XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E TRANSMISSÃO DE ENERGIA ELÉTRICA

22 a 25 de outubro de 2017
Curitiba - PR

CB/GTL/27

GRUPO - XV

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL

SEGURANÇA CIBERNÉTICA – INTEGRAÇÃO ENTRE AS EQUIPES DE TI E TO E AS AÇÕES DA COPEL PARA GARANTIR A SEGURANÇA NAS REDES OPERATIVAS

Claudio Hermeling (*)
Copel GeT

Arlenio Carneiro Frisch
Copel GeT

Tiago Manczak
Copel GeT

RESUMO

O uso do padrão Ethernet em redes operativas implicou em uma convergência entre ambientes de Tecnologia da Informação - TI e Tecnologia da Operação - TO. Isto leva à adoção de procedimentos e melhores práticas de segurança da informação em TO, já estabelecidas em TI.

Essa convergência conferiu aos sistemas de automação uma grande flexibilidade para integração com os demais sistemas. Considerando que a convergência foi lenta e gradativa, muitos conceitos e controles aplicados em sistemas de TI não foram necessariamente replicados ou aplicados na TO, preocupando-se exclusivamente com questões operacionais dos sistemas.

Para reverter esse cenário, um grupo multidisciplinar de segurança cibernética foi criado para implementar controles e procedimentos necessários à TO da Copel.

PALAVRAS-CHAVE

Tecnologia da Informação, Tecnologia de Operação, Convergência TI x TO ,Segurança cibernética, Automação

1.0 - INTRODUÇÃO

Muitas tecnologias utilizadas em sistemas de TI (Tecnologia de Informação) também tem sido aplicadas em sistemas de TO (Tecnologia da Operação), também chamado de TA – Tecnologia de Automação, ao longo do tempo, em virtude de origens comuns baseadas em computadores, redes de comunicação, protocolos de comunicação, linguagens de programação e bancos de dados.

Porém, TI e TO, como áreas distintas nas empresas, apesar de baseadas em processos muito semelhantes, fizeram com que esta falta de convivência levasse ao uso de procedimentos, técnicas e controles de forma bem diferente: a TI corporativa, a partir de exigências das demais áreas da empresa e também de órgãos externos e entidades legais, levou a uma revisão de seus processos e a uma adequação de seus procedimentos às melhores práticas mundiais, enquanto que as áreas de TO, por sua vez, por não ter tido este tipo de exigência, e também por se tratar de ambiente mais técnico e controlado, e de certa forma desconhecido pelas demais áreas da empresa, não teve, até o momento, uma cobrança por maior transparência em seus processos, e uma exigência de controles mais rígidos.

Como as tecnologias adotadas por TI e TO estão cada vez mais semelhantes, isto pode ser um ponto a ser preservado rumo à integração. A integração entre estas áreas, no sentido de convivência e troca de experiências é inevitável, mesmo se persistirem algumas pequenas diferenças no caminho, que são transponíveis por meio da

(*) rua José Izidoro Biazetto, n° 158 – Bloco A – CEP 81200-240 Curitiba, PR, – Brasil
Tel: (+55 41) 3331-2186 – Fax: (+55 41) 3331-3575 – E-mail: hermeling@copel.com

melhor definição dos papéis de cada uma das duas áreas. Para a avaliação da situação atual da segurança da informação em TO, a comparação com a TI e proposta de ações, foi criado um grupo multidisciplinar para o tratamento do assunto.

2.0 - DESENVOLVIMENTO

Pretende-se demonstrar as origens comuns aos dois ambientes, relativo às tecnologias de comunicação adotadas e suas semelhanças, bem como um comparativo das diferenças entre algumas de suas atividades, e que explicam parcialmente a situação atual. Também é sugerido, ao final do artigo, que há necessidade do início de um diálogo entre as partes para o entendimento e comparação entre os processos e procedimentos, similaridades e diferenças, de forma a evoluir para uma forma de convivência e contribuição entre as áreas, para um maior ganho entre as mesmas, e por consequência, à própria corporação.

2.1 Conceituação dos Sistemas SCADA

Sistemas SCADA são sistemas que permitem monitorar, através da aplicação de sensores e equipamentos diversos, partes ou o todo de um processo industrial. Este processo industrial pode ser um processo de manufatura de uma fábrica, os processos de geração, transmissão ou distribuição de energia elétrica, processos de tratamento e distribuição de água, de gás, etc., com o objetivo de supervisionar e controlar o processo através das variáveis do mesmo.

2.2 Dispositivos utilizados

Estas variáveis são coletadas a partir de dispositivos de sistemas de controle, como CLPs – Controladores Lógicos Programáveis, UTRs – Unidades Terminais Remotas, relés de proteção ou outros dispositivos, que estão diretamente ligados às grandezas e equipamentos do processo controlado, como sensores, que monitoram grandezas físicas, bem como atuadores, que permitem ações de controle sobre o sistema.

Estes dispositivos convertem os parâmetros físicos de medidas (como corrente, tensão, potência, fluxo, velocidade, etc.) e de estados de equipamentos (disjuntores, chaves, válvulas, etc) em sinais elétricos que serão recebidos pelos dispositivos de sistemas de controle, e estão instalados junto ao processo. A informações de entrada e de saída destes dispositivos podem ser do tipo analógico ou digital. As saídas destes dispositivos, que são as medidas ou os estados dos equipamentos supervisionados do processo são enviadas ao sistema de supervisão e controle, para o devido tratamento. As entradas destes dispositivos são os comandos vindos do sistema de controle, do tipo digital para ligar ou desligar equipamentos, ou ainda, do tipo analógico, para controle de determinada grandeza física, em que o dispositivo deve fazer com que determinada medida do processo evolua do valor atual para o valor recebido.

2.2.1 Conexão entre dispositivos e sistemas de controle

Estes dispositivos de sistemas de controle são conectados ao sistema de supervisão e controle através de canais de comunicação, utilizando-se *drivers* específicos, utilizando-se uma variedade de protocolos de comunicação. Estes *drivers* são programas de computador instalados tanto no lado do dispositivo como no sistema supervisório, que são responsáveis pela comunicação entre o sistema operacional e o sistema de supervisão. Esta comunicação refere-se à troca de mensagens previamente estabelecida entre os dois equipamentos, de forma a transferir os dados do dispositivo para o sistema de supervisão, bem como para o sistema de supervisão emitir comandos para os dispositivos. Este conjunto de mensagens definidas é chamado protocolo de comunicação. O mercado utiliza a sigla SCADA para os sistemas de Supervisão, Controle e Aquisição de Dados.

2.3 Protocolos de comunicação

Estes protocolos podem ser proprietários ou padronizados. Os proprietários são protocolos ditos fechados pois, a princípio, são conhecidos apenas pelo fabricante que o desenvolveu. Estes tipos de protocolo foram muito comuns nas décadas iniciais dos processos de automação, uma vez que não existia interesse da indústria em padronizá-los. A partir de determinado momento, o mercado percebeu a necessidade de padronização dos protocolos, para facilitar o intercâmbio de componentes dos sistemas, independentemente do fornecedor e também, para diminuição de custos da fabricação e da integração dos equipamentos, uma vez que o fabricante utilizaria a base definida de um protocolo padrão, sem necessidade de investimentos, comparando-se com um protocolo proprietário. Por parte da integração, o processo também fica mais eficiente, uma vez que o protocolo padronizado evita o desenvolvimento de gerenciadores de comunicação por parte do integrador, que é a empresa responsável pela implementação e implantação do sistema automatizado, assim como também ocorre a diminuição de custos com formação e treinamento de equipes de campo em diversos tipos de protocolos.

2.3.1 Protocolos utilizados em sistemas de supervisão para energia

Os protocolos de comunicação entre equipamentos e sistemas de supervisão e controle para a área de energia evoluíram da forma descrita acima. Inicialmente foram utilizados protocolos proprietários, definidos pelo próprio fabricante do dispositivo ou ainda, pelo fabricante de toda a solução de supervisão e controle.

A partir da década de 90, baseado no protocolo IEC 60870-5, foi proposto o protocolo DNP3 (*Distributed Network Protocol*) por um grupo de fabricantes e empresas, principalmente norte-americanas, para permitir a interoperabilidade entre vários fornecedores SCADA para a rede elétrica. Este protocolo baseia-se em um conjunto de protocolos de comunicação utilizados entre componentes de automação de processos de sistemas. Seu principal uso é em concessionárias de serviços, tais como empresas de energia elétrica e saneamento. Desenvolvido para comunicação entre dispositivos de aquisição de dados e equipamentos de controle, o protocolo desempenha um papel crucial nos sistemas , onde é utilizado pelas estações SCADA dos centros de controle, nas UTRs - Unidades Terminais e em IEDs – *Intelligent Electronic Devices*, ou Dispositivos Eletrônicos Inteligentes.

Também na década de 90, a partir 1995, um grupo de trabalho do IEC - *International Electrotechnical Commission*, ou ainda, Comissão Eletrotécnica Internacional, formado por cerca de 60 membros de diferentes países, iniciou a definição de outro protocolo de comunicação para sistemas elétricos, o IEC 61850. Os objetivos definidos para o padrão foram: um protocolo único para subestação completa, considerando dados de modelos diferentes necessários para subestação; definição de serviços básicos necessários para transferir dados para que todo o mapeamento para protocolo de comunicação pode ser feita à prova de futuro; promoção de alta interoperabilidade entre os sistemas de diferentes fornecedores; um método/ formato comum para armazenar dados completos; e a definição de um teste completo necessário para o equipamento que está em conformidade com a norma.

2.3.2 Meios de comunicação entre os equipamentos

A conexão entre os sistemas e equipamentos era estabelecida através de canais de comunicação seriais em ambientes completamente controlados, em comunicação chamada mestre-escravo, na década de 80. O dispositivo era conectado ao computador através de cabos metálicos, com velocidades baixas, tipicamente entre 300 a 19.200 bps – bits por segundo, podendo chegar a 115.200 bps, e com restrição de distância entre os mesmos, devido à queda de sinal ao longo do cabo. Exemplos desta comunicação serial são os padrões RS-232, criado originalmente pela EIA – Electronics Industries Association, ou Aliança das Indústrias Eletrônicas e o RS-485, mantido pela Modbus Organization, ou Organização Modbus.

Esta conexão evoluiu para comunicação ponto-a-ponto na década de 90, e utilizada até o final da década de 90 e início dos anos 2000. Este tipo de comunicação é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central. Cada computador da rede é um nó (ponto de interconexão da rede) e fica responsável por uma parcela dos recursos da rede, tais como armazenamento, poder de processamento e largura de banda. Os recursos são divididos diretamente entre cada participante da rede sem a necessidade de uma coordenação central de um servidor ou *host*. Nesse modelo de rede, cada par de computadores são fornecedores e consumidores de recurso, diferentemente do modelo cliente-servidor, onde o servidor alimenta toda a rede e os clientes somente consomem.

A partir de meados da década de 90, o mercado direcionou os meios de comunicação entre estes sistemas e os dispositivos para a utilização de redes padrão Ethernete TCP/IP, que permitiu uma maior facilidade de instalação, interligação e comunicação entre os equipamentos. Esta rede é uma arquitetura de interconexão para redes locais - Rede de Área Local (LAN – *Local Area Network*) - baseada no envio de pacotes. Ela define cabeamento e sinais elétricos para a camada física, em formato de pacotes e protocolos para a subcamada de controle de acesso ao meio. A partir dos anos 90, ela vem sendo a tecnologia de LAN mais amplamente utilizada e tem tomado grande parte do espaço de outros padrões de rede.

2.3.3 Rede Ethernet TCP/IP em Redes Operativas

No início da década de 90, com a necessidade de expansão das redes locais, iniciou-se o uso de redes ethernet TCP/IP em redes operativas, sendo criticada inicialmente, por não ser determinística, pois não permite determinar com precisão o tempo necessário para a transferência de informações entre os integrantes da rede. Mesmo assim, foram adotadas, permitindo então chegar a taxas de velocidade de 10 Mbps e, a partir de testes realizados, verificar que o fato de não ser determinística não seria um problema. Com a facilidade e praticidade de uma rede única, foi possível integrar equipamentos de diversos fornecedores. Além da velocidade e da praticidade de uma rede única, ganhou-se também no custo, pois as placas Ethernet eram produzidas em larga escala e a um custo mais baixo, comparando-se com placas dedicadas de mercado restrito.

2.4 Convergência TI x TO

O uso do padrão Ethernet em redes operativas, aliado ao uso de outras tecnologias típicas de TI em ambiente TO, implicou em uma convergência técnica entre os ambientes de TI – Tecnologia da Informação e de TO – Tecnologia da Operação.

A migração das tecnologias de TI para o ambiente industrial continua ocorrendo em diversas frentes, como segurança da informação, integração de sistemas e gerenciamento da produção.

2.4.1 Comparação entre TI e TO

Em uma definição mais simples, Tecnologia da Informação pode ser definida basicamente como o uso de computadores, software, hardware e outros dispositivos utilizados para realizar operações de negócio, sendo que estes dispositivos estão localizados principalmente em locais de escritórios, salas de servidores e *data centers*, ou centro de dados. Esta tecnologia está associada com funções de base da empresa, que são utilizadas para executar várias operações de negócio, como contabilidade, faturamento, arrecadação, recursos humanos, gerenciamento de ativos, etc.

Também em uma definição mais simplificada, a Tecnologia de Operação está associada com os dispositivos baseados e instalados em campo junto ao processo produtivo, tais como computadores, software, hardware, roteadores e outros dispositivos, e que são utilizados para realizar operações no processo, sendo que eles estão operando em ambiente em tempo real ou quase tempo real.

Considerando-se as definições acima e as tecnologias adotadas descritas, pode-se afirmar que são áreas que utilizam equipamentos equivalentes, mas com objetivo e formas diferenciadas.

Em TI, as redes de comunicação coletam e distribuem dados e informações para tomada de decisão, sendo que a largura de banda é compartilhada. Em TO, são os dispositivos e métodos definidos, como regras e algoritmos, que controlam, manual ou automaticamente, um processo industrial, sendo que o processo exige largura de banda dedicada.

Em ambientes de TI, procura-se ocupar o máximo uso da banda, em uma forma de uso de muitos para muitos. As configuração dos ambientes e tecnologias é avançada, utilizando-se ao máximo as funcionalidades, com ambiente com mudanças frequentes. Em TO, a latência deve ser mínima e determinística, para a garantia da execução dos processos dentro de faixas de tempo aceitáveis e previamente definidas, com um ambiente de poucos para poucos. A configuração do ambiente é simplificada, com poucas mudanças, para evitar a execução de testes de aceitação repetitivos.

Com relação a endereços, enquanto em TO utiliza-se endereço MAC estático e configuração de IP fixo, em TI, MAC e IP não são fixos, adotando-se outras técnicas de identificação.

Com relação a aplicações, em ambiente TO, estas são específicas para o processo sob supervisão e controle e exigem robustez, para evitar-se descontinuidades desnecessárias, enquanto que em TI as aplicações são diversas.

Como exemplo, na comparação de características entre TI e TO, uma diferença importante entre estas tecnologias é que a TI "**movimenta**" as informações, enquanto que a TO "**utiliza**" as informações.

De uma forma geral, utilizando-se um exemplo mais abrangente, apesar da semelhança de uso de equipamentos e tecnologias, e da adoção de processos similares, há uma grande diferença entre as políticas de redes de TI e de TO. Parte destas diferenças é mostrado em um comparativo na tabela 1, abaixo:

Tabela 1 – Comparativo de políticas de rede entre TI e TO

Redes e computadores de TI	**Redes SCADA**
Perda de dados e interrupções toleradas (restauração de back-ups e reinicialização de máquinas)	Perda de dados e interrupções não tolerados (podem resultar em sérias consequências – danos a equipamentos e possíveis perdas de vidas
Altas taxas de dados são necessários, atrasos podem ser tolerados	Tempos de resposta determinística em loops de controle; respostas em tempo real são necessárias; atrasos e downtimes não podem ser tolerados
Recuperação sempre após reboot	Sistemas devem ser tolerantes a falhas – redundantes, ou ter "hot Backups"
Software antivírus largamente usado	Software antivírus é difícil de ser aplicado na maioria das

Redes e computadores de TI	Redes SCADA
	vezes, porque atrasos não podem ser tolerados e determinismo nos tempos de resposta devem ser preservados
Treinamento e conscientização em segurança de sistemas é razoavelmente alto	Treinamento em segurança raramente ocorre
Uso de criptografia	Maioria dos sistemas transmite dados e mensagens de controle em texto claro, ou protocolos conhecidos.
Testes de invasão amplamente utilizados	Testes de invasão não são rotineiros e, quando realizados, não podem afetar os sistemas de controle
Implementação de patches é comum	Implementação de patches feita com pouca frequência e normalmente requer apoio dos fabricantes
Auditorias de segurança são necessárias e realizadas rotineiramente	Auditorias de segurança da informação normalmente não realizadas.
Equipamentos normalmente substituídos a cada 3 a 5 anos	Equipamentos utilizados por longos períodos de tempo, sem substituição

2.4.2 Integração entre TI e TO

Em função das similaridades entre ambientes TI e TO e apesar de suas diferenças de uso e forma de aplicação, é importante que as empresas percebam a necessidade de uma integração entre as equipes envolvidas. Esta integração entre equipes não envolve, necessariamente, a reestruturação destas áreas, ou ainda, a sua junção ou separação de atividades entre as mesmas, mas uma convivência para a troca de experiências e conhecimentos, do entendimento das características, das funcionalidades e da complexidade do ambiente de uma equipe, pela outra equipe, de forma a identificar exatamente as semelhanças e as diferenças entre as mesmas. Isto pode permitir um olhar mais abrangente no qual, práticas e procedimentos mais elaborados de uma equipe possa ser entendida e aplicada na outra e vice-versa.

Baseado em modelos existentes e adotados como referência em empresas de TI e também em áreas de TI de empresas, são diversos processos adotados pela TI e que podem ser comparados e adotados em TO, como por exemplo, entre outros:

- Prover e manter soluções de software;
- Prover e manter infraestrutura;
- Gerenciar mudanças;
- Gerenciar ativos;
- Gerenciar a segurança da informação;
- etc.

Isto pode levar à adoção de procedimentos e melhores práticas de segurança em TO, já estabelecidas em ambiente TI, em função da exigência da existência destes controles pelo negócio.

2.5 Ações da Copel GeT – Copel Geração e Transmissão

O sistema de automação de subestações e usinas da Copel Geração e Transmissão SA – Copel GeT foi concebido inicialmente, ainda na década de 1980, com protocolos proprietários que integravam equipamentos dedicados via comunicação serial ponto-a-ponto. Durante 20 anos, esse padrão de integração prevaleceu nas instalações, criando um conceito de sistema isolado de protocolos obscuros. Entretanto, gradativamente, houve uma convergência de tecnologias de sistemas aplicados entre a tecnologia de informação e a tecnologia de automação. Além disso, os protocolos outrora proprietários e considerados obscuros também foram substituídos por aqueles padronizados por normas dos quais citam-se IEC60870-5-104, DNP3, IEC61850.

Essa convergência conferiu aos sistemas de automação uma grande flexibilidade para integração com demais sistemas, como centros de operação centralizados e sistemas corporativos. Considerando que a convergência foi lenta e gradativa, muitos conceitos e controles aplicados em sistemas de tecnologia da informação não foram replicados na tecnologia de automação, preocupando-se exclusivamente com as questões operacionais dos sistemas. Conceitos como o de rede isolada e o de obscuridade de protocolos continuaram sendo adotados nas redes de automação, apesar de em alguns casos não serem mais aplicáveis.

Para reverter esse cenário, um grupo multidisciplinar de segurança cibernética foi criado para implementar os controles e procedimentos necessários à tecnologia de automação da Copel GeT, e composto por profissionais de diversas áreas de conhecimento, como automação de sistema elétricos, ou TO, da geração, transmissão e distribuição; de TI, desenvolvimento de sistemas, infraestrutura TI de redes e segurança em redes e *endpoints*; de

segurança da informação corporativa; e de telecomunicações, na parte de planejamento e fornecimento de redes IP.

Entre as ações que estão sendo tomadas para mitigar qualquer falha que possa ocorrer nas redes operativas, se destaca:

- Mapeamento de todas as redes de automação: de usinas, de subestações da Transmissão e de subestações e redes da Distribuição;
- Participação em Eventos de segurança cibernética;
- Participação de grupo de trabalho em segurança cibernética do setor elétrico;
- Provas de conceito para ajudar nas definições soluções de *firewall* de próxima geração e software de monitoramento de rede, visando melhoria nas proteções de fronteiras com outros sistemas e outros agentes do setor elétrico;
- Projeto piloto para estudo de implementação de soluções para melhoria na segurança cibernética das redes de automação da Copel GeT;
- Comparativo de segurança entre as redes corporativas e as redes operativas;
- Mapeamento das necessidades de trabalho para adequação dos procedimentos e normas de segurança para as redes operativas; e
- Mapeamento das necessidades de alterações na segurança física de equipamentos.

2.5.1 Prova de conceito

O principal objetivo desse trabalho foi a análise da captura dos pacotes da rede IP de automação de subestações e usinas de Copel. A análise desse tráfego visava evidenciar presença de pacotes indesejados, o que seria um indício de vulnerabilidades presentes nos sistemas de automação. Outro objetivo foi utilizar esse estudo para orientar a definição de uma especificação técnica de *firewall* de próxima geração para aplicação nas redes operativas.
Foram selecionados 3 fabricantes de *firewall* para inspecionar o tráfego em diferentes instalações da Copel. Como critério de seleção foi utilizado o quadrante mágico para *firewall* corporativos do relatório da Gartner de 2016.
Os resultados serão analisados e irão direcionar algumas ações importantes para a segurança das redes.

2.5.2 Projeto piloto

Está sendo elaborado um projeto piloto em segurança cibernética para as redes operativas, que permitirá aperfeiçoar e monitorar as redes de infraestrutura críticas da Copel GeT. O escopo do projeto inclui o estudo e implementação das soluções de segurança cibernética em instalações que representam uma amostra dos diferentes modelos de instalações sob concessão da Copel GeT.

2.5.3 Comparativo de segurança entre redes corporativas e as redes operativas

Foi realizado o comparativo entre as redes de TI e TO e verificado onde as soluções adotadas em TI podem ser utilizadas no ambiente TO e as devidas adequações para minimizar custos e impactos nas implementações.

2.5.4 Plano de ação

Com base nos mapeamentos realizados nas redes operativas foi elaborado e apresentado à Diretoria da Copel GeT o plano de ação com todas as atividades e ações relacionadas que precisam ser realizadas ao longo do ano, incluindo os projetos e solicitação das verbas necessárias para o ano seguinte.

3.0 - CONCLUSÃO

A partir das informações apresentadas neste documento e alguns exemplos mostrados, pode-se afirmar que as tecnologias adotadas por TI e TO estão cada vez mais semelhantes, especialmente no que se refere aos desafios na gestão de sistemas. Até porque TI e TO possuem algumas raízes comuns, e isto pode ser um ponto a ser preservado rumo à integração.

Com o passar do tempo, as divergências devem despertar o conhecimento visando a convivência necessária e saudável entre TI e TA, e isso graças à tecnologia. Com base nesse histórico, a integração é inevitável, mesmo ao se persistirem algumas pequenas pedras pelo caminho, totalmente transponíveis por meio da melhor definição dos papéis de cada uma das duas áreas. E essa disposição pode gerar espaço ilimitado para um acordo e, mais do que isso, a descoberta de infinitas possibilidades conjuntas entre TI e TA.

Contudo, não se deve imaginar que seja tarefa fácil e que possa ser alcançada em curto ou médio prazos. A persistência é o grande valor agregado nessa discussão. Persistência em continuar na atitude proativa de concórdia e entendimento, o que tem trazido rica experiência aos profissionais envolvidos e resultados

surpreendentes para as empresas, mesmo para as que tenham tido de implementar mudanças drásticas em suas estruturas. Vale lembrar que inovação não é moda, mas uma alternativa – se não a única – para uma companhia manter-se competitiva em um mercado globalizado, mesmo em situação confortável economicamente.

Não há previsão de que TI e TO trabalhem juntas no futuro, mas sim que a convivência gere sinergia tal que permita aproveitar todas as competências e habilidades de cada lado. TI ocupando-se de otimizar e garantir o pleno funcionamento do sistema de gestão dos processos corporativos e TO, ou TA, cuidando do bom funcionamento e da segurança dos processos de produção. Não se trata de convergência, nem mesmo de divergência, e sim de convivência.

4.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) BRANQUINHO, Marcelo Ayres, et al., *Segurança de Automação Industrial e SCADA*, Editora Elsevier, 2014.

(2) Campos, Márcia; Paiola, Carlos, M. Sc., *Tecnologia da Informação na Automação: Convergência ou Conflito?* Artigo. Site. <http://www.aquarius.com.br/Boletim/Artigo_Aquarius_InTech123_TAxTI.pdf>, acesso em: 14/07/2016.

(3) Ramos, Jorge, *TI e TA: convergência ou divergência?* Artigo. Site. <http://computerworld.com.br/blog/opiniao/2012/08/06/ti-e-ta-convergencia-ou-divergencia>, acesso em: 14/07/2016.

(4) Copel/ Tecnologia da Informação Intranet. Site. Disponível em: <http://webprd/intra/root/intranetNivel2.jsp?endereco=%2Fintra%2Froot%2Fintranet.nsf%2Flinknomesecoes%2F53EAB7E1865140810325792E0045A1B3>, acesso em 19/09/2016.

5.0 - DADOS BIOGRÁFICOS

Claudio Hermeling nasceu em Porto Alegre, Rio Grande do Sul em 1966. Possui formação técnica em Eletrônica pelo Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense (1990), graduação em Informática pelo Centro Universitário Franciscano do Paraná - UNIFAE (2008), Especialista em Automação Industrial pela Universidade Tecnológica do Paraná - UTFPR (2012). Experiência na área de usinas hidroelétricas , com ênfase em Regulação, Automação Eletrônica e Sistemas digitais, atuando em: Reguladores eletrônicos de velocidade e tensão, controles digitais, controladores lógicos programáveis, comunicação de processos, equipamentos de informática, redes de automação, sistemas de supervisão e controle, banco de dados, programação de sistemas e treinamentos de automação. Experiência em educação na área de informática e automação.