c_1 \prod c_2).(p.f)$ equação (3)

Porém temos situação em que os cenários/incidentes são mutuamente exclusivos, portanto a probabilidade é calculada em paralelo. Se dois eventos são mutuamente exclusivos, a probabilidade da união deve ser igual a soma das respectivas probabilidades, sendo considerada todas as instâncias, $c_1 \amalg c_2$. Nessa regra vemos que c_1 ou c_2 ocorrem, mas não ambos, desde que eles sejam mutuamente exclusivos. Sendo, conforme equação 4, se os dois eventos são estatisticamente independentes, ou seja não há probabilidade de um ter relação na probabilidade do outro, logo a probabilidade da união dos dois eventos será igual a soma individual das probabilidades.

$(c_1(p_1) \,.\, c_2(p_2)\,) \,/\, ((c_1 \amalg c_2).(p_1+p_2))$ equação (4)

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

$(c_1(p_1) \,.\, c_2(p_2)) \,/\, ((c_1 \prod c_2).(p_1+p_2 - p_1.p_2))$ equação (5)

As probabilidades são inseridas no sistema do CORAS, vide figura 8.

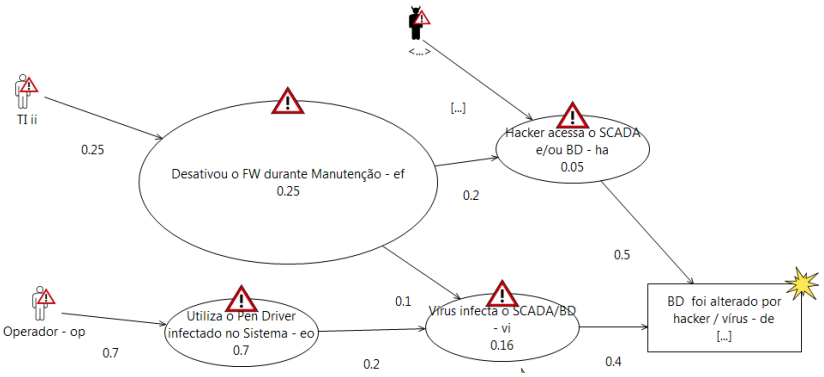


Figura 8 - Diagrama de Ameaças com estimativas.

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

A análise qualitativa é fundamental para identificar qual a característica do risco e se o mesmo é aceitável ou não. Usa-se como referência a tabela de análise de risco que deve ser preenchida com a identificação qualitativa do nível do risco.

Tabela 6: Análise de Risco Qualitativo.

	Insignificante	Menor	Moderado	Maior	Catastrófico
Raro					
Pouco Provável					
Possível	R3		R1		
Provável	R4			R2	
Certamente					

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

O diagrama de tratamento baseia-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, vide figura 9.

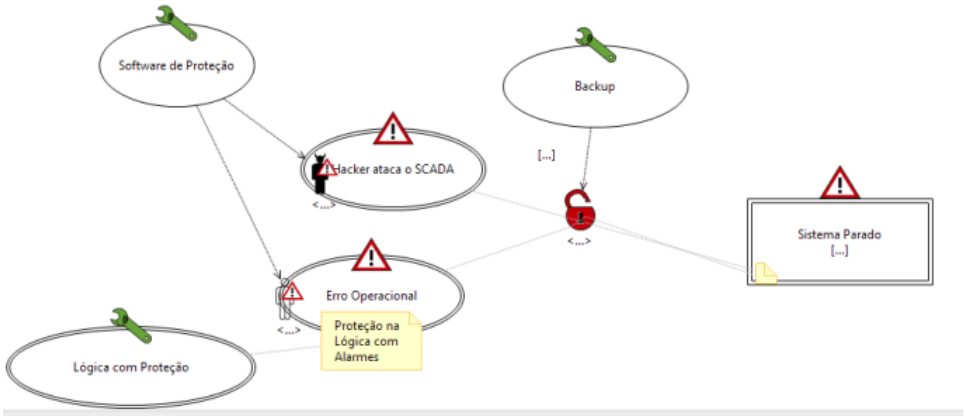


Figura 9 - Diagrama de Tratamento de Risco.

MODELAGEM POR MARKOV E CORAS

A integração da cadeia de Markov ao método CORAS, possibilita a avaliação de análise de falha quantitativa em várias situações, por exemplo: Considere que a unidade dosadora de cloro de gás que hoje está funcionando perfeitamente pode, amanhã, apresentar uma pequena avaria (que a permita continuar operando), com probabilidade 30%, ou quebrar completamente, sem possibilidade de conserto, com probabilidade 20%. Por outro lado, se a unidade apresenta hoje uma pequena avaria, a probabilidade de que amanhã ela esteja totalmente quebrada é 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 avaliado conforme tendência por:

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, temos: (0,3 * 0,7 + 0,2 + 0,5 * 0,2) = 0,21 + 0,2 + 0,1 = 0,5; ou seja, 50% de probabilidade que esteja quebrada após dois dias.

Vemos que a análise por Markov é aplicável desde que as seguintes restrições sejam respeitadas:

- As probabilidades de transição entre os estados permanecem constantes ao longo do tempo.
- A probabilidade de um estado futuro independe dos estados anteriores, excetuando-se o estado imediatamente precedente (propriedade de falta de memória).

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 estes estados permaneçam constantes. Esta imposição é uma limitação significativa e implica no uso de distribuições de probabilidade exponenciais para a modelagem das taxas de falha e de reparo. Pode 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. Recomenda-se sua utilização hibrida com outras modelagens (VOLOVOI, 2004) (MAILLART; POHL, 2005).

Um processo estocástico é dito ser um processo Markoviano se o estado futuro depende apenas do estado presente e não dos estados passados. Este 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 {Xt}, onde o índice t pertence a um dado conjunto T . O conjunto T é

normalmente composto de números inteiros não negativos, e Xt 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 chamadados estados, e o conjunto de todos os possíveis valores forma o espaço de estado do processo. Análise de Markov é, entre outras técnicas indicada para 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 assumi independência por completo. Uma análise de Markov considera o sistema como um número de estados, e as transições entre estes estados. Os estados são modelados graficamente e cálculos estatísticos são realizados para determinar a probabilidade de transição entre os estados.

Conforme 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 dicretos. 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 destas 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 é uma função apenas de X_n, vide equação 6, onde x é algum estado do processo. A identidade define a propriedade de Markov:

$$Pr(X_{n+1} = x \mid X_0, X_1, X_2, ..., X_n) = Pr(X_{n+1} = x \mid X_n) \qquad \text{equação (6)}$$

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,...; 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. Em nosso estudo de caso um exemplo de estado, são as Bombas da Estação Elevatória, cujos estados podem ser máquina funcionando, máquina parada e em reparo, 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 Pij , é a probabilidade de um objeto que se encontra no estado i após um intervalo de tempo fixo predeterminado ser $P(X_{t+1} = j \mid X_0 = i)$, encontrado no estado j , para todo t = 0,1,2,... .Para n passos à frente, é possível escrever as probabilidades de transição para cada i e j, com n= 0,1,2,..., conforme a equação 7:

$$P(X_{t+n} = j \mid X_t = i) = P(X_n = j \mid X_0 = i) \qquad \text{equação (7)}$$

Para todo t = 0,1,2,... . Temos a equação 8:

$$P(X_1 = j \mid X_0 = i) = p_{ij} ; \; P(X_n = j \mid X_0 = i) = p_{ij}(n) \qquad \text{equação (8)}$$

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 $P(X_0 = j \mid X_0 = i)$, sendo se i=j igual a 1, senão será 0 (zero).

Uma maneira simples de visualizar um tipo específico de cadeia de Markov é através 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 Pij = Pr(Xn+1 = i|Xn =j), e é independente do tempo n. As integrações na

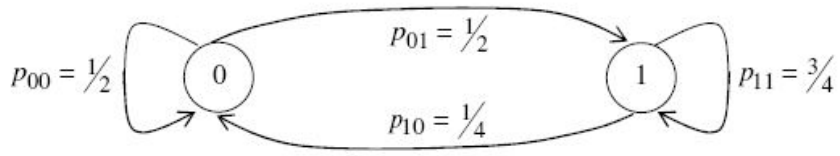
probabilidade de transição de k passos são somatórios, e podem ser calculados como a k-ésima potência da matriz de transição. Isto é, se P é a matriz de transição para um passo, então Pk é a matriz de transição para a transição de k passos. Estes tipos de cadeia de Markov finitas e discretas podem também 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. Este grafo é denominado diagrama de transição.

Para melhor compreendermos vamos inicialmente exemplificar com apenas dois possíveis estados (parado e operando), portanto, com apenas dois passo, sendo o espaço de estados S = {0, 1}. Consideremos que os estados parado e operando são representados pelos índices 0 e 1, respectivamente. A partir de observações históricas de manutenção, foram obtidos as probabilidades de transição supostas contantes, uma bomba em operação continuará em operação com probabilidade igual a ¾ e, entrará em falha, com probabilidade ¼ de estado parado. Bombas parada continuará parada com probabilidades iguais a ½, equanto que, a probabilidade de uma bomba parada suceder uma bomba em operação é ½.

O produto cartesiano, SxS , é {(0,0), (0,1), (1,0), (1,1)}. A matriz de probabilidades de transição para um passo, será:

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

A representação em grafo, seria:



Ainda buscando a solução para o exemplo mencionado podemos também fazer uso do diagrama em árvore partindo do estado 0, e vamos considerar apenas 4 passos, sabendo que os eventos são independentes e que precisamos multiplicar todas as probabilidades do percurso trilhado no diagrama que levam ao estado da probabilidade desejada, vide tabela 7.

Tabela 7: Representação do diagrama de passos $P_0(4)$

	1º PASSO	2º PASSO	3º PASSO	4º PASSO
PARADO	OPERANDO	OPERANDO	OPERANDO	OPERANDO
				PARADO
			PARADO	OPERANDO
				PARADO
		PARADO	OPERANDO	OPERANDO
				PARADO
			PARADO	OPERANDO
				PARADO
	PARADO	OPERANDO	OPERANDO	OPERANDO
				PARADO
			PARADO	OPERANDO
				PARADO
		PARADO	OPERANDO	OPERANDO
				PARADO
			PARADO	OPERANDO
				PARADO

Tabela 8: 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

Portanto a probabilidade do equipamento encontra-se no estado parado $P_0(4) = 0,3359375$, enquanto que no estado operando será $P_1(4) = 0,6640625$. Se consideramos um periodo de 1 ano teremos 2.942 horas da maquina 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. Esta classificação diz respeito à probabilidade do processo retornar a um dado estado inicial se o processo partiu deste 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,...,M} o conjunto finito de estados, e seja o par de estados (i,j) ϵ S x S, se asociarmos a cada par (i,j) um número real Pij(n), de modo que sejam satisfeita as propriedades estabelecidas na equação 9:

$0 \leq P_{ij}(n) \leq 1$ para ¥ (i,j) Ɛ SxS e $\Sigma_{j\,\varepsilon\,s} P_{ij}(n) = 1$ para ¥ i Ɛ S equação (9)

Define-se a matriz P:

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

Portanto vemos que se n = 0, teremos a própria matriz identidade, P_0 é $P_{ij}(0) = P(X_0 = j| X_0 = i)$, logo, temos:

$$P_{ij}(0) = \begin{cases} 1, se\ i = j \\ 0, se\ i \neq j \end{cases}$$

Se n > 0, tomando como base o teorema da probabilidade total, equação 10:

$P_{ij}(n) = P(X_n = j|X_{n-1} = 1)$ equação (10)

Teremos para o estado j em n passos a equação 11:

$P_j(n) = P(X_n = j) = \Sigma_i P_i(0)P_{ij}(n)$ equação (11)

Em resumo, P(n)=P(0)Pn.

Em nosso estudo de caso os estados estabelcidos para os componentes em plantas de saneamentos são finitos (contáveis), portanto é relativamente fácil a aplicação do processo Markov, considerando o cálculo de Pn. Porém a modelagem matematica não é nada trivial para casos em que o espaço de estados tendem a infinitos, ou seja o comportamento é assintótico, $n \rightarrow \infty$, de p(n) e Pn, ou seja situações em que deseja-se utilizar Markov para controle de dosagem no tratamento de água.

Considere um sistema de recalque de esgoto com dois conjuntos de motor bomba idênticos. Seja Xn 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 reignição 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 tn ; 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 na 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 estragadas, apenas uma operando e ambas operando. Então temos:

Ambas em operação, $P(X_n = 2|X_{n-1} = 2) = P_{22} = 0,9 \times 0,9 = 0,81$

Uma bomba em operação e a outra em falha, $P(X_n = 1| X_{n-1} =2) P_{21} = 0,9 \times 0,1 + 0,1 \times 0,9 = 0,18$

Ambas em falha, $P(X_n = 0| X_{n-1} = 2) = P_{20} = 1 – P_{22} – P_{22} = 0,01$

Uma em operação e a outra em operação após reparo, $P(X_n = 2 | X_{n-1} = 1) = P_{12} = 0,9 \times 0,6 = 0,54$

Nenhuma em operação, sendo que apenas uma estava boa, $P (X_n = 0 | X_{n-1} = 1) = P_{10} = 0,1 \times 0,4 = 0,04$

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 abandona-lo exceto se o processo partir novamente, portanto, $P_{00} = 1$.

A matriz de probabilidades de transição para um passo será:

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

Em todas as áreas da atividade humana busca-se quantificar eventos que possuem certo grau de incerteza de ocorrência. Isto implica de certa forma na necessidade de “prever o futuro”. Modelos matemáticos probabilísticos são concebidos para auxiliar o homem na tomada de decisão, e nessa situação, como vimos, Markov é bastante útil para apoiar de modo quatitativo a Análise de Risco.

RESULTADOS OBTIDOS OU ESPERADOS

Aspectos de confiabilidade (*Reliability*) de sistemas de segurança devem ser projetados para ser ativado em situações de desvios de processo, para proteger as pessoas, o meio ambiente e os bens materiais. Conforme Rausand e Hoyland (2004*) Safety System* possuem diversas camadas de proteção, que podemos aplicar em nosso estudo de caso na estação de condicionamento efluente doméstico, tais como:

- O sistema de desligamento do efluente de entrada que compreendendo sensores de nível, de vazão, inversores de frequência e sistema PID programado para desligamento automático das bombas.

- O sistema de descarga de pressão que compreendendo válvulas multijato com alívio de pressão, e atuadores programados para fechamento automático da válvula.

- Além de comportas com atuadores para fechamento automático em caso de extravasamento do efluente.

Neste estudo de caso instrumentos de campo são instalados como meio de monitorar e criar as devidas camadas de proteção, a demanda potencial de processo que é geralmente identificada pelos perigos e operabilidade de estudo (HAZOP) conforme IEC 61882.

Demandas do processo podem ser classificadas de acordo com sua frequência de ocorrência. Algumas demandas do processo ocorre com tanta frequência que o sistema de segurança é operado quase que continuamente, é o caso da válvula multijato neste estudo de caso, ou mesmo o exemplo do freio de um carro como citado por Rausand e Hoyland (2004*)* em outro extremo temos os processo que ocorrem muito raramente, portanto permanece 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 até que o sistema é testado. Para revelar falhas ocultas, sistemas de segurança com o modo de baixa demanda de operação são normalmente testados em intervalos regulares, tais como ocorre com as comportas de segurança do sistema de efluente.

A IEC 61508, *Functional safety of electrical /electronic /programmable electronic safety-related*, apresenta 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 partes normativas e lidar com a avaliação do risco de processo industrial e com o hardware dos instrumentos e a confiabilidade do software, as quatro partes restantes tratam das definições.

Integridade e Segurança são conceitos fundamentais na norma IEC 61508, e é definida como a probabilidade do sistema *Safety* realizar satisfatoriamente as funções de segurança dentro de um período de tempo especificado, que são especificados em quatro níveis, conhecidos como SIL (*Safety Integrity Levels*).

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, pag. 453).

Seja X (t) o estado do sistema *Safety* no tempo t, e que X = {0,1, ..., r}, um conjunto finito de todos os estados possíveis. Suponha que podemos dividir o espaço de estado X em duas partes, um conjunto B de estados em funcionamento, e um conjunto F de estados 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, será conforme equação 13:

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

equação (13)

Para n= 1,2,.... Se uma demanda para a segurança ocorre no intervalo n, a probabilidade (média) de que o sistema de *Safety* é 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 $(n-1)t \leq t < nt, para\ n = 1,2,....$ Seja $P_{jk}(t) = \Pr(X(t) = k \mid X(0) = j)$, indica a transição da probabilidade para $j,k \in X, e\ seja\ P(t)$, de modo que corresponde a matriz. Falhas detectadas por falhas de diagnóstico auto teste pode ocorrer e ser reparado 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 nós assumirmos que Z_n é independente das transições do sistema antes do tempo nt. Seja $\Pr(Z_n = j \mid Y_n = i) = R_{ij}\ para\ todo\ i,j \in X$. A transição da probabilidade, e seja R o correspondente a matriz de transição. Se o estado do sistema é $Y_n = i$ antes do teste n, a matriz R apresenta a probabilidade do sistema está 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.

CONCLUSÕES

Com base neste estudo que contemplou a aplicação de uma análise de risco com a utilização de metodologias híbridas, CORAS e modelagens matemáticas de Markov, concluiu-se que:

O CORAS é uma ferramenta eficiente para desenvolvimento da análise de risco em plantas de saneamento, pois consolida diversas técnicas e simplifica o processo de coordenação e geração de informações para tomada de decisão e definição do nível de risco do processo, porém possui aspectos pouco quantitativo e necessita de aprimoramento, como apresentado neste estudo com modelagem realizada por Markov.

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 estes estados permaneçam constantes. Esta imposição é uma limitação significativa e implica no uso de distribuições de probabilidade exponenciais para a 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.

Pode 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. Desta forma, conclui-se que este método é mais adequado para análise da confiabilidade de sistemas de pequeno porte ou recomenda-se sua utilização hibrida com outras modelagens. Como vimos realizamos a combinação do CORAS, que consolida diversas técnicas de análise de risco, com a modelagem matemática de Markov.

A principal contribuição deste trabalho é de apresentar uma metodologia sistêmica para análise de falhas 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.

Finalmente conclui-se que os resultados obtidos foram muito promissores apesar da quantidade de modos de falha documentado e do escopo de aplicação das análises ser apenas de uma pequena parte do processo.

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.

REFERÊNCIAS BIBLIOGRÁFICAS

1. BAYBUTT, P. Sneak Path Security Analysis (SPSA) for Industrial cyber security. Intech, v.51, n.9, set.2004.
2. BRAENDELAND, G., REFSDAL, A., STOLEN, K.. Modular analysis and modelling of risk scenarios with dependencies. Journal of Systems and Software. Volume 83, Issue 10. 2010.
3. CARVALHO, L. Alessandra. Análise de Disponibilidade Utilizando Abordagem Nebulosa. Tese de Doutorado na Escola de Engenharia da Universidade Federal de Minas Gerais. BH. 2008.
4. ISO/IEC 31000:2009. International Organization for Standardization, Switzerland, 2009.
5. IEC 61508-ed 2.Commission Electrotechnique Internationale. Functional safety of eletrical/electronic/programmable electronic safety-related systems. Commission Electrotechnique Internationale, 2010.
6. LIMNIOS,N. Fault trees: control systems, robotics & manufacturing series. Wiley-ISTE, 2007.
7. MAILLART L.M, POHL AE. Introduction to Markov-Chain Modeling and Analysis. In: Annual Reliability and Maintainability Symposium, 51o, 2005, Alexandria. Conference Tutorials …, Alexandria: IEEE, 2005.
8. PALADY, Paul. FMEA: Análise dos Modos de Falha e Efeitos:prevendo e prevenindo problemas antes que ocorram. IMAM,São Paulo, 2007.
9. RAUSAND, M., HOYLAND, M. “System Reliability Theory Models, Statustucal Methods, and Application”. Second Edition, Wiley Series In Probability and Statistics , New Jersey. 2004.
10. VOLOVOI, V. Modeling of System Reliability Petri Nets with Aging Tokens. Elsevier Science Publishers. Reliability Engineering and System Safety, v.84, p. 149-161, 2004.
11. WANG, Z., ZENG,H..Study on the Risk Assessment Quantitative Method of Information Security. 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE). IEEE. 2010.