UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO

CURSO DE ESPECIALIZAÇÃO EM INDÚSTRIA 4.0

EDEMILSON BUENO DE CAMARGO

INDÚSTRIA 4.0 NA PRÁTICA A PARTIR DA INTEGRAÇÃO DA TECNOLOGIA DE INFORMAÇÃO E TECNOLOGIA DE AUTOMAÇÃO: UM ESTUDO DE CASO DE MONITORAMENTO DOS ATIVOS DE AUTOMAÇÃO EM UMA FÁBRICA DE CELULOSE DOS CAMPOS GERAIS (PR).

TRABALHO DE CONCLUSAO DE CURSO DE ESPECIALIZAÇÃO

PONTA GROSSA

2020

EDEMILSON BUENO DE CAMARGO

INDÚSTRIA 4.0 NA PRÁTICA A PARTIR DA INTEGRAÇÃO DA TECNOLOGIA DE INFORMAÇÃO E TECNOLOGIA DE AUTOMAÇÃO: UM ESTUDO DE CASO DE MONITORAMENTO DOS ATIVOS DE AUTOMAÇÃO EM UMA FÁBRICA DE CELULOSE DOS CAMPOS GERAIS (PR).

Trabalho de Conclusão de Curso de Especialização apresentada como requisito parcial à obtenção do título de Especialista em Indústria 4.0, da Universidade Tecnológica Federal do Paraná, Câmpus Ponta Grossa.

Orientador: Joseane Pontes
Coorientador: Ivo Neitzel

PONTA GROSSA
2020

TERMO DE APROVAÇÃO DE TCCE

Indústria 4.0 na prática a partir da integração da tecnologia de informação e tecnologia de automação: um estudo de caso de monitoramento dos ativos de automação em uma fábrica de celulose dos Campos Gerais (PR).

Edemilson Bueno de Camargo

Este Trabalho de Conclusão de Curso de Especialização (TCCE) foi apresentado em 08 de fevereiro de 2020 como requisito parcial para a obtenção do título de Especialista em Industria 4.0. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Profª. Joseana Pontes
Prof. Orientador

_____
Prof. Marcelo Vasconcelos de Carvalho
Membro titular

_____
Prof. Rui Tadashi Yoshino
Membro titular

A FOLHA DE APROVAÇÃO ENCONTRA-SE ASSINADA NA SECRETARIA DO CURSO

RESUMO

CAMARGO, Edemilson Bueno. **Indústria 4.0 na prática a partir da integração da tecnologia de informação e tecnologia de automação: um estudo de caso de monitoramento dos ativos de automação em uma fábrica de celulose dos Campos Gerias (PR)**. 2020. 23f. Monografia (Especialização em Engenharia de Indústria 4.0), Universidade Tecnológica Federal Do Paraná. Ponta Grossa, 2020.

Uma das mudanças propostas pela Industria 4.0, a integração entre Tecnologia da Informação (TI) e Tecnologia da Automação (TA), que promove a eficiência dos processos, pode trazer consigo riscos e possibilidades para a rede de automação, que até então era praticamente isolada de outras áreas. Para manter-se segura e aproveitar as oportunidades dessa nova integração, alguns protocolos, layouts, sistemas de controle destinado ao monitoramento e gerenciamento dos ativos da automação como por exemplo estações de operação, servidores, etc., devem ser abordados. Com isso, o objetivo deste trabalho é demonstrar como foi integrado a tecnologia de informação e tecnologia de automação através via monitoramento dos ativos de toda a automação para a melhoria de visibilidade em uma indústria de celulose dos Campos Gerais (PR). Para isso, será mostrado o cenário real de uma empresa que passa por mudanças atualmente, com seus ganhos e dificuldades neste processo de gerenciamento da mudança e forte foco em manter a disponibilidade do ativo. Para ilustrar este trabalho, o estudo de caso baseou-se na aplicação de ferramentas *"open source"* de mercado para gerenciamento de servidores e estações e também soluções de monitoramento de vulnerabilidades avançadas. Após a aplicação do estudo de caso, verificou-se o ganho na visibilidade e controle dos ativos sob responsabilidade da automação (estações, servidores, etc.), tanto na antecipação de falhas em estações e servidores, quanto na identificação de vulnerabilidades que trafegam na rede de TA. Neste caso, embora as mudanças sejam desafiadoras, trazem consigo uma série de itens e ferramentas da TI/TA que proporcionarão uma redução de tempo indisponível nos ativos de automação de diversas áreas e que proporcionarão a elas novos ciclos de melhoria.

Palavras-chaves: Integração TI/TA. Monitoramento de Ativos. Vulnerabilidades.

ABSTRACT

CAMARGO, Edemilson Bueno. **Industry 4.0 in practice from the integration of information technology and automation technology: a case study of monitoring of automation assets in a Campos Gerais (PR) pulp mill**. 2020. 23p. Monograph (Especialization in Industry 4.0) , Federal Technology University - Paraná. Ponta Grossa, 2020.

One of the changes proposed by Industry 4.0, the integration between Information Technology (IT) and Automation Technology (TA), which promotes process efficiency, can bring risks and possibilities to the previously used automation network. Practically isolated from other areas. To remain secure and take advantage of the opportunities of this new integration, some protocols, layouts, control systems for monitoring and managing automation assets such as operating stations, servers, etc., should be addressed. Thus, the aim of this paper is to demonstrate how information technology and automation technology have been integrated by monitoring the assets of all automation to improve visibility in a pulp industry in Campos Gerais (PR). For this, it will be shown the real scenario of a company that is undergoing change today, with its gains and difficulties in this change management process and strong focus on maintaining asset availability. To illustrate this work, the case study was based on the application of open source tools for server and station management as well as advanced vulnerability monitoring solutions. After applying the case study, there was a gain in visibility and control of assets under the responsibility of automation (stations, servers, etc.), both in anticipation of failures in stations and servers, and in identifying vulnerabilities that travel in the TA network. In this case, while the changes are challenging, they bring with them a host of IT / TA items and tools that will provide downtime on automation assets in various areas and provide them with new improvement cycles.

Key-words: IT / TA Integration. Asset Monitoring. Vulnerabilities.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

DCS	*Digital Control System*
DDoS	*Distributed Denial of Service*
HIDS	*Host-based Intrusion Detection Systems*
IDS	*Intrusion Detection System*
MRC	*Maintenance Response Center*
NAT	*Network Address Translation*
PoC	*Proof of Concepts*
UTFPR	Universidade Tecnológica Federal do Paraná

SUMÁRIO

1 INTRODUÇÃO

Neste início de uma nova fase industrial denominada, aqui no Brasil chamada de "Industria 4.0", onde um grande volume de iniciativas ligadas a transformação digital das industrias estão em andamento, uma das propostas está na integração entre Tecnologia da Informação (TI) e a Tecnologia de Automação (TA). Com isso, novos layouts que convergem para essa integração tendem a elevar a eficiência nos processos da informação da indústria. Segundo Flores (2014), para a integração funcionar, é importante que a nova solução oferecida em seu portfólio não demande muito esforço de sua equipe. O foco precisa continuar na linha de produção primária. Pensando em linha primária e na manutenção dos ganhos atuais, vale ressaltar que esta integração traz consigo também riscos, além das inúmeras possibilidades as redes de automação, redes estas que até então eram praticamente isoladas, agora estão começando a se expor a esta nova fase, trazendo consigo uma nova necessidade as equipes que as mantém, visibilidade.

Naturalmente esperado por engenheiros das indústrias que precisam extrair resultados com base em análises, ter dados de campo ou de dispositivos inteligentes e encontrar correlações, causas de problemas, possibilidade de redução de custos, esforços e perdas, é o objeto de desejo das empresas que estão buscando se capacitar tecnologicamente para prover esta integração dos dados.

Segundo Lee *et al.* (2013), o desenvolvimento de sensores inteligentes e o aumento da capacidade de armazenamento de dados vêm disponibilizando cada vez mais informações desses processos, o que aliado a essa integração, que também está de certa forma no centro da nossa discussão, proporcionará volume de dados para alimentar modelos e estudos, com variadas técnicas baseadas em dados, visando o aumento da detecção antecipada e diagnóstico cada vez mais precisos de falhas em processos industriais.

Processos industriais competitivos não toleram paradas, isso tornaria esse processo menos eficaz e esta empresa menos competitiva, pois custos de repartida não são bem vindos, nem tão pouco paradas indesejadas devido a testes para prover esta integração. Logo, para obter estes dados é necessário planejar e capacitar os sistemas de controle e, dentro das possibilidades e momento de cada entidade, ter um sistema de monitoramento e resposta a anomalias.

Ceron (2009) ressalta que todo incidente deve ser tratado seguindo uma metodologia previamente definida pela instituição. Essa metodologia é chamada de processo de resposta a incidentes de segurança. Para que ambos os processos, de conhecer os eventos e de trata-los seguindo uma metodologia, algumas etapas devem ser observadas e respeitadas previamente para que este sistema funcione plenamente. Outro ponto fundamental é capacitar pessoas para que estejam antenadas para o que este novo processo possa gerar de consequências a médio e longo prazo.

Para conseguir ter disponível os processos e ativos aos quais a automação está ligada, gerir seus ativos é parte fundamental. Segundo Lafraia (2014), gestão de ativos pode ser defi-

nida como a atividade coordenada de uma organização para produzir o valor a partir dos ativos, otimizar ao máximo a produtividade de cada um deles, com equilíbrio de custos, riscos, oportunidades e desempenhos. Ao correlacionar esta reflexão proposta sobre um conceito de gestão de ativos, com os ativos de automação, conseguir extrair o máximo a produtividade deste bem, está diretamente ligado a disponibilidade em desempenhar sua função. Para tanto, dentro do estudo em questão, será observado a importância deste monitoramento dos dispositivos presente na rede de automação, seja qual for o nível, se de campo ou de controle.

Não há como citar integração TI/TA, sem considerar alguns riscos desta modalidade. Uma das principais são as vulnerabilidades que os sistemas de automação passam a estar expostas quando se interligam a mundos externos. Para o monitoramento, hoje estão disponíveis diversas ferramentas. Para ANSI (2007), ferramentas de detecção de intrusão (do inglês, *Intrusion Detection System* - IDS) rodam em computadores e observam os recursos e aplicações à procura de anomalias, tradicionalmente denominadas de HIDS (*host-based intrusion detection systems*). Outra variação de IDS existente é quando a observação está no tráfego de rede, nesse caso, são denominadas de NIDS (*network-based intrusion detection systems*). Independentemente de o foco ser na rede (NIDS) ou nos servidores (HIDS), as ferramentas IDS rodam, na sua maioria, em protocolos baseados em tecnologia IP.

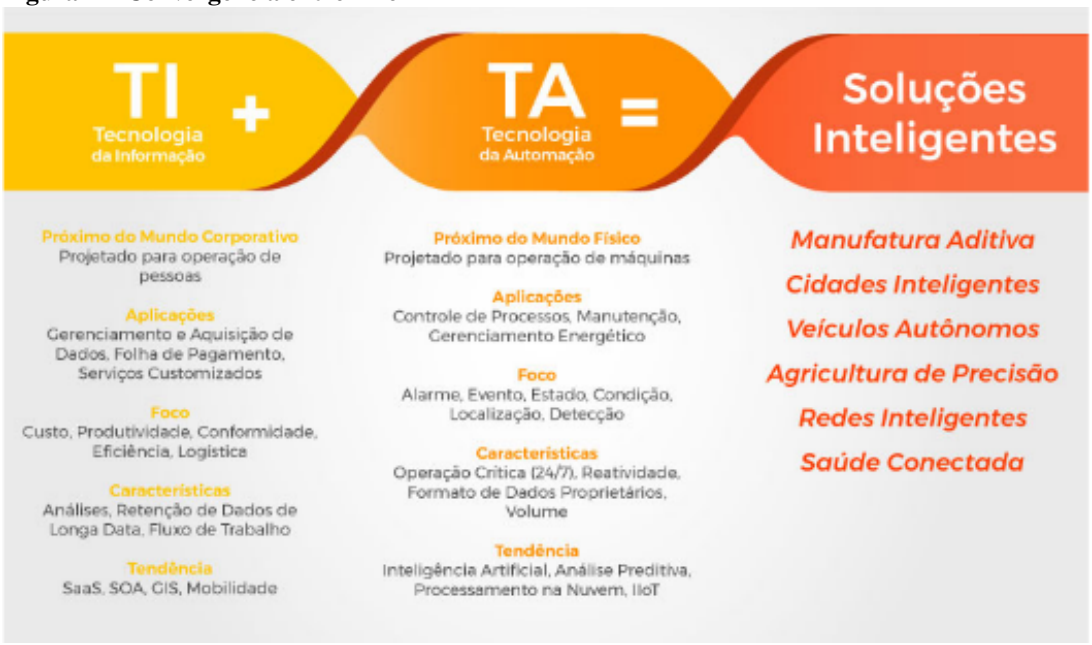
Sabendo que este processo da integração presente na indústria 4.0 é inevitável e irreversível, o melhor é focar na infraestrutura e nas contramedidas necessárias para ter um sistema robusto suficiente para conseguir manter os resultados e com possibilidade de ser escalável. Para tal, um conjunto de produtos estão disponíveis para capacitar um sistema de controle, que podem ser de origem *"open source"* disponível na internet para baixar e o próprio usuário configurar e usar ou de empresas de serviços voltados especificamente para a necessidade de cada segmento. Tem-se como exemplo que será abordado neste trabalho, a utilização do ZABBIX, uma ferramenta *"open source"* para monitoramento de dispositivos utilizando o protocolo SNMP, normalmente nativos em sistemas operacionais, sendo uma ferramenta para gerenciamento de estações e servidores, monitorar a performance e disponibilidade de todos serviços e ativos da rede. O benefício disso é a visibilidade dos eventos que esses ativos são submetidos, um primeiro passo para gerenciar é conhece-los. Com isso, o trabalho tem como objetivo demonstrar um processo de implantação para se monitorar ativos de automação e exemplos de ferramentas que podem ser implementadas em um fabrica, seja ela de celulose ou não.

2 REFERENCIAL TEÓRICO

2.1 INTEGRAÇÃO TI/TA

Segundo TECLÓGICA (2018) as integrações de ambientes de TA e TI podem vir de duas formas estruturadas, sendo a primeira delas a integração horizontal, que diz respeito à capacidade da área de TI em acompanhar, automatizar e unir processos em toda uma cadeia de produção, desde o tratamento com os fornecedores até o cliente. Esse é geralmente um mecanismo de monitoramento linear que garante eficiência em cada etapa de manufatura. A essa segunda forma de estruturação que permite o compartilhamento das informações em cadeia do chão de fábrica até os executivos da empresa é chamado de integração vertical. Ou seja, se a integração horizontal é uma linha, a vertical é uma pirâmide que coleta os dados de produção e os filtra em relatórios e sistemas que podem dar uma noção muito mais aprimorada sobre os obstáculos e as oportunidades de melhorar o desempenho da indústria. Ramos (2012) traz uma avaliação muito interessante, onde, nem sempre as equipes de TI estão aptas para manusear dados como as unidades de tempo de segundos e milissegundos, tradicionais da automação. Ao mesmo tempo, os especialistas de automação nem sempre conhecem em profundidade as metodologias de gestão e de segurança de sistemas, já velhas conhecidas pela TI. Essas barreiras precisam ser superadas, via que a implementação de sistemas de gerenciamento integrado da produção, com o objetivo de permitir a integração entre os sistemas corporativos e os de manufatura, cada um sob responsabilidade um time (TI/TA), visando implementar programas de melhoria, dar sustentabilidade a projetos e extrair o máximo desempenho dos ativos das indústrias. ALTUS (2012) mostra na Figura 1 que a união de esforços, conhecimentos, informações pode trazer soluções inteligentes, como as presentes na manutenção aditiva, cidades inteligentes, veículos autônomos, agricultura de precisão, redes inteligentes, saúde conectada, etc., isso será visto no case em questão, onde duas áreas com informações, conhecimentos distintos unidos, podem gerar resultado para as organizações.

Figura 1 – Convergência entre TI e TA



Fonte: (ALTUS, 2012)

A seguir, será apresentado o tema monitoramento de ativos.

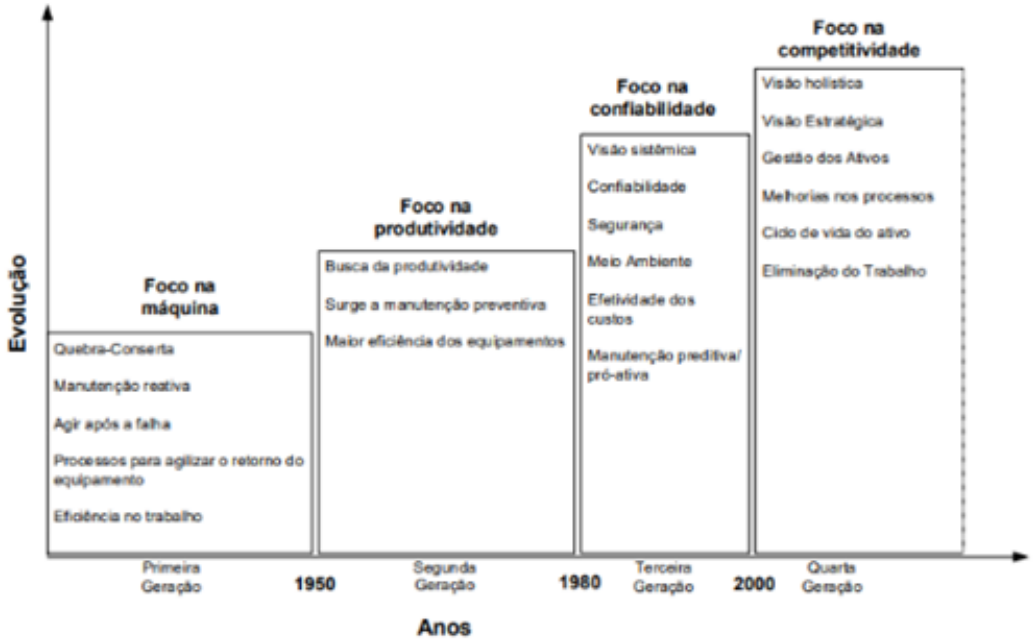
2.2 MONITORAMENTO DE ATIVOS

Um termo conhecido de William Edwards Deming diz que: “Não se gerencia o que não se mede, não se mede o que não se define, não se define o que não se entende, e não há sucesso no que não se gerencia". Com isso, antes de se chegar a etapa de monitoramento, Tammela, Chaves e Neto (2016) apresenta que a prática de diagnosticar falhas é uma das ferramentas da Gestão de Ativos, normatizada pela ISO 55.000 (ISO; SC, 2014), que define ativo como algo que tenha valor real, ou potencial, para uma organização. Ainda de acordo com a norma, a Gestão de Ativos é a atividade coordenada de uma organização para produzir o valor dos ativos, que envolve equilibrar os benefícios de custos, riscos, oportunidades e desempenhos. Segundo Dutta (2015, apud Tammela et al, 2016, p. 2) afirma que a segurança e a produtividade podem ser maximizadas quando se melhoram a capacidade humana (experiência e treinamento), a confiabilidade operacional (maturidade dos processos) e a confiabilidade da manutenção (equipamentos disponíveis e confiáveis).

A ISO 55.000 (ISO; SC, 2014) de forma geral define que os fatores que influenciam o tipo de ativos que uma organização requer para atingir seus objetivos, e como os ativos são gerenciados, inclua a natureza e o objetivo da organização, seu contexto operacional, suas restrições financeiras e requisitos regulatórios, as necessidades e expectativas da organização e de seus *stakeholders*. Esses fatores de influência precisam ser considerados ao estabelecer, implementar, manter e aprimorando continuamente o gerenciamento de ativos. O controle e a governança

eficazes dos ativos pelas organizações são essenciais para obter valor através de gerenciar riscos e oportunidades, a fim de alcançar o equilíbrio desejado entre custo, risco e desempenho. Fica claro que para atender os requisitos da norma, um sistema de gerenciamento precisa ser organizado e eficaz, não somente pela complexidade de atender por completo uma norma, mas a junção da complexidade das indústrias de porte somadas as da norma. É visível nas grandes corporações, não somente em projetos, mas também na rotina, a preocupação com o melhor retorno dos investimentos e um forte trabalho na redução de custos para buscar competitividade. Uma das formas de se conseguir isso é através de eficiência fabril, onde a tomada de decisão assertiva ajuda a equilibrar os custos, reduzir riscos. Estes benefícios são citados na norma ISO e SC (2014) e podem ser vistos no ambiente fabril de forma prática, de forma que, revisar e aprimorar processos, procedimentos e desempenho de ativos pode melhorar a eficiência e efetividade e a consecução dos objetivos organizacionais. Nesse contexto, Mosquin e Rodrigues (2017) complementa a linha de raciocínio na figura da manutenção, em que atualmente vive a sua quarta geração evolutiva, onde o foco é a competitividade e a busca pela competitividade conforme Figura 2, e que isso exige da manutenção uma visão sistêmica, holística, estratégica, em que o quebra-conserta não faz mais sentido e que a excelência da manutenção durante todo o ciclo de vida do ativo deve ser buscada.

Figura 2 – Evolução da função Manutenção



Fonte: (MOSQUIN; RODRIGUES, 2017)

Explorar os dados dos sistemas vem sendo praticada pelas empresas atualmente. As experiências e ganhos vivenciados no dia a dia, mostram que o caminho é promissor.

2.3 VULNERABILIDADES

Uma análise trazida por Barford Plonka (2001 apud Turcato et al, 2015, p. 219), ataques em redes são considerados anomalias definidas como ações diferentes observadas no comportamento normal do tráfego esperado, que podem ser indicativos de ataques, abuso (mau uso) na rede, eventos de falha, problemas de infraestrutura na coleta de dados, entre outros. Assim, Turcato *et al.* (2015) conclui que, nem toda anomalia pode ser considerada um ataque, mas sempre representa uma informação suspeita que deve ser analisada. Segundo Igure et al (2006, apud Freitas, 2018, p. 17), a crescente tendência do aumento de interconectividade entre dispositivos de chão de fábrica reforçada pela ascendente Indústria 4.0 modificam completamente o cenário original dos sistemas SCADA o que possibilita a inclusão de vulnerabilidades. Ainda os mesmos reforçam que a segurança digital não é garantida pelas barreiras físicas pois qualquer nó ou má configuração pode permitir acesso com o exterior da infraestrutura. Já a TECLÓGICA (2018) avalia que os dados são cada vez mais valiosos para as empresas, eles também se tornam alvos para criminosos. São tantas informações sendo geradas e trocadas na Indústria 4.0 (comunicação M2M, monitoramento automatizado, acompanhamento de relatórios por operadores, etc.) que é impossível garantir a proteção delas sem integrar todo esse controle em um só ambiente. De forma geral Fernandes (2017) informa que, são três modalidades de ataque que precisam ser consideradas, a saber: ataques de fora para dentro (uma empresa brasileira atacada por um invasor de outro país, por exemplo); de dentro para fora (quando um computador já invadido é usado como uma espécie de "trampolim" para um ataque externo); e de dentro para dentro, nos casos em que o malware age de forma horizontal dentro da mesma rede, em busca de novos privilégios de acesso e informações. Métodos e vetores de ataques são discutidos de forma profunda em livros e artigos do ramo atividade, tais como Wright Stevens (1995, apud Freitas, 2018, p. 18) trazem que os ataques conhecidos como *Denial of Service* (DoS) e *Distributed Denial of Service* (DDoS) são responsáveis por causar a negação de serviço no computador ou dispositivo embarcado alvo, ou seja, a função para qual o dispositivo foi projetado não será mais executada devido ao ataque. Um ataque de negação de serviço é chamado de DDoS quando orquestrado por um número de computadores maior que um, pois nesse caso o ataque tem várias fontes, caracterizando um ataque DoS distribuído. Os métodos ou vetores utilizados por um ataque de negação são complexos e podem variar de acordo com o perfil de tráfego nominal do alvo. Com base no exposto, ter soluções de segurança que bloquem vulnerabilidades ou as identifiquem, de modo a atuar eficientemente reduzem o grau de risco das empresas.

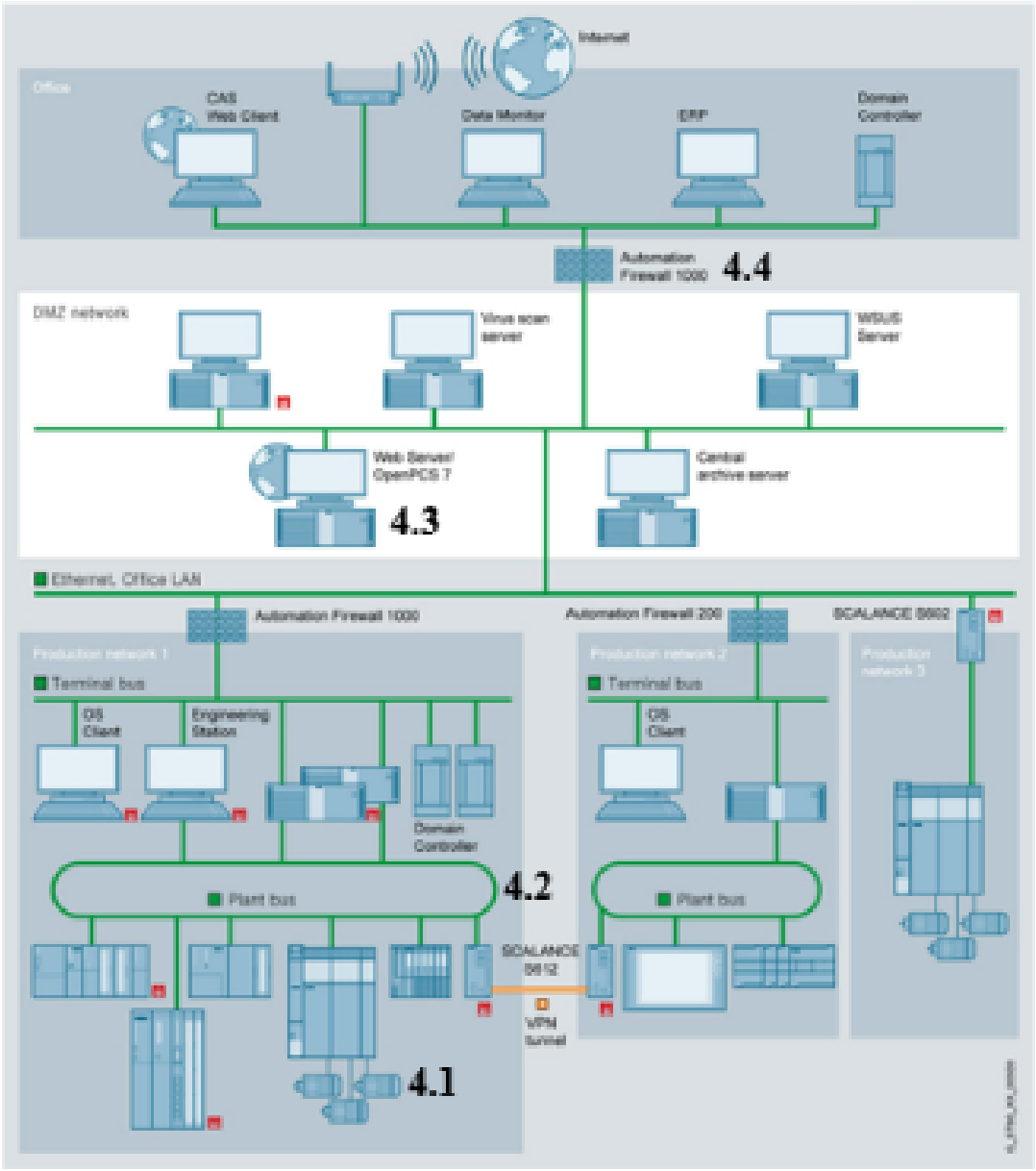
3 METODOLOGIA

Quanto à caracterização da pesquisa, o presente artigo possui natureza da pesquisa aplicada, quanto ao objetivo, é exploratório, quanto a abordagem do problema, é qualitativo e quanto ao método de pesquisa, baseia-se em estudo de caso. Neste sentido, o presente trabalho baseia-se no estudo de caso de uma fábrica de celulose na região dos Campos Gerais (Paraná). Para este estudo de caso foram avaliados itens do chão de fábrica (relés, estações, servidores) até o limite de baterias (*Firewall* entre TI/TA) juntamente ao departamento de Tecnologia da Informação, com foco nos ativos de automação. O estudo de caso em questão iniciou-se no ano de 2016, onde a equipe de projetos (Gerencia de Projetos – equipe que gerenciou a construção da fábrica) finalizou sua etapa no processo de construção e entregou a unidade fabril para a equipe de operação e manutenção. Natural de projetos de grande porte, itens residuais continuaram a ser tratados com fornecedores e equipes de suporte e, em paralelo, iniciaram os testes de performance para os TAF's (Teste de Aceitação de Fábrica), momento em que itens não conformes começam a aparecer e necessitar de tratativas. Neste sentido, será apresentado o estudo de caso a seguir.

4 APLICAÇÃO

Conforme apontado anteriormente, o estudo de caso foi focado na área de automação no intuito de melhorar a visibilidade das condições dos ativos estudados (relés, redes industriais, estações, servidores, etc.). Para isso um projeto especifico envolvendo as equipes de elétrica, instrumentação e automação, cujo objetivo era que cada especialidade anteriormente citada, buscassem melhorar o diagnóstico dos ativos que cada equipe mantém. Para melhorar o entendimento do estudo de caso, será segmentado em quatro seções: ativos de campo (instrumentos que se comunicam via HART e PROFIBUS, especificação de projeto para dispositivos de campo), redes de automação, ativos da rede de controle (Estações, Servidores, Roteadores, *Switches*, etc.) e integração com TI. Estas seções encontram-se destacadas na Figura 3, onde a distribuição e figura combinam num *layout* desde o chão de fábrica até o limite de baterias entre TI e TA (normalmente um firewall de borda).

Figura 3 – Exemplo de uma rede de automação com subdivisões do artigo



Fonte: (RAMOS, 2012)

4.1 ATIVOS DE CAMPO

Com o projeto de construção da fábrica, a empresa adquiriu um software de gerenciamento de ativos (instrumentos Hart) chamado MRC (*Maintenance Response Center* – Centro de Resposta da Manutenção) da empresa Schneider Electric, o qual tem por objetivo coletar informações ou alertas dos instrumentos de campo ligados ao DCS (*Digital Control System*) e remete-los a um servidor que disponibiliza estes alertas para ser gerenciado pelas equipes de manutenção. Estes alertas são classificados conforme a NAMUR 107 (a NAMUR é uma associação internacional de usuários de automação em indústrias de processo) e seguem as classificações de falha conforme Figura 4.

Figura 4 – Descrição dos Sinais de Status

Failed	Out of Specification	Maintenance Required	Check Function
			
High severity: signal invalid due to malfunction in the device, sensor, or actuator	Medium severity: permissible ambient or process conditions exceeded or the measuring uncertainty of sensors or deviations from the set value in actuators is probably greater than expected	Low severity (advisory): although the signal is valid, the remaining life is nearly exhausted or a function will soon be restricted due to operational conditions e.g. aging of a pH-electrode.	Signal temporarily invalid (e.g. frozen) due to on-going work on the device.

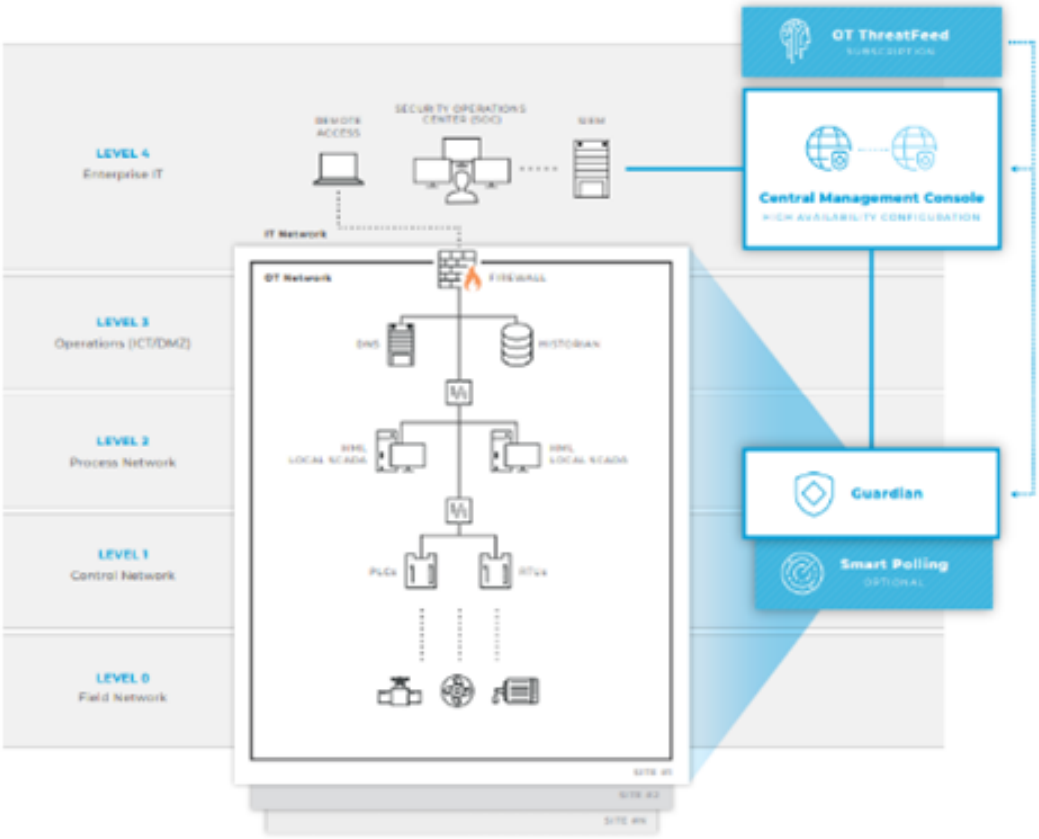
Fonte: NAMUR (2019)

Mais de 3.500 instrumentos são monitorados em diferentes ilhas de processo via este sistema de gerenciamento. Para este trabalho, a gerencia de manutenção criou um centro de soluções industriais no início de 2017 com expansão em 2018 e 2019. Atualmente uma equipe composta de 8 pessoas monitora os instrumentos no regime 8/5 (horas/dias) e endereça os problemas identificados.

4.2 REDES DE AUTOMAÇÃO

No cenário inicial recebido da equipe de projeto, para a rede de automação não foram previstos ou recebidos softwares de gerenciamento. Neste caso, a equipe de manutenção fez um diagnóstico para implementar um sistema de gerenciamento das redes. Para as redes de campo (PROFIBUS), foi testado ferramentas tais como COMBRICKS via PoC (*Proof of Concepts*) para monitoramento de redes industriais em uma das grandes áreas da fábrica, ferramenta esta que reporta para um centro de soluções e analistas específicos avaliam as mensagens e alertas, para as demais áreas será expandido nos próximos anos padronizando o parque todo. Para as redes Ethernet foi testado através de PoC uma ferramenta de detecção de vulnerabilidade chamada *Scada Guardian* da Nozomi Networks, a qual monitora toda a rede TCP/IP da rede de automação. Esta ferramenta fornece monitoramento 24/7, onde todos os pacotes de comunicação são espelhados e analisados pela ferramenta, que é passiva e possui característica de IDS (*Intrusion Detection System*) e um layout está representado na Figura 5.

Figura 5 – Exemplo de uma topologia que pode receber o monitoramento de redes de Automação via Scada Guardian da Nozomi Networks.



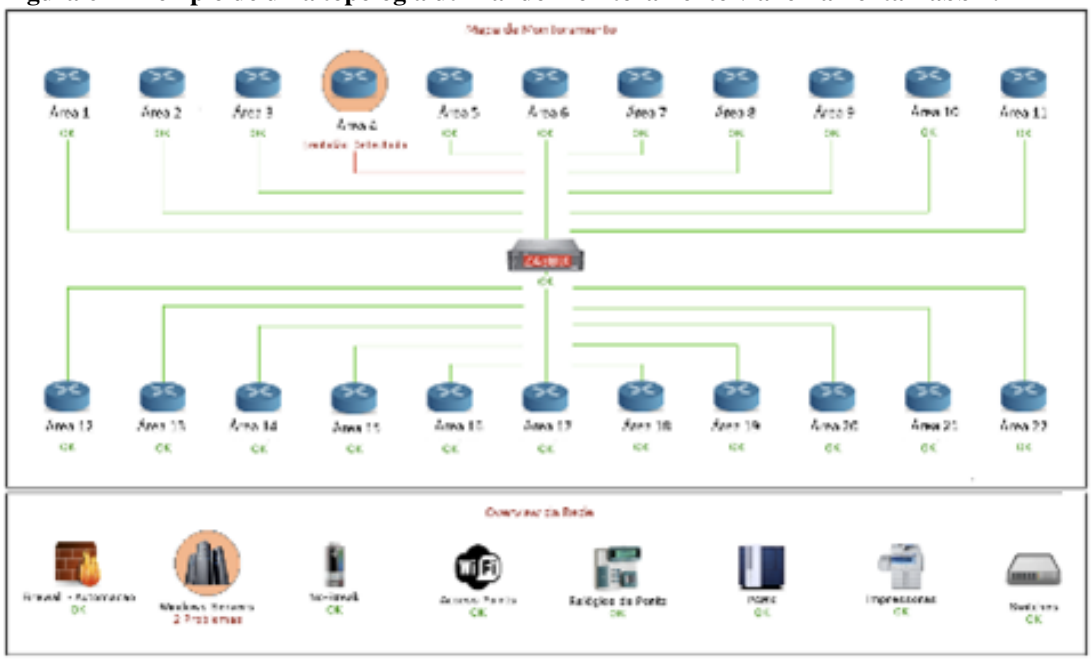
Fonte: (NETWORKS, 2020)

O modelo da Figura 5 é montado automaticamente pela ferramenta, utilizando modelo de Purdue, facilitando a visualização entre zonas ou níveis.

4.3 ATIVOS DA REDE DE CONTROLE

Quanto aos ativos da rede de controle, estações, servidores, *switches*, roteadores, não foi planejado nenhuma ferramenta para monitorar estes ativos. Para tal foi observado outras fábricas do grupo, a qual utilizavam uma ferramenta *"open source"* chamada Zabbix, a qual é uma solução de monitoração integrada, que provê diversos recursos de monitoração em um único pacote e suporta SNMP (tanto "*trapping*" quanto "*polling*"), IPMI, JMX, monitoração VMware conforme exemplo da Figura 6.

Figura 6 – Exemplo de uma topologia utilizando monitoramento via ferramenta Zabbix.



Fonte: (NETWORKS, 2020)

Esta ferramenta foi instalada numa máquina na DMZ do segmento de automação e que monitora estações e servidores através do protocolo SNMP utilizando *polling*, um protocolo já consagrado e passivo as redes de controle. No processo de implantação, dificuldades devido segmentação de rede foi encontrado, bem como endereços IP's da rede de automação duplicados em diferentes áreas de processo. Regras de *firewall* precisaram ser construídas para permitir acessos bem como NAT's (*Network Address Translation*) para permitir as conversões de endereço IP necessária em áreas onde haviam duplicações.

4.4 INTEGRAÇÃO COM TI

Um dos itens que limitavam integrações futuras, a duplicação de endereços IP's entre rede de TA e TI (item que foi planejado e corrigido em 2017) e dentro da rede TA de diferentes ilhas de processos. Essa duplicação dentro da rede ainda não está totalmente corrigida devido complexidade de se alterar sem gerar efeitos colaterais, e foi contornado por NAT's (*Network Address Translation*) feitos em roteadores. Outro item trabalhado no case em questão, foram regras de *firewall*, de maneira a dar consistência nas proteções inicialmente inseridas.

5 DISCUSSÃO

Com a aplicação das ferramentas MRC (Schneider Electric) para monitorar ativos de campo (instrumentos e dispositivos eletroeletrônicos), Zabbix monitorando estações e servidores e, Scada Guardian e COMBRIKs monitorando as redes, os elementos presentes na unidade fabril estão sendo monitorados 24/7 (horas/dia). Com um centro de soluções que faz a interpretação dos alertas, ainda no modelo 8/5 (horas/dia), um número substancial de eventos tem disso evitados por estarem sendo diagnosticados antecipadamente. Há potencial de maximizar estes monitoramentos e expandir o programa ainda mais, fazendo a abrangência do monitoramento de redes Profibus, bem como a expansão do plano de ação para demais unidades do grupo estudado. Independente da ferramenta que for usada, monitorar ativos traz ganhos na redução da indisponibilidade, antecipação das falhas via alertas trazidos dos instrumentos de campo, podendo programar correção antes do ativo entra em falha fatal (falha onde gera indisponibilidade do equipamento ou quando há perda de função do ativo). Ter um sistema de gerenciamento de ativos possibilita flexibilidade ao time de manutenção e operação, aumento competitividade devido redução de indisponibilidade e redução de custo.

6 CONCLUSÃO

Pode-se concluir que o caminho é promissor no monitoramento de ativos, especialmente os ativos de automação, que por si só possuem tecnologia embarcadas já a há algum tempo, mas que tem sido cada vez mais explorada usando os avanços da Industria 4.0 e da integração entre TI/TA. Conclui-se também, que esta experiência relatada neste trabalho que teve por objetivo vivenciar uma experiência de implantação de um sistema de monitoramento de ativos de automação (estações, servidores, etc.) foi concluída com sucesso, onde através de um conjunto de três ferramentas foi possível monitorar desde o instrumento de campo, passando pela rede de campo (até chegar nos controladores) e pelas redes de controle até o limite de baterias com TI (Firewall). Pode-se notar que, evitar paradas não programadas, maximizando o resultado da empresa é algo muito bem aceito e necessário. Neste trabalho, foi possível perceber que, com ferramentas disponíveis em mercado, sejam elas "*open source*" como o Zabbix para monitoramento via protocolo SNMP, ou como COMBRIKs/Scada Guardian, há um potencial muito grande para ser explorado e que espera ser potencializado com a Industria 4.0 e com integração entre TI/TA, contudo se não for planejado pode tomar caminho reverso, em vez de ter redução de indisponibilidade, podem haver ocorrências de perda de função de dispositivos ou abertura para exploração de vulnerabilidades. Conclui-se também que ainda há muito o que se fazer para dar como concluído o step atual do case analisado, contudo bons resultados já foram apresentados com base nas ferramentas apresentadas neste artigo, em visibilidade das redes industriais e dos dispositivos de campo. Julga-se importante a continuidade dessa discussão com mais abordagens, mais ferramentas, comparativos, etc.

REFERÊNCIAS

ALTUS. **Como fica a segurança cibernética com a convergência entre TI e TA**. 2012. <https://www.altus.com.br/blog/categoria/2/detalhe/148/como-fica-a-seguranca-cibernetica-com-a-convergencia-entre-ti-e-ta-3F>. Acesso em: 21 de setembro de 2019.

ANSI. Isa–99.00. 01–2007 security for industrial automation and control systems part 1: Terminology. **Concepts, and Models**, 2007.

FERNANDES, Luciana. **Cibersegurança: conheça as principais ameaças e entenda porque a automação é relevante.** 2017. <https://suntech.com.br/artigos/ciberseguranca-conheca-as-principais-ameacas-e-entenda-porque-automacao-e-relevante/>. Acesso em: 22 de setembro de 2019.

FLORES, Sandra. **Citação de referências e documentos eletrônicos**. 2014. <https://www.lecom.com.br/blog/7-pontos-positivos-sobre-integracao-vertical-em-revendedoras-de-tecnologia-da-informacao>. Acesso em: 21 de setembro de 2019.

ISO, TC; SC, N. Asset management—overview, principles and terminology. 2014.

LAFRAIA, J.R.B. Gestão de ativos: Benefícios de desafios. **1º Encontro de Gestão de Ativos para Empresas do Setor Elétrico. Barueri/SP**, 2014.

LEE, Jay *et al.* Recent advances and trends in predictive manufacturing systems in big data environment. **Manufacturing letters**, Elsevier, v. 1, n. 1, p. 38–41, 2013.

MOSQUIN, João Carlos; RODRIGUES, Daniel Lyra. Gestão de projetos como um processo da gestão de ativos - uma integração necessária. **VI Simpósio Internacional de Gestão de Projetos, Inovação e Sustentabilidade (SINGEP), São Paulo, S.P.**, p. 3–4, 2017.

NETWORKS, Nozomi. **Centralized OT Visibility and Cyber Security for Distributed Deployments**. 2020. <https://www.nozominetworks.com/products/central-management-console/>. Acesso em: 10 de fevereiro de 2020.

RAMOS, Jorge. **TI e TA: convergência ou divergência.** 2012. <https://computerworld.com.br/2012/08/06/ti-e-ta-convergencia-ou-divergencia>. Acesso em: 21 de setembro de 2019.

TAMMELA, Iara; CHAVES, Luiz A. O.; NETO, Edio P. Gestão de ativos de automação: Uma aplicação em plataformas marítimas de produção de petróleo. **XXXVI Encontro Nacional de Engenharia De Producão, 16., João Pessoa. João Pessoa: UFF – Centro de Tecnologia.**, p. 3, 2016.

TECLÓGICA. **Citação de referências e documentos eletrônicos**. 2018. <https://blog.teclogica.com.br/integracao-vertical-na-industria-4-0/>. Acesso em: 21 de setembro de 2019.

TURCATO, Afonso Celso *et al.* Ataque denial of service em redes profinet: Estudo de caso. **XII Simpósio Brasileiro de Automação Inteligente, Natal, RN**, p. 217–222, 2015.