A importância da análise de falhas para o ensino técnico em automação industrial

Resumo: *O artigo averígua algumas falhas técnicas e métodos de investigação de problemas no contexto do estudante e tenta reforçar a importância desse conhecimento não sistematicamente abordado para os cursos técnicos de automação industrial. O trabalho analisa sobre métodos de resolução de problemas, problemas com controladores tipo PID, atuadores, configurações de equipamentos, além de abordar sobre cibersegurança em plantas de automação. O trabalho conclui sobre a importância da sistematização desse conhecimento para a formação profissional e tecnológica, tanto na modalidade integrada, como subsequente, e reforça os variados âmbitos de aplicação dessas habilidades. O artigo considera que tais estudos devem contribuir para a pesquisa e desenvolvimento de recursos didáticos com a finalidade de ajudar a atender essa dificuldade nos currículos desses cursos.*

Frederson Fogaça[1,A], Andre Luis Dias[2], Frederico Fonseca da Silva[3]

1- Instituto Federal Catarinense
2 - Instituto Federal de São Paulo
3 - Instituto Federal do Paraná
A - Contato principal: frederson.fogaca@ifc.edu.br

1. Introdução

Verifica-se no perfil de egresso do profissional técnico em Automação Industrial, no Catálogo Nacional de Cursos Técnicos (CNCT) do MEC (BRASIL, 2007), que o mesmo atende a posições de trabalho como: linhas de produção automatizadas, manutenção e reparos, funções variadas em empresas integradoras de sistemas de automação, entre outras, que denotam um sombreamento comum: a capacidade de, dada uma situação-problema, construir uma lógica de pensamento através do diagnóstico da situação, e então construir um procedimento de solução, único e contextualizado para aquele caso; tal habilidade de análise é primordial para esse ofício.

Os sistemas de automação, como integração entre várias tecnologias de níveis de complexidade e aplicação diferentes que se relacionam de maneira multiforme através de redes industriais diversas, requerem variados aparatos de conversão, diversos tipos de cabeamento, visto que cada rede na indústria requer o meio físico específico de acordo com o seu nível de aplicação, configurações variadas em softwares de diferentes fabricantes, além da estratégia de controle e especificidades de instalação e manuseamento pra cada tecnologia, e tal pluralidade excede a simplicidade de compreensão da perspectiva técnica comum, em razão da quantidade de influências diferentes que o sistema sofre para manter seu funcionamento.

A Indústria 4.0, como é chamada o que a literatura define como uma quarta revolução industrial, que está sendo estudada antes e durante seu acontecimento, é alicerçada fortemente na eficiência e autonomia do processo, busca inteligência dos objetos e interconectividade através da internet (PEREIRA E SIMONETTO, 2018). Nesse cenário, o monitoramento constante de falhas é essencial e feito de maneira inteligente através de sistemas como próprios dessa indústria, que interconectam equipamentos do campo a fim de trocar informações e avaliar constantemente o estado de seus sensores, atuadores e até mesmo da própria rede. (DINARDO, FABBIANO E VACCA, 2018)

Por exemplo, Kurien e Srivastav (2018), usam técnicas de monitoramento de condição

dos equipamentos, como corrente e vibração, para encontrar problemas de processo que resultam vir do estado físico de bombas e válvulas. Também em Dinardo et al. (2018), propõe um sistema diagnóstico de máquinas rotativas monitorando sua vibração. Tal importância de se conhecer a origem dos problemas também é vista por Coughran (2000) para o blog da ISA (*International Society of Automation*), que investiga problemas, a princípio, atribuídos ao controle do processo, mas que se manifestam em elementos improváveis. Mobley (1999) aponta importantes técnicas para sistematizar essa análise e reforça que, sem uma organização lógica dessa análise, há um prejuízo no trabalho efetivo da prática de automação.

Outro assunto importante e transcendente, além de muito novo, visto, inclusive, a natureza dessa nova modalidade de indústria que tá surge, inteligente e altamente interconectada (PEREIRA E SIMONETTO, 2018), é a cyber segurança nos sistemas industriais de controle: a proteção dos elementos como sistemas supervisórios tipo SCADA, CLPs, instrumentos de campos, entre outros - contra invasores e possíveis ataques a planta industrial, o que pode causar não só perdas a produção, como também de recursos humanos. Bhamare et al. (2019), mostram que já há tecnologias de inteligência artificial sendo desenvolvidas para sistemas de detecção de intrusos na rede. Além disso, a pesquisa também mostra a importância desse tema atualmente através de várias pesquisas sobre diferentes abordagens dessas ameaças e propostas de solução.

Vê-se, porém, na construção atual da Proposta Pedagógica Curricular do curso Técnico em Automação Industrial dos Institutos Federais, tanto na sua modalidade subsequente, como integrada ao Ensino Médio, uma fragmentação dos conhecimentos técnicos da área, que não favorece ao aluno uma compreensão integral de aplicação dos conhecimentos (GALLO, 2002). O déficit no pensamento diagnóstico de problemas fica evidente quando essas disciplinas do curso são relacionadas através de projetos integrados que frequentemente resultam em problemas técnicos que excedem o ensino específico de cada disciplina, tal como na indústria, e exige a intervenção de um professor.

O artigo busca, então, a importância desse pensamento diagnóstico nas falhas dos sistemas de controle industrial e, dentro dos limites acadêmicos do foco dessas pesquisas, quais são essas falhas. Ele analisa os problemas técnicos e métodos de investigação de problema nesse contexto do estudante para que, através dessas informações, seja possível a elaboração de um protótipo, com um recorte essencial, e que trabalhe com situações e problemas através de uma abordagem por falhas técnicas, contribuindo para a adequação do ensino à perspectiva do ensino integral e contextualizado em situações e habilidades da vida real, com vistas à incorporação do trabalho como princípio educativo.

2. Referencial Teórico

A educação é uma necessidade básica para o homem se tornar o que é (BORGES, 2017), porque a educação constrói o homem socialmente e o ajuda a instrumentalizar o seu entorno por meio de mediações, de acordo com as suas necessidades. O aprendizado empírico, então, motiva e trabalha essa evolução e deve ser buscado na educação, como maneira de formar o sujeito omnilateralmente (CIAVATTA, 2014), importante conceito nesse trabalho.

Nas instituições de ensino, porém, frequentemente, a metodologia comum fragmenta o ensino de maneira a não favorecer no aluno uma compreensão integral de aplicação dos conhecimentos (GALLO, 2002). Ao invés, então, se deve lutar e contribuir para uma formação onde atividades e experiências integradas mostrem esse retorno positivo no aprendizado

dos alunos e contribuía para o seu sucesso profissional e uma formação de excelência. Sobre a importância dessas práticas transversais em sala de aula pode-se ver em Carvalho e Lacerda (2010) quando tratam sobre o complexo cenário que retrata a modernidade da ciência e tecnologia:

> "... no que diz respeito à formação profissional, diversos autores têm denunciado o descompasso das instituições de ensino para ajustarem-se ao novo modo de produção do conhecimento e para corresponderem às novas demandas sociais relacionadas à citada mudança qualitativa no processo produtivo."

Os autores ainda reiteram que meio a essas novas demandas sociais, há a possibilidade da adequação dos paradigmas de ensino à realidade concreta, para que o ensino se torne, além de significativo, valorado meio aos atuais de produção de conhecimento e tecnologia. Tal necessidade se enquadra no contexto da politécnica, como tratada por Saviani, sendo o domínio tanto de fundamentos científicos quanto de técnicas, e tem uma natureza como bem definida por Moura (2010):

> "... a educação escolar, particularmente o ensino médio deveria propiciar aos estudantes a possibilidade de (re)construção dos princípios científicos gerais sobre os quais se fundamentam a multiplicidade de processos e técnicas que dão base aos sistemas de produção em cada momento histórico."

Bons exemplos podem ser encontrados em trabalhos com o de Martins, Oliveira e Oliveira (2012), que aponta a robótica como ponto de conjugação das diversas áreas de conhecimento presentes no curso, através de um desafio maior, mais próximo da realidade que as disciplinas isoladas e aponta para a autonomia ganhada pelos discentes no processo de participação de competições de robôs.

Também em Oliveira *et al.* (2012), apontam-se no uso de uma planta didática, que conta com processos de nível, vazão, temperatura e pressão, assim como equipamentos para medição e atuação nessas áreas, como objeto de prática dos alunos do curso de engenharia no CEFET - MG, simulando assim, a ideia de atuação em um processo de fabricação real, onde várias redes de automação acontecem ao mesmo tempo e misturados no mesmo espaço e aponta que a planta pode ser aplicada em diversas áreas e atende a muitas atividades, contribuindo positivamente para o aprendizado do aluno e aproximando a sua experiência da prática da indústria.

Tais práticas, se acrescidas das dificuldades reais dentro de uma contextualização possível para a sala de aula, permitiria que se trabalhasse com situações de aprendizagem que adéquam ao mundo real e à visão integral do ensino, seus problemas típicos, falhas recorrentes e natureza complexa.

2.1 Sistemas de Controle Industrial

Os sistemas de controle industrial têm base na Revolução Industrial, no século 19, em seus desdobramentos na mecanização da produção e na gradual substituição da força humana por mecanismos que o poupavam desse desgaste e operavam com mais eficiência em tarefas antes manuais (ZHANG, 2010). Pelos anos 80, esses sistemas já passam a incluir softwares de supervisão de processo e controladores lógicos programáveis (CLPS) - que executam um controle de informações entre sensores e atuadores do processo personalizados por um programador. Pelos anos 90, com o avan ço da microeletrônica, os sistemas de controle industriais começaram a incorporar computadores (ZHANG, 2010).

Nesse tipo de controle, dito embarcado, há um sistema único de *hardware* e *software* que controla, se relaciona como sensores e atuadores e supervisiona o processo. Um tipo importante desse sistema é o controle distribuído: essa estratégia definida como DCS (*Distributed Control Systems*), é um sistema de controle que distribui instrumentos no processo que tem uma capacidade de processamento local e se comunicam entre si (ZHANG, 2010).

A estrutura desses sistemas de automação é composta por camadas que diferenciam entre si através do nível de aplicação dos equipamentos dessa camada no processo (Figura 1).

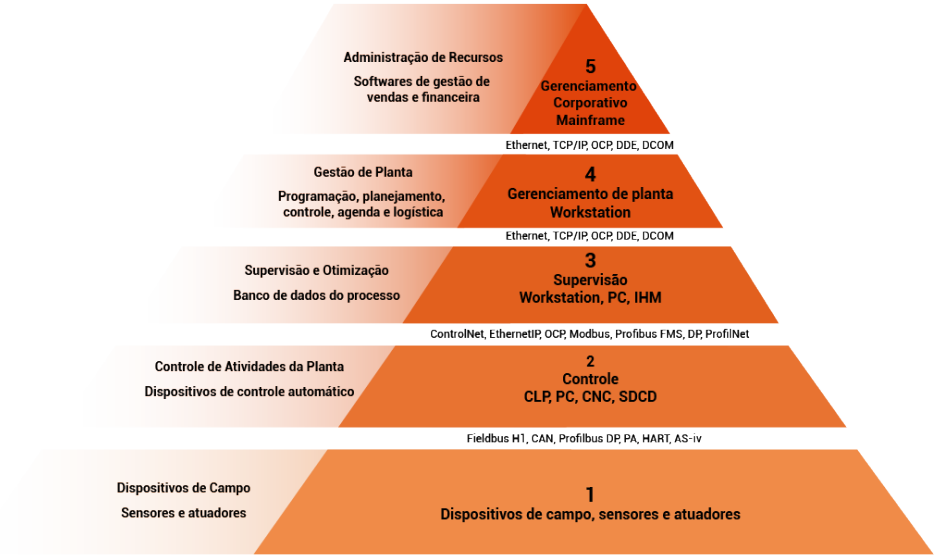

Figura 1. Pirâmide da Automação Industrial
Fonte: https://instrumentacaoecontrole.com.br/piramide-da-automacao-industrial/ (acesso em 31/07/2020)

No primeiro nível, o de dispositivos de campos encontra-se sensores, que medem as grandezas diretamente no processo, como parâmetros para futuras tomadas de decisão para o controle. Tais medições podem ser discretas, ou seja, binárias: ligado ou desligado, o que se diversifica pra uma gama de aplicações como sensores magnéticos ou capacitivos; ou podem ser analógicos, como sensores de pressão, nível ou vazão. Também dentre os dispositivos de campos, tem-se os atuadores, na outra ponta do controle, que são equipamentos que atuam diretamente no processo, fazendo modificações no seu estado de acordo com a prevista na lógica de controle. Exemplos de atuadores, que também podem ser analógicos ou discretos, são sinais sonoros e luminosos, válvulas, resistências, motores elétricos etc.

No segundo nível, o de controle encontra-se os principais dispositivos que fazem o controle do processo. Todos esses dispositivos têm uma base comum: a função de ler sinais de que vem das medições do campo, ou seja, sensores, e associá-los a uma lógica que de controle que vai acionar os atuadores. Dessa classe de dispositivos, os mais comuns são o CLP, ou Controlador Lógico Programável, e tem a função específica de ser o intermediário do processo, executando segundo a lógica explicada acima. Além disso, muitas vezes podem ser adereçados a ele módulos para expandir a quantidade de saídas ou entradas, se comunicar com outros tipos de equipamentos ou comunicação diferentes. O PC (*Personal Computer*) industrial já uma estrutura mais complexa, que une a praticidade de um PC com sistema operacional próprio com as funcionalidades industriais de um CLP: se conectando diretamente ao processo e com uma estrutura mais robusta que um PC doméstico (ZHANG, 2010).

No terceiro nível, de supervisão, tem-se o meio por onde um operador, gerente ou até um desenvolvedor interage com o processo, podem esse meio ser tanto uma tela

industrial fabricada especificamente para o uso robusto do chão de fábrica e comunicação com os equipamentos, quanto um PC comum também pode fazer o mesmo papel. A partir dessas estações de trabalho, remotas ao processo, se acessam todos os sinais de sensores e atuadores e visualiza-se graficamente o processo.

No quarto e quinto nível, temos níveis de gerência geral, que não mais se preocupam especificamente com sinais do campo, mas com decisões estratégicas de lucro e eficiência. Tais sistemas podem, e muitas vezes usam sim, sinais de que vem do campo, mas como maneira de ter indicadores da produção, como quantidade, tempo de fabricação, possíveis desperdícios etc. Todas essas informações são importantíssimas para esse tipo de planejamento estratégico.

Interligando todos esses níveis do processo, geograficamente separados em uma planta e no cenário comum, até mesmo chegando a quilômetros de distância, há comunicações que se baseiam no mesmo padrão que redes que normalmente usamos em escritórios ou no wi-fi disponível em todo tipo de estabelecimento. Redes essas, especificamente classificadas de Industriais, são dívidas em muitos padrões que podem coabitar uma mesma planta dependendo da estratégia como foi planejada (ZHANG, 2010). Vale dizer que há diferentes padrões de rede que podem coexistir numa mesma planta, cada uma delas com suas especificidades. Nesse contexto, utiliza-se conversores para que exista uma interoperabilidade.

Nesse contexto de complexidade é que nos aplicamos a explorar como algumas falhas no processo se relacionam com suas causas. Os estudos, então, podem dar subsídios para o planejamento de uma dinâmica pedagógica que possibilidade uma melhor compreensão geral desses sistemas e a facilite a análise lógica do processo dentro das possibilidades da sala de aula; uma habilidade transversal da área que se aplica a vários fins. Além disso, essa visão aprofunda o estudante da perspectiva real do seu objeto de estudo (ZHANG, 2010).

2.2 Análise de Falhas

Existem técnicas que embasam e contribuem para a análise de falhas e não só em um processo de automação, são técnicas úteis para resoluções de problemas de modo geral, aplicáveis na busca das causas reais de falhas de processo. Algumas dessas técnicas são: (I) *Failure Mode and Effects Analysis*: ele analisa a confiabilidade de sistemas e falhas em equipamentos utilizados. A vantagem do método é diminuir a frequência de falhas até eliminá-las, além da economia que decorre de um processo reduzido em falhas. O FMEA é aplicado, a princípio, identificando todos os possíveis modos de falha e documentando-os com uma escala de riscos própria do método, essa classificação dos riscos da falha serve para priorizar que falhas exigem uma ação mais rápido caso ocorram (MOBLEY, 1999);

Outro método (II) é o *Fault Tree Analysis*, e é baseado num processo lógico e dedutivo que, a partir de um evento indesejado que o método chama de evento topo, busca-se as causas desse evento a partir do sintoma de volta até a raiz do problema (Figura 2). A vantagem desse método é que ele é bastante intuitivo e existem algumas padronizações próprias dele que estruturam essa análise, facilitando a organização do pensamento na reflexão do problema (MOBLEY, 1999).

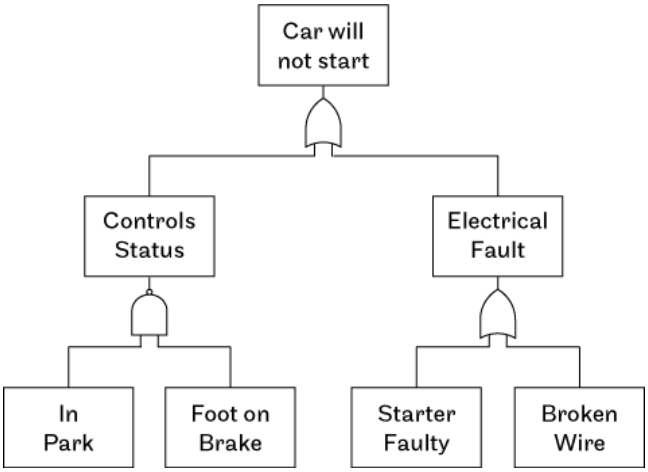

Figura 2. DIAGRAMA FTA
Fonte: https://accendoreliability.com/brief-introduction-fault-tree-analysis/ (acesso em 02/08/2020)

Volkanovski *et al.* (2009), por exemplo, usam o método *Fault Tree Analysis* na análise de confiabilidade em sistemas de distribuição de energia. Assim, se torna possível avaliar a interrupção de fornecimento de energia desde os geradores até pontos específicos de uso; outro exemplo de aplicação do FTA é na análise de falhas em uma fábrica de cimento, como visto em Gharahasanlou *et al.* (2014), onde os autores analisam um setor específico da produção de cimento e, a partir desse ponto, abrem o leque para os sistemas que formam esse setor até chegar nos menores subsistemas do processo. Dessa maneira, é possível uma visão ampla de por onde uma falha pode percorrer até sua causa.

Há também o (III) *Cause and effect analysis* (Figura 3), que também é um método bastante lógico, mas bem direto e simples, tanto que se torna aplicável não somente num contexto industrial, mas também em qualquer outro tipo de problema. A técnica, que também é conhecida como *fishbone analysis*, ou análise de espinha de peixe, como o nome sugere, tem como principal característica um diagrama em forma espinha de peixe, onde um evento problemático é associado com várias possíveis causas (MOBLEY, 1999). A desvantagem que faz esse método ser limitado a problemas mais simples e que não possibilita nenhuma sequência dos eventos que levaram à falha.

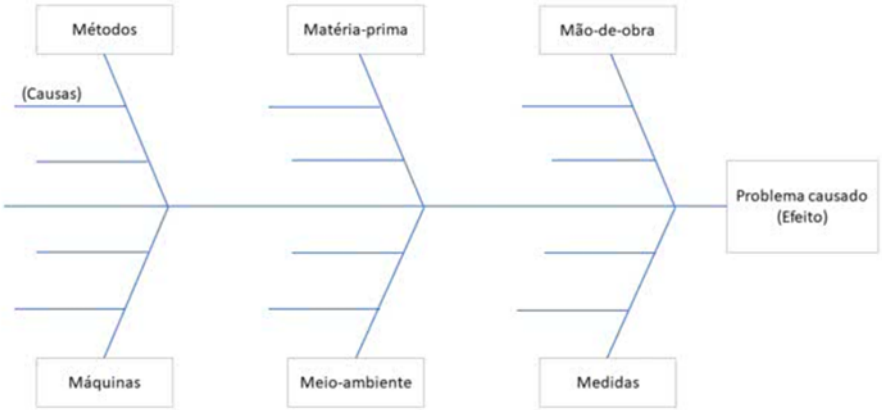

Figura 3. DIAGRAMA ESPINHA DE PEIXE
Fonte: https://www.dicionariofinanceiro.com/diagrama-de-ishikawa/ (acesso em 08/09/2020)

Vemos em Luo *et al.* (2018), um exemplo interessante de uso do CEA em conjunto com o FTA, que avaliava o risco de tanques esféricos de gás natural, assim como as probabilidades de acontecer. O tanque esférico, diferente de tubulação enterrada, é exposto a todas as influências do contexto: defeitos de construção, corrosão, temperatura etc. Além disso, é localizado em um lugar onde um vazamento de gás pode levar a explosão, causando danos e até mortes. Nessa maneira, os autores adaptam no diagrama de espinha de peixe, todas os tipos de problema que pode levar a um vazamento e causas específicas que causam isso.

Um método muito abrangente no uso é o (IV) *Sequence of Events Analysis*, e é uma técnica usada inclusive na área forense, para resolução de casos criminais. O método utiliza o diagrama de sequência de eventos, que estrutura aos detalhes a investigação da causa do erro. O diagrama contém os principais eventos problemáticos e inicia, a partir dele, as consequências desse acontecido (MOBLEY, 1999), suposições de razões, ações de operadores, ações do processo etc. A grande vantagem desse método é sua própria análise estruturada e consistente do problema (Figura 4).

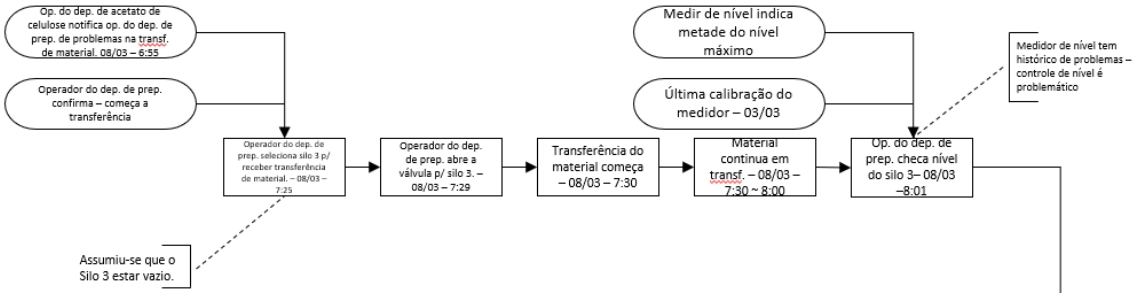

FIGURA 4. DIAGRAMA SEQUÊNCIA DE EVENTOS
FONTE: Mobley, R. K. (1999, p. 12)

O trabalho de Bhattacharjee *et al.* (2020), faz uma análise de origem de falha de uma explosão em uma mina subterrânea de carvão na Índia e se utiliza desse diagrama para expor de maneira compreensível e lógica os eventos na ordem em que leva ao desastre. A importância de compreender a causa de falhas é expressa muito claramente nesse caso que levou à morte de quatorze pessoas e deixou cinco gravemente feridas. A importância de organizar isso em um diagrama é clara para que se possa verificar todo tipo de influência na explosão, não somente de origem técnica – como também acontece na indústria – mas também influências de fatores organizacionais, condições de trabalho etc.

Dentro do contexto dos sistemas de controle industrial, essas técnicas são muito aplicáveis em plantas de produção e podem embasar o pensamento diagnostico necessário e importante para o técnico em automação (MOBLEY, 1999). Além disso, a análise das causas reais de falhas são uma sequência de passos lógicos, fáceis de aplicar, que tem em comum o fato de girarem em torno do evento da falha. Também em comum, todas elas buscam recriar as condições de falha.

2.3 Falhas nos Sistemas Industriais de Controle

Estudaremos problemas representativos dos três primeiros níveis da automação: no primeiro nível, com alguns tipos de falhas físicas em bombas; já no segundo nível, nos voltaremos ao uso e problemas à cerca do PID e, no terceiro nível, com software supervisório e problemas de rede, além de incluirmos também ciber segurança em plantas de controle industrial, um tema que tem emergido com a crescente de ataques em sistemas de automação desprotegidos (LAMB, 2017).

Deve-se destacar que o PID (controlador proporcional integral derivativo), é uma estratégia de controle baseado em uma fórmula de três termos onde temos três constantes ajustáveis que mudam a maneira como o processo vai responder. Na prática, usando como exemplo simples como um controle de nível em uma caixa d'água, o controle PID, programado dentro de CLP, lê através dos sensores deste, o sinal do nível no tanque. Com este dado em mãos, o PID compara o nível real da caixa d'água com um nível desejado, determinado pelo técnico, e baseado nessa diferença, o PID controle uma válvula de entrada de água da caixa. A ideia é que este controle seja feito par impedir que a caixa saia do nível desejado, então ele ajusta o fornecimento a proporção da demanda para que a diferença entre o nível real e o desejado seja menos possível (GARCIA, 2018).

O PID pode ser aplicado de diversas maneiras, para diversos fins (QUADROS e PINTO, 2013). Os autores aplicaram essa estratégia em sistemas de abastecimento de hídrico. Considerando as grandes perdas de água em vazamentos da tubulação, uma solução foi dividir a rede em áreas de abastecimento menores e utilizar-se de válvulas de redução de pressão quando há pressão excedente, assim reduzindo também os vazamentos em tubulação. Um controle PID então, foi proposto para o controle automático dessas válvulas, para que nem falte pressão na água quando este estiver já com pouca pressão na linha, nem alcance um pico de sobre pressão e comprometa as tubulações da área de abastecimento.

A estratégia de controle também pode ser usada em outros fins que não com válvulas e CLPs. Brito *et al.* (2014), aplicaram a estratégia de controle PID em um LEGO® Mindstorms para fazer com que o robô siga uma linha traçada no chão. Através de um sensor de luminosidade o robô identificava a diferença de tons da linha gravada no chão e sua posição, com o objetivo de manter-se sempre sobre a linha, o programa do PID no LEGO® ajustava o veículo para seguir corretamente o rumo certo do seu caminho; outro uso interessante do PID foi feito por Mattiello et al. (2015), como uma das estratégias de controle abordada em seu artigo. Nesse caso, apesar de não se provar a estratégia mais eficiente, ela controlava a atitude de um quadricóptero, ou seja, baseado nos dados do sensor de estabilidade, o PID tomava decisões de modificação das forças de cada um dos quatro rotores, pra o manter o veículo estável ou movimentá-lo para qualquer direção desejada.

Mas, ainda sobre o trabalho de Mattiello *et al.* (2015), relataram que a aplicação do PID não gera uma resposta rápida o bastante para esse caso em que tomadas de decisão são cruciais ao voo do veículo, além dos ajustes do controle PID serem mais difíceis para esse caso. Os autores também apontaram que o PID não reagiu bem às influências externas do ambiente, que desestabilizam o controle.

Coughran (2018), por sua vez, registra experiências em plantas de automação, de eventos de falha que a princípio foram postas na conta do controle PID, mas descobriu-se, através de uma análise mais lógica e com uma visão mais geral do processo como um todo, as verdadeiras fontes das falhas, por exemplo: em uma estação de gasodutos havia muitas oscilações na pressão e vazão dos produtos, o que tornava inseguro a entrega do combustível. Fazendo testes manuais no sistema, descobriu-se que a válvula usada no atuador do processo não dava uma resposta correta e o ajuste no controle PID não resolvia esse problema.

Com uma inspeção mais de perto na válvula, o técnico descobriu que o problema era na própria válvula que estava instalada de maneira incorreta; em outro exemplo no mesmo artigo, um par idêntico de extrusoras de plástico mostravam uma diferença no seu funcionamento: enquanto uma delas respondia bem ao controle, a outra reagia lentamente. As configurações de PID eram idênticas também, o que não justificaria o motivo, mas numa investigação com os operadores do setor, descobriu-se que foi trazido um equipamento de

outra parte da planta que, devido ao seu contexto de instalação original, estava configurado para uma conexão mais lenta (COUGHRAN, 2018).

Ang e Chong (2005) mostram que apesar de haver muitas publicações de pesquisas, há pouca discussão de análise, o que pode levar um desentendimento entre a academia e a indústria. Os autores apontam, como exemplo, não haver uma estrutura padrão de PID para a prática da engenharia do controle; com os PID's analógicos, mais antigos, sendo substituídos por digitais, estes últimos podem receber muitos tipos de personalização, o que aumenta essa discrepância de padrões. Eles apontam ainda que os problemas relacionados ao PID geralmente são de sintonia, ou seja, do seu ajuste de configurações, mas muitas patentes criadas nessa área tentam solucionar isso com sistemas automáticos e inteligentes de autoajuste, mas ainda apresentam dificuldades em se adaptar perfeitamente aos fins propostos.

Puig e Quevedo (2001), apontam para os crescentes estudos em torno de uma estratégia de controle de sistemas de automação tolerante às falhas, dada a necessidade de segurança e performance da planta de fabricação, além de evitar catástrofes. Tais sistemas apontam a importância da análise de falhas para um funcionamento confiável do processo. Os sistemas descritos pelos autores funcionam analisando os dados de sensores e atuadores no passar do tempo e os comparando com um modelo matemático do processo, permitindo assim a detecção de problemas caso haja comportamentos estatisticamente muito fora dos padrões.

A importância desse tipo de análise de falhas também pode ser vista no trabalho de Kurien e Srivastava (2019), que analisa a condição de bombas numa planta de usina termoelétrica. Esse monitoramento busca prevenir alguns defeitos mais graves que evitem catástrofes, parada de produção ou ineficiências no processo. Um dos casos relatados pelos autores foi de uma bomba auxiliar de resfriamento de água, usada para bombear água em um sistema de troca de calor. Foi instalado no equipamento um sensor que mede vibração e durante o funcionamento normal na planta, foi detectado que vibrações com interferências fora do comum, analisando mecanicamente os equipamentos, descobriu-se um rolamento desgastado, porque já se desconfiava que o motor estava operando em seus limites normais. Outro assunto relevante é a segurança digital das plantas automatizadas, uma preocupação crescente de ataques como o Stuxnet no sistema de automação em uma Usina Nuclear no Irã. O vírus, provavelmente trazido por um pen drive, não se sabe se intencionalmente ou não, se passava por partes de software do computador para passar despercebido e ficava observando o sistema, procurando por CLPs conectados a esses computadores. O vírus era uma estrutura complexa que se passava pelo funcionamento dos equipamentos que procurava. Sua intenção era encontrar um CLP específico que controlava centrífugas e tinha duas estratégias de ataque: acelerar sua rotação até prejudicar sua estrutura e quebrasse, ou abaixar sua rotação no mínimo, que também prejudicaria seu funcionamento e em ambos os casos, causariam uma catástrofe. O Stuxnet ainda tinha a capacidade de continuar mandando sinais aos sistemas de supervisão que tudo estava funcionamento normalmente, pois durante seu tempo de dormência no equipamento, até que começasse a agir, ele "aprendia" o padrão de comportamento do sistema e se tornava hábil a controlar esses sinais (FALLIERE, MURCHU e CHIEN, 2011).

Bhamare et al. (2019), apontam que os sistemas de controle industriais, de um modo geral, desde que começam a conectar plantas inteiras à internet para acesso remoto e usar recursos na nuvem, se expõe a riscos de invasão e conexão por vírus desse tipo do Stuxnet descrito anteriormente, já que: tanto essa não é uma das maiores preocupações pensadas durante o planejamento de novas plantas, como esses tipos de ataque podem se esconder

muito bem na comunicação dos equipamentos e do computador.
Na maioria das vezes, inclusive, os padrões de comunicação são de uso livre das empresas e tem seus dados muito expostos na internet, o que os torna facilmente uma ferramenta para essas invasões. Os autores expõem várias pesquisas recentes nessa área, que apontam já estratégias de inteligência artificial para a detecção desse tipo de intruso, uma boa quantidade de análise de vulnerabilidades já está disponível na academia, mas apontam que ainda faltam estudos para usos de recursos na nuvem, por exemplo (Bhamare et al. 2019).

3. Metodologia

A presente pesquisa se pauta na necessidade de trabalhar nos discentes a habilidade de solucionar problemas, mantendo uma visão do todo, e subsidia a possível decisão de construção de recursos didáticos para levar aos alunos essa experiência prática de ter contato com problemas que normalmente só aconteceriam em um ambiente da indústria.
Inicialmente foi utilizado referências das bases conceituais do Programa de Mestrado Profissional em Educação Profissional e Tecnológica, uma pesquisa bibliográfica

A partir deste ponto, um recorte foi sugerido entorno de problemas relacionados a sistemas hidráulicos, vastamente utilizados em processos indústrias, representando o nível 1 de automação. Falhas destes tipo de sistemas como escorva e cavitação, além de falhas em sensores, e atuadores; também foram considerados problemas de configuração de software e ajustes de PID, representando o nível 2 de automação, além de problemas de comunicação, o que conecta ao nível 3, onde esses problemas de comunicação também são presentes e se relacionam com o nível 2, trocando os dados do processo. Nesse mesmo último nível abordado, incluem-se problemas com supervisório, o que incluí por um tema de relevância, que é a cibersegurança nas plantas de automação.

Finalmente, para criar a proposta de uma planta didática, uma busca de obras publicadas respeito do tema proposto ou em áreas correlatas foi realizada nas bases de dados Scopus, Web of Science e Google Scholar, empregando-se os termos: “condition monitoring”, “fault diagnosis”, “fault detection”, “hidraulic pumps”, “cyber attack”, “PID tunning”, “failure analysis”.

4. Resultados e Discussão

Durante as pesquisas, muito se encontrou em relação a soluções específicas para problemas conhecidos e pouca exploração de problemas comuns de uso de equipamentos ou setores da indústria, e o estudo de suas causas. Outro assunto pouco abordado nos estudos são os métodos de análise de falha em si, como os apontados por Mobley (1999) aplicados nos processos industriais.

Mas Coughran (2018) e Kurien e Srivastava (2019), apesar, mostram a importância desse conhecimento sobre o processo como uma totalidade interdependente para a compreensão das causas das falhas e entram de acordo com Mobley (1999), se pensarmos nos métodos para análise daqueles problemas relatados.

Puig e Quevedo (2001) já apontam pra estratégias de tolerância às falhas e mesmo Kurien e Srivastava (2019) propõe um sistema de monitoramento que é passível de estratégias que inteligentemente identificariam possíveis causas, o que reforça essas habilidades transversais como uma área de estudo e também de trabalho, principalmente em um cenário onde a automação se desenvolve e encontra a tecnologia da informação. Apesar de escassa as fontes, se vê a importância dessa área não explorada pelas ementas, ainda

que indiretamente alcançada por meio de trabalhos como os de Martins, Oliveira e Oliveira (2012) e Oliveira et al., Teixeira et al. (2012), esse tipo de habilidade precisa ser explorado de maneira mais consolidada e estruturada, assim como repensada a estratégia fragmentada que se encontra normalmente nas escolas, que aponta Gallo (2002).

Sobre esse avanço das áreas correlatas, também os riscos antigos da computação começam a entrar para a indústria. O dossiê de Alliere, Murchu e Chien (2011) mostra como esse vírus foi inovador em incluir em si códigos que acessavam CLP e mudavam sua linguagem interna, ataques antes não vistos na computação. Bhamare et al. (2019) entram de acordo quando apontam várias pesquisas que estudam as vulnerabilidades dos sistemas mais comuns usados na indústria e já começa a propor soluções para os variados cenários. O quadro atual reforça que esse conhecimento ainda não explorado nos cursos comece a ser abordado e aprofundado, para os estudantes de hoje não saiam inocentes dos riscos da nova indústria.

Propõe-se, então, como um recurso de didático e ferramenta para trabalhar tais habilidades, uma bancada didática, representada graficamente na Figura 5, com um sistema hidráulico com tubulação e uma bomba, sensores de corrente, pressão e vazão e controlado por um CLP, com supervisão através de uma tela IMH. Com esse protótipo é possível pôr em prática problemas na bomba, na rede, de configuração, de sensor e, a partir daí, trabalhar com a análise dessas falhas e sua maneira de investigação.

Nesta planta didática, busca-se investigar os seguintes tipos de falhas: falhas mecânicas em bombas hidráulicos, que representam as falhas nos processos produtivos; falhas em relação a ajuste de controladores tipo PID; falha de medição de grandezas medidas pelos sensores; e finalmente cibersegurança de sistemas de automação.

O detalhamento e construção da planta, bem como um guia suporte para sua utilização serão desenvolvidas como trabalho futuro.

5. Conclusões

Essa pesquisa justifica a necessidade de um aprofundamento em conhecimentos emergentes da área de automação industrial pelas instituições de ensino, e tem a intenção de construir uma base bibliográfica para um sólido argumento em favor de atividades que abordem essas temáticas e, como uma proposta concreta, uma bancada de equipamentos simulando processos da indústria e que abordem falhas como as estudadas aqui, dos níveis 1, 2 e 3 dos sistemas de automação, trazendo pro aluno uma vivência mais próxima a essas experiências.

Posteriormente, estudos com alunos devem ser feitos usando atividades temáticas na forma da bancada proposta, como maneira de validar a eficiência dessa abordagem na sala de aula, para o ensino tecnológico.

Agradecimentos

Agradeço à Deus, minha família, meus orientadores e coorientadores pelo apoio dado até agora nesse processo de mestrado.

Referências Bibliográficas

ANG, K.H.; CHONG, G. PID Control System Analysis, Design and Technology. IEEE

TRANSACTIONS ON CONTROL SYSTEMS TECHNOLOGY, vol. 13, n. 4, p. 559-576. Estados Unidos: 2005.

BHAMARE, D.; ZOLANVARI, M.; ERBAD, A.; JAIN, R.; KHAN, K.; MESKIN, N. Cybersecurity for industrial control systems: A survey. Computer & Security, Vol. 89. Estados Unidos: 2020.

BHATTACHARJEE, R.M.; DASH, A.K. PAUL, P.S. A root cause failure analysis of coal dust explosion disaster – gaps and lessons learnt. Engineering Failure Analysis, v. 111. India: Elsevier 2020.

BORGES, L.F.P. Educação, escola e humanização em Marx, Engels e Lukács. Revista Educação em Questão, v. 55, n. 45, p. 101-126, 2017. Disponível em: <https://periodicos.ufrn.br/educacaoemquestao/article/view/12747> e acessado em 09.08.2020.

BRASIL. Ministério da Educação, Catálogo Nacional de Cursos Técnicos, Brasília, D.F., 2017. Disponível em: <http://portal.mec.gov.br/docman/novembro-2017-pdf/77451-cnct-3a-edicao-pdf-1/file> e acessado em 09.08.2020.

BRITO, R.C.; MADALOSSO, E.; GUIBES, G.A.O. Seguidor de Linha Para LEGO® Mindstorms Utilizando Controle PID. Computer onthe Beach 2014, p. 310-319. Itajai: 2014.

CARVALHO, O.F.; LACERDA, G. Dualismo versus congruência: diálogo entre o novo modelo brasileiro para a formação profissional eu modelo didático ESC (Experimental, Científico e Construtivista). Educação profissional e tecnológica no Brasil contemporâneo: desafios tensões e possibilidades, p. 301 – 312. Porto Alegre: Artmed, 2010.
CIAVATTA, M. Ensino Integrado, a Politecnia e a Educação Omnilateral: por que lutamos? Revista Trabalho & Educação, v. 23, n. 1, p. 187–205, 2014. Disponível em: <https://seer.ufmg.br/index.php/trabedu/article/view/9303> e acessado em 09.08.2020.

COUGHRAN, M. How to Fix Process Control Loop Problems That PID Tuning Cannot Correct. ISA Interchange blog. Disponível em: <https://blog.isa.org/how-to-fix-process-control-loop-problems-that-pid-tuning-cannot-correct?utm_campaign=smm-blog-post-20180725-Imerso-How-to-Fix-Process-Control-Loop-Problems-That-PID-Tuning-Cannot-Correct&utm_medium=social&utm_source=twitter>. Acessoem: 09.08.2020.

DINARDO, G.; FABBIANO, L.; VACCA, G. A smart and intuitive machine condition monitoring in the Industry 4.0 scenario. Measurement, vol. 126, p. 1-12. Italy: 2018

FALLIERE, N.; MURCHU, L.O.; CHIEN, E. W32. Stuxnet Dossier. SYMANTEC. Estados Unidos, 2011. Disponível em: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-044.pdf> e acessado em 10.08.2020.

GALLO, S. Transversalidade e educação: pensando uma educação não-disciplinar. In: ALVES, N.; GARCIA, R.L. (Orgs.) O sentido da escola.Rio de Janeiro: DP&A, 2002. 3a edição.

GHARAHASANLOU, A.N.; MOKHTAREI, A.; KHODAYAREI, A.; ATAEI, M. Fault tree analysis of failure cause of crushing plant and mixing bed hall at Khoy cement factory in Iran. Case studies in engineering Failure Analysis. Vol 2, p. 33-38. Iran: Elsevier 2014.

KURIEN, C.; SRIVASTAVA, A.K. Case study on the effectiveness of condition monitoring techniques for fault diagnosis of pumps in thermal power plant. Mechanics and Mechanical Engineering, vol. 23, p. 70-75. India: 2019.

LOU, T.; WU, C.; DUAN, L. Fishbone diagram and risk matrix analysis method and its application in safety assessment of natural gas spherical tank. Journal of Cleaner Production, vol. 174, p. 296-304. China: Elsevier 2018.

MARTINS, F.N.; OLIVEIRA, H.C.; OLIVEIRA, G.F. Robótica como meio de promoção da interdisciplinaridade no ensino profissionalizante. Anais do Workshop de Robótica Educacional. 2012. Disponível em: <http://www.natalnet.br/wre2012/pdf/106420.pdf>, e acessado em 09.08.2020.

MATTIELLO, C.D.; BORSOI, B.T.; LINARES, K.C.; FAVARIM, F. Controle de atitude para veículos aéreos não tripulados do tipo quadricóptero: PID vs Lógica Fuzzy. Computer on the Beach 2015, p. 111-120. Itajai: 2015.

MOBLEY, R.K. Root Cause Failure Analysis. 2ª edição. Estados Unidos: Newnes, 1999.

MOURA, D.H. Ensino médio e educação profissional: dualidade histórica e possibilidades de integração. Educação profissional e tecnológica no Brasil contemporâneo: desafios tensões e possibilidades, p. 58 – 78. Porto Alegre: Artmed, 2010.

OLIVEIRA, L.M.; TEIXEIRA, D.P.; OLIVEIRA, A.R.; CARMO JUNIOR, M.; ARAUJO JUNIOR, L.O. Utilização de uma planta didática Smar para complementação do ensino de engenharia de controle e automação. Congresso Brasileiro De Educação Em Engenharia. 2012. Disponível em: <http://www.abenge.org.br/cobenge/arquivos/7/artigos/104420.pdf>. e acessado em 09.08.2020

PEREIRA, A.; SIMONETTO, E.O. Indústria 4.0: conceitos e perspectivas para o Brasil. Revista da Universidade Vale do Rio Verde, vol. 16, n. 1, p. 1-9. Belo Horizonte: 2018.

PUIG, V.; QUEVEDO, J. Fault-tolerent PID controllers using a passive robust fault diagnosis approach. Control Engineering Practice 9, p. 1221-1234. Estados Unidos: 2001.

QUADROS, A.S.; PINTO, A.M.A. Controle com sintonia automática e adaptativa de válvulas redutoras de pressão em sistemas de abastecimento de água. Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, vol. 1, n. 1. São Carlos: 2013.

VOLKANOVSKI, A.; CEPIN, M.; MAVKO, B. Application of the fault tree analysis for assessment of power reliability. Reliability Engineering and System Safety. Vol. 94, p. 1116-1127. Slovenia: Elsevier 2009.

ZHANG, P. Advanced Industrial Control Technology. 1ª edição. Inglaterra: Elsevier, 2010.