



INSTITUTO TECNOLÓGICO VALE



**Programa de Pós-Graduação em Instrumentação, Controle e
Automação de Processos de Mineração - PROFICAM
Universidade Federal De Ouro Preto - Escola de Minas
Associação Instituto Tecnológico Vale**

Dissertação

**ABORDAGEM SISTÊMICA APLICADA À PERFURATRIZ
AUTÔNOMA: UMA ANÁLISE COM FOCO NA SEGURANÇA
OPERACIONAL E CIBERNÉTICA**

Luiz Rogério de Freitas Júnior

**Ouro Preto
Minas Gerais, Brasil**

2018

Luiz Rogério de Freitas Júnior

**ABORDAGEM SISTÊMICA APLICADA À PERFURATRIZ
AUTÔNOMA: UMA ANÁLISE COM FOCO NA SEGURANÇA
OPERACIONAL E CIBERNÉTICA**

Dissertação apresentada ao curso de Mestrado Profissional em Instrumentação, Controle e Automação de Processos de Mineração da Universidade Federal de Ouro Preto e do Instituto Tecnológico Vale, como parte dos requisitos para obtenção do título de Mestre em Engenharia de Controle e Automação.

Orientador: Ph.D. Luis Guilherme Uzeda

DS.C. Thiago Antônio Melo Euzébio

DS.C. Francisco de Lemos

Ouro Preto

2018

F866a

Freitas Júnior, Luiz Rogério de.

Abordagem sistêmica aplicada à perfuratriz autônoma [manuscrito]: uma análise com foco na segurança operacional e cibernética / Luiz Rogério de Freitas Júnior. – 2018.

99f.: il.: color; grafs; tabs.

Orientador: Prof. Dr. Luis Guilherme Uzeda Garcia.

Coorientador: Prof. Dr. Francisco Luiz de Lemos.

Dissertação (Mestrado) - Universidade Federal de Ouro Preto. Escola de Minas. Departamento de Engenharia de Controle e Automação e Técnicas Fundamentais. Programa de Pós Graduação em Instrumentação, Controle e Automação de Processos de Mineração.

Área de Concentração: Engenharia de Controle e Automação de Processos Minerais.

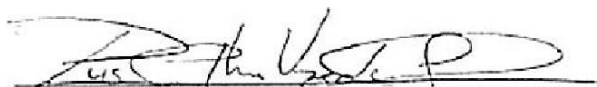
1. Teoria de sistemas. 2. Segurança operacional. 3. Segurança digital. I. Garcia, Luis Guilherme Uzeda. II. Lemos, Francisco Luiz de. III. Universidade Federal de Ouro Preto. IV. Título

Mestrado Profissional em Instrumentação, Controle e Automação de Processos de
Mineração – PROFICAM

Abordagem Sistêmica Aplicada à Perfuratriz Autônoma: Uma Análise com Foco na
Segurança Operacional e Cibernética

Luiz Rogério de Freitas Júnior

Dissertação defendida e aprovada em 17 de abril de 2018 pela banca examinadora
constituída pelos professores:



Ph.D. Luís Guilherme Uzeda Garcia

Orientador — Instituto Tecnológico Vale (ITV)



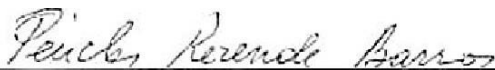
D.Sc. Thiago Antonio Melo Euzébio

Coorientador — Instituto Tecnológico Vale (ITV)



D.Sc. Francisco Luiz de Lemos

Coorientador - Instituto de Pesquisas Energéticas e Nucleares



Ph.D. Péricles Rezende Barros

Membro externo — Universidade Federal de Campina Grande

AGRADECIMENTOS

Agradeço primeiramente a Deus, por dar-me saúde e forças para concluir mais esta etapa da minha vida.

A minha família, por serem, para mim, uma fonte inesgotável de inspiração e amor. Sou grato também ao orientador Luis Uzeda e Thiago Euzébio, pela disponibilidade e confiança.

Ao Francisco Lemos, pela imensa contribuição e motivação a evoluir cada vez mais. Aos professores e funcionários do ITV e UFOP, grandes aprendizados.

À turma pioneira do mestrado em instrumentação, controle e automação de processos do ITV e UFOP, pela amizade.

Aos gestores da mineradora Vale, pela oportunidade.

A toda equipe da mina autônoma, pela ajuda essencial durante execução do projeto. Muito obrigado especial à Aline, pelo companheirismo e incentivo durante cada passo desta jornada.

Por fim, agradeço muito a todos (e foram muitos) que, de alguma maneira, contribuíram para a conclusão de mais este desafio.

Esta conquista também é vocês.

Muito obrigado!

“Nunca ande por trilhas, pois assim só irá até onde outros já foram. ”

(Alexander Graham Bell)

RESUMO

Resumo da Dissertação apresentada à Escola de Minas/UFOP e ao ITV, como parte dos requisitos necessários para a obtenção do título de Mestre em Ciências (M.Sc.)

ABORDAGEM SISTÊMICA APLICADA À PERFURATRIZ AUTÔNOMA: UMA ANÁLISE COM FOCO NA SEGURANÇA OPERACIONAL E CIBERNÉTICA

Luiz Rogério de Freitas Júnior

Abril/2018

Orientadores: Luis Guilherme Uzeda Garcia

Francisco de Lemos

Thiago Antônio Melo Euzébio

Dentro de todos os processos que compõem a cadeia produtiva dos minerais, a segurança operacional dos ativos e, mais recentemente cibernética deve ser, e é uma preocupação constante. Com toda evolução nos processos produtivos, os métodos de análise precisavam evoluir juntos, uma vez que a análise baseada em erros humanos ou de falhas individuais de componentes, não estão conseguindo evitar efetivamente os casos de acidentes. Nesse contexto, neste trabalho estuda-se a viabilidade da aplicação da teoria de sistemas com a metodologia STAMP (*Systems-Theoretic Accident Model and Process*) e uma de suas ferramentas, STPA, incluindo sua derivação com foco em segurança cibernética STPA-Sec, dentro do ambiente da indústria mineral. Para isso foi realizada uma aplicação da ferramenta na operação unitária de perfuração, mais especificamente em uma perfuratriz autônoma. Como resultado deste trabalho, foram percebidas diversas restrições de segurança e ações de mitigação para reduzir os riscos operacionais e digitais do equipamento. Dessa maneira, foi percebida a boa eficiência e flexibilidade da ferramenta quando aplicada a sistemas complexos, como é o caso da perfuratriz autônoma, objeto no qual foi realizado o teste de conceito.

Palavras-chave: Teoria de sistemas, Segurança operacional, Segurança digital; Perfuratriz autônoma, STAMP, STPA, STPA-sec.

ABSTRACT

Abstract of the Dissertation presented to the School of Mines / Federal University of *Ouro Preto*-MG/UFOP and to Vale Institute of Technology (ITV) as part of the requisites required to obtain a Master's Degree in Sciences (M.Sc.)

SYSTEMIC APPROACH APPLIED TO THE AUTONOMOUS DRILLS: AN ANALYSIS FOCUSING ON OPERATIONAL AND CYBERNETIC SECURITY

Luiz Rogério de Freitas Júnior

April – 2018

Advisors: Luis Guilherme Uzeda Garcia

Francisco de Lemos

Thiago Antônio Melo Euzébio

In all processes that make up the minerals production chain, the operational safety of assets and, more recently cybernetics should be, and is a constant concern. With all evolution in the productive processes, the methods of analysis needed to evolve together, since the analysis based on human errors or individual component failures are not managing effectively to prevent accidents. In this context, in this work studies the feasibility of the systems theory application with the STAMP (Systems-Theoretic Accident Model and Process) methodology and one of its tools, STPA (Systems-Theoretic Process Analysis) including its derivation with focus on STPA-Sec cybernetics security in the mineral industry environment. For this, an application of the tool in the unitary drilling operation was performed, more specifically in an autonomous drill. As a result of this work, several safety restrictions and mitigation actions were perceived to reduce the operational and digital risks of the equipment. In this way, it was perceived the good efficiency and flexibility of the tool when applied to complex systems, as is the case of the autonomous drill, object in which the concept test was performed.

Keywords: Systems theory, Operational safety, Digital security; Autonomous drill, STAMP, STPA, STPA-sec.

LISTA DE FIGURAS

Figura 1: Cronologia ferramentas de análise	2
Figura 2: Inter-relação entre a segurança digital e operacional.	3
Figura 3 - Exemplo da utilização de software para planejamento de lavra.....	6
Figura 4 - Perfuratriz percussiva.....	8
Figura 5: Perfuratriz Rotativa Industrial.	8
Figura 6: Operação de Carregamento na Mineração	10
Figura 7: Transporte de Minérios.	10
Figura 8: Fluxograma típico de processamento de minério de ferro	11
Figura 9: Categorias de Sistemas.....	13
Figura 10: Representação de sistema de controle em blocos.	18
Figura 11: Ferramentas e processos desenvolvidos a partir de STAMP.....	19
Figura 12 - Perfuratriz Autônoma objeto do estudo	23
Figura 13: Macro fluxo de mercado na Indústria Mineral.	26
Figura 14: Zoom in no Macro fluxo do Complexo Industrial.	28
Figura 15: Zoom in no Macro Fluxo da Operação de Lavra.	30
Figura 16: Zoom in no Macro fluxo do processo de perfuração.	32
Figura 17: Perfuratriz com haste na posição de perfuração.	37
Figura 18: Estrutura de controle Macro do Processo de Perfuração.....	39
Figura 19: PC Industrial.	41
Figura 20: PLC.	42
Figura 21: Estrutura de controle do processo de Perfuração.....	43
Figura 22: Fatores causais para criação dos cenários	59

LISTA DE TABELAS

Tabela 1:	Perdas e Perigos – Perfuratriz.....	35
Tabela 2:	Requisitos de Segurança.	38
Tabela 3:	Ações de controle inseguras (ACI) do Técnico de mineração para o perigo da perfuratriz sair da zona de trabalho.....	44
Tabela 4:	Ações de controle inseguras do Técnico de mineração para o perigo da distância inadequada entre os equipamentos.....	45
Tabela 5:	Ações de controle inseguras do Técnico de mineração para o perigo da perfuratriz ultrapassar a inclinação limite.	46
Tabela 6:	Ações de controle inseguras do Operador de Centro de Controle (OCC) para o perigo da perfuratriz sair da zona de trabalho.	47
Tabela 7:	Ações de controle inseguras do Operador de Centro de Controle para o perigo da distância inadequada entre os equipamentos.	48
Tabela 8:	Ações de controle inseguras do Operador de Centro de Controle para o perigo da perfuratriz ultrapassar a inclinação limite.....	49
Tabela 9:	Ações de controle inseguras do Controlador de Segurança para o perigo da perfuratriz sair da zona de trabalho.....	50
Tabela 10:	Ações de controle inseguras do Controlador de Segurança para o perigo da distância inadequada entre a perfuratriz e outros equipamentos.	50
Tabela 11:	Ações de controle inseguras do Controlador de Segurança para o perigo da perfuratriz ultrapassar inclinação limite.....	51
Tabela 12:	Ações de controle inseguras do PC industrial para o perigo da perfuratriz sair da zona de trabalho.	51
Tabela 13:	Ações de controle inseguras do PC industrial de Controle para o perigo da distância inadequada entre os equipamentos.....	52
Tabela 14:	Ações de controle inseguras do PC industrial de Controle para o perigo da perfuratriz ultrapassar a inclinação limite.	52
Tabela 15:	Ações de controle inseguras do PLC para o perigo da perfuratriz sair da zona de trabalho.	53
Tabela 16:	Ações de controle inseguras do PLC de Controle para o perigo da distância inadequada entre os equipamentos.	53

Tabela 17: Ações de controle inseguras do PLC de Controle para o perigo da perfuratriz ultrapassar a inclinação limite.	54
Tabela 18: Requisitos de segurança (RS) para o Técnico de Mineração (TM).....	55
Tabela 19: Requisitos de segurança (RS) para o Operador do Centro de Controle (CC).	56
Tabela 20: Requisitos de segurança (RS) para o Controlador de Segurança (CS).	57
Tabela 21: Requisitos de segurança (RS) para o PC Industrial (PCI).....	57
Tabela 22: Requisitos de segurança (RS) para o Controlador Lógico Programável (PLC)...	58
Tabela 23: Fatores causais para determinação do polígono de maneira incorreta / incompleta.	60
Tabela 24: Fatores causais que podem levar o TM a movimentar perfuratriz para área incorreta.....	62
Tabela 25: Fatores causais que podem levar o TM a deixar de observar outros equipamentos ou barreiras.....	63
Tabela 26: Fatores causais que podem levar o TM a inclinar a broca sobre / muito próxima a outros equipamentos ou barreiras. (Continua)	65
Tabela 27: Fatores causais que podem levar o TM a aprovar área com irregularidades no solo.....	67
Tabela 28: Fatores causais que podem levar o TM a movimentar a perfuratriz com a lança fora da posição.....	68
Tabela 29: Fatores causais que podem levar o TM a movimentar a perfuratriz em área não apropriada.	69
Tabela 30: Fatores causais que podem levar o TM a inclinar a broca para um ângulo diferente do previsto / permitido.....	70
Tabela 31: Fatores causais que podem levar o OCC a não acionar a emergência em caso de a perfuratriz entrar em situação de emergência.	71
Tabela 32: Fatores causais que podem levar o OCC a acionar a emergência tardiamente em situação de emergência.....	73
Tabela 33: Fatores causais que podem levar o OCC a enviar as coordenadas incorretas para o PC Industrial.	74
Tabela 34: Fatores causais que podem levar o OCC a movimentar a perfuratriz não respeitando os limites do polígono quando operando em modo remoto.....	75
Tabela 35: Autorizar operação com equipamentos indevidos na área de perfuração.	76

Tabela 36: Fatores causais possíveis para o OCC autorizar a operação da perfuratriz sem que a área e os equipamentos estejam prontos.	77
Tabela 37: Fatores causais para o OCC movimentar a perfuratriz sobre algum equipamento	78
Tabela 38: Fatores causais possíveis para o OCC inclinar o mastro sobre ou muito próximo de outros equipamentos.....	79
Tabela 39: Fatores causais possíveis para o OCC movimentar a perfuratriz com o mastro fora da posição prevista.....	81
Tabela 40: Fatores causais possíveis para o OCC movimentar a perfuratriz em área irregular.	81
Tabela 41: Fatores causais para o OCC inclinar o mastro para um ângulo diferente do previsto ou permitido.	82
Tabela 42: Fatores casuais podem levar o controlador de segurança a não acionar a emergência em caso de emergência.	83
Tabela 43: Fatores casuais podem levar o controlador de segurança a acionar tardiamente a emergência em caso de emergência operacional.	84
Tabela 44: Fatores causais para o PC industrial definir a direção do movimento incorretamente.	85
Tabela 45: Fatores causais para o PC industrial definir a distância do movimento incorretamente.	86
Tabela 46: Fatores causais para definir PC industrial definir o angulo do mastro acima ou abaixo do angulo permitido.	87
Tabela 47: Fatores causais para o PLC movimentar a perfuratriz na direção diferente da prevista.	88
Tabela 48: Fatores causais para o PLC não interromper a tempo a movimentação quando atingido a posição esperada.	89
Tabela 49: Fatores causais para o PLC movimentar a perfuratriz na direção de algum equipamento ou obstáculo quando este estiver próximo.....	90
Tabela 50: Fatores causais para o PLC movimentar a perfuratriz com o mastro fora da posição.....	91
Tabela 51: Fatores causais para o PLC movimentar o mastro para um ângulo diferente do previsto / permitido.	92

SUMÁRIO

1	INTRODUÇÃO	1
2	OBJETIVOS	3
	2.1 Geral	3
	2.2 Específicos	3
3	REFERENCIAL TEÓRICO E FUNDAMENTAÇÃO CIENTÍFICA	5
	3.1 Mineração.....	5
	3.1.1 Planejamento.....	5
	3.1.2 Decapeamento	6
	3.1.3 Perfuração	7
	3.1.4 Desmonte	9
	3.1.5 Carregamento	9
	3.1.6 Transporte	10
	3.1.7 Processamento.....	11
	3.2 Operações autônomas	12
	3.3 Teoria de sistemas	13
	3.4 STAMP e a segurança operacional e da informação	16
	3.4.1 STPA	20
4	MATERIAIS E MÉTODOS.....	22
	4.1 Materiais	22
	4.1.1 Software XSTAMPP	22
	4.1.2 Perfuratriz Autônoma	22
	4.2 Método de Trabalho.....	23
	4.2.1 Estudo do Caso.....	23
	4.2.2 Aplicação da Ferramenta STPA.....	23
	4.2.3 Análise crítica da abordagem e abrangência.....	24
5	RESULTADOS.....	25
	5.1 Estudo de caso	25
	5.2 Aplicando a ferramenta STPA	34
	5.2.1 Estabelecimento dos fundamentos de engenharia do sistema.....	35
	5.2.2 Identificando as ações de controle potencialmente inseguras.....	44
	5.2.3 Criando os requerimentos e requisitos de segurança.....	54

5.2.4	Determinando cenários para ocorrências das ações de controle inseguras.....	58
5.2.5	Análise crítica da abordagem e abrangência.....	93
6	CONCLUSÃO	95
7	TRABALHOS FUTUROS	96
	REFERÊNCIAS.....	97

1 INTRODUÇÃO

A mineração é um negócio naturalmente volátil. Em todo momento está sujeita aos ciclos e caprichos da natureza, à política local e às bruscas variações de preços e demandas dos mercados de *commodities*. Nesse contexto, as maiores empresas de mineração do mundo estão lutando para sobreviver e manterem-se competitivas no mercado. Algumas empresas têm investido fortemente em automação de processos críticos, incluindo novas tecnologias de perfuração (HEADRICK, 2015).

Um passo importante para essa plena automação das operações unitárias na etapa de lavra são os equipamentos e processos autônomos. Nessas operações, por exemplo, perfuratrizes são posicionadas automaticamente via GPS (*Global Positioning System*) de alta precisão e executam a perfuração com pouca ou nenhuma intervenção humana (EIMOWAFY, 2009). Os índices operacionais são monitorados, armazenados e utilizados para otimizações da lavra garantindo maior produtividade e menores custos (FREITAS, 2015).

Nesse cenário, onde os mundos digital e físico se sobrepõem, a preocupação com acidentes, falhas operacionais e segurança cibernética aumentam ainda mais. Isso ocorre porque, no passado, a maioria dos acidentes ou vulnerabilidades poderia ser rastreada com foco somente em componentes não confiáveis ou falhas súbitas. Felizmente, as técnicas de engenharia de segurança se tornaram muito eficazes na prevenção de desvios causados por falhas de componente. Na verdade, elas se tornaram tão eficazes em prevenir falhas causadas somente por componentes isolados que a maioria dos grandes acidentes, hoje, é causada somente por complexas e, muitas vezes, inesperadas interações entre os componentes (ocorrendo em alguns casos mesmo que os componentes, individualmente, estejam funcionando como projetado). Essa aparente contradição se deve ao fato de os sistemas modernos (incluindo os críticos) estão cada vez mais dependentes e integrados a softwares (THOMAS, 2013) complexos, sendo frequentemente responsáveis por um grande número de interações dinâmicas. Nesse caso, a análise dos aspectos de segurança operacional e digital é extremamente difícil, uma vez que as abordagens tradicionais, frequentemente, não são suficientemente eficientes.

Portanto, em um sistema complexo e inovador como de equipamentos autônomos é importante que se busque uma nova abordagem para se evitar os acidentes e melhorar a segurança cibernética (PAPADOPOULOS et al., 2001). Isso se deve ao fato que, conforme

exemplificado na figura 1, as ferramentas e métodos tradicionais de análise de falhas (FMEA, FTA, HAZOP, ETA, etc.) (KHAN; ABBASI, 1998) são provenientes de uma época com outro nível de tecnologia e não acompanham a evolução dos processos e equipamentos (WHITELEY et al., 2016).

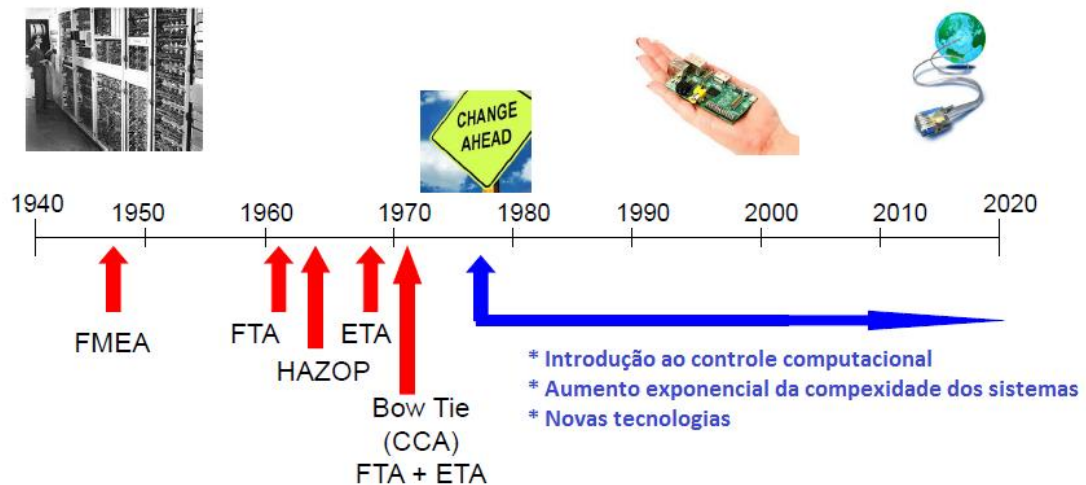


Figura 1: Cronologia ferramentas de análise.

Adaptado de (WHITELEY et al., 2016)

Nesse contexto, em que os sistemas assumem uma maior complexidade, a utilização da abordagem STAMP (*Systems-Theoretic Accident Model and Process*) (LEVESON, 2011) mostra-se como promissora do ponto de vista de eficiência dos resultados. Isso ocorre porque, ao contrário dos métodos de análise tradicionais, ela percebe (além das falhas ou acidentes ocasionados por uma série de eventos individuais ou causas raízes) as falhas e acidentes resultantes de interações entre componentes de um sistema, que resultaram em uma violação das restrições de segurança (ARNOLD, 2009). Em resumo, a diferença de percepção entre os métodos de análise deve-se ao fato que: STAMP vê os problemas baseado na teoria de sistemas, focando os problemas de segurança como um problema de controle, ou seja, busca analisar o sistema como um todo (incluindo todos os componentes e suas interações). Isso se dá em contraponto a maioria das abordagens tradicionais; nessas abordagens, frequentemente, o foco da análise é somente a confiabilidade dos componentes do sistema tratados individualmente (LEVESON, 2011).

2 OBJETIVOS

2.1 Geral

Verificar a viabilidade da aplicação da metodologia STAMP no problema de segurança cibernética e operacional em uma perfuratriz autônoma em uma mineradora no estado de Minas Gerais. Nesse sentido, o foco neste trabalho, conforme explicitado na Figura 2, é identificar as possíveis vulnerabilidades que possam impactar na segurança operacional das pessoas e processos produtivos da mineradora, mais especificamente os que envolvem uma perfuratriz autônoma. Esse tipo de abordagem é relevante, uma vez que em sistemas *cyber* físicos estes dois ambientes (físico e digital) se aglutinam.



Figura 2: Inter-relação entre a segurança digital e operacional.

Além disto, busca-se a aplicação de ferramentas pouco ou nunca utilizadas na área de mineração para análise de possíveis vulnerabilidades de segurança da informação e operacionais.

2.2 Específicos

- Conhecer, utilizando as ferramentas baseadas na teoria de sistemas, pontos de melhorias na segurança operacional e cibernética do equipamento de perfuração, objeto deste estudo.
- Conhecer diferentes interações entre os sistemas que compõem a perfuratriz autônoma e suas implicações.

- Servir como aplicação piloto da metodologia STAMP na indústria mineral.
- Verificar a aplicabilidade da abordagem STAMP em outras áreas da exploração mineral, como por exemplo, no transporte autônomo de minérios em áreas de lavra, infraestrutura de controle e otimização de beneficiamento de minérios, máquinas de retomada e empilhamento em pátios de estocagem e manuseio, entre outros.
- Conhecer possíveis pontos de atenção, com objetivo de aumentar a segurança operacional e digital na operação autônoma de perfuração em áreas de lavra de mineração.

3 REFERENCIAL TEÓRICO E FUNDAMENTAÇÃO CIENTÍFICA

3.1 Mineração

Os recursos minerais têm uma relevância significativa para a sociedade desde o início da evolução da humanidade. Com esse objetivo da disponibilização desses recursos para o homem vários empreendimentos minerários são desenvolvidos. Esses empreendimentos possuem frequentemente uma longa duração cronológica, em alguns casos esses empreendimentos se mantêm ativos por séculos. De acordo com (ROBERT PEELE, 1941), o empreendimento de mineração pode ser dividido em quatro fases:

- prospecção: etapa que desenvolve a busca por minérios;
- pesquisa: etapa que realiza os estudos necessários para definição da jazida, modelamento e avaliação, consequentemente demonstrado a viabilidade do empreendimento;
- desenvolvimento: atividades a serem realizadas com objetivo de deixar disponível para a lavra da jazida pesquisada;
- exploração: etapa que realizada a extração do minério em seu local de origem e o transporta ao ponto de uso ou beneficiamento.

Alguns autores costumam introduzir mais uma fase nos empreendimentos de mineração. Essa fase corresponde à recuperação dos terrenos degradados pelas atividades mineiras e desativação (ou descomissionamento) da mina.

A etapa de exploração ou lavra, contexto em que a perfuratriz, foco deste trabalho, está inserida, é a etapa em que o empreendimento se encontra em sua fase produtiva. Essa etapa pode ser dividida em diversas atividades que vão do planejamento da lavra até a entrega dos minérios à etapa de processamento.

3.1.1 Planejamento

Toda a atividade em que se deseja obter melhores resultados durante a sua execução passa, necessariamente, por um bom planejamento, e na exploração mineral não é diferente. A atividade de planejamento é essencial, principalmente quando se tem como objetivo a

otimização dos recursos utilizados na exploração, bem como na reserva disponível. Steffen (2005) propõe que este planejamento deva ser feito com três enfoques:

Planejamento de Vida da Mina: etapa inicial do processo de planejamento, em que são definidos o inventário das reservas, as capacidades de produção, requisitos de infraestrutura, além dos custos operacionais e de investimento.

Planejamento de longo prazo: este planejamento busca obter uma estratégia de lavra que maximize a vida útil da mina e retorno financeiro do empreendimento.

Planejamento de curto prazo: este planejamento objetiva atender ao controle de qualidade do material lavrado, custos, produtividade operacional baseado nos requisitos definidos no planejamento de longo prazo.

Atualmente, devido à complexidade dos modelos e objetivando a uma maior otimização das operações é comum a utilização de softwares dedicados para esta atividade.

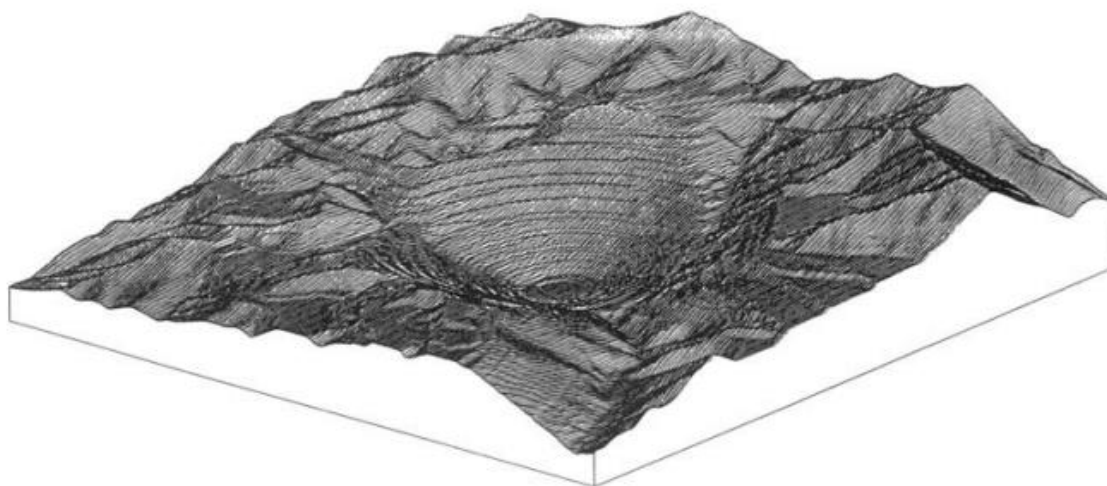


Figura 3: Exemplo da utilização de software para planejamento de lavra.

Fonte: (HUSTRULID; KUCHTA; MARTIN, [s.d.])

3.1.2 Decapeamento

Em se tratando de jazidas minerais a serem lavradas a céu aberto é comum elas se encontrarem recobertas por material terroso, areia, cascalho e outras misturas. Portanto, para que se tenha acesso ao minério de interesse é necessária a remoção desses materiais. À remoção deles é dada o nome de decapeamento ou *stripping*. Esse processo, normalmente, é

feito com equipamentos básicos de terraplanagem como *scrapers* e tratores de esteira (GIRODO; RONDEAU; SILVA, 2005).

3.1.3 Perfuração

Uma vez que o corpo do minério o qual se deseja explorar já está disponível, faz-se necessária a “ruptura” das rochas para que sejam carregadas. Em muitos casos se faz essa ruptura através da escavação mecânica, que é o caso em que a rocha é inteiramente removida da face da mina pela ação de ferramentas de corte. Esse tipo de método se tornou muito comum nos últimos anos devido à sua maior segurança, principalmente quando são aplicados em minas subterrâneas (DARLING, 2011). Todavia, em alguns casos, como nos casos em que o material a ser desmontado apresenta grande dureza é utilizado o desmonte a fogo. Nesse caso é feito o uso da perfuração e em seguida o desmonte através de explosivos.

Nos casos em que é feito o desmonte através de explosivos são necessários furos no corpo de minério a ser detonado, a fim de se inserir o material explosivo. Para execução desses furos são utilizadas as perfuratrizes. De maneira geral (apesar de não estar limitado a estes) as perfuratrizes podem ser divididas em dois grupos:

Perfuratrizes percussivas: nesse tipo de perfuração, a rocha é “quebrada” através da rotação da broca e a da alta frequência de impactos percussivos transmitidos da broca para a rocha. Comumente esses impactos são gerados através de pressões pneumáticas e/ou hidráulicas (DARLING, 2011). Na Figura 4 é representada uma perfuratriz com esse princípio de funcionamento.



Figura 4: Perfuratriz percussiva.

Fonte: (CAT, 2017)

Perfuratrizes rotativas: nesse tipo de equipamento a broca de perfuração é rotacionada contra a rocha, resultando na remoção de materiais da face do furo. Com exceção de algumas aplicações especiais, grandes furos são tipicamente realizados por perfuratrizes rotativas. A energia necessária para rotação da broca e consequente execução do furo, frequentemente é proveniente de energia elétrica ou combustão de diesel (DARLING, 2011). Na Figura 5 é representada uma perfuratriz do tipo rotativa.



Figura 5: Perfuratriz Rotativa Industrial.

Fonte: (CAT, 2017)

É importante salientar, todavia, que a utilização da perfuração da mineração não está restrita somente a furos para detonação. Ela é largamente utilizada em pesquisas geológicas, instalações de aterramentos e suporte, drenagem, entre outros.

3.1.4 Desmonte

Após a conclusão dos furos previstos nos planos de fogo, é necessário completá-los com explosivos. Os explosivos são substâncias que usando ativados por algum agente externo decompõem-se quimicamente, gerando grandes volumes de *cases* e altas temperaturas, o que proporciona o faturamento e o desmonte da rocha. Uma vez feito o desmonte do minério, este é transformado em blocos com dimensões tais que permitem o seu carregamento para transporte. Nesse momento o minério passa a ser chamado ROM (*run-of-mine*) (PAULA, 2008).

3.1.5 Carregamento

Uma vez o minério detonado, faz-se necessário fazer o carregamento desse material nos meios de transporte que o levarão ao seu destino final. A operação de carregamento é uma das etapas de menor complexidade dentro do processo de mineração. Todavia esta impacta, consideravelmente, nos custos totais da lavra, além de em alguns casos ser o gargalo dessas operações.

A operação de carregamento está intimamente ligada à operação de transporte, nesse sentido a escolha dos equipamentos comumente é feita baseada nos equipamentos utilizados na operação de transporte, além, é claro, de sua produtividade, custo e custos de aquisição e operação. Existem os mais variados tipos de equipamentos para o carregamento de minérios, como por exemplo, *draglines* e *clam shells*. Todavia, na maioria das minerações ao redor do mundo as carregadeiras frontais e as escavadeiras são as mais comumente utilizadas (GIRODO; RONDEAU; SILVA, 2005).



Figura 6: Operação de Carregamento na Mineração.

Fonte: (JOY GLOBAL, 2017)

3.1.6 Transporte

A operação de transporte na etapa de lavra consiste em levar o minério, anteriormente carregado, até o seu destino final. Conforme abordado anteriormente, esse transporte geralmente é feito através de caminhões, entretanto em alguns casos essa movimentação é feita através de correias transportadoras ou mesmo a combinação de caminhos e correias. Analogamente a etapa de carregamento, a escolha do transporte adequado se dá em virtude de diversos fatores, como por exemplo, produtividade esperada, investimento inicial e custos de operação. É comum nas explorações de minério de ferro que o destino final seja a britagem primária, etapa que inicia o processo de beneficiamento dos minérios.



Figura 7: Transporte de Minérios.

Fonte: (“Mitsui & Co.”, 2017)

3.1.7 Processamento

Os minérios provenientes da mina, normalmente, não estão prontos para sua comercialização ou uso. Em geral para se ter valor comercial é necessário que o ROM passe por um processo de processamento ou beneficiamento. Essa etapa consiste em ajustar a granulometria do material, bem como em alguns casos fazer a separação do minério de interesse em teores adequados para a sua comercialização. Esse processo de beneficiamento ocorre em diversas etapas e varia principalmente de acordo com as características do minério a ser tratado e as características aceitas pelo mercado. A Figura 8 é o fluxograma macro de um processo de beneficiamento de minério de ferro.

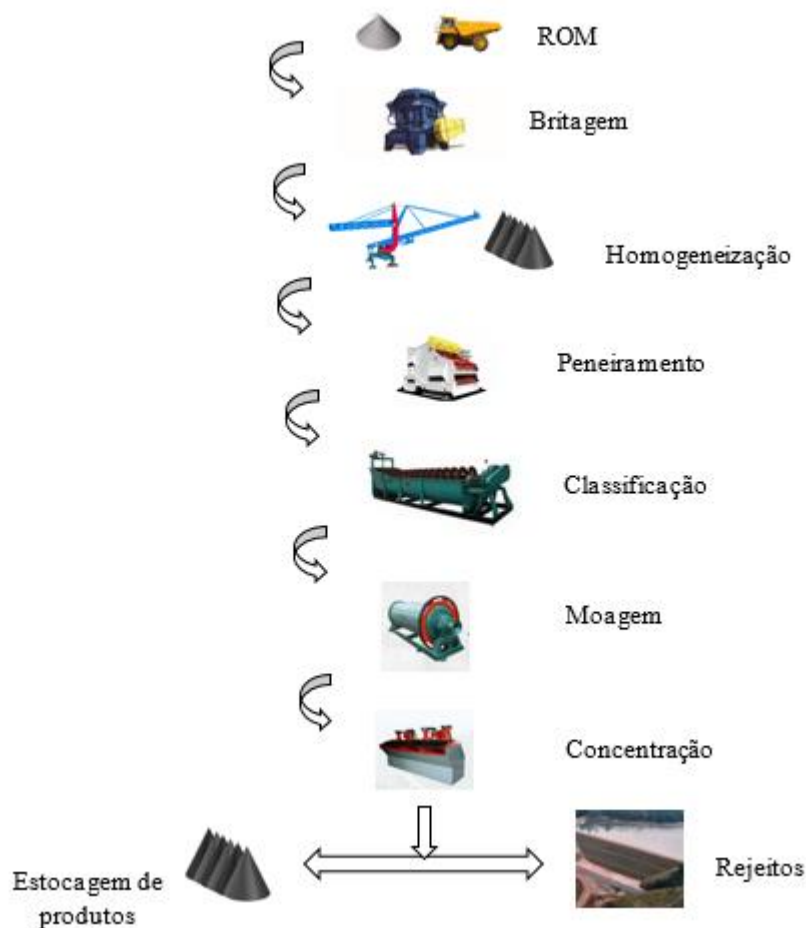


Figura 8: Fluxograma típico de processamento de minério de ferro.

Fonte: (FREITAS JÚNIOR, 2016)

3.2 Operações autônomas

O uso crescente da automação também está mudando a natureza da interação homem e a máquina. No passado, os operadores, muitas vezes, tinham tarefas simples com instruções simples e precisas. No entanto, os sistemas têm empregado cada vez mais automação, reduzindo assim a carga de trabalho do operador e os recursos humanos necessários. Por conseguinte, cada vez mais operadores têm a necessidade de se adaptar a um novo papel de supervisão desses sistemas avançados e executar tarefas diversas que não podiam ser automatizadas. Assim, ao invés de executar procedimentos básicos e aprender comportamentos fundamentados em regras simples, os operadores ficaram responsáveis por decisões muito mais complexas, tais como diagnosticar novos problemas e desenvolver soluções mais assertivas ainda não previstas. Essa tendência aumenta significativamente a interação entre homem e máquina. Nesse contexto, os erros humanos já não são vistos como problemas triviais, como lapsos ou distrações, mas sim por processos complexos que dependem do tipo, da qualidade dos *feedbacks* recebidos pelos seres humanos, além do contexto em que o sistema em que eles estão operando está inserido. (THOMAS, 2013).

De acordo com (RALSTON et al., 2014) o processo produtivo pode ser classificado em cinco níveis de automação a conhecer:

- controle manual local: o operador tem linha de visão direta e imediata do processo de mineração e opera o equipamento através de uma interface de controle local e com fio;
- controle manual remoto: o operador tem linha de visão direta e imediata do processo de mineração e opera o equipamento através de uma interface portátil;
- tele operação: o operador tem linha de visão direta do processo de mineração, porém controla o processo através de sensores que fornecem informações a respeito da situação operacional;
- tele supervisão: o operador não tem visão direta do processo de mineração e o monitora em alto nível, sendo facilitado por tecnologias de automação assistida;
- automação completa: o operador não tem linha direta de visão do processo de mineração nem com seus equipamentos, a maioria dos componentes do processo, se não todos, operam de maneira autônoma.

Nesse contexto, além dos já conhecidos ganhos relacionados à produtividade, a elevação do nível de automação dos processos deve estar intimamente ligada à mudança de cultura relacionada à segurança das operações.

3.3 Teoria de sistemas

A definição do conceito de sistema possui diversas vertentes, conforme já apontado por Backlund (BACKLUND, 2000). Uma dessas definições é feita por Skyttner (SKYTTNER, 1996) que propõe que um sistema é um conjunto de elementos ou unidades que integram um todo, com objetivo de realizar alguma função. Weinberg (WEINBERG, 1975) propôs a classificação dos sistemas em categorias, com o objetivo de melhor descrever e entender os sistemas existentes.

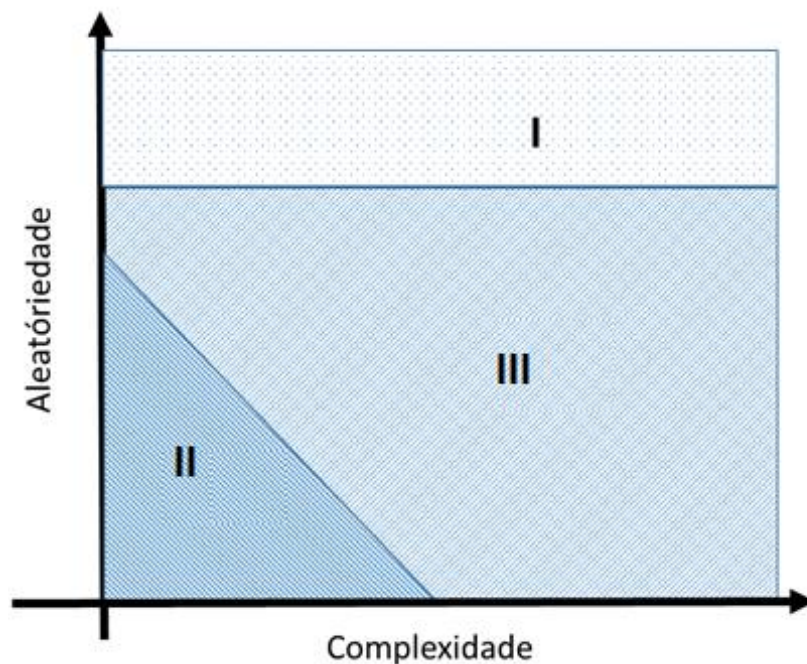


Figura 9: Categorias de Sistemas.

Adaptado de (WEINBERG, 1975)

Conforme pode ser visto na Figura 9, a proposta de Weinberg (WEINBERG, 1975) foi classificar os sistemas de acordo com sua complexidade e aleatoriedade. Sendo as seguintes categorias definidas:

- categoria I - Complexidade desorganizada: esse tipo de sistema, apesar de não poder ser descrito ou reduzido em uma única estrutura, é regular e aleatório o suficiente para

ter seu comportamento descrito estatisticamente. Inclui-se nesta categoria de sistemas, por exemplo, softwares em que as entradas são totalmente aleatórias, podendo esses parâmetros ser analisados estatisticamente determinando com certo grau de certeza seu comportamento;

- categoria II – Simplicidade Organizada: nessa categoria se enquadram os sistemas mais simples. O sistema possui pouca complexidade, podendo, portanto, ser reduzido, todavia sua aleatoriedade não é grande o suficiente que permita a utilização de recursos estatísticos para analisar seu comportamento. Pode-se incluir, por exemplo, softwares simples em que as entradas e saídas são pré-determinadas;
- categoria III – Complexidade organizada. Nessa região, os sistemas são muito complexos para utilização dos métodos científicos tradicionais, além de muito organizados para que possam ser utilizadas análises estatísticas (WEINBERG, 1975). Esse tipo de sistema pode ter, como exemplo, o desenvolvimento de softwares complexos (LEVESON, 2011).

Para cada categoria de sistema é interessante que se tenha uma abordagem diferente para desenvolvimento de análises.

Para os sistemas de complexidade desorganizada, conforme já abordado, é interessante uma abordagem estatística. Nesse sentido, a base da análise deve ser a existência de um grande número de dados observados, com isso sendo possível prever, por exemplo, valores médios, esperados entre outros (LEVESON, 2011).

Para análise dos sistemas ditos de simplicidade organizada, são utilizados métodos científicos tradicionais, frequentemente ditos como dividir e conquistar. Nesses métodos, os sistemas são quebrados em partes distintas que podem ser analisadas com dois focos: aspectos físicos e comportamentos. Nos aspectos físicos os sistemas são divididos baseados na separação física dos componentes. No aspecto comportamento os sistemas são decompostos em eventos discretos ao longo do tempo. Essa divisão do sistema, também chamada de redução analítica, parte do princípio que a separação é factiva, ou seja, cada componente ou subsistema opera de maneira independente.

Assim, a análise dos resultados não é distorcida quando os componentes são considerados separadamente. Essas premissas implicam que os componentes ou eventos de um sistema não estão sujeitos a ações provenientes de outros componentes, nem mesmo

interações não lineares. Em outras palavras, o componente se comporta e falha exatamente da mesma maneira, seja quando operando isoladamente, seja quando faz parte de um sistema.

Uma outra premissa assumida é que: os princípios da montagem dos componentes do sistema ocorrem de maneira estritamente direta, ou seja, as interações entre os subsistemas são simples o suficiente para serem consideradas separadas do próprio comportamento interno do subsistema (LEVESON, 2011).

Para a análise dos sistemas de complexidade organizada, foco deste estudo, foi desenvolvida a teoria de sistemas. A teoria de sistemas teve seus primeiros estudos nas décadas de 30 e 40 com objetivo de preencher as lacunas deixadas pelas técnicas de análises até então desenvolvidas. Essas lacunas foram se tornando ainda maiores à medida que os sistemas foram ficando cada vez mais complexos (CHECKLAND, 1993). Diferentemente dos métodos tradicionais, esse tipo de abordagem foca no sistema como um todo, e não em partes separadas. Uma das premissas é que algumas propriedades do sistema somente podem ser analisadas adequadamente quando observado o todo, ou seja, levando em conta todo o contexto, desde os aspectos sociais até os aspectos técnicos.

De acordo com Leveson (LEVESON, 2011) a teoria de sistemas tem como pilares pares de conceitos:

- hierarquia e emergência.

Um modelo de um sistema complexo pode ser expressado em termos da hierarquia dos níveis de organização, cada nível é mais complexo que o seu nível inferior, em que um nível é caracterizado por possuir propriedades emergentes. Um outro ponto é que as propriedades emergentes não existem ou fazem sentido nos níveis mais inferiores. Visto isso, pode-se dizer que o conceito de emergente é a ideia de que em um determinado nível de complexidade, algumas propriedades características desse nível (emergentes nesse nível) são irreduzíveis.(LEVESON, 2011).

A teoria da hierarquia lida com as diferenças fundamentais entre um nível de complexidade e outro. Seu objetivo final é explicar a relação entre dois níveis, ou seja, o que os separa e o que os liga. As propriedades emergentes associadas a um conjunto de componentes em um nível da hierarquia estão associadas ao grau de liberdade desses componentes. Sendo assim, descrevendo as propriedades emergentes resultadas da imposição de restrições requer uma linguagem de alto nível, o que é, portanto, diferente de descrever os

componentes somente. Nesse sentido, diferentes descrições são apropriadas para cada nível de complexidade (LEVESON, 2011).

- Comunicação e controle

Um exemplo de ação de controle é a imposição de restrições sobre uma atividade em um determinado nível de hierarquia. Essas ações definem as “regras de comportamento” nesse nível; sendo que essas regras de comportamento produzem algum efeito nos níveis superiores. Hierarquias, são caracterizadas, portanto, pelo controle de processo operando na interface entre os níveis (CHECKLAND, 1993). Um ponto importante nessa afirmação elaborada por Chekland (CHECKLAND, 1993) é que o controle sempre está associado à imposição de restrições. Nesse contexto, o foco em evitar falhas, frequentemente utilizado pelas abordagens de análises tradicionais, é substituído por um conceito mais abrangente: impor restrições no comportamento do sistema que evitem eventos ou condições de perigo para o sistema.

De acordo com Bertalanffy (LOPREATO; VON BERTALANFFY, 1970) sistemas fechados são sistemas que seus componentes não modificam seu estado quando em equilíbrio, já os sistemas abertos podem sair do estado de equilíbrio através das mudanças no ambiente. Nesse sentido, os sistemas abertos implicam na necessidade de comunicação. No contexto da teoria de controle, sistemas abertos são vistos como componentes inter-relacionados que são mantidos no estado de controle dinâmico a partir das retroalimentações das informações e controle (LEVESON, 2011).

3.4 STAMP e a segurança operacional e da informação

A preocupação com a segurança das pessoas, ativos e da informação é uma constante em toda indústria que busca sustentabilidade; e na mineração não é diferente. Todavia, no novo modelo de processo, mais automatizado, as técnicas para se evitar essas perdas e eventos indesejados, também devem passar por evoluções. Enquanto aprender com as investigações de acidentes ou falhas ocorridas é uma maneira de melhorar a segurança de um sistema ou processo, um segundo método de fazer isso consiste na análise da segurança do sistema durante o seu desenvolvimento ou operação.

As abordagens atuais neste segundo método são fundamentalmente modelos baseados em cadeias ou sequências de eventos. Nesses modelos, se assume que cenários improváveis ocorrem em sucessão, por isso passam pelas múltiplas barreiras de defesa, consequentemente

levando assim ao acidente ou falha. Como exemplo, desses métodos (baseados neste modelo) as avaliações probabilísticas de risco (PRA), árvores de falhas, árvores de eventos, modo de falha e efeitos (FMEA) e estudos de operabilidade (HAZOP) (KHAN; ABBASI, 1998). Esses métodos de análise de risco são fundamentados nos sistemas eletromecânicos simples existentes no passado. Nesses sistemas, a confiabilidade de cada componente analisado, individualmente, era sinônimo da segurança de todo o sistema. Embora heurísticamente razoável, essa mentalidade se iguala à confiabilidade dos componentes com a segurança de todo o sistema, o que não é verdade. Além disso, esses modelos aproximam o operador humano como apenas mais um componente do sistema e atribui a essas probabilidades simples para a “falha”. Como tal, não é de se surpreender que as análises feitas para segurança operacional e cibernética tradicionais ainda não conseguem descobrir as causas e prevenir os acidentes de hoje (THORNBERRY, 2014).

À medida que os sistemas tornam-se mais complexos, a linearidade da cadeia dos eventos proposta pelos métodos atuais de análise de acidentes nem sempre capta as complexas interações entre os componentes dos sistemas, visto, por exemplo, que falhas e acidentes podem ocorrer mesmo sem que ocorra nenhuma falha em componente específico do sistema (SAMOST, 2015). Nesses casos complexos, a utilização da metodologia STAMP (Systems-Theoretic Accident Model and Process) pode ser uma boa abordagem, uma vez que esta busca descrever e tratar as “não linearidades” do modelo.

O STAMP é um modelo teórico de causalidade de acidentes. Esse modelo é construído em cima de quatro conceitos: restrições de segurança, estrutura de controle de segurança hierárquico, modelos de processos, além dos conceitos de teoria de controle. Nesse tipo de abordagem, o sistema é visto como a inter-relação de componentes. Esses componentes são mantidos sob um equilíbrio dinâmico a partir das realimentações dos “*loops*” de controle (LEVESON, 2011).

Sob a ótica da abordagem STAMP, a segurança é vista como um problema de controle; conforme exemplificado na Figura 10.

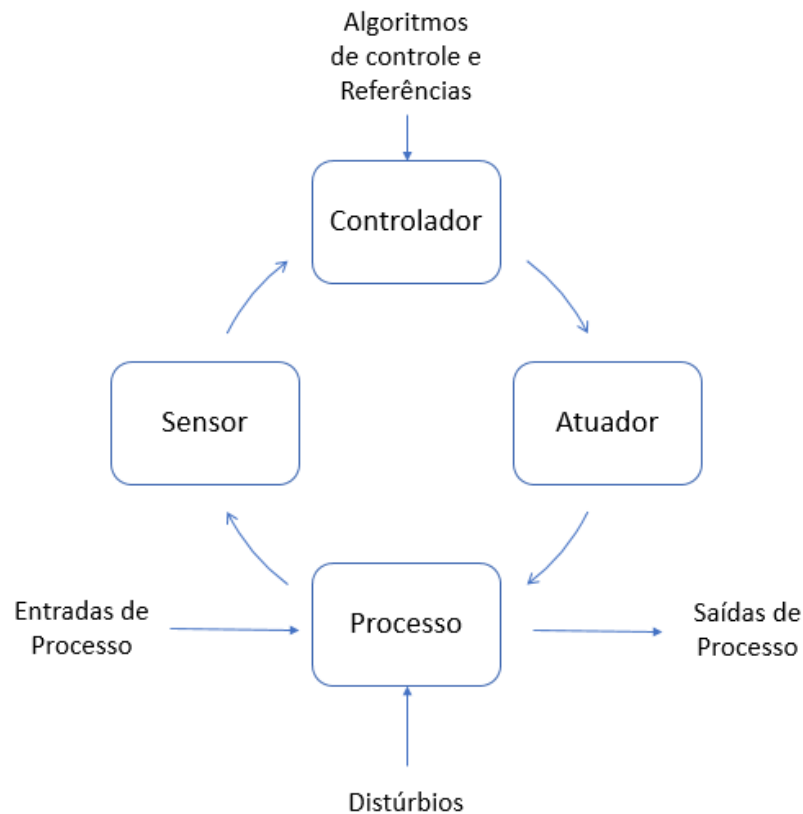


Figura 10: Representação de sistema de controle em blocos.

Acidentes ocorrem quando componentes (atuadores, sensores ou equipamentos do processo) falham, distúrbios externos não previstos ocorrem, e/ou interações inesperadas entre os componentes que não são bem tratadas pelo controlador, isto é, erros de modelagem acontecem; sendo, portanto necessário analisar todos esses casos. Além disto, o STAMP trata os sistemas controlados não como um modelo estático, mas sim como um processo dinâmico que continuamente se adapta para atingir seus objetivos, alterando seu comportamento de acordo com as mudanças internas e do ambiente (ARNOLD, 2009).

A utilização das ferramentas dessa metodologia de análise mostrou-se eficiente em diversas aplicações, como na indústria nuclear (THOMAS; LEVESON, 2012), médica (SAMOST, 2015), aviação (ISHIMATSU et al., 2014), entre outros. A adaptabilidade do método a diferentes processos é outro ponto interessante, portanto, mostra como promissora a utilização do STAMP com foco na segurança operacional e digital aplicada à perfuratriz autônoma, como proposto neste trabalho.

Um ponto importante a se destacar é que: STAMP é somente um modelo para análise de causas de acidentes, não sendo, portanto, uma técnica de engenharia propriamente dita.

Entretanto, fazendo a utilização de STAMP como uma fundamentação teórica, novas ferramentas e processos foram desenvolvidos (LEVESON, 2013). Na Figura 11 é ilustrado esse conceito:

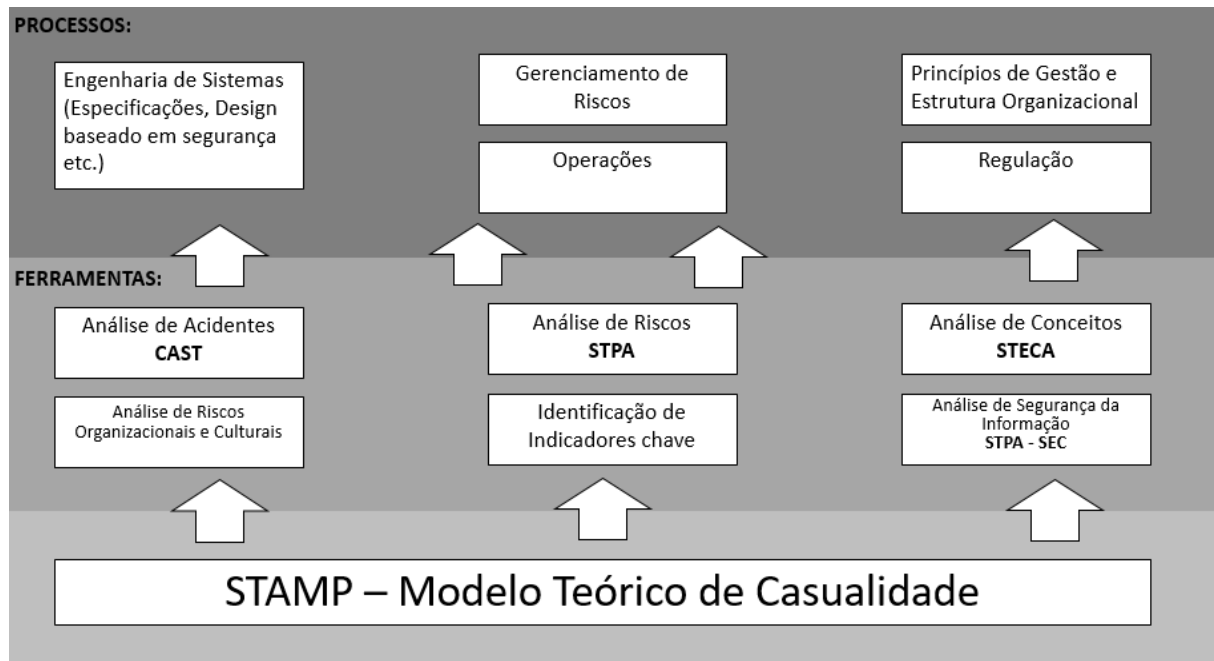


Figura 11: Ferramentas e processos desenvolvidos a partir de STAMP.

Adaptado de: (LEVESON, 2013)

Como pode ser percebido, uma série de ferramentas já foram desenvolvidas ou estão em desenvolvimento, baseadas no modelo STAMP. Na Figura 11 são explicitadas as principais ferramentas até então desenvolvidas e seu foco de atuação. Segue abaixo alguns exemplos das principais ferramentas:

- **CAST** (Causal Analysis using System Theory) – ferramenta que tem como foco a análise de eventos ou acidentes já ocorridos.
- **STPA** (Systems-Theoretic Process Analysis) – ferramenta que tem como foco principal a análise de eventos ou acidentes já ocorridos.
- **STECA** (System Theoretic Early Concept Analysis) – ferramenta que tem como foco principal a análise de segurança em projetos conceituais, ou seja, na fase de desenvolvimento.

Um outro ponto que pode ser observado na Figura 11 é a variedade e diversidade de processos em que essas ferramentas podem ser aplicadas, demonstrando assim a grande flexibilidade da abordagem.

3.4.1 STPA

STPA (Systems-Theoretic Process Analysis), conforme já abordado, é uma técnica de análise de riscos baseada em teoria de controle e sistemas. Nesse sentido essa técnica contrasta com as abordagens tradicionalmente utilizadas uma vez que estas se baseiam na teoria da confiabilidade. Apesar da diferença conceitual, a abordagem STPA tem o mesmo objetivo das técnicas tradicionalmente utilizadas: reunir o maior número de informações a respeito de possíveis cenários em que eventos indesejados possam ocorrer. Baseado nessas informações reduzir e controlar os riscos dos sistemas (LEVESON, 2013).

Uma vez que STPA não se baseia na teoria de confiabilidade, ele não tem como objetivo determinar um número relacionado à probabilidade de ocorrer determinado evento de falha. Isso porque, a única maneira de se chegar a esse valor em sistemas complexos é omitir os fatores casuais que não são estocásticos e suas informações probabilísticas em diversos casos não existem. A inexistência de um histórico probabilístico ocorre principalmente quando a análise é realizada em sistemas que ainda estão em fase de desenvolvimento ou foram recentemente implantados. Dado essas omissões e/ou inferências sem dados históricos, a geração de análises probabilísticas podem não refletir verdadeiramente o risco associado de cada evento. Nesse contexto, por vezes, as tomadas de decisão, baseadas nesses dados podem levar a uma falha. Isso ocorre, por exemplo, devido a não correção de determinado risco, previamente identificado, porém desconsiderado em virtude de uma probabilidade de ocorrência erroneamente subestimada (LEVESON, 2013).

Um outro ponto a se destacar é que: diferentemente das abordagens tradicionais, STPA é bastante eficaz quando se busca identificar fatores casuais em cenários de risco, principalmente quando estes estão relacionados à softwares, *design* de sistemas e comportamento humano. Um outro ponto importante é que a ferramenta STPA pode ser utilizada desde os conceitos iniciais do desenvolvimento de projeto, até em sistemas já existentes, gerando assim, requisitos de segurança de alto nível em todas as fases dos projetos de engenharia.

O processo STPA pode ser separado em quatro etapas, todavia diversas atividades podem e devem interagir para que se obtenha resultados mais efetivos. Estas etapas são:

1. Estabelecer a base de engenharia do sistema para a análise e para o desenvolvimento do sistema;

Nessa etapa são definidos os conceitos básicos do sistema relacionados à segurança. Nesse sentido, são previstos os acidentes ou perdas que serão consideradas, além disso são identificados os perigos que levam a essas perdas e por fim especificadas as restrições de segurança. Com base nesses dados, a estrutura de controle preliminar é definida, sendo usada durante as análises subsequentes.

2. Identificar ações de controle potencialmente inseguras;

Para cumprimento desta atividade, são identificadas, dentro da estrutura de controle, as ações de controle que podem levar o sistema à condição de falha ou acidente.

3. Criar requisitos e restrições de segurança

Para cada ação de controle identificada na etapa anterior são elaboradas barreiras ou requisitos que “impeçam” a ocorrência dessas. Um ponto importante abordado por CASTILHO (2015) é que: na teoria STAMP e consequentemente na abordagem STPA, os requisitos e restrições são frequentemente considerados sinônimos, apesar dos termos restrição e requisito serem naturalmente negativos e positivos respectivamente. Neste trabalho esses termos são adotados como sinônimos, sendo omitidos por vezes o termo restrição.

4. Determinar como cada ação de controle com risco potencial pode ocorrer.

A última etapa da aplicação da ferramenta consiste no levantamento dos cenários e dos fatores causais motivadores das ações de segurança. Esse levantamento deve servir como base para a elaboração de ações mitigadoras relacionadas a esses riscos.

4 MATERIAIS E MÉTODOS

Inicialmente, o desenvolvimento do trabalho para esta pesquisa consistiu na procura e análise de material bibliográfico referente aos processos de extração mineral, níveis de automação de processo, da teoria de sistemas, além de estudos a respeito da abordagem STAMP, incluindo *cases* já realizados. Nesse estudo inicial buscou-se fundamentar as análises de aplicabilidade propostas neste trabalho.

A seguir, nos próximos subitens os materiais e métodos previstos para consecução dos objetivos deste trabalho são expostos.

4.1 Materiais

4.1.1 Software XSTAMPP

Durante a aplicação da ferramenta STPA foi utilizado, como apoio no desenvolvimento das estruturas de controle, o software XSTAMPP, desenvolvido na Universidade de Stuttgart da Alemanha.

4.1.2 Perfuratriz Autônoma

A perfuratriz e o processo, objetos deste estudo, da qual são referentes as informações, bem como onde é prevista a aplicação da abordagem STAMP é pertencente a uma mineradora no estado de Minas Gerais, Brasil.

A perfuratriz, modelo MD6420, segundo informações do fabricante possui carga da broca de 41,346 kg e realiza furos de até 311 mm de diâmetro. Esse equipamento que a princípio operava de maneira manual, sofreu adaptações de modo a aumentar o seu nível de automação. Com isso as operações de deslocamento, perfuração e em alguns casos acréscimo de haste passaram a contar com a possibilidade de operação em modo remoto ou autônomo.



Figura 12 - Perfuratriz Autônoma objeto do estudo.

4.2 Método de Trabalho

4.2.1 Estudo do Caso

Com o objetivo de explicitar o contexto em que a ferramenta STPA será abordada, foi realizada uma análise a respeito das diversas etapas do processo de execução dos furos da qual a perfuratriz autônoma, objeto deste estudo, está inserida. Essa análise, além de demonstrar o contexto (técnico e organizacional) em que a perfuratriz está inserida, serviu como referência para a elaboração das bases da engenharia e estrutura de controle previstas na aplicação da ferramenta STPA.

4.2.2 Aplicação da Ferramenta STPA

Para o presente trabalho foi realizada uma aplicação prática da abordagem STAMP nas perfuratrizes autônomas, atualmente em desenvolvimento na mineradora, em Minas Gerais. Para isso, será utilizada a ferramenta STPA. A aplicação dessa ferramenta se deu a partir do desenvolvimento das quatro etapas anteriormente descritas, e novamente elencadas para maior facilidade referencial.

1. Estabelecer a base de engenharia do sistema para a análise e para o desenvolvimento do sistema.
2. Identificar ações de controle potencialmente inseguras.
3. Criar requisitos e restrições de segurança.
4. Determinar como cada ação de controle com risco potencial pode ocorrer.

Para esse desenvolvimento, foram realizadas diversas atividades com uma equipe multidisciplinar que estava trabalhando no projeto (engenharia de desenvolvimento, operações e manutenção da perfuratriz autônoma). Entre as atividades destaca-se:

- reunião de alinhamento com objetivo de apresentar a ferramenta STPA e seus objetivos;
- visitas *in loco* para análise do processo / contexto no qual a perfuratriz está inserida;
- análise da documentação técnica do equipamento e procedimentos operacionais;
- entrevistas com integrantes da equipe multidisciplinar;

4.2.3 Análise crítica da abordagem e abrangência

A partir dos dados obtidos da aplicação prática, foi feita uma análise crítica a respeito da efetividade das ferramentas e suas análises na identificação de melhorias de segurança operacional e da informação baseada no estudo de caso proposto.

Por fim, uma conclusão propondo uma possível extensão da aplicabilidade da abordagem há, em outros ambientes da mineração, como por exemplo, usinas de beneficiamento e equipamentos de manuseio foi realizada.

5 RESULTADOS

5.1 Estudo de caso

A área de lavra mineral é uma área extremamente dinâmica uma vez que as suas condições variam frequentemente. Entre essas mudanças estão as alterações climáticas em decorrência de ser operações a céu aberto, relevo em decorrência do avanço da lavra, tamanho e tipos de equipamentos utilizados que variam em decorrência da disponibilidade destes, de processo em decorrência do corpo de minério disponível e do planejamento, quadro operacional em decorrência das mudanças organizacionais, entre outros.

De modo a melhor entender o contexto em que a perfuratriz, objeto do estudo, está inserido, é representado primariamente pela Figura 13, iniciando pelo contexto macro do mercado de mineração. Note que as ações a serem realizadas por cada agente do diagrama são simplificadas, ou seja, as ações tomadas por esses agentes não se limitam às expostas neste trabalho, principalmente nos diagramas mais macros.

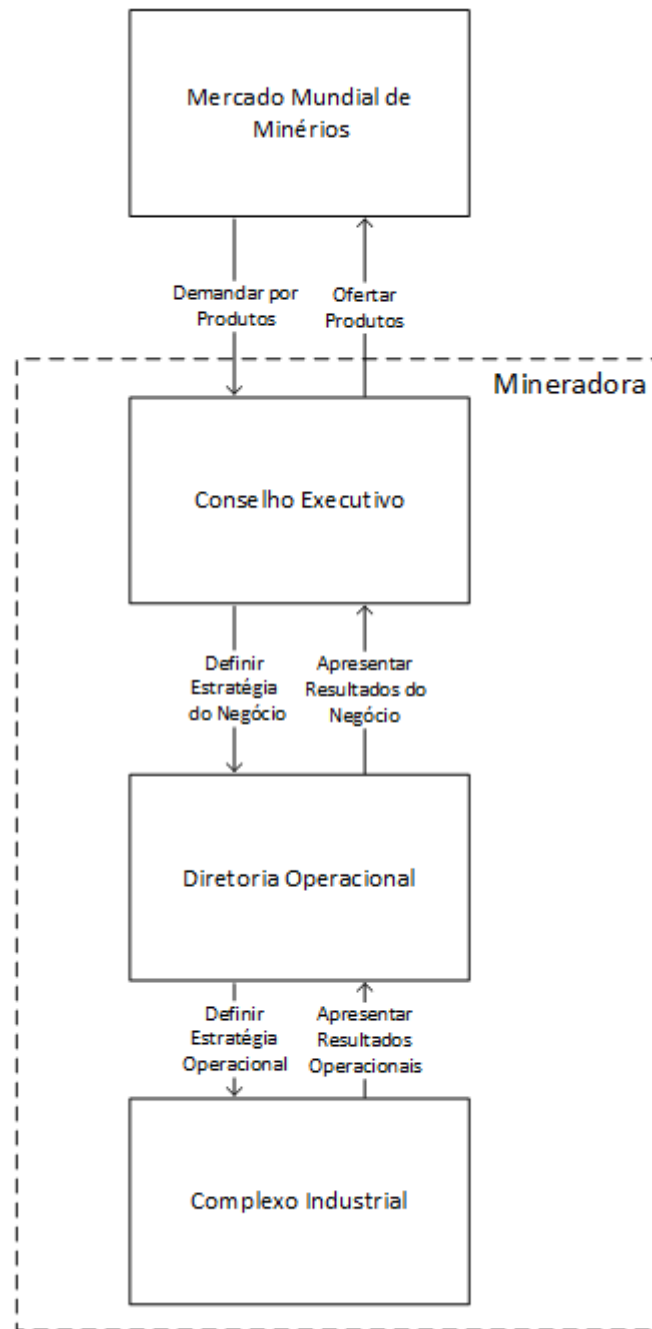


Figura 13: Macro fluxo de mercado na Indústria Mineral.

Conforme pode ser observado na Figura 13, o processo produtivo (mineradora) é influenciado, naturalmente, pelo mercado mundial de minérios. Esses processos, aqui, inicialmente representados pelo mercado de minérios que é afetado por diversos fatores, como por exemplo, o crescimento dos países consumidores dessa commodity. Esse mercado é o responsável por demandar os produtos à mineradora e recebe dela essa oferta de produtos.

O conselho executivo, baseado nas demandas minerais do mercado e dos resultados apresentados pelas diretorias operacionais, elabora e define as estratégias do negócio. Essas

estratégias são especialmente importantes uma vez que apontam rumos a serem tomados pelas operações.

A diretoria operacional de posse da estratégia do negócio elaborada pelo conselho, e dos resultados e capacidades operacionais dos complexos industriais definem as estratégias para cada complexo industrial.

Por fim, quando analisada a Figura 13 temos o complexo industrial. Esse complexo tem a função de receber as estratégias operacionais definidas pela diretoria e apresentar os resultados dentro do esperado. Nesse complexo industrial é onde a extração e o beneficiamento de minérios ocorrem, nesse sentido, na Figura 14 é demonstrado com maior detalhe o complexo industrial dentro do qual o processo de extração mineral está inserido.

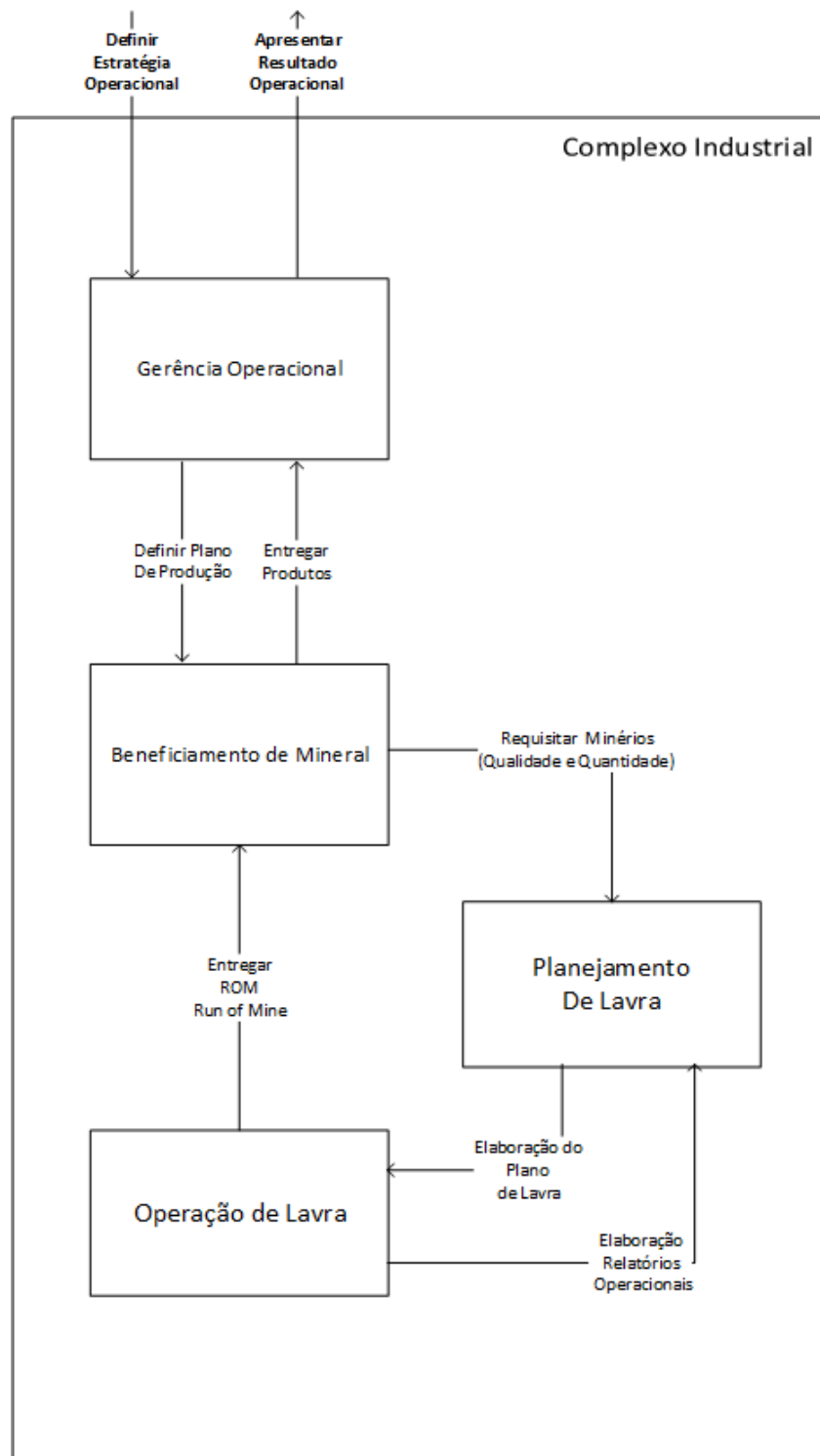


Figura 14: Zoom in no Macro fluxo do Complexo Industrial.

Conforme já abordado, e explicitado na Figura 14, o complexo industrial recebe como *input* a estratégia operacional previamente estabelecida. A partir dessa estratégia é definido pela gerência operacional o plano de produção a ser cumprido, recebendo como *feedback* os produtos.

O plano de produção elaborado pela gerência operacional é entregue à equipe de beneficiamento mineral que com base na quantidade e qualidade de produtos previstos no plano de produção requisitam à equipe de planejamento de lavra a quantidade e quantidade de ROM (*Run of Mine*) necessários para entrega desses produtos.

A equipe de planejamento de lavra de posse dos requisitos do ROM, das frentes de lavra e equipamentos disponíveis e dos relatórios operacionais elaboram o plano de lavra a ser entregue à equipe de operação de lavra.

Como último ente relacionado na Figura 14 temos a equipe de operação de lavra. Essa equipe é responsável pela extração mineral propriamente dita. Essa operação se dá a partir do plano de lavra previamente estabelecido e tem como resultado o *feedback* para o planejamento de lavra os resultados operacionais que servem como insumo para ajustes nos planos de lavra, além do ROM para a instalação de tratamento de minérios que os beneficiará até ter as características solicitadas no plano de produção.

Dentro desse contexto, é representado na Figura 15 uma visão ampliada da área de operação de lavra.

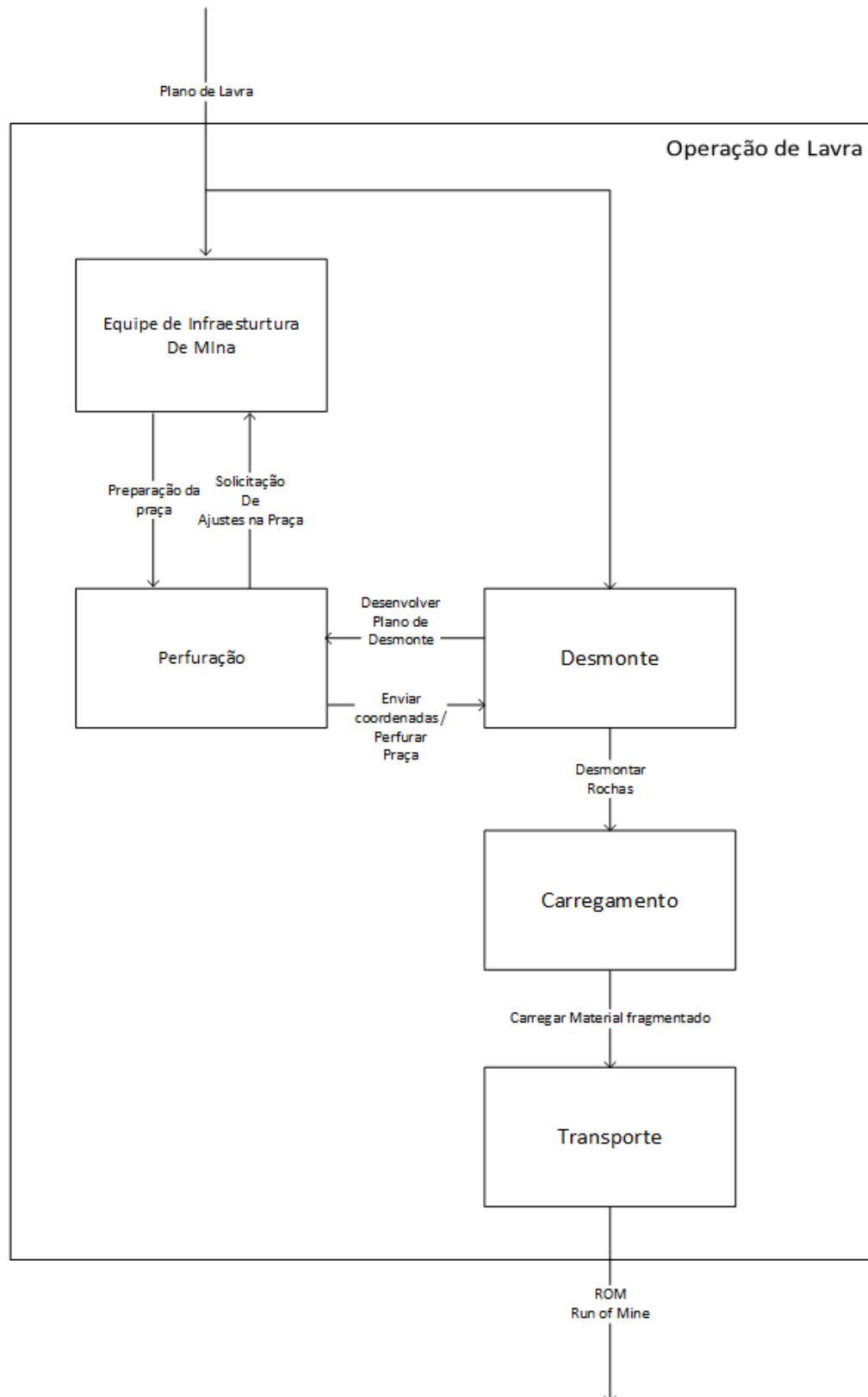


Figura 15: Zoom in no Macro Fluxo da Operação de Lavra.

Conforme já apontado anteriormente, o plano de lavra é um *input* essencial para a equipe de operação de lavra. Nesse plano, entre outros dados, constam informações a respeito do sequenciamento de lavra a ser realizado. Essas informações contribuem para o direcionamento dos esforços da equipe de infraestrutura de mina na preparação dos acessos (utilizados pelos equipamentos de carga e transporte) e das praças a serem posteriormente perfuradas.

Um outro agente que também faz uso do plano de lavra é a equipe de desmonte. A equipe de desmonte é responsável pela elaboração de um outro plano, o de fogo. O plano de fogo é baseado além das informações do plano de lavra, ele utiliza outras informações coletadas pela equipe de perfuração, como as coordenadas e condições da área a ser detonada. Esse plano de fogo, uma vez pronto, é enviado para a equipe de perfuração para que os furos sejam feitos.

Como pode ser observado, a etapa de perfuração tem interação com as equipes de desmonte e de infraestrutura de mina. Após receber o plano de perfuração pela equipe de desmonte e ter a área perfurada preparada pela equipe de infraestrutura de mina, os furos são executados na localização, profundidade e ângulo planejados.

Uma vez concluído, o furo é de responsabilidade da equipe de desmonte e a detonação do material, entregando assim o material desmontado para a equipe de carregamento e transporte.

Por fim, temos a equipe de carregamento que a é responsável por carregar o material desmontado nos caminhões, que por sua vez têm a função de fazer o transporte desse material até o seu destino.

Sendo a operação da perfuratriz autônoma, foco deste trabalho, é feito mais um zoom na etapa de perfuração, etapa na qual essa operação unitária está inserida. Esse zoom está representado na Figura 16.

Uma vez a perfuratriz pronta para realizar os furos é de responsabilidade do operador da sala de controle inserir os dados referentes ao plano de desmonte no software da perfuratriz. Entre as informações a serem inseridas estão as posições de cada furo, posições do polígono, marcadas possíveis irregularidades no piso, ângulo em que cada furo deve ser realizado, entre outros. Uma vez enviado esses dados para o equipamento, o operador autoriza o início da perfuração e inicia o monitoramento das condições operacionais enviadas pelo equipamento, intervindo somente nos casos em que os parâmetros monitorados saiam das condições esperadas.

Por fim, como último componente da Figura 16 temos a perfuratriz. Esse equipamento quando recebido, as coordenadas, a inclinação de cada furo e permissão para iniciar a perfuração se deslocam ao local do primeiro furo e é iniciada sua execução. Uma vez concluído o furo, a broca é retirada e se desloca para a execução do próximo furo. Esse trabalho é realizado até que todos os furos estejam concluídos. Note, porém, que é dada ênfase à perfuração no modo autônomo (foco deste estudo), modo no qual todo o deslocamento, posicionamento e perfuração são feitos sem a intervenção de um operador. Todavia, a perfuratriz objeto deste estudo, tem a possibilidade de operar também nos modos local (modo no qual o operador opera localmente o equipamento), e remoto manual (modo no qual o operador opera remotamente o equipamento).

Em resumo, mais especificamente, o processo no qual a perfuratriz, no modo autônoma, está inserida (perfuração) ocorre nas seguintes etapas:

1. **Definição da área a ser detonada:** nesta etapa, baseado no plano de produção, equipamentos disponíveis, e áreas possíveis de serem lavradas é definida a área a ser detonada;
2. **Demarcação da área a ser detonada:** uma vez definido o local em que será feita a detonação, o profissional de mineração faz a demarcação da área, coletando as coordenadas das “bordas” da área a ser detonada;
3. **Elaboração do plano de fogo:** de posse dos dados da área a ser detonada, é elaborado o plano de fogo que consiste em determinar a malha dos furos, incluindo distância entre furos, ângulos de inclinação e profundidade;
4. **Análise de condições de área e deslocamento da perfuratriz:** é realizada uma avaliação das condições operacionais da praça, incluindo as leras nas laterais para a

perfuratriz. Em acordo com os requisitos é feita a movimentação da perfuratriz até o local onde serão realizados os furos;

5. Perfuração: a perfuratriz é posicionada no local do primeiro furo e preparada a broca para início da perfuração. A maneira que é feita a comunicação das informações, a respeito do posicionamento do equipamento, bem como os ângulos e a profundidade de perfuração, dependem do modo que a perfuratriz irá operar (manual, remoto ou no modo autônomo). Esse modo de operação também define como será feita a mudança de posição entre os furos da malha previamente definida. Todavia, independentemente do modo de operação do equipamento, esta etapa é concluída após o termino de todos os furos previstos no plano de fogo.

6. Retirada dos equipamentos de perfuração: a perfuratriz e os outros equipamentos são retirados do local para inserção dos explosivos nos furos e detonação.

Note que é dado o foco na operação autônoma da perfuratriz uma vez que esse modo é o foco deste estudo, todavia o equipamento possui outros modos de operação que eventualmente são citados neste estudo.

5.2 Aplicando a ferramenta STPA

No tópico anterior foi apresentado o modo de operação da perfuratriz autônoma bem como o contexto em que ela está inserida. Nesse ponto, alguns conceitos precisam ser explicitados uma vez que alguns detalhes de sua essência podem variar de autor para autor. Nesse sentido são abordados dois conceitos que estão alinhados com a abordagem STPA.

- Condições de Perigo

Um estado do sistema que, quando em conjunto com o pior caso de condições do ambiente levará a um acidente ou perda (PEPER, 2017).

- Acidente

Um evento indesejado ou não planejado que resulta em alguma perda, incluindo perdas de vidas ou ferimentos em humanos, destruição de propriedades, poluição do meio ambiente, perda da missão, entre outros (LEVESON, 2013).

Tendo em vista essas definições, nos próximos tópicos é apresentada a aplicação da ferramenta STPA que, conforme já abordado anteriormente é feita em quatro etapas.

5.2.1 Estabelecimento dos fundamentos de engenharia do sistema

Para a aplicação da técnica STPA, inicialmente, deve-se definir quais perdas são consideradas inaceitáveis e que, portanto, devem ser tratadas no desenvolvimento do trabalho. A partir dessa definição são apontados os perigos que podem levar a esses acidentes. Nesse sentido, especificamente para o estudo de caso, foram definidos, a partir de entrevistas com as diversas equipes que desenvolvem, operam e realizam as manutenções da perfuratriz autônoma, os seguintes:

Tabela 1: Perdas e Perigos – Perfuratriz.

Acidentes	Perigo
Colisão entre equipamentos (A1)	Distância inadequada entre a perfuratriz e outros equipamentos (P1). Perfuratriz sair da zona de trabalho (P2).
Queda de bancada (A2)	Perfuratriz sair da zona de trabalho (P2)
Tombamento da Perfuratriz (A3)	Perfuratriz ultrapassar a inclinação limite (P3).

O primeiro acidente (A1) da Tabela 1 é a colisão entre a perfuratriz e outros equipamentos. As colisões entre equipamentos de mineração frequentemente têm consequências graves, apesar de normalmente serem baixas as suas velocidades de operação. Essa gravidade se dá, principalmente, devido ao tamanho dos equipamentos envolvidos nos processos. Neste trabalho, foram considerados como exemplo de equipamentos que possam colidir com a perfuratriz: caminhonetes, caminhões fora de estrada, caminhões de anfo, outras perfuratrizes e outros equipamentos que possam vir a adentrar a área de trabalho da perfuratriz.

Entre as consequências possíveis da colisão desses equipamentos destaca-se: lesões (temporárias ou permanentes) ou até mesmo a morte dos funcionários envolvidos. Uma outra grave consequência desse tipo de evento é o grande prejuízo monetário acarretado. Esses prejuízos decorrem do conserto ou substituição desses equipamentos (dependendo da gravidade), além do impacto no processo produtivo resultante da indisponibilidade dos equipamentos.

A queda de bancada (A2) é o evento decorrente da queda da perfuratriz em uma das diversas bancadas existentes no ambiente de mineração. Em outras palavras, é a queda do equipamento entre diferentes níveis (cotas) da área de lavra. As consequências desse tipo de evento também são graves, vão desde a quebra ou perda da perfuratriz e/ou outros equipamentos envolvidos no evento (por exemplo equipamentos que estejam trabalhando na bancada do nível inferior), impactos negativos no processo produtivo até a lesão ou morte de pessoas.

O último acidente analisado é o tombamento da perfuratriz (A3). Esse evento, análogo aos eventos anteriores pode ocasionar consequências graves e muitas vezes irreversíveis no que tange seres humanos, além é claro dos impactos financeiros ocasionados pela quebra do equipamento e impactos operacionais na lavra.

Existem diversas situações ou perigos que podem levar aos acidentes (A1, A2 E A3). É importante perceber que quando definimos os perigos estamos tratando a nível de sistema, e que os perigos estão ligados aos acidentes conforme é apontado na Tabela 1. O primeiro perigo (P1) que pode levar a esses acidentes é referente à distância inadequada entre a perfuratriz e os outros equipamentos. Essa distância é necessária para que seja possível a reação por parte do operador ou sistema em caso de alguma eventualidade como distração (operador) ou manobra indevida (sistema), evitando assim uma possível colisão.

Conforme já abordado anteriormente, no ambiente operacional de mineração é comum a utilização de equipamentos de grande porte. Esses equipamentos quando em movimento (dado sua massa) guardam grande energia cinética, portanto, necessitam de maior tempo para alcançar a velocidade zero e evitar a colisão, reforçando ainda mais o perigo de não se manter a distância mínima. Essas distâncias mínimas são previamente configuradas no software da perfuratriz, bem como tida como regra operacional para os indivíduos que venham operar o equipamento. Em outras palavras, o perigo passa a existir quando essas distâncias não são respeitadas.

O segundo perigo (P2) é referente à saída indevida da perfuratriz do local inicialmente previsto para execução dos furos. No ambiente de lavra, por motivos de segurança e organização das frentes de trabalho, a circulação de pessoas e equipamentos de cada área é restrita às operações unitárias que estão ocorrendo naquele momento. Nesse sentido, a perfuratriz deve-se manter rigorosamente dentro dos limites previamente estipulados e

ajustados pelos profissionais de mineração em campo. Sendo que o perigo passa a existir quando ela deixa de atender à essa premissa.

O último perigo é o ângulo da base da perfuratriz ultrapassar o ângulo de inclinação previsto como seguro na operação do equipamento (P3). Esse perigo se torna ainda mais iminente quando a haste da perfuratriz está na posição perpendicular (ou próximo disso) ao restante equipamento, alterando ainda mais seu centro de gravidade como pode ser observado na Figura 17. Nesse sentido para cada posição da haste, ou direção de inclinação da base do equipamento um ângulo máximo deve ser respeitado.



Figura 17: Perfuratriz com haste na posição de perfuração.

Uma vez definido em alto nível os perigos que possam levar aos acidentes, foram levantadas as restrições de segurança, ou seja, foram definidos os requisitos dentro do

processo para que o sistema não chegue à condição de perigo. Esses requisitos definidos podem ser observados na Tabela 2:

Tabela 2: Requisitos de Segurança.

Perigo	Requisitos de Segurança
Distância inadequada entre a perfuratriz e outros equipamentos (P1).	Perfuratriz nunca deve se movimentar com equipamentos próximos (distância menor que a permitida).
Perfuratriz sair da zona de trabalho (P2)	Perfuratriz nunca deve sair da zona de trabalho
Perfuratriz ultrapassa a inclinação limite (P3).	Perfuratriz nunca deve se movimentar caso a inclinação ultrapasse os níveis seguros.

A identificação de acidentes e perigos é uma prática padrão nas análises de segurança do sistema; um ponto adicional e fundamental necessário para executar o STPA é uma estrutura de controle do sistema, que conforme abordado anteriormente, é uma representação funcional do sistema como loops de controle hierárquico (PLACKE, 2014). Nesse sentido, conforme é mencionado por Leveson (2013), uma vez identificado os acidentes, perigos e requisitos de segurança a definição da estrutura funcional de controle deve ser definida.

Para o estudo de caso da perfuratriz autônoma, demonstrado na Figura 18 de maneira macro, as diversas interações possíveis entre os entes que compõem e têm alguma relação com o processo de perfuração.

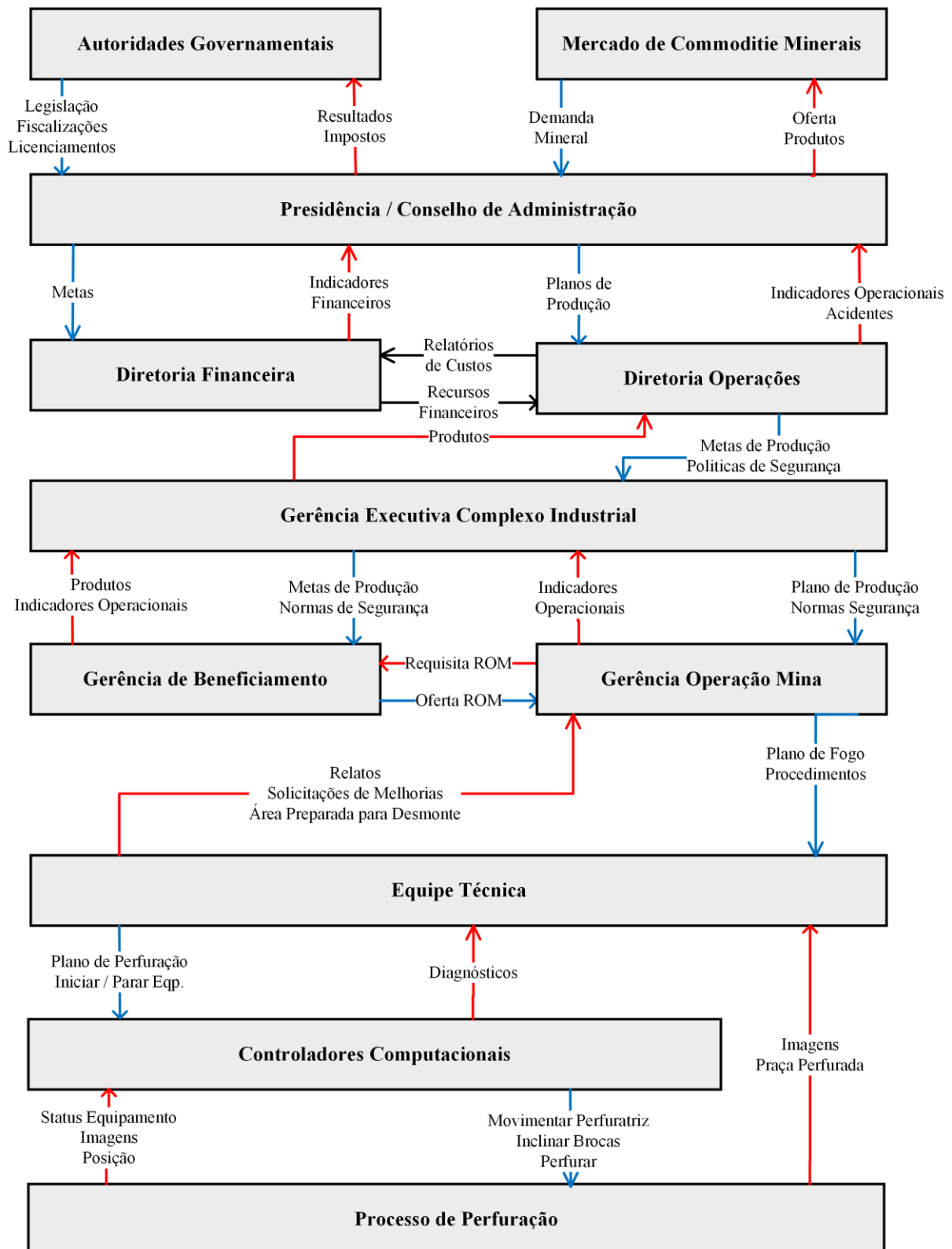


Figura 18: Estrutura de controle Macro do Processo de Perfuração.

De modo a melhor explicitar a estrutura de controle, é expandida a Figura 18, com foco nos entes que têm interação direta e com o processo de perfuração. A responsabilidade de cada componente da estrutura de controle (não exaustiva) é assim definida:

EQUIPE TÉCNICA

OPERADOR CENTRO DE CONTROLE

Responsabilidades:

- ✓ Garantir a segurança e performance operacional dos equipamentos durante o processo de locomoção e perfuração. Para isso são realizadas por este operador as análises de imagens e indicadores operacionais.

TÉCNICO DE CAMPO ou TÉCNICO DE MINERAÇÃO

Responsabilidades:

- ✓ Garantir que a área a ser perfurada esteja correta e dentro dos critérios pré-estabelecidos.
- ✓ Preparar a perfuratriz para perfuração no modo autônomo.

CONTROLADORES COMPUTACIONAIS

PC INDUSTRIAL

Responsabilidades:

- ✓ Controlar todo o processo de perfuração no modo autônomo de modo a garantir que os furos sejam realizados na posição, ângulo e profundidade previstos no plano de fogo.



Figura 19: PC Industrial.

CONTROLADOR DE SEGURANÇA

Responsabilidades:

- ✓ Interromper o funcionamento da perfuratriz em caso de falha grave observada pelo operador ou em caso de falhas de comunicação.

PLC

Responsabilidades:

- ✓ Atender aos comandos mantendo os parâmetros de segurança operacionais dentro dos limites previamente estabelecidos.



Figura 20: PLC.

Tendo, portanto, em vista responsabilidades e ações de cada componente que se relaciona diretamente com o processo de perfuração, esse processo é demonstrado na Figura 21:

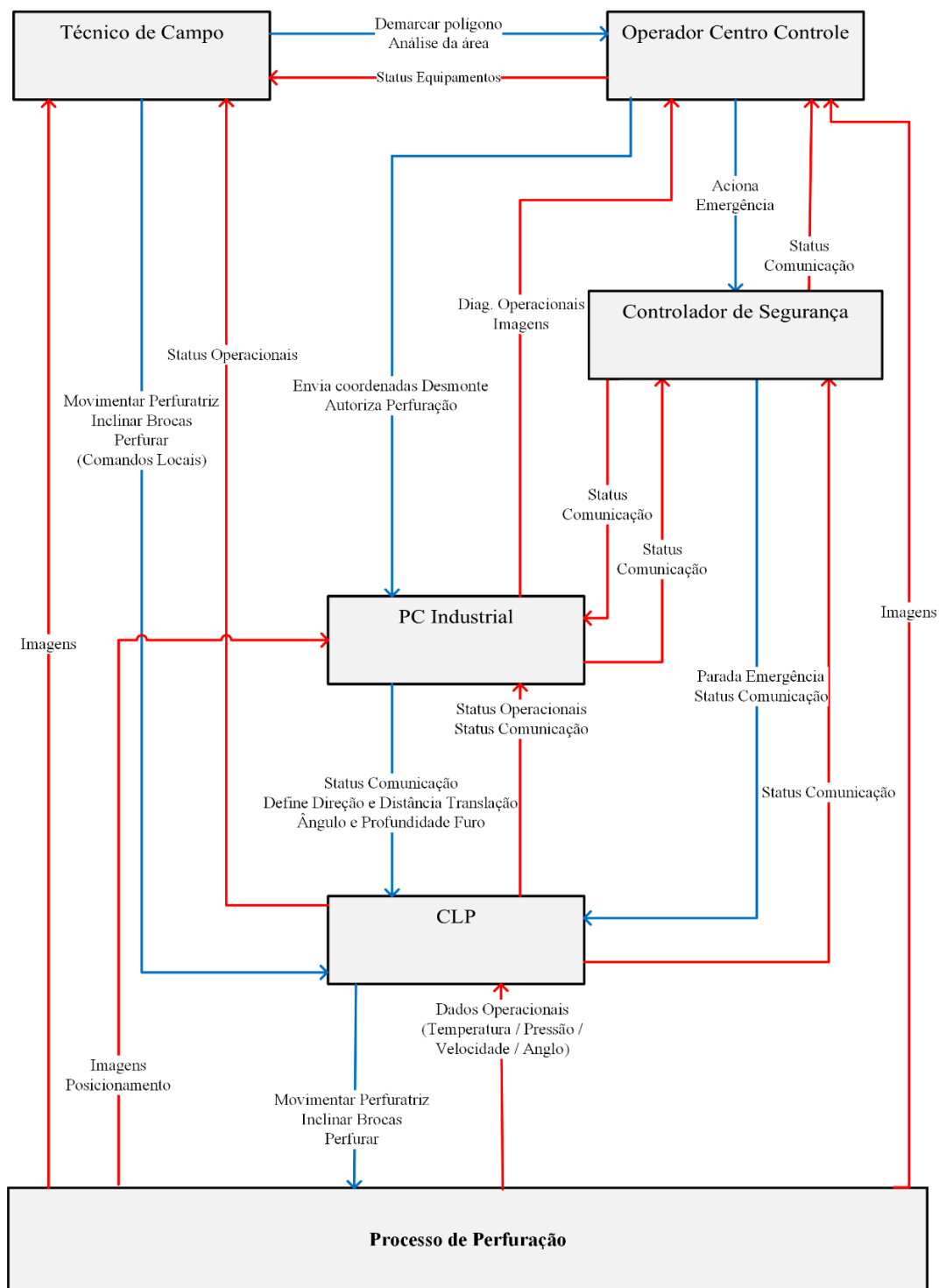


Figura 21: Estrutura de controle do processo de Perfuração.

5.2.2 Identificando as ações de controle potencialmente inseguras

Uma vez definida a estrutura de controle do processo de perfuração, foi realizada a etapa de identificação das ações de controle potencialmente inseguras, ou seja, ações que em determinadas condições podem levar o sistema a uma situação de perigo. Essas ações de controle são identificadas a partir da Tabela 3 até a Tabela 17 e com objetivo de melhor organizá-las, estão separadas por cada controlador (seja ele humano ou computacional).

Ações de Controle potencialmente inseguras (ACI) do Técnico em mineração (TM):

Tabela 3: Ações de controle inseguras (ACI) do Técnico de mineração para o perigo da perfuratriz sair da zona de trabalho.

Perigo: Perfuratriz sair da zona de trabalho (P1)				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Delimitar polígono de perfuração	NA	Determinar polígono de maneira incompleta / incorreta (ACI-TM-01).	NA	NA
Analisar e aprovar área de perfuração	NA	NA	NA	NA
Movimentar Perfuratriz (Local)	NA	Movimentar Perfuratriz para área Incorreta (ACI-TM-02).	NA	NA
Inclinar Broca de perfuração (Local)	NA	NA	NA	NA
Executar Perfuração (Local)	NA	NA	NA	NA

Tabela 4: Ações de controle inseguras do Técnico de mineração para o perigo da distância inadequada entre os equipamentos.

Perigo: distância inadequada entre a perfuratriz e outros equipamentos (P2)				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Delimitar polígono de perfuração	NA	Determinar polígono de maneira incompleta / incorreta (ACI-TM-01).	NA	NA
Analisar e aprovar área de perfuração	NA	NA	NA	NA
Movimentar Perfuratriz (Local)	NA	Movimentar perfuratriz deixando de observar outros equipamentos ou barreiras (ACI-TM-03).	NA	NA
Inclinar Broca de perfuração (Local)	NA	Inclinar broca sobre / muito próximo de outros equipamentos ou barreiras (ACI-TM-04).	NA	NA
Executar Perfuração (Local)	NA	NA	NA	NA

Tabela 5: Ações de controle inseguras do Técnico de mineração para o perigo da perfuratriz ultrapassar a inclinação limite.

Perigo: perfuratriz ultrapassar a inclinação limite (P3)				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Delimitar polígono de perfuração	NA	NA	NA	NA
Analisar e aprovar área de perfuração	NA	Aprovar área com irregularidades no solo (ACI-TM-05).	NA	NA
Movimentar Perfuratriz (Local)	NA	Movimentar Perfuratriz com lança fora da posição (ACI-TM-06). Movimentar perfuratriz em área não apropriada (ACI-TM-07).	NA	NA
Inclinar Broca de perfuração (Local)	NA	Inclinar broca para um ângulo diferente do previsto / permitido (ACI-TM-08).	NA	NA
Executar Perfuração (Local)	NA	NA	NA	NA

Ações de Controle potencialmente inseguras do Operador de Centro de Controle:

Tabela 6: Ações de controle inseguras do Operador de Centro de Controle (OCC) para o perigo da perfuratriz sair da zona de trabalho.

Perigo: Perfuratriz sair da zona de trabalho (P1)				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Acionar Emergência (Autônomo)	Não acionar em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-01).	NA	Acionar tardiamente em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-02).	NA
Enviar Coordenadas (Autônomo)	NA	Enviar coordenadas incorretas (ACI-OCC-03).	NA	NA
Autorizar Perfuração (Autônomo)	NA	NA	NA	NA
Movimentar Perfuratriz (Remoto)	NA	NA	NA	Movimentar em excesso e não respeitar os limites do polígono (ACI-OCC-04).
Inclinar Broca de perfuração (Remoto)	NA	NA	NA	NA
Executar Perfuração (Remoto)	NA	NA	NA	NA

Tabela 7: Ações de controle inseguras do Operador de Centro de Controle para o perigo da distância inadequada entre os equipamentos.

Perigo: distância inadequada entre a perfuratriz e outros equipamentos				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Acionar Emergência (Autônomo)	Não acionar em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-01).	NA	Acionar tardiamente em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-02).	NA
Enviar Coordenadas (Autônomo)	NA	Enviar coordenadas incorretas (ACI-OCC-03).	NA	NA
Autorizar Perfuração (Autônomo)	NA	Autorizar com equipamentos indevidos na área de perfuração (ACI-OCC-05).	Autorizar sem a área / equipamentos estarem prontos (ACI-OCC-06).	NA
Movimentar Perfuratriz (Remoto)	NA	Movimentar perfuratriz sobre algum equipamento (ACI-OCC-07).	NA	Movimentar em excesso e não respeitar os limites do polígono (ACI-OCC-04).
Inclinar Broca de perfuração (Remoto)	NA	Inclinar broca sobre / muito próximo de outros equipamentos (ACI-OCC-08).	NA	NA
Executar Perfuração (Remoto)	NA	NA	NA	NA

Tabela 8: Ações de controle inseguras do Operador de Centro de Controle para o perigo da perfuratriz ultrapassar a inclinação limite.

Perigo: perfuratriz ultrapassar a inclinação limite				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Acionar Emergência (Autônomo)	Não acionar em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-01).	NA	Acionar tardiamente em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-02).	NA
Enviar Coordenadas (Autônomo)	NA	Enviar coordenadas incorretas (ACI-OCC-03).	NA	NA
Autorizar Perfuração (Autônomo)	NA	Autorizar com equipamentos indevidos na área de perfuração (ACI-OCC-05).	NA	NA
Movimentar Perfuratriz (Remoto)	NA	Movimentar Perfuratriz com lança fora da posição (ACI-OCC-09). Movimentar perfuratriz em área inclinada ou irregular (ACI-OCC-10).	NA	NA
Inclinar Broca de perfuração (Remoto)	NA	Inclinar broca para um ângulo diferente do previsto / permitido (ACI-OCC-11).	NA	NA
Executar Perfuração (Remoto)	NA	NA	NA	NA

Ações de Controle potencialmente inseguras do Controlador de Segurança:

Tabela 9: Ações de controle inseguras do Controlador de Segurança para o perigo da perfuratriz sair da zona de trabalho.

Perigo: perfuratriz sair da zona de trabalho				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Enviar comando Parada de Emergência	Não acionar em caso de a perfuratriz entrar em situação de emergência (ACI-CS-01).	NA	Acionar tardiamente em caso de a perfuratriz entrar em situação de emergência (ACI-CS-02).	NA

Tabela 10: Ações de controle inseguras do Controlador de Segurança para o perigo da distância inadequada entre a perfuratriz e outros equipamentos.

Perigo: distância inadequada entre a perfuratriz e outros equipamentos				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Enviar comando Parada de Emergência	Não acionar em caso de a perfuratriz entrar em situação de emergência (ACI-CS-01).	NA	Acionar tardiamente em caso de a perfuratriz entrar em situação de emergência (ACI-CS-02).	NA

Tabela 11: Ações de controle inseguras do Controlador de Segurança para o perigo da perfuratriz ultrapassar inclinação limite.

Perigo: perfuratriz ultrapassar inclinação limite				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Enviar comando Parada de Emergência	Não acionar em caso de a perfuratriz entrar em situação de emergência (ACI-CS-01).	NA	Acionar tardiamente em caso de a perfuratriz entrar em situação de emergência (ACI-CS-02).	NA

Ações de Controle potencialmente inseguras do PC Industrial:

Tabela 12: Ações de controle inseguras do PC industrial para o perigo da perfuratriz sair da zona de trabalho.

Perigo: perfuratriz sair da zona de trabalho				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Definir direção movimentação equipamento (Autônomo)	NA	Definir a direção de movimento incorretamente (ACI-PCI-01).	NA	NA
Definir distancia movimentação equipamento (Autônomo)	NA	Definir a distância para movimentação Incorretamente (ACI-PCI-02).	NA	NA
Definir ângulo da broca (Autônomo)	NA	NA	NA	NA
Definir profundidade do furo (Autônomo)	NA	NA	NA	NA

Tabela 13: Ações de controle inseguras do PC industrial de Controle para o perigo da distância inadequada entre os equipamentos.

Perigo: distância inadequada entre a perfuratriz e outros equipamentos				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Definir direção movimentação equipamento (Autônomo)	NA	Direcionar a perfuratriz no sentido de outro equipamento ou obstáculo (ACI-PCI-03).	NA	NA
Definir distancia movimentação equipamento (Autônomo)	NA	Definir a distância para movimentação Incorretamente (ACI-PCI-02).	NA	NA
Definir ângulo da broca (Autônomo)	NA	NA	NA	NA
Definir profundidade do furo (Autônomo)	NA	NA	NA	NA

Tabela 14: Ações de controle inseguras do PC industrial de Controle para o perigo da perfuratriz ultrapassar a inclinação limite.

Perigo: perfuratriz ultrapassar inclinação limite				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Definir direção movimentação equipamento (Autônomo)	NA	NA	NA	NA
Definir distancia movimentação equipamento (Autônomo)	NA	NA	NA	NA
Definir ângulo da broca (Autônomo)	NA	Definir ângulo acima ou abaixo do ângulo permitido. (ACI-PCI-03).	NA	NA
Definir profundidade do furo (Autônomo)	NA	NA	NA	NA

Ações de Controle potencialmente inseguras do PLC:

Tabela 15: Ações de controle inseguras do PLC para o perigo da perfuratriz sair da zona de trabalho.

Perigo: perfuratriz sair da zona de trabalho				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Movimentar Perfuratriz	NA	Movimentar a perfuratriz na direção diferente da prevista (ACI-PLC-01).	NA	Não interromper a tempo a movimentação quando atingida a posição inesperada (ACI-PLC-02).
Inclinar Brocas	NA	NA	NA	NA
Perfurar	NA	NA	NA	NA

Tabela 16: Ações de controle inseguras do PLC de Controle para o perigo da distância inadequada entre os equipamentos.

Perigo: distância inadequada entre a perfuratriz e outros equipamentos				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Movimentar Perfuratriz	NA	Movimentar na direção de algum equipamento ou obstáculo quando estiver próximo (ACI-PLC-03).	NA	Não interromper a tempo a movimentação quando atingida a posição inesperada (ACI-PLC-02).
Inclinar Brocas	NA	NA	NA	NA
Perfurar	NA	NA	NA	NA

Tabela 17: Ações de controle inseguras do PLC de Controle para o perigo da perfuratriz ultrapassar a inclinação limite.

Perigo: perfuratriz ultrapassar inclinação limite				
Ações de Controle	Não executar causa perigo	Executar Causa Perigo	Iniciar ação muito cedo ou muito tarde / Ordem incorreta	Interromper ação muito cedo / Executar por muito tempo
Movimentar Perfuratriz	NA	Movimentar perfuratriz em terreno não adequado (ACI-PLC-03). Movimentar perfuratriz com o mastro fora da posição (ACI-PLC-04).	NA	NA
Inclinar Brocas	NA	Inclinar broca para um ângulo diferente do previsto / permitido (ACI-PLC-05).	NA	NA
Perfurar	NA	NA	NA	NA

5.2.3 Criando os requerimentos e requisitos de segurança

Uma vez definidos as ações de controle que podem levar a condição de perigo, devem-se definir os requisitos de segurança. Estes requisitos, devem ser definidos de tal maneira que, quando seguidos, o sistema não entrará no estado de risco como resultado de alguma das ações de controle. Desta maneira, para cada ação de controle insegura, requisitos de segurança são recomendados.

A partir da Tabela 18 até a Tabela 22 são representados os requisitos de segurança (RS) para cada controlador.

Tabela 18: Requisitos de segurança (RS) para o Técnico de Mineração (TM).

Requisito de Segurança	Ações de Controle inseguras Relacionadas	Motivo
RS-TM-01 – O Técnico de Mineração deve sempre mapear o polígono de perfuração de maneira completa e correta.	ACI-TM-01	A perfuratriz pode ir a uma área não desejada caso as bordas de sua área de atuação (polígono) não estejam corretamente e completamente definidas.
RS-TM-02 – O Técnico de Mineração deve sempre movimentar a perfuratriz para a área prevista no plano de lavra.	ACI-TM-02	A operação ou presença da perfuratriz em uma área não prevista pode gerar problemas de interferência negativa com outros equipamentos e/ou operações da área de lavra.
RS-TM-03 – O Técnico de Mineração não deve movimentar a perfuratriz quando da existência de equipamentos próximos e quando possível evitar a movimentação próxima a barreiras físicas.	ACI-TM-03, 04	Apesar de ser lenta a movimentação da perfuratriz, este é um equipamento de porte razoavelmente grande, e qualquer possibilidade de colisão entre os equipamentos e barreiras podem levar aos acidentes.
RS-TM-04 – O Técnico de Mineração nunca deve aprovar para operação uma área de perfuração das especificações.	ACI-TM-05, 07	Os desníveis na praça da lavra podem gerar sérios problemas de tombamento em virtude do deslocamento do centro de gravidade do equipamento quando da lança elevada.
RS-TM-04 – Toda movimentação da perfuratriz ou do seu mastro de perfuração deve atender aos requisitos de ângulo de inclinação do mastro.	ACI-TM-06, 08	O deslocamento da perfuratriz com o mastro fora do ângulo recomendado pode levar ao tombamento em virtude do deslocamento do centro de gravidade.

Tabela 19: Requisitos de segurança (RS) para o Operador do Centro de Controle (CC).

Requisito de Segurança	Ações de Controle inseguras Relacionadas	Motivo
RS-OCC-01 – É necessário que toda informação relativa às condições de emergência estejam claras e objetivas para o operador do centro de controle.	ACI-OCC-01, 02	Informações imprecisas ou não objetivas podem levar à uma decisão errônea ou atraso por parte do operador.
RS-OCC-02 – O acesso ao comando de emergência e o operador estejam sempre disponíveis durante a operação do equipamento.	ACI-OCC-01, 02	O não acesso ao botão de emergência ou a não presença do operador na sala de controle pode levar a um atraso na resposta à condição de emergência.
RS-OCC-03 – As coordenadas do polígono e plano de fogo enviadas para a perfuratriz devem ser precisas sempre.	ACI-OCC-03	Com base em informações referentes ao plano de fogo imprecisas o PC Industrial pode gerar comandos e solicitações incorretos.
RS-OCC-04 – Nunca se deve movimentar remotamente a perfuratriz para fora da área prevista no polígono de perfuração.	ACI-OCC-04, 07, 08	Fora da área prevista no polígono é uma área não controlada e que possivelmente não passou por inspeção para operação do equipamento.
RS-OCC-05 – Nunca se deve autorizar a entrada de equipamentos na praça de perfuração com a perfuratriz se movimentando no modo autônomo.	ACI-OCC-05, 07, 08	Equipamentos não autorizados dentro da área de perfuração pode levar a possível colisão.
RS-OCC-05 – Nunca se deve autorizar o início das operações da perfuratriz remotamente sem que as verificações de condições de praça e do equipamento tenham sido feitas e liberadas.	ACI-OCC-06, 07, 10	Condições básicas como condições da praça não podem ser verificadas a distância, dessa maneira deve-se sempre fazer a inspeção antes da liberação para operação pelo técnico de mineração.
RS-OCC-06 – Os ângulos máximos e mínimos de inclinação devem estar claros e devem ser fielmente seguidos.	ACI-OCC-09, 11	O ângulo de inclinação do mastro muda o centro de gravidade da máquina, o que é um fator crítico para a segurança do equipamento.

Tabela 20: Requisitos de segurança (RS) para o Controlador de Segurança (CS).

Requisito de Segurança	Ações de Controle inseguras Relacionadas	Motivo
RS-OCC-01 – É necessário que todo comando de emergência chegue à perfuratriz e em tempo satisfatório.	ACI-CS-01, 02	Falhas ou atrasos na comunicação entre o centro de controle agrava ainda mais uma situação, levando um equipamento de uma condição de perigo a um acidente.

Tabela 21: Requisitos de segurança (RS) para o PC Industrial (PCI).

Requisito de Segurança	Ações de Controle inseguras Relacionadas	Motivo
RS-PCI-01 – A perfuratriz deve sempre manter uma distância segura de outros equipamentos ou obstáculos, considerando inclusive sua posição posterior após a movimentação.	ACI-PCI-01, 02, 03	Um equipamento com essas dimensões e peso deve possuir qualquer movimento uma vez que qualquer choque pode levar a graves consequências.

Tabela 22: Requisitos de segurança (RS) para o Controlador Lógico Programável (PLC).

Requisito de Segurança	Ações de Controle inseguras Relacionadas	Motivo
RS-PLC-01 - Nunca se deve realizar movimentações na direção de um obstáculo quando estiver muito próximo dele.	ACI-PLC-01, 02, 03	Um equipamento com essas dimensões e peso deve possuir qualquer movimento uma vez que qualquer choque pode levar a graves consequências.
RS-PLC-03 - Nunca se deve realizar movimentações na direção ou distância diferente da prevista.	ACI-PLC-01, 03	Um equipamento com essas dimensões e peso deve possuir qualquer movimento uma vez que qualquer choque pode levar a graves consequências.
RS-PLC-03 – Sempre que existir a condição de parada o equipamento deve realizá-la.	ACI-PLC-01, 02, 03, 04	Qualquer movimentação do equipamento não deve infringir nenhuma condição de segurança ou operacional do equipamento.
RS-PLC-04 - Nunca se deve realizar movimentações da perfuratriz com a praça fora dos padrões.	ACI-PLC-03	A praça fora do padrão previsto para operação pode levar a movimentação (de mastro ou de translação) inesperada do equipamento.

Como pode ser observado, foram identificados os requisitos de segurança para cada ação de controle insegura em cada um dos controladores. Um ponto importante nesta etapa da análise é que somente foram analisados ou descritos comportamentos inseguros, ou seja, com foco nas ações de controle inseguras do sistema. Todavia, causas potenciais desses comportamentos, falhas humanas, erros de construção ou falha nos requisitos são parte da análise STPA e STPA-sec e devem fazer parte da análise. Essas causas foram percebidas durante a análise dos cenários que levam às ações de controle inseguras; e estas são apresentadas no próximo tópico.

5.2.4 Determinando cenários para ocorrências das ações de controle inseguras

Uma vez conhecidos as ações de controle inseguras e suas restrições gerais de segurança, o passo final na abordagem STPA é identificar os possíveis cenários em que as ações de controle inseguras possam ocorrer. Dessa maneira é possível realizar possíveis recomendações de segurança que podem levar a melhorias no design do sistema, políticas organizacionais, entre outros (LEE, 2018).

Para a identificação dos possíveis cenários, é realizada uma análise do loop de controle para identificar os cenários de risco e fatores causais que possam levar a alguma violação de

uma das restrições de segurança. Na Figura 22 são representados alguns dos fatores causais utilizados na elaboração dos cenários.

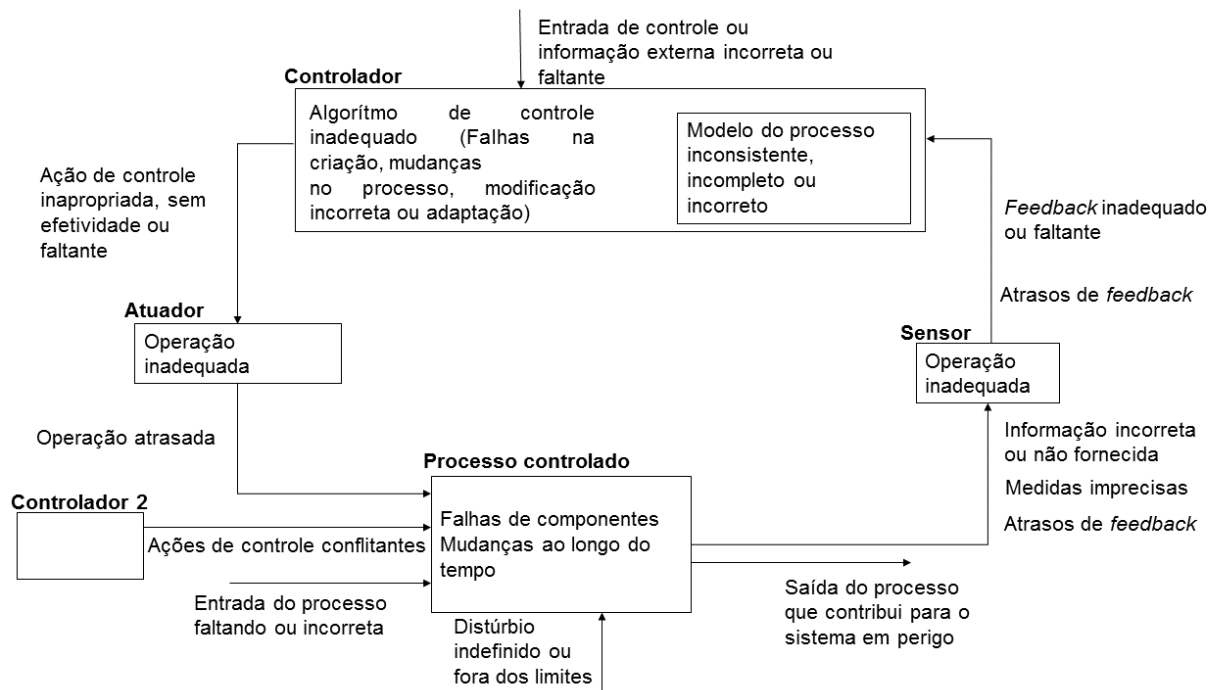


Figura 22: Fatores causais para criação dos cenários

Adaptado de (LEVESON, 2011)

Dito isso, e com base nas principais ações de controle inseguras, a Tabela 23 até a Tabela 50 representam uma lista de cenários potenciais, fatores causais associados, possível racional bem como propostas de ações mitigadoras do risco (importante ressaltar que essa lista não é exaustiva). As principais ações de controle foram determinadas a partir da sua influência e relevância na operação do equipamento quando da sua preparação e operação no modo autônomo.

Tabela 23: Fatores causais para determinação do polígono de maneira incorreta / incompleta.
(Continua)

Determinar polígono de maneira incompleta / incorreta (ACI-TM-01)		
Cenário	Fator Causal Associado	Racional
O técnico demarca os vértices de maneira incorreta por não saber utilizar o equipamento de demarcação ou desconhecer os procedimentos.	Falta de instrução ou treinamento.	A falta de conhecimento pode levar o colaborador a realizar as atividades incorretamente.
Por falha no GPS, os vértices não são registrados corretamente.	Equipamento com defeito.	Todo equipamento é passível de falhas.
Transmissão de dados do GPS é indevidamente alterada por agente malicioso.	Alteração indevida dos dados das coordenadas do polígono.	Dados que trafegam na rede correm risco de segurança digital.
Técnico demarca área incorretamente devido à incoerência do plano de lavra.	Plano de lavra contém informações incorretas ou imprecisas.	São constantes as mudanças nos planos de lavra, por isso devem sempre estar revisados e atualizados.
O plano de lavra é alterado indevidamente por agente malicioso.	Alteração indevida dos dados do plano de lavra.	Dados que trafegam na rede correm risco de segurança digital.
O Técnico coleta os pontos erroneamente por falta de atenção.	Falta de atenção do técnico.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem afetar o trabalho.

Tabela 23: Fatores causais para determinação do polígono de maneira incorreta / incompleta.
(Conclusão)

Ações Mitigadoras
Organizacionais / procedimentos de trabalho • Elaborar plano de treinamento e manter todos os profissionais com os treinamentos atualizados no que se refere a demarcações de polígonos. Software de planejamento e o plano de Lavra • O plano de lavra enviado para o técnico de mineração deve estar sempre revisado. • O software deve sempre estar atualizado com todos os patches de segurança. • Importante existir uma confirmação digital se a área mapeada para o plano de fogo é a mesma prevista para no plano de lavra. GPS • Devem ser testados a calibração e o funcionamento do GPS, periodicamente. Redes de transmissão de dados e comunicação • A transmissão de dados referentes às coordenadas do polígono deve ser sempre feita em rede segura protegida. • A transmissão do plano de lavra para o TM deve ser realizada utilizando uma rede de dados segura e protegida.

Tabela 24: Fatores causais que podem levar o TM a movimentar perfuratriz para área incorreta.

Movimentar Perfuratriz para área Incorreta (ACI-TM-02)		
Cenário	Fator Causal Associado	Racional
O técnico em mineração com base no plano de lavra impreciso ou incorreto leva à perfuratriz para área incorreta.	Plano de lavra contém informações incorretas ou imprecisas.	São constantes as mudanças nos planos de lavra, por isso devem sempre estar revisados e atualizados.
O plano de lavra é alterado indevidamente por agente malicioso.	Alteração indevida dos dados do plano de lavra.	Dados que trafegam na rede correm risco de segurança digital.
O técnico em mineração conduz a perfuratriz para a área incorreta por desconhecer a área de lavra.	Alteração indevida dos dados do plano de lavra.	A área de lavra muda constantemente, dessa maneira o profissional deve sempre estar ciente das alterações que estejam ocorrendo no ambiente de lavra.
O Técnico coleta e transporta a perfuratriz para o local errado por falta de atenção.	Falta de atenção do técnico.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem afetar o trabalho.
Ações Mitigadoras		
Organizacional / procedimentos de trabalho • Todos os técnicos devem ter um treinamento de reconhecimento de área de lavra e passar por reciclagem sempre que se ausentarem por período longo o suficiente para existirem alterações relevantes. • Deve existir no procedimento a confirmação da área à ser movimentada a perfuratriz pelo centro de controle. Software de planejamento e o plano de Lavra • O plano de lavra enviado para o técnico de mineração deve estar sempre revisado. Redes de transmissão de Dados e comunicação • A transmissão do plano de lavra para o TM deve ser realizada utilizando uma rede de dados segura e protegida.		

Tabela 25: Fatores causais que podem levar o TM a deixar de observar outros equipamentos ou barreiras. (Continua)

Movimentar perfuratriz deixando de observar outros equipamentos ou barreiras – Modo Local - (ACI-TM-03)		
Cenário	Fator Causal Associado	Racional
O técnico não percebe a entrada de novos equipamentos na área de perfuração.	Equipamentos desconhecidos dentro da área de perfuração.	É grande a movimentação de equipamentos dentro da área de lavra, principalmente veículos de pequeno porte.
O técnico não tem a visibilidade de todo o entorno da perfuratriz durante a movimentação.	Pontos cegos no entorno do equipamento.	Dentro da cabine de controle não é possível perceber todo o entorno do equipamento.
As imagens das câmeras ao redor do equipamento são alteradas por agente malicioso.	Alteração indevida das imagens de campo.	Câmeras digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
O Técnico deixa de observar alguma câmera ou o entorno da perfuratriz.	Falta de atenção do técnico durante as movimentações.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos.
Movimentação do equipamento não obedece aos comandos do técnico por falha no manete de comando.	Falha na manete de comando.	Travamentos ou outros problemas eletromecânicos podem levar o equipamento a operações inesperadas.

Tabela 25: Fatores causais que podem levar o TM a deixar de observar outros equipamentos ou barreiras. (Conclusão)

Ações Mitigadoras
Organizacionais / procedimentos de trabalho • Deve ser restrita a entrada de equipamentos na área de perfuração. • Sempre que se fizer necessária a entrada de um novo equipamento o técnico que estiver controlando a perfuratriz deve ser comunicado e deve autorizar a entrada. Perfuratriz • Devem existir câmeras em quantidade e posição suficientes que permitam a visualização em 360 graus ao redor da perfuratriz. • Sempre que possível, no modo local, deve existir um aviso sonoro quanto à aproximação da perfuratriz a equipamentos e barreiras. • Sempre que possível, emitir avisos sonoros quando da movimentação da perfuratriz. • Deve sempre existir na perfuratriz um botão para parada total do equipamento em caso de emergência. Redes de transmissão de Dados e comunicação • As transmissões de dados referentes às imagens das câmeras devem ser realizadas em rede protegida. • Sempre que possível, manter as imagens das câmeras em rede privada reduzindo a possibilidade de invasões.

Tabela 26: Fatores causais que podem levar o TM a inclinar a broca sobre / muito próxima a outros equipamentos ou barreiras. (Continua)

Inclinar broca sobre / muito próximo de outros equipamentos ou barreiras – Modo Local (ACI-TM-04)		
Cenário	Fator Causal Associado	Racional
O técnico não percebe a entrada de novos equipamentos na área de perfuração.	Equipamentos desconhecidos dentro da área de perfuração.	É grande a movimentação de equipamentos dentro da área de lavra, principalmente veículos de pequeno porte.
O técnico não tem a visibilidade de todo o entorno da perfuratriz durante a movimentação.	Pontos cegos no entorno do equipamento.	Dentro da cabine de controle não é possível perceber todo o entorno do equipamento.
As imagens das câmeras ao redor do equipamento são alteradas por agente malicioso.	Alteração indevida das imagens de campo.	Câmeras digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
O Técnico deixa de observar alguma câmera ou o entorno da perfuratriz.	Falta de atenção do técnico durante as movimentações.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Movimentação do equipamento não obedece aos comandos do técnico por falha no manete de comando.	Falha na manete de comando.	Travamentos ou outros problemas eletromecânicos podem levar o equipamento a operações inesperadas.

Tabela 26: Fatores causais que podem levar o TM a inclinar a broca sobre / muito próxima a outros equipamentos ou barreiras. (Conclusão)

Ações Mitigadoras
Organizacionais / procedimentos de trabalho • Deve ser restrita a entrada de equipamentos na área de perfuração. • Sempre que se fizer necessária a entrada de um novo equipamento o técnico que estiver controlando a perfuratriz deve ser comunicado e autorizar a entrada. Perfuratriz • Devem existir câmeras em quantidade e posição suficientes que permitam a visualização em 360 graus ao redor da perfuratriz. • Sempre que possível, no modo local, deve existir um aviso sonoro quanto à aproximação do mastro da perfuratriz a equipamentos e barreiras. • Sempre que possível, emitir avisos sonoros quando da movimentação do mastro da perfuratriz. • Deve sempre existir na perfuratriz um botão para parada total do equipamento em caso de emergência. Redes de transmissão de dados e comunicação • As transmissões de dados referentes às imagens das câmeras devem ser realizadas em rede protegida. • Sempre que possível, manter as imagens das câmeras em rede privada reduzindo a possibilidade de invasões.

Tabela 27: Fatores causais que podem levar o TM a aprovar área com irregularidades no solo.

Aprovar área com irregularidades no solo (ACI-TM-05)		
Cenário	Fator Causal Associado	Racional
Técnico avalia erroneamente a área a ser liberada para a perfuratriz.	Erro em virtude de critérios de avaliação não claros.	Critérios não claros podem levar a decisões incorretas.
Técnico aprova área irregular por estar sob pressão operacional.	Decisão incorreta devido à pressão operacional.	Pressão operacional acerca da produção do equipamento pode levar o técnico a tomar uma decisão equivocada.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho • Os critérios para avaliação das áreas devem ser claros e objetivos e previstos no procedimento específico evitando sempre critérios genéricos. • A proibição de aprovação de área “não conforme” deve existir explicitamente e ser de conhecimento de todos que possuem alguma interface com o técnico em mineração. • Elaborar plano de treinamento e manter todos os profissionais com os treinamentos atualizados. • Elaborar plano de treinamento e manter todos os profissionais com os treinamentos atualizados no que diz respeito aos critérios de avaliação de área de perfuração.		

Tabela 28: Fatores causais que podem levar o TM a movimentar a perfuratriz com a lança fora da posição.

Movimentar Perfuratriz com lança fora da posição – Modo Local - (ACI-TM-06)		
Cenário	Fator Causal Associado	Racional
Técnico desconhece os ângulos limite para cada movimento da perfuratriz.	Falta de conhecimento / treinamento.	Os requisitos referentes a limites do equipamento devem ser de conhecimento do técnico.
Sensor de inclinação apresenta valor incorreto.	Defeitos no sensor de inclinação.	Informações incorretas do instrumento pode levar a decisões equivocadas.
Ações Mitigadoras		
Perfuratriz - Os valores dos ângulos limites devem estar de fácil acesso na cabine de operação. - Devem existir referências físicas (ex.: demarcações com placas, sinais ou instrumentação mecânica) acerca do ângulo em que o mastro da perfuratriz se encontra. - Elaborar plano de treinamento e manter todos os profissionais atualizados no que diz respeito à operação da perfuratriz. PLC - Deve existir intertravamentos no PLC que impeça a movimentação da perfuratriz com a lança fora da posição.		

Tabela 29: Fatores causais que podem levar o TM a movimentar a perfuratriz em área não apropriada.

Movimentar perfuratriz em área não apropriada – Modo Local - (ACI-TM-07)		
Cenário	Fator Causal Associado	Racional
Técnico desconhece ou não compreende os critérios para movimentação da perfuratriz.	Falta de conhecimento / treinamento.	Os requisitos referentes a limites do equipamento devem ser de conhecimento do técnico.
Técnico movimenta equipamento em área irregular por pressões operacionais.	Decisão incorreta devido à pressão operacional.	Pressão operacional acerca da produção do equipamento pode levar o técnico a tomar uma decisão equivocada.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho. • Os critérios para movimentação da perfuratriz devem ser claros, objetivos e previstos no procedimento específico, evitando sempre critérios genéricos. • A proibição da movimentação da perfuratriz em área não apropriada deve existir explicitamente e ser de conhecimento de todos que possuem alguma interface com o técnico em mineração. • Elaborar plano de treinamento e manter todos os profissionais atualizados no que diz respeito à operação da perfuratriz.		

Tabela 30: Fatores causais que podem levar o TM a inclinar a broca para um ângulo diferente do previsto / permitido.

Inclinar broca para um ângulo diferente do previsto / permitido – Modo Local - (ACI-TM-08)		
Cenário	Fator Causal Associado	Racional
Técnico desconhece os critérios para movimentação da perfuratriz.	Falta de conhecimento / treinamento.	Os requisitos referentes a limites do equipamento devem ser de conhecimento do técnico.
Técnico movimenta equipamento de maneira irregular por pressões operacionais.	Decisão incorreta devido à pressão operacional.	Pressão operacional acerca da produção do equipamento pode levar o técnico a tomar uma decisão equivocada.
Sensor de inclinação apresenta valor incorreto.	Defeitos no sensor de inclinação.	Informações incorretas do instrumento pode levar a decisões equivocadas.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho - Os critérios para inclinação da perfuratriz devem ser claros, objetivos e previstos no procedimento específico, evitando sempre critérios genéricos. - A proibição de inclinação do mastro fora dos limites especificados ser de conhecimento de todos que possuem alguma interface com o técnico em mineração. - Elaborar plano de treinamento e manter todos os profissionais atualizados no que diz respeito à operação da perfuratriz. Perfuratriz - Os valores dos ângulos limites devem estar de fácil acesso na cabine de operação. - Devem existir referências físicas (ex.: demarcações com placas, sinais ou instrumentação mecânica) acerca do ângulo em que o mastro da perfuratriz se encontra.		

Tabela 31: Fatores causais que podem levar o OCC a não acionar a emergência em caso de a perfuratriz entrar em situação de emergência. (Continua)

Não acionar em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-01)		
Cenário	Fator Causal Associado	Racional
O operador não reconhece o evento como emergência.	Falta de clareza quanto ao que é ou não uma anormalidade operacional a ponto de acionar a emergência.	As situações de emergência devem ser claras.
Operador não vê o evento de emergência.	Falta de atenção por parte do operador.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
As imagens das câmeras e supervisório não são fidedignas com a realidade do processo.	As imagens das câmeras e supervisório são alteradas por algum agente malicioso.	Sistemas digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
Operador envia comando, mas não é percebido pelos controladores.	Falhas de rede impedem de enviar os comandos.	Falhas nas redes podem impedir o bom funcionamento da comunicação entre os controladores.
O operador aciona a emergência, mas existe um problema no botão de emergência.	Defeito na botoeira ou cabos.	Falhas em dispositivos eletromecânicos.

Tabela 31: Fatores causais que podem levar o OCC a não acionar a emergência em caso de a perfuratriz entrar em situação de emergência. (Conclusão)

Ações Mitigadoras
Organizacionais / procedimentos de trabalho - Os critérios para emergência devem ser claros e objetivos e previstos no procedimento específico, evitando sempre critérios genéricos. Centro de Controle - Deve-se evitar ao máximo a ausência do operador do centro de controle e quando da existência de alguma perfuratriz em operação e quando possível possuir avisos sonoros em caso de emergência. - Deve existir mais de um atuador para acionamento da emergência. PC Industrial - A perfuratriz, deve possuir gatilhos para interrupção da operação de forma segura sem a intervenção do operador em casos de emergência ou risco. - Sempre que houver uma perda da comunicação entre o centro de controle e a perfuratriz, esta deve realizar a interrupção da operação de maneira segura.

Tabela 32: Fatores causais que podem levar o OCC a acionar a emergência tardiamente em situação de emergência.

Acionar tardiamente em caso de a perfuratriz entrar em situação de emergência (ACI-OCC-02)		
Cenário	Fator Causal Associado	Racional
O operador não reconhece rapidamente o evento como emergência.	Falta de clareza quanto ao que é ou não uma anormalidade operacional a ponto de acionar a emergência.	As situações de emergência devem ser claras.
Operador não vê a tempo o evento de emergência.	Falta de atenção por parte do operador.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
As imagens das câmeras e supervisório não são fidedignas com a realidade do processo.	As imagens das câmeras e supervisório são alteradas por algum agente malicioso.	Sistemas digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
Operador envia comando, mas não é percebido pelos controladores.	Lentidões na rede impedem de enviar os comandos.	Falhas nas redes podem impedir o bom funcionamento da comunicação entre os controladores.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho Os critérios para emergência devem ser claros, objetivos e previstos no procedimento específico, evitando sempre critérios genéricos.		
Centro de Controle - Deve-se evitar ao máximo a ausência do operador do centro de controle e quando da existência de alguma perfuratriz em operação possuir, quando possível, avisos sonoros em caso de emergência. - Deve existir mais de um atuador para acionamento da emergência.		
PC industrial - A perfuratriz deve possuir gatilhos para interrupção da operação de forma segura, sem a intervenção do operador em casos de emergência ou risco. - Sempre que houver uma perda da comunicação entre o centro de controle e a perfuratriz esta deve realizar a interrupção da operação de maneira segura.		

Tabela 33: Fatores causais que podem levar o OCC a enviar as coordenadas incorretas para o PC Industrial.

Enviar coordenadas incorretas para o PC Industrial (ACI-OCC-03)		
Cenário	Fator Causal Associado	Racional
Operador se equivoca e envia dados incorretos para a perfuratriz.	Falta de atenção por parte do operador.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Os dados recebidos pelo plano de fogo estão corretos, porém são alterados por algum agente malicioso.	Dados do plano de fogo são alterados por algum agente malicioso.	Sistemas digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho • O plano de fogo a ser executado pela perfuratriz deve ser validado pelo operador antes da sua autorização para execução. PC Industrial • O PC Industrial deve possuir um mecanismo de análise de consistência de dados recebidos pelo centro de controle. • Os dados referentes ao envio de coordenadas devem ser trafegados em rede segura.		

Tabela 34: Fatores causais que podem levar o OCC a movimentar a perfuratriz não respeitando os limites do polígono quando operando em modo remoto.

Movimentar em excesso e não respeitar os limites do polígono (modo remoto) - (ACI-OCC-04)		
Cenário	Fator Causal Associado	Racional
Operador não observa que a perfuratriz saiu dos limites e continua avançando.	Falta de atenção.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Operador perde a comunicação com a perfuratriz durante o comando de avanço	Por problemas de rede a comunicação é interrompida.	Falhas por problemas nos equipamentos ou posicionamentos ou antenas de transmissão / recepção de dados.
Por falha no GPS, a posição da perfuratriz é determinada incorretamente.	Equipamento com defeito.	Todo equipamento é passível de falhas.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho • Elaborar plano de treinamento e manter todos os profissionais atualizados no que diz respeito à operação da perfuratriz. • Sempre que possível, durante a operação remota devem possuir leras ou outras barreiras físicas durante a operação remota. Perfuratriz • Devem existir câmeras em quantidade e posição suficientes que permitam a visualização em 360 graus ao redor da perfuratriz. GPS • Devem ser testados a calibração e o funcionamento do GPS, periodicamente. PC Industrial • A movimentação da perfuratriz fora dos limites estabelecidos deve ser restrita a movimentações locais. • A perfuratriz deve possuir gatilhos para interrupção da operação de forma segura sem a intervenção do operador em casos de emergência ou risco.		

Tabela 35: Autorizar operação com equipamentos indevidos na área de perfuração.

Autorizar com equipamentos indevidos na área de perfuração (ACI-OCC-05)		
Cenário	Fator Causal Associado	Racional
O operador do centro de controle não percebe a entrada de novos equipamentos na área de perfuração.	Equipamentos desconhecidos dentro da área de perfuração.	É grande a movimentação de equipamentos dentro da área de lavra, principalmente veículos de pequeno porte.
O operador do centro de controle não tem a visibilidade de todo o entorno da perfuratriz durante a movimentação.	Pontos cegos no entorno do equipamento.	Dentro da cabine de controle não é possível perceber todo o entorno do equipamento.
As imagens das câmeras ao redor do equipamento são alteradas por agente malicioso.	Alteração indevida das imagens de campo.	Câmeras digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
O operador do centro de controle deixa de observar alguma câmera ou o entorno da perfuratriz.	Falta de atenção do operador.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho • Deve ser restrita a entrada de equipamentos na área de perfuração. • Sempre que se fizer necessária a entrada de um novo equipamento e o equipamento estiver operando remotamente o operador do centro de controle deve ser comunicado e autorizar a entrada. Perfuratriz • Devem existir câmeras em quantidade e posição suficientes que permitam a visualização em 360 graus ao redor da perfuratriz. • Sempre que possível, e a perfuratriz estiver em modo remoto, deve existir um aviso sonoro no centro de controle quanto à aproximação da perfuratriz a equipamentos e barreiras. Redes de transmissão de dados e comunicação • As transmissões de dados referentes às imagens das câmeras devem ser realizadas em rede protegida. • Sempre que possível, manter as imagens das câmeras em rede privada reduzindo a possibilidade de invasões.		

Tabela 36: Fatores causais possíveis para o OCC autorizar a operação da perfuratriz sem que a área e os equipamentos estejam prontos.

Autorizar sem a área / equipamentos estarem prontos (ACI-OCC-06)		
Cenário	Fator Causal Associado	Racional
Operador do centro de controle não percebe equipamentos ou praça em manutenção / preparação.	Falta de atenção do técnico durante as movimentações.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos.
As imagens das câmeras ao redor do equipamento são alteradas por agente malicioso.	Alteração indevida das imagens de campo.	Câmeras digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho • Imediatamente antes de autorizar a operação autônoma ou movimentar a perfuratriz, o operador do centro de controle deve confirmar a condição da área com o técnico de campo. Redes de transmissão de dados e comunicação • As transmissões de dados referentes às imagens das câmeras devem ser realizadas em rede protegida.		

Tabela 37: Fatores causais para o OCC movimentar a perfuratriz sobre algum equipamento

Movimentar perfuratriz sobre algum equipamento (modo remoto) (ACI-OCC-07)		
Cenário	Fator Causal Associado	Racional
O operador do centro de controle não percebe a entrada de novos equipamentos na área de perfuração.	Equipamentos desconhecidos dentro da área de perfuração.	É grande a movimentação de equipamentos dentro da área de lavra, principalmente veículos de pequeno porte.
O operador do centro de controle não tem a visibilidade de todo o entorno da perfuratriz durante a movimentação.	Pontos cegos no entorno do equipamento.	Dentro do centro de controle toda a visualização da área periférica à perfuratriz é feita através das câmeras.
As imagens das câmeras ao redor do equipamento são alteradas por agente malicioso.	Alteração indevida das imagens de campo	Câmeras digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
O operador do centro de controle deixa de observar alguma câmera ou o entorno da perfuratriz.	Falta de atenção do técnico durante as movimentações.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Movimentação do equipamento não obedece corretamente aos comandos do operador do centro de controle.	Alteração dos comandos por algum agente malicioso.	Controladores (comandos) informatizados possuem risco de possuírem problemas relacionados à segurança digital.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho • Deve ser restrita a entrada de equipamentos na área de perfuração. • Sempre que se fizer necessária a entrada de um novo equipamento, o técnico que estiver controlando a perfuratriz deve ser comunicado e autorizar a entrada. Perfuratriz • Devem existir câmeras em quantidade e posição suficientes que permitam a visualização em 360 graus ao redor da perfuratriz. • Sempre que possível, no modo remoto, deve existir um aviso sonoro no centro de controle quanto à aproximação da perfuratriz a equipamentos e barreiras. Redes de transmissão de dados e comunicação • As transmissões de dados referentes às imagens das câmeras devem ser realizadas em rede protegida.		

Tabela 38: Fatores causais possíveis para o OCC inclinar o mastro sobre ou muito próximo de outros equipamentos. (Continua)

Inclinar broca sobre / muito próximo de outros equipamentos (ACI-OCC-08)		
Cenário	Fator Causal Associado	Racional
O operador do centro de controle não percebe a entrada de novos equipamentos na área de perfuração.	Equipamentos desconhecidos dentro da área de perfuração.	É grande a movimentação de equipamentos dentro da área de lavra, principalmente veículos de pequeno porte.
O operador do centro de controle não tem a visibilidade de todo o entorno da perfuratriz durante a movimentação.	Pontos cegos no entorno do equipamento.	Dentro do centro de controle toda a visualização da área periférica à perfuratriz é feita através das câmeras.
As imagens das câmeras ao redor do equipamento são alteradas por agente malicioso.	Alteração indevida das imagens de campo.	Câmeras digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
O operador do centro de controle deixa de observar alguma câmera ou o entorno da perfuratriz.	Falta de atenção do técnico durante as movimentações.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Movimentação do equipamento não obedece corretamente aos comandos do operador do centro de controle.	Alteração dos comandos por algum agente malicioso.	Controladores (comandos) informatizados possuem risco de possuírem problemas relacionados à segurança digital.

Tabela 38: Fatores causais possíveis para o OCC inclinar o mastro sobre ou muito próximo de outros equipamentos. (Conclusão)

Ações Mitigadoras
Organizacionais / procedimentos de trabalho • Deve ser restrita a entrada de equipamentos na área de perfuração. • Sempre que se fizer necessária a entrada de um novo equipamento, o operador do centro de controle que estiver controlando a perfuratriz deve ser comunicado autorizar a entrada. Perfuratriz • Devem existir câmeras em quantidade e posição suficientes que permitam a visualização em 360 graus ao redor da perfuratriz. • Sempre que possível, no modo local, deve existir um aviso sonoro quanto à aproximação do mastro da perfuratriz a equipamentos e barreiras. • Sempre que possível, emitir avisos sonoros quando da movimentação do mastro da perfuratriz. • Deve sempre existir na perfuratriz um botão para parada total do equipamento em caso de emergência. Redes de transmissão de dados e comunicação • As transmissões de dados referentes às imagens das câmeras devem ser realizadas em rede protegida. • Sempre que possível, manter as imagens das câmeras em rede privada reduzindo a possibilidade de invasões.

Tabela 39: Fatores causais possíveis para o OCC movimentar a perfuratriz com o mastro fora da posição prevista

Movimentar Perfuratriz com lança fora da posição (ACI-OCC-09)		
Cenário	Fator Causal Associado	Racional
Operador do centro de controle desconhece os ângulos limite para cada movimento da perfuratriz.	Falta de conhecimento / treinamento.	Os requisitos referentes a limites do equipamento devem ser de conhecimento do operador do centro de controle.
Sensor de inclinação apresenta valor incorreto.	Defeitos no sensor de inclinação.	Informações incorretas do instrumento pode levar a decisões equivocadas.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho - Os valores dos ângulos limites devem estar de fácil acesso no centro de controle. PLC - Deve existir intertravamentos no PLC que impeçam a movimentação da perfuratriz com a lança fora da posição.		

Tabela 40: Fatores causais possíveis para o OCC movimentar a perfuratriz em área irregular.

Movimentar perfuratriz em área inclinada ou irregular (ACI-OCC-10)		
Cenário	Fator Causal Associado	Racional
Operador movimenta a perfuratriz no modo remoto sem conhecer o procedimento de condições de praça.	Falta de instrução ou treinamento.	A falta de conhecimento pode levar o colaborador a realizar as atividades incorretamente.
Operador movimenta a perfuratriz acreditando que a praça está em boas condições.	Falha na comunicação entre os colaboradores.	O mal entendimento das informações prestadas de um controlador a outro podem gerar ações inesperadas.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho - Imediatamente, antes de autorizar a operação autônoma ou movimentar a perfuratriz, o operador do centro de controle deve confirmar a condição da área com o técnico de campo. Perfuratriz - Devem existir câmeras em quantidade e posição suficientes que permitam a visualização em 360 graus ao redor da perfuratriz.		

Tabela 41: Fatores causais para o OCC inclinar o mastro para um ângulo diferente do previsto ou permitido.

Inclinar broca para um ângulo diferente do previsto / permitido (ACI-OCC-11)		
Cenário	Fator Causal Associado	Racional
Operador do centro de controle desconhece os critérios para inclinar mastro da perfuratriz.	Falta de conhecimento / treinamento	Os requisitos referentes a limites do equipamento devem ser de conhecimento do técnico.
Técnico movimenta equipamento de maneira irregular por pressões operacionais.	Decisão incorreta devido à pressão operacional.	Pressão operacional acerca da produção do equipamento pode levar o técnico a tomar uma decisão equivocada.
Sensor de inclinação apresenta valor incorreto.	Defeitos no sensor de inclinação.	Informações incorretas do instrumento podem levar a decisões equivocadas.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho - Os critérios para inclinação do mastro perfuratriz devem ser claros e objetivos e previstos no procedimento específico evitando sempre critérios genéricos. - A proibição de inclinação do mastro fora dos limites especificados ser de conhecimento de todos que possuem alguma interface com o técnico em mineração. - Elaborar plano de treinamento e manter todos os profissionais atualizados no que diz respeito à operação da perfuratriz. Centro de Controle - Os valores dos ângulos limites devem estar de fácil acesso no centro de controle. PLC - Deve existir intertravamentos no PLC que impeçam a inclinação do mastro da perfuratriz fora dos critérios de segurança pré-estabelecidos.		

Tabela 42: Fatores casuais podem levar o controlador de segurança a não acionar a emergência em caso de emergência.

Não acionar em caso de emergência (ACI-CS-01)		
Cenário	Fator Causal Associado	Racional
Controlador de segurança não consegue enviar comando de emergência por falha de comunicação.	Interrupções no funcionamento da rede.	Falhas por problemas nos equipamentos ou posicionamentos ou antenas de transmissão / recepção de dados.
Falha na comunicação entre os controladores não é percebida por ação de agente malicioso.	Agente malicioso simula o bom funcionamento da comunicação mesmo quando esta é interrompida.	Equipamentos informatizados possuem risco de possuírem problemas relacionados à segurança digital.
Ações Mitigadoras		
Controlador de Segurança - Sempre que perceber a falha de comunicação deve ser reportado ao operador do centro de controle a anomalia. PC Industrial - Sempre que perceber a falha de comunicação com o PLC ou controlador de Segurança este deve iniciar o procedimento de parada segura. PLC - Sempre que perceber a falha de comunicação com o PC industrial ou controlador de Segurança este deve iniciar o procedimento de parada segura. Redes de transmissão de Dados e comunicação - As transmissões de dados referentes à emergência ou segurança devem ser prioritárias na rede e constantemente monitoradas. - A comunicação referente aos status de segurança e comunicação entre os diversos controladores devem ocorrer de maneira a evitar a ação de agentes maliciosos e quando possível em rede privada, evitando assim a ação de agentes externos.		

Tabela 43: Fatores casuais podem levar o controlador de segurança a acionar tardiamente a emergência em caso de emergência operacional.

Acionar tardiamente em caso de emergência operacional (ACI-CS-02)		
Cenário	Fator Causal Associado	Racional
Controlador de segurança não consegue enviar comando de emergência rapidamente por lentidões na rede.	Interrupções no funcionamento da rede.	Falhas por problemas nos equipamentos ou posicionamentos ou antenas de transmissão / recepção de dados.
Ações Mitigadoras		
Redes de transmissão de dados e comunicação - As transmissões de dados referentes à emergência ou segurança devem ser prioritárias na rede e constantemente monitoradas. PC Industrial - O tratamento dos comandos de segurança e emergência devem ter ação prioritária. PLC - O tratamento dos comandos de segurança e emergência devem ter ação prioritária.		

Tabela 44: Fatores causais para o PC industrial definir a direção do movimento incorretamente.

Definir a direção de movimento incorretamente (ACI-PCI-01)		
Cenário	Fator Causal Associado	Racional
Operador se equivoca e envia dados incorretos para a perfuratriz.	Falta de atenção por parte do operador.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Os dados recebidos pelo plano de fogo estão corretos, porém são alteradas por algum agente malicioso.	Dados do plano de fogo são alterados por algum agente malicioso.	Sistemas digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
Por falha no GPS, a posição da perfuratriz é determinada incorretamente.	Equipamento com defeito.	Todo equipamento é passível de falhas.
Transmissão de dados do GPS é indevidamente alterada por agente malicioso.	Alteração indevida dos dados da posição atual da perfuratriz.	Dados que trafegam na rede correm risco de segurança digital.
Ações Mitigadoras		
GPS - Devem ser testados a calibração e o funcionamento do GPS, periodicamente. PC Industrial - O PC Industrial deve possuir um mecanismo de análise de consistência de dados recebidos pelo centro de controle. - Os dados referentes ao envio de coordenadas devem ser trafegados em rede segura.		

Tabela 45: Fatores causais para o PC industrial definir a distância do movimento incorretamente.

Definir a direção de movimento incorretamente (ACI-PCI-01)		
Cenário	Fator Causal Associado	Racional
Operador se equivoca e envia dados incorretos para a perfuratriz.	Falta de atenção por parte do operador.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Os dados recebidos pelo plano de fogo estão corretos, porém são alterados por algum agente malicioso.	Dados do plano de fogo são alterados por algum agente malicioso.	Sistemas digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
Por falha no GPS, a posição da perfuratriz é determinada incorretamente.	Equipamento com defeito.	Todo equipamento é passível de falhas.
Transmissão de dados do GPS é indevidamente alterada por agente malicioso.	Alteração indevida dos dados da posição atual da perfuratriz.	Dados que trafegam na rede correm risco de segurança digital.
Ações Mitigadoras		
GPS - Devem ser testados a calibração e o funcionamento do GPS, periodicamente. PC Industrial - O PC Industrial deve possuir um mecanismo de análise de consistência de dados recebidos pelo centro de controle. - Os dados referentes ao envio de coordenadas devem ser trafegados em rede segura.		

Tabela 46: Fatores causais para definir PC industrial definir o angulo do mastro acima ou abaixo do angulo permitido.

Definir ângulo acima ou abaixo do ângulo permitido. (ACI-PCI-03)		
Cenário	Fator Causal Associado	Racional
Operador se equivoca e envia dados incorretos para a perfuratriz	Falta de atenção por parte do operador.	Por se tratar de um controlador humano, causas relacionadas a fatores emocionais ou físicos podem ocorrer.
Os dados recebidos pelo plano de fogo estão corretos, porém são alteradas por algum agente malicioso	Dados do plano de fogo são alteradas por algum agente malicioso	Sistemas digitais são passíveis de falhas e/ou invasões que manipulem seu funcionamento normal.
Por falha no inclinômetro a posição do mastro é desconhecida pelo PC industrial	Equipamento com defeito	Todo equipamento é passível de falhas
Ações Mitigadoras		
Inclinômetro: • Deve se possuir redundância do senso de inclinação do mastro, quando possível, que utilizem diferentes configurações ou princípios tecnológicos. PC Industrial: • O PC Industrial deve possuir um mecanismo de análise de consistência de dados recebidos pelo centro de controle. • Os dados referentes ao envio de coordenadas devem ser trafegados em rede segura.		

Tabela 47: Fatores causais para o PLC movimentar a perfuratriz na direção diferente da prevista.

Movimentar a perfuratriz na direção diferente da prevista (ACI-PLC-01)		
Cenário	Fator Causal Associado	Racional
PLC envia comando para acionamento para uma direção e a perfuratriz se movimenta em outra	Falha na configuração dos inversores ou relés	Falhas na configuração dos acionamentos podem gerar execuções incorretas das ações solicitadas pelo PLC
Acionamento recebe informação de direção do movimento diferente da enviada pelo PLC	Comandos enviados via rede de comunicação são alterados por agentes maliciosos.	Dados que trafegam na rede correm risco de segurança digital
Ações Mitigadoras		
PC Industrial: - O PC Industrial deve sempre verificar se os movimentos que são solicitados ao PLC são executados corretamente, parando o equipamento em emergência em casos anormais. Redes de transmissão de Dados e comunicação: - A comunicação entre o PLC e acionamentos deve ocorrer quando possível em rede isolada, ou com segurança contra agentes externos.		

Tabela 48: Fatores causais para o PLC não interromper a tempo a movimentação quando atingido a posição esperada.

Não interromper a tempo a movimentação quando atingido a posição esperada (ACI-PLC-02)		
Cenário	Fator Causal Associado	Racional
Por falha no GPS, os a posição da perfuratriz e determinada incorretamente	Equipamento com defeito	Todo equipamento é passível de falhas
Transmissão de dados do GPS é indevidamente alterada por agente malicioso	Alteração indevida dos dados da posição atual da perfuratriz	Dados que trafegam na rede correm risco de segurança digital
Transmissão de dados entre CLP / PC industrial e acionamentos são indevidamente alteradas	Dados alterados por agente malicioso	Dados que trafegam na rede correm risco de segurança digital
PLC não recebe as informações do PC Industrial quando do termino da movimentação	Falhas de comunicação	Falhas de comunicação entre dispositivos podem ocorrer de maneira inesperada
Durante a execução do movimento a comunicação entre o acionamento e o PLC é perdida	Falhas de comunicação	Falhas de comunicação entre dispositivos podem ocorrer de maneira inesperada
Ações Mitigadoras		
GPS: - Devem ser testados a calibração e o funcionamento do GPS, periodicamente. Acionamentos - Sempre que ocorrer falha de comunicação entre os controladores o acionamento deve interromper o movimento em condição de emergência. Redes de transmissão de dados e comunicação - A comunicação entre o GPS, PLC, PC industrial e acionamentos deve ocorrer quando possível em rede isolada, ou com segurança contra agentes externos.		

Tabela 49: Fatores causais para o PLC movimentar a perfuratriz na direção de algum equipamento ou obstáculo quando este estiver próximo.

Movimentar na direção de algum equipamento ou obstáculo quando estiver próximo (ACI-PLC-03)		
Cenário	Fator Causal Associado	Racional
Sensor e / ou câmera não reconhece a presença do obstáculo próximo.	Falha no equipamento.	Todo equipamento é passível de falhas.
Transmissão de dados da câmera é indevidamente alterada por agente malicioso.	Agente malicioso adultera os dados do equipamento.	Dados que trafegam na rede correm risco de segurança digital.
PLC não recebe as informações do PC Industrial quando do término da movimentação.	Falhas de comunicação.	Falhas de comunicação entre dispositivos podem ocorrer de maneira inesperada.
Durante a execução do movimento a comunicação entre o acionamento e o PLC é perdida.	Falhas de comunicação.	Falhas de comunicação entre dispositivos podem ocorrer de maneira inesperada.
Ações Mitigadoras		
Organizacionais / procedimentos de trabalho - Sempre que possível a área a ser perfurada deve estar livre de agentes externos. Acionamentos - Sempre que ocorrer falha de comunicação entre os controladores o acionamento deve interromper o movimento em condição de emergência. Redes de transmissão de dados e comunicação: - A comunicação entre o GPS, PLC, PC industrial e acionamentos deve ocorrer quando possível em rede isolada, ou com segurança contra agentes externos.		

Tabela 50: Fatores causais para o PLC movimentar a perfuratriz com o mastro fora da posição.

Movimentar perfuratriz com o mastro fora da posição (ACI-PLC-04)		
Cenário	Fator Causal Associado	Racional
Inclinômetro não indica corretamente o ângulo do mastro.	Falha no equipamento.	Todo equipamento é passível de falhas.
PLC solicita a movimentação da perfuratriz com mastro na posição incorreta.	Falhas na programação.	Programação ou inabilidade ou inadvertência do programador.
Comandos aos acionamentos gerados pelo PLC é indevidamente alterada por agente malicioso.	Agente malicioso adultera os dados do equipamento.	Dados que trafegam na rede correm risco de segurança digital.
Ações Mitigadoras		
Inclinômetro - Deve se possuir redundância do senso de inclinação do mastro, quando possível, que utilizem diferentes configurações ou princípios tecnológicos. PC Industrial - Sempre que ocorrer falha de comunicação entre os controladores o acionamento deve interromper o movimento em condição de emergência. - Toda movimentação do equipamento solicitada pelo PLC deve ser “auditada” pelo PC industrial e em caso de anormalidade o equipamento deve interromper o movimento e parar em condição de emergência. Redes de transmissão de dados e comunicação: - A comunicação entre o GPS, PLC, PC industrial e acionamentos deve ocorrer quando possível em rede isolada, ou com segurança contra agentes externos.		

Tabela 51: Fatores causais para o PLC movimentar o mastro para um ângulo diferente do previsto / permitido.

Inclinar broca para um ângulo diferente do previsto / permitido (ACI-PLC-05)		
Cenário	Fator Causal Associado	Racional
Inclinômetro não indica corretamente o ângulo do mastro.	Falha no equipamento.	Todo equipamento é passível de falhas.
PLC solicita a movimentação do mastro não observando os requisitos operacionais.	Falhas na programação.	Programação ou inabilidade ou inadvertência do programador.
Comandos aos acionamentos gerados pelo PLC indevidamente alterado por agente malicioso.	Agente malicioso adultera os dados do equipamento.	Dados que trafegam na rede correm risco de segurança digital.
Ações Mitigadoras		
Inclinômetro • Deve se possuir redundância do senso de inclinação do mastro, quando possível, que utilizem diferentes configurações ou princípios tecnológicos. PC Industrial • Sempre que ocorrer falha de comunicação entre os controladores o acionamento deve interromper o movimento em condição de emergência. • Toda movimentação do equipamento solicitada pelo PLC deve ser “auditada” pelo PC industrial e em caso de anormalidade o equipamento deve interromper o movimento e parar em condição de emergência. Redes de transmissão de dados e comunicação • A comunicação entre o GPS, PLC, PC industrial e acionamentos deve ocorrer quando possível em rede isolada, ou com segurança contra agentes externos.		

5.2.5 Análise crítica da abordagem e abrangência

A partir das análises realizadas no tópico 0, relacionados à aplicação da ferramenta, é possível perceber como esta aborda os acidentes em um contexto *top – down*, em outras palavras, a partir de um foco macro de todo o sistema é possível definir ações específicas para evitar os acidentes, no caso deste trabalho, dentro do ambiente de exploração mineral.

Esse tipo de abordagem (*top – down*) é, especialmente, interessante quando tratamos de sistemas complexos, como é o caso da perfuratriz autônoma, foco deste trabalho. Essa complexidade fica bastante evidente quando juntamos sistemas computacionais complexos de automação, tratamento de imagens, entre outros, a controladores e interações humanas.

Equipamentos autônomos requerem uma elevada utilização de softwares e sensores de alta precisão, além da interação com outros equipamentos que não possuem o mesmo nível tecnológico e, em alguns casos, quando as diferentes tecnologias não se interagem. (ABRECHT; LEVESON, 2016) demonstram a aplicação da ferramenta STPA / STPA-sec em grandes embarcações que utilizam softwares complexos para seus sistemas de posicionamento, seja ela tanto para a segurança operacional quanto para a segurança cibernética. Nesse caso, como é o caso da perfuratriz autônoma, fica evidente a grande quantidade de fatores que podem influenciar na segurança do sistema.

Apesar de a perfuratriz possuir a sua operação de maneira autônoma, a interação dos seus controladores com controladores humanos é inevitável. Dessa maneira, tornando o sistema ainda mais complexo. (CASTILHO, 2015) em seu trabalho relacionado à aplicação STPA em operação de aeronaves, evidencia uma característica comportamental dos controladores humanos que é necessidade de experimentar, operar e perceber as diferentes maneiras de interagir com a operação dos equipamentos. Dessa maneira, caracterizando os controladores como algoritmos de controle dinâmico que se adaptam constantemente ao cenário percebido por seus sensores.

Nos tópicos 0 e 0 ficam evidenciadas a amplitude das restrições de segurança e as possíveis ações mitigadoras levantadas. As ações e restrições estão relacionadas a praticamente todos os componentes do sistema, sejam eles, humanos ou computacionais. Esse tipo de amplitude é excelente, uma vez que, conforme já abordado anteriormente neste trabalho, não foca somente em falhas específicas do sistema e sim em um contexto mais

amplo que pode abranger diversas outras análises que visam identificar outras possíveis vulnerabilidades do sistema.

Um ponto de atenção percebido durante a aplicação da ferramenta é a diversidade de maneiras que ela pode ser utilizada. Em primeira análise, essa flexibilidade demonstra a boa aderência da ferramenta a vários tipos de processos, por outro lado, requer do facilitador que estiver conduzindo a abordagem uma maior habilidade, uma vez que diferentes estratégias de execução dos passos podem gerar diferentes resultados.

Dito isso, é possível perceber quão robusta é a abordagem, principalmente em contextos complexos. Essa robustez se dá em virtude da enorme gama de possíveis aplicações e da boa abrangência quando se observa resultados apresentados. Nesse cenário, ferramentas como STPA / STPA-sec se tornam muito relevantes; especialmente dentro do setor mineral, em que até pequenas colisões entre equipamentos, podem gerar resultados catastróficos como a perda de vidas humanas e / ou perdas de grandes valores econômicos e de imagem.

6 CONCLUSÃO

A execução deste trabalho demonstrou como STAMP e suas ferramentas (STPA / STPA-sec) podem ser utilizadas em sistemas complexos com múltiplos controladores (humanos e computacionais) dentro do ambiente de mineração.

Para isso, inicialmente, foi realizada uma abordagem acerca do cenário no qual a ferramenta seria aplicada. Essa fundamentação abrangeu uma visão geral acerca das operações unitárias que compõe o processo de lavra de minérios, além da fundamentação da teoria de sistemas e suas ferramentas atualmente desenvolvidas.

Uma vez contextualizado, foi realizado um estudo sobre o caso no qual as ferramentas STPA e STPA-sec seriam aplicadas. Nesse estudo, foram abrangidas análises acerca do contexto macro que a perfuratriz está inserida, incluindo assim os cenários externos (mercado e governo, por exemplo) e internos (estrutura organizacional) da empresa mineradora. Esse tipo de estudo, principalmente quando se trata de análises de vulnerabilidades, é importante uma vez que ações ou decisões tomadas em âmbitos em uma primeira vista alheios podem influenciar na operação do equipamento.

A partir desses estudos foi realizada a aplicação prática da ferramenta STPA no processo de perfuração executado por uma perfuratriz autônoma pertencente a uma mineradora em Minas Gerais. Como resultado da aplicação foram obtidas diversas restrições de segurança e ações mitigadoras que quando implantadas podem gerar uma maior segurança operacional para a etapa de perfuração das áreas a serem desmontadas no processo de exploração mineral. Dessa maneira, embora os riscos inerentes às atividades de exploração mineral continuem a existir, é possível mitigar boa parte deles a partir da abordagem apresentada por este trabalho.

Nesse sentido, este trabalho deixa como contribuição para o meio acadêmico e industrial, um estímulo para uma maior exploração da abordagem STAMP no aumento da segurança operacional e cibernética. Além disso, a utilização da ferramenta dentro do ambiente de mineração pode ser considerada outra contribuição feita pelo trabalho, uma vez que existem poucas aplicações práticas dentro dessa indústria. Podendo este trabalho inclusive, servir como um exemplo prático ou referência para engenheiros e pesquisadores dentro da academia e indústria em outras possíveis aplicações.

7 TRABALHOS FUTUROS

Dado à grande flexibilidade e aplicabilidade da abordagem STPA é proposto como trabalho futuro a aplicação da ferramenta em outros pontos do processo de mineração como:

- sistemas SCADA que controlam as plantas de beneficiamento de minérios;
- sistemas de despacho de caminhões (autônomos e convencionais);

Além desses, é proposta também a aplicação da abordagem CAST para reanálise de acidentes operacionais ocorridos previamente.

Dessa maneira contribuindo para o aumento da segurança cibernética e operacional dentro do ambiente de mineração.

REFERÊNCIAS

ABRECHT, B.; LEVESON, N. **Systems Theoretic Process Analysis (STPA) of an Offshore Supply Vessel Dynamic Positioning System**, 2016.

ARNOLD, R. **A qualitative comparative analysis of soam and stamp in atm occurrence investigation**. [s.l.] Lund University, 2009.

BACKLUND, A. The definition of system. **Kybernetes**, v. 29, n. 4, p. 444–451, jun. 2000.

CASTILHO, D. S. **Aplicação da técnica STPA na análise de risco de decolagem de aeronaves leves com vento cruzado limítrofe**. [s.l.] Instituto Tecnológico de Aeronáutica, 2015.

CAT. **Perfuratrizes**.

CHECKLAND, P. **Pensamiento de Sitemas, Práctica de Sistemas**. [s.l: s.n.].

DARLING, P. **SME Mining Engineering Handbook**. [s.l.] Society for Mining, Metallurgy, and Exploration, Inc., 2011.

EI-MOWAFY, A. MACHINE AUTOMATION USING RTK GPS POSITIONING
Department of Spatial Sciences Spatial Data Directorate. p. 1–6, 2009.

FREITAS, S. B. M. **Planejamento estocástico de lavra: metodologias de simulação, otimização e gestão de risco para a mina do futuro**. [s.l.] Universidade de São paulo, 2015.

FREITAS JÚNIOR, L. R. DE. **Otimização de Retomadora de Granéis via Controle Multivariável**Ouro Preto, 2016. Disponível em:
<<http://www.repositorio.ufop.br/handle/123456789/7095>>

GIRODO, A. C.; RONDEAU, S.; SILVA, C. **Projeto APA SUL RMBH - Estudos do Meio Físico**. Belo Horizonte: [s.n.].

HEADRICK, D. Global mining at the edge of transformation. **Research-Technology Management**, 2015.

HUSTRULID, W.; KUCHTA, M.; MARTIN, R. **Open Pit Mine Planning & Design**. 3. ed. [s.l.] CRC Press, [s.d.].

ISHIMATSU, T. et al. Hazard Analysis of Complex Spacecraft Using Systems-Theoretic Process Analysis. **Journal of Spacecraft and Rockets**, v. 51, n. 2, p. 509–522, mar. 2014.

JOY GLOBAL. **No Title.**

KHAN, F. I.; ABBASI, S. A. Techniques and methodologies for risk analysis in chemical process industries. **Journal of Loss Prevention in the Process Industries**, v. 11, n. 4, p. 261–277, 1998.

LEE, C. W. **A System Theoretic Approach to Cybersecurity Risks Analysis of Passenger Autonomous Vehicles.** [s.l.] Massachusetts Institute of Technology, 2018.

LEVESON, N. G. **Engineering a Safer World: Systems Thinking Applied to Safety.** [s.l.: s.n.].

LEVESON, N. G. An STPA Primer. **Version 1**, v. 2013, n. August, p. 80, 2013.

LOPREATO, J.; VON BERTALANFFY, L. General System Theory: Foundations, Development, Applications. **American Sociological Review**, v. 35, n. 3, p. 543, jun. 1970.

Mitsui & Co.

PAPADOPOULOS, Y. et al. Analysis and synthesis of the behaviour of complex programmable electronic systems in conditions of failure. **Reliability Engineering and System Safety**, v. 71, n. 3, p. 229–247, 2001.

PAULA, R. GUIMARÃES DE. **Caracteriação técnico Jurídica da insalubridade e periculosidade e sua aplicação.** [s.l.] USP - Universidade de São Paulo, 2008.

PEPER, N. A. **Systems Thinking Applied to Automation and Workplace Safety by.** [s.l.] Massachusetts Institute of Technology, 2017.

PLACKE, M. S. **Application of STPA to the Integration of Multiple Control Systems: A Case Study and New Approach.** [s.l.] Massachusetts Institute of Technology, 2014.

RALSTON, J. et al. Sensing for advancing mining automation capability: A review of underground automation technology development. **International Journal of Mining Science and Technology**, v. 24, n. 3, p. 305–310, 2014.

ROBERT PEELE. **Mining engineers handbook.** 3. ed. New York: John Wiley & Sons, Inc, 1941.

SAMOST, A. **A Systems Approach to Patient Safety: Preventing and Predicting Medical Accidents Using Systems Theory.** [s.l.] Massachusetts of Tecnology, 2015.

SKYTTNER, L. **General Systems Theory**. London: Macmillan Education UK, 1996.

STEFFEN, O. **Planning of Open Pit Mines**. Australia: Curtin University and University of Western Australia, 2005.

THOMAS, J. **Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis**. [s.l.] Massachusetts Institute of Technology, 2013.

THOMAS, J.; LEVESON, N. Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants. p. 1–66, 2012.

THORNBERRY, C. **Extending the Human-Controller Methodology in Systems-Theoretic Process Analysis**. [s.l.] Massachusetts Institute of Technology, 2014.

WEINBERG, G. M. **An Introduction to General Systems Thinking**. [s.l.: s.n.].

WHITELEY, S. et al. **Webinar Introduction To: Systems Theoretic Accident Modelling & Processes (STAMP)**. Cambridge: 2016