ISSN 2237-0234

A CONTRIBUIÇÃO DA TI PARA AUMENTO DA SEGURANÇA NO AMBIENTE INDUSTRIAL[1]

Cláudio Magno do Carmo[2]
Gleison Marques[3]

Resumo
Os Sistemas de Controle e Supervisão (SCADA) e Sistemas de Controle Industrial com suas tradicionais redes e hardware proprietários, têm sido considerados imunes aos ciberataques que vem causando tantos estragos em sistemas de corporativos. Infelizmente, hoje essa realidade esta bastante mudada. A mudança para padrões abertos, tais como Ethernet, TCP/IP e outras tecnologias da Web vêm deixando hackers e criadores de vírus muito próximos da indústria e estes podem se aproveitar do relaxamento existente em função desta "crença". Como resultado, vemos um crescente número de eventos de segurança impactando na disponibilidade dos sistemas industriais. Um contexto de busca da produção com altos níveis de qualidade e prazos curtos de produção tem levado as empresas a implantar sistemas fortemente integrados, buscando avaliar os resultados em tempo real acelerando a tomada de decisões na cadeia produtiva. Nesta "era da informação", o PIMS é uma das ferramentas mais usadas nesta integração. Além do PIMS, os gerenciadores de ativos, otimizadores de processo e sistemas de execução da manufatura (MES) são integrados aos sistemas corporativos. Esta integração acaba por interligar sistemas antes isolados em ilhas de processo à rede corporativa das empresas. Assim, os sistemas de controle industrial precisam agora de uma atenção especial para o quesito segurança. Este artigo discute os mecanismos de defesa disponíveis atualmente e como a experiência da TI corporativa pode contribuir para aumento da segurança no ambiente da TA durante a implantação de um sistema PIMS, identificando e reduzindo as fragilidades de segurança para uma integração segura nas plantas industriais.
Palavras-chave: Segurança da informação; PIMS; Integração de sistemas.

THE CONTRIBUTION OF INFORMATION TECHNOLOGY TO INCREASE SECURITY IN INDUSTRIAL ENVIRONMENT

Abstract
The Supervision and Control Systems (SCADA) and Industrial Control Systems with their traditional proprietary hardware and networks, have been considered immune to cyber attacks which has caused so much havoc on corporate systems. Unfortunately, today the reality is quite changed. The move to open standards such as Ethernet, TCP / IP and other web technologies is letting hackers and virus writers too close to the industry and they can take advantage of the relaxation existent due to this "belief". As a result we see an increasing number of security events impacting the availability of industrial systems. A context of high levels of production quality, with tight deadlines and low production costs in internal processes has led Brazilian companies to deploy highly integrated systems, with greater collaboration between different users at different levels of the corporation. This integration allows us to evaluate the results in real time enabling the decision-making in the supply chain industries. In this "information age ", PIMS is one of the most appropriate tools for this integration. In the PIMS applications such as asset managers, process optimizers and manufacturing execution systems (MES) are integrated to corporate systems. This integration will eventually interconnect systems previously isolated islands of process to the corporate network of companies. Thus, industrial control systems now need to pay special attention to the safety issue. This article aims to discuss the defense mechanisms available and how the experience of corporate IT can contribute to improved security environment in the TA during the deployment of a PIMS system, identifying and reducing vulnerabilities of security for a safe integration in industrial plants.
Key words: Information security; PIMS ; Systems integration.

[1] *Contribuição técnica ao 16° Seminário de Automação e TI Industrial, 18 a 21 de setembro de 2012, Belo Horizonte, MG.*
[2] *Tecnólogo em Informática, Analista de Sistemas do Departamento de Engenharia e Automação da TSA – Tecnologia em Sistemas de Automação, Belo Horizonte – MG, Brasil.*
[3] *Engenheiro Eletricista, Especialista em Engenharia de Sistemas da TSA – Tecnologia em Sistemas de Automação, Belo Horizonte – MG, Brasil.*

ISSN 2237-0234

1 INTRODUÇÃO – ENTENDENDO O PIMS

O PIMS também chamado de historiador de processo constitui-se num conjunto de módulos de software responsáveis pela coleta, armazenamento e exibição de dados de processo.(1) A função primordial do PIMS é historiar dados por um longo período de tempo e para isto dispõe de algoritmos de compactação e compressão de dados que garantem alto desempenho no armazenamento e recuperação dos dados.
Com os resultados de produção e de qualidade coletados diretamente dos equipamentos de automação, dispensando o preenchimento manual de planilhas, integrados aos sistemas corporativos e gerenciais, pode-se alcançar uma série de benefícios no acompanhamento da produção e da qualidade dos produtos, transformando dados isolados em informações preciosas que poderão ser utilizadas na melhoria contínua da produção. Através das ferramentas analíticas do PIMS podem-se visualizar os dados históricos ou em tempo-real, montar tabelas, gráficos de tendências, sinóticos e relatórios dinâmicos em Excel.
De acordo com a norma internacional ISA-95, que sugere um padrão para integração entre os sistemas industriais (modelo de 5 níveis), o PIMS está inserido no nível 3 e na Figura 1 onde agrupamos os níveis 0,1 e 2, podemos considerar o PIMS na camada intermediária. Nesta arquitetura o PIMS é o elo com a camada inferior (chão-de-fábrica) e o MES com a camada superior.

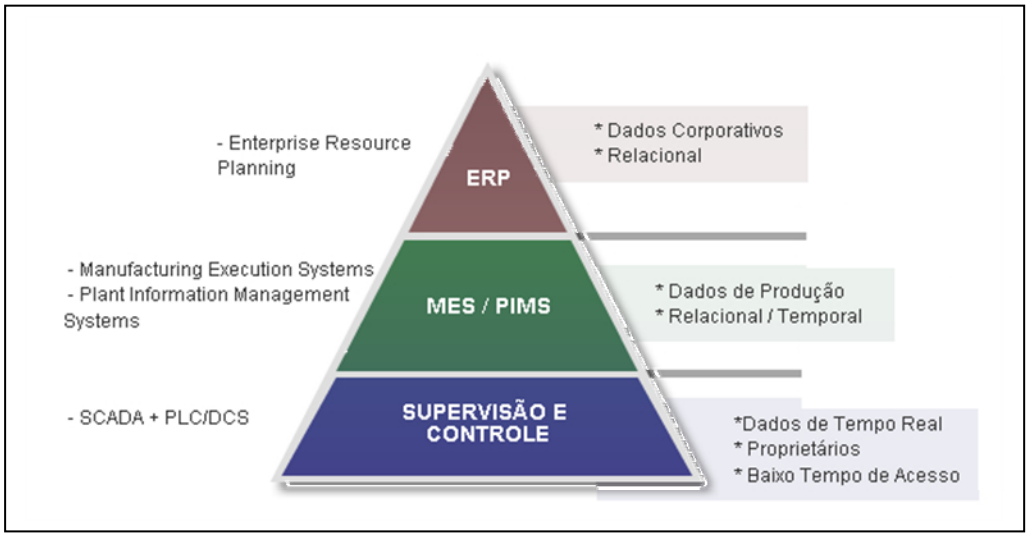

Figura 1- Pirâmide automação.

O desenvolvimento de aplicativos no PIMS permite, além do aprimoramento da qualidade, o acompanhamento dos indicadores (KPI) relacionados a tempos de produção, meio ambiente, saúde e segurança, ocupação, produtividade de equipamentos e pessoas e em alguns casos até custos. A implantação do PIMS com pouquíssima customização e curto prazo, traz alguns benefícios imediatos para os engenheiros e operadores de processo:

- facilidade de análise em tempo-real ou histórica das variáveis de processo;
- interface gráfica similar à fornecida pelos softwares do tipo SCADA, disponível na rede de escritório e não apenas nas salas de controle; e
- análise de falhas e melhorias de processo em função da comparação e correlação de variáveis de processo.

Entretanto, aplicações mais elaboradas podem efetivamente impactar na melhoria de qualidade e redução de custos de produção. Importante reforçar o caráter democrático do PIMS, que permite que os dados exibidos aos operadores dos equipamentos fiquem disponíveis, em tempo-real, para todos os usuários do PIMS em qualquer unidade da empresa.

Aplicativos desenvolvidos usando a plataforma PIMS, baseados em dados de processo coletados em tempo real, executam funções de verificação dos parâmetros operacionais e indicam a ocorrência ou não de desvios nas principais grandezas, como temperatura, pressão, velocidade, corrente, vazão e outras. Em cada etapa de produção é verificada a aderência dos produtos às regras de qualidade, correlacionando as grandezas mencionadas acima, definidas nas normas e procedimentos da empresa. A partir da análise on-line destes desvios, profissionais de processo, de qualidade e de operação, podem tomar decisões quanto à utilização dos subprodutos nas etapas seguintes do processo produtivo, evitando re-trabalhos, desperdícios etc. Esta forma de tratar a qualidade, com foco nas variáveis de processo, reflete diretamente nos índices de produção e qualidade dos produtos finais.

Nas indústrias brasileiras de processos contínuos como: mineração, papel e celulose, cimento, praticamente todos os equipamentos do chão-de-fábrica já estão com alto nível de automação implantado, mas ainda há dificuldade de integração das informações. É bem verdade que há uma grande diversidade de ambientes formados por diferentes tecnologias, mas os coletores de dados do PIMS possuem interfaces genéricas e específicas que garantem a leitura de dados das mais variadas fontes.

1.1 Principais Fabricantes de PIMS

Quadro 1 – Fabricantes de PIMS

Empresa	Produto	Portal
Aspentech	Infoplus.21	www.aspentech.com
OSISoft	PI System	www.osisoft.com
ABB	Enterprise Historian Knowledge Manager	www2.abb.com
Honeywell	Uniformance Process History Database (PHD)	www.hispec.com
Yokogawa	Exaquantum	www.yokogawamarex

1.2 Arquitetura básica do sistema PIMS

Um sistema PIMS basicamente é composto pelos seguintes componentes:

- Servidor Principal do PIMS;
- Servidor de Comunicação do PIMS (coletor); e

- Ferramentas Analíticas.

Além dos componentes duas características importantes devem ser observadas para o melhor funcionamento do sistema PIMS:

- sincronização da base de tempo; e
- disponibilidade do sistema (redundância de servidores e coleta).

A Figura 2 mostra uma arquitetura padrão para uma instalação de PIMS:

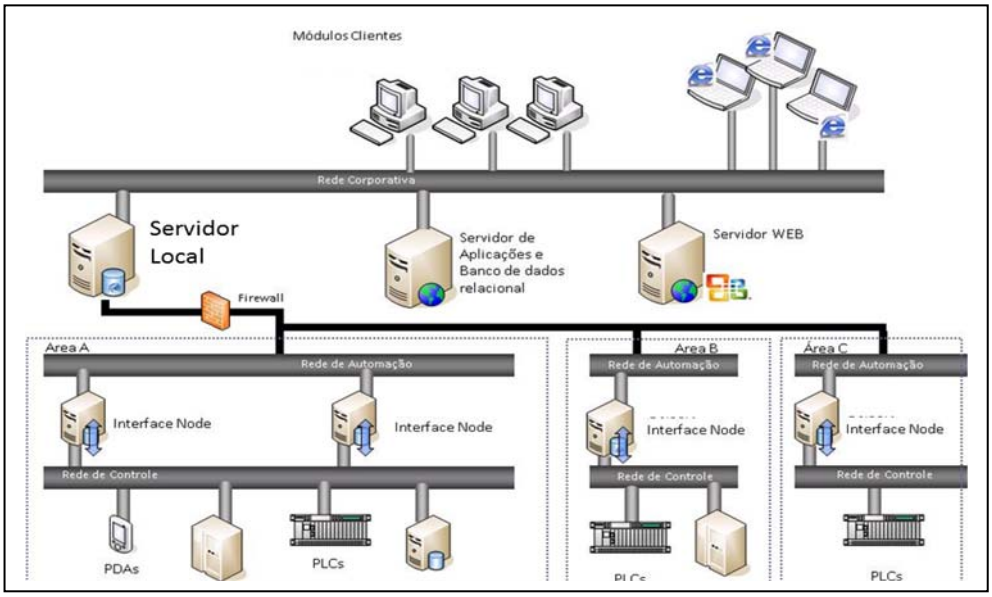

Figura 1 - Arquitetura padrão do PIMS para cada unidade.

1.2.1 Servidor PIMS

O Servidor PIMS, também chamado de Servidor Principal, é o local onde todas as configurações do sistema estão definidas, como segurança, backup, tags, particularidades de coletas e principalmente o banco de dados temporal.

Os dados são coletados do processo através dos servidores de comunicação e enviados ao servidor principal para armazenamento. Os clientes acessam o servidor principal do PIMS para consultar os dados históricos armazenados. Assim, o servidor principal do PIMS é o elo entre os dados e os clientes sendo conectado a dois ambientes computacionais: fontes de dados localizadas no ambiente de T.A. (tecnologia da automação) e usuários locais ou da intranet instalados no ambiente de T.I. (tecnologia da informação).

O PIMS possui diversas aplicações clientes que permitem uma maior integração entre os dados. Estas aplicações podem ser voltadas para processos em bateladas, cálculos avançados, CEP, entre outros, que podem também ficar instaladas neste Servidor, não sendo esta a melhor prática. A recomendação geral é disponibilizar um segundo servidor (Servidor de Aplicações) para hospedar estas aplicações.

1.2.2 Servidor de Comunicação do PIMS (Coletor)

Os computadores responsáveis pela aquisição de dados originados das diversas fontes existentes no site, como: CLPs, SCADA, SDCDs são chamados de servidores de comunicação. Em um sistema PIMS podem existir vários servidores de comunicação atendendo um conjunto de fontes agrupadas por tecnologia, área de processo ou outra regra definida conforme estratégia de negócio ou da estrutura organizacional de uma determinada planta.

Os módulos de softwares que fazem esta coleta são chamados de interfaces, sendo a interface OPC a mais usada atualmente. Os dados podem ser lidos ciclicamente pelo PIMS ou enviados por iniciativa do dispositivo de campo (unsolicited messages/advised). Uma vez aquisitados os dados do processo, a interface se encarrega de enviá-los ao servidor local do banco de dados do PIMS para armazenamento e disponibilização para os usuários através dos aplicativos desenvolvidos especificamente para cada unidade e das ferramentas analíticas de cada fornecedor do PIMS.
Os dados podem ser aquisitados do sistema de controle através da comunicação com o SDCD, ou CLP ou o supervisório (SCADA). A opção de aquisição via SCADA deve ser utilizada somente quando NÃO existir opção de leitura direta do processo (SDCD ou CLP).
As vantagens de se buscar os dados diretamente nos CLPs/SDCD são:

- busca dos eventos com menor atraso temporal, com menor atraso temporal, independente do ciclo de leitura definida no SCADA.
- para redes homogêneas de CLPs (equipamentos de mesmo fabricante) podem-se coletar os dados em um ponto único, se todas as redes de CLPs estiverem interligadas;
- CLPs são mais confiáveis e apresentam menor suscetibilidade a falhas que os sistemas SCADA;
- CLPs são mais estáveis que sistemas SCADA. É normal se fazer o upgrade de sistemas SCADA a cada dois anos devido a novas versões do aplicativo e do sistema operacional. Os aplicativos de CLPs raramente sofrem atualizações na área de interface; e
- sistemas SCADA muitas vezes operam em *hot-standby* o que implica em se definir um mecanismo de redundância também para a aquisição de dados do PIMS.

Estes servidores devem ser especificados conforme características de cada planta, levando em consideração as particularidades de cada ilha de coleta, principalmente o volume de dados.

- **Servidor OPC**

OPC (*OLE for Process Control*) é uma interface de programação padrão, independente de fabricante, através do qual um aplicativo cliente de automação (SCADA, MES, ERP, planilha Excel) pode acessar os dados provenientes de dispositivos remotos, tais como PLCs, SDCD, SCADA, dispositivos de campo. O objetivo é integrar diferentes aplicações dentro da plataforma Windows. O OPC é originário do OLE (*Object Linking and Embedding*) e baseado na tecnologia COM/DCOM desenvolvidos pela Microsoft (1990).
Normalmente, o fabricante do dispositivo de automação (Rockwell, Yokogawa, Siemens, Emerson, Invensys) desenvolve um servidor OPC que se comunica com seus dispositivos através de um protocolo proprietário, mas apresenta uma interface cliente que esconde estas particularidades. Um servidor OPC pode gerenciar vários dispositivos do mesmo tipo. Vários servidores podem ser executados em paralelo e cada servidor pode ser acessado por vários clientes.
Atualmente os Servidores OPCs podem ser diferenciados conforme os tipos de dados solicitados pelas aplicações clientes. São eles:

- OPC DA - *Data Access* - coleta de dados em tempo real;
- OPC HDA - *Historical Data Access* - coleta de dados históricos;
- OPC A&E - Alarmes e Eventos; e

- OPC UA - *Unified Architecture* - inclui todos os tipos acima (DA, HDA, A&E).

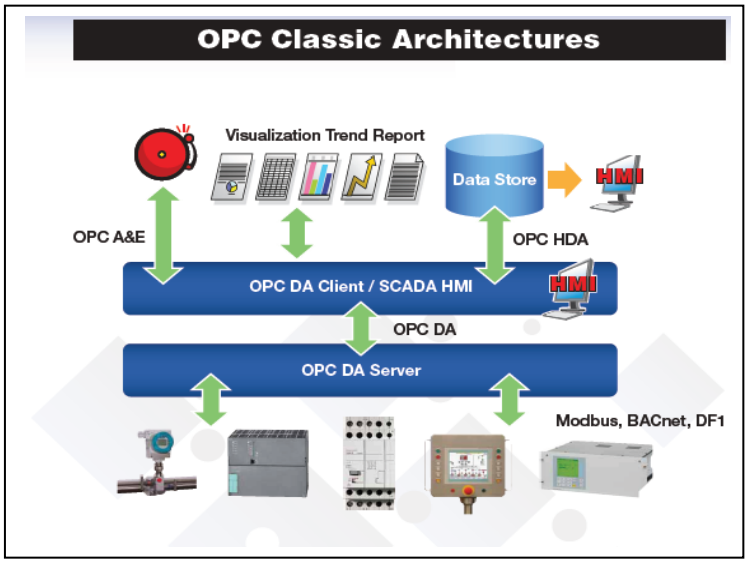

Figura 2 - Arquitetura Clássica OPC.

Devido às características dos sistemas de controle de cada complexo, principalmente fornecedores, estes componentes serão especificados em cada tópico dedicado neste relatório, ou seja, não temos um padrão a ser seguido, apenas recomendamos a utilização mínima de servidores OPC que atendam a especificação OPC DA.

1.3 Base de Tempo do PIMS

O horário de coleta dos dados deve ter uma atenção especial para o PIMS, pois o mesmo é o elo de relacionamento entre as variáveis e os usuários. Dois pontos básicos precisam ser observados neste processo, visando garantir a confiabilidade do sistema:
1 – definir a fonte dos horários: Os coletores possuem as seguintes estratégias de hora: fornecida pelo coletor e fornecida pelo servidor OPC; e
2 - os coletores devem estar com a base de tempo sincronizada.
Para os principais sistemas de mercado o banco de dados do PIMS é dedicado e proprietário, com características temporais, propiciando um maior desempenho na busca de dados. A precisão de tempo do PIMS é bem maior que a sua capacidade de coleta dos dados, ou seja, é possível armazenar dados em intervalos bem menores do que as interfaces têm capacidade de leitura dos dados. Através de interfaces binárias, ou especiais, os dados com intervalos de até micro segundos são lidos de tabelas ou arquivos onde é fornecido o momento exato do evento e então inseridos na base de dados do PIMS.

1.4 Disponibilidade do Sistema PIMS

A confiabilidade dos dados e sua disponibilidade são fundamentais no sistema PIMS devido ao caráter de decisão e grau de utilização da informação em tempo real. Para garantir a disponibilidade do sistema devem-se garantir dois níveis de redundância:

1.4.1 No armazenamento dos dados no servidor

O objetivo é manter o acesso aos dados pelos usuários e garantir que os últimos valores recebidos do processo estejam sempre disponíveis. Esta redundância garante ao usuário que em situações de falha do servidor outro servidor com a mesma configuração e com a base de dados atualizada responda às requisições do usuário de forma transparente. Este nível de disponibilidade em algumas plataformas PIMS pode ser alcançado através da instalação de um servidor em sistema de cluster de máquinas ou pela instalação de uma camada de software que garanta a atualização dos dados em dois servidores ou mais. No caso de redundância de servidores é desejável que o caminho físico de rede seja diferente, garantindo a disponibilidade em caso de rompimento de fibra ou sinistro nas instalações dos equipamentos de rede.

1.4.2 Na coleta dos dados do processo

Garante que a coleta de dados do processo seja mantida mesmo em caso de falha de um coletor ou interface através dos mecanismos:

- “Buferização” dos dados no coletor;
- Configuração de um servidor OPC secundário para o caso de falha de comunicação com o servidor OPC primário. Neste nível de redundância, a coleta de dados pode ser configurada para mudar de um servidor OPC primário para outro servidor OPC quando ocorrer uma anormalidade na comunicação ativa. Os eventos de anormalidade podem ser falha de comunicação na rede com o servidor atual, ou quando um item lido pelo servidor OPC muda o seu estado de qualidade para ruim (*Bad Quality*). Esta solução é normalmente usada em sistemas que possuem redundância de CPUs como nos SDCDs.
- Configuração de uma máquina de coleta redundante e com caminho físico de rede diferente da máquina principal. Neste nível de redundância, o módulo de comunicação com o servidor do PIMS é instalado em duas máquinas e a partir de um mecanismo de monitoramento uma das máquinas é eleita a principal e em caso de falha neste monitoramento a outra máquina automaticamente assume o controle do envio dos dados.
- Monitoramento de indicadores de desempenho do sistema de coleta como: ocupação de CPU, taxa de envio e recebimento de dados, ping, ocupação de disco.

1.5 Ferramentas Analíticas

Normalmente os principais fornecedores de sistemas PIMS possuem duas importantes ferramentas para visualização dos dados de processo:

- *Visualização gráfica do processo:* é um aplicativo que possibilita ao usuário construir e visualizar telas de processos, gráficos e valores das variáveis envolvidas, através de um pacote gráfico fácil de utilizar, que permitem criar gráficos dinâmicos, gráficos interativos mostrando dados em tempo real. Também permite que sejam criadas telas de processo para acompanhamento em tempo real.
- *Suplemento do Excel*: é um *add-in* para Microsoft Excel que possibilita a visualização de dados de processo de diversas formas, bem como copiá-los para uma planilha para realizar análises adicionais. As funções do suplemento são acessadas dentro do Microsoft Excel por um “menu” que

aparece depois que o mesmo é instalado. Através do suplemento o usuário pode trocar informação diretamente com o banco de dados. Essa ferramenta, combinada com as funcionalidades da planilha eletrônica, forma um recurso poderoso e fácil de usar por reunir, analisar e listar dados do PIMS.

Além destas ferramentas os sistemas PIMS também disponibilizam aplicações específicas para acompanhamento de processos em bateladas (*Batch*), controle estatístico de processo (C.E. P), cálculos avançados, envio de notificações de email, gestão de ativos e tratamento de alarmes. Normalmente, na primeira fase de implantação do PIMS, os usuários que mais geram valor com a ferramenta do PIMS são os engenheiros de processo. A partir de uma estação de trabalho eles podem acessar o PIMS para visualização dos dados tanto em tempo real quanto histórico, montando gráficos, tabelas e sinóticos. Posteriormente, os gerentes, supervisores e até operadores passam a interagir com o sistema e também colhem os seus benefícios.

2 MATERIAL E MÉTODOS

Este estudo constitui-se de uma revisão da literatura especializada, realizada entre fevereiro e julho de 2012, no qual realizamos uma consulta a livros e periódicos presentes na Biblioteca da Empresa (TSA), por artigos científicos selecionados através de busca no banco de dados do Scielo, e discussões em sites especializados na web.

3 RESULTADOS

Não apresentamos nesse estudo resultados quantitativos sobre o aumento da segurança no ambiente industrial em razão da aplicação das contribuições da TI, mas durante a discussão e conclusões são apresentadas boas práticas de configuração do ambiente e de arquitetura de rede para uma implantação segura do PIMS.

4 DISCUSSÃO

As empresas têm investido em um grande número de aplicações para gerenciamento e controle da produção e com consequente integração com o chão-de-fábrica. Assim, aplicações como: gerenciadores de ativos, historiadores (PIMS), inventários, otimizadores de processo, sistemas de execução da manufatura (MES) são integrados aos sistemas de controle da produção. Esta integração acaba por interligar sistemas antes isolados em ilhas de processo à rede corporativa das empresas.

Assim, os sistemas de controle industrial (DCS/SDCD, CLP e SCADA) com suas tradicionais redes e hardware proprietários, até então considerados imunes aos ciberataques precisam agora de uma atenção especial para o quesito segurança. A utilização de padrões abertos, tais como Ethernet, TCP/IP e outras tecnologias da Web alteram o cenário de vulnerabilidade dos sistemas industriais, deixando hackers e criadores de vírus muito próximos da indústria e estes podem se aproveitar do relaxamento existente em função desta relativa imunidade (padrões fechados e proprietários). Como resultado, temos um crescente número de eventos de segurança impactando na disponibilidade dos sistemas industriais, sendo inclusive

discutido em um relatório técnico da ISA99 publicado em 2007 com a definição clara de requerimentos e regras de utilização.
Abaixo discutiremos os mecanismos de defesa disponíveis e como a experiência da TI corporativa pode contribuir para aumento da segurança no ambiente da TA durante a implantação de um sistema PIMS. Na discussão procuramos identificar e reduzir as fragilidades de segurança de informação e vulnerabilidades das redes, definindo a estratégia e políticas mais adequadas e uma arquitetura mínima de hardware e software para atendimento das necessidades de integração entre os ambientes de TI e TA.

4.1 Segurança nos Sistemas de Controle

A norma ISO/IEC 17799:2005 define segurança da informação como sendo “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.
Com o objetivo de minimizar as ameaças e vulnerabilidades, as empresas têm focado esforços na segurança da informação[(2)] definindo normas e procedimentos específicos visando preservar as informações quanto à:

- *integridade*: garantindo que a informação seja mantida em seu estado original, protegida contra alterações intencionais ou acidentais;
- *confidencialidade*: garantindo o acesso à informação somente por pessoas autorizadas; e
- *disponibilidade*: garantindo que os usuários autorizados tenham acesso à informação sempre que necessário.

Quando consideramos segurança digital nos sistemas industriais, é importante destacar algumas diferenças em relação aos cenários clássicos de escritório gerenciados pelas equipes de TI. Enquanto em ambientes de escritório os objetivos de segurança tipicamente dominantes são confidencialidade e autenticidade, nos sistemas industriais a disponibilidade e integridade vêm em primeiro lugar. Além disto, nos sistemas de controle industrial ataques podem retardar a resposta dos computadores de operação das plantas e interferir na velocidade das redes ou até mesmo provocar uma parada completa dos serviços de operação e monitoramento das plantas.
Os sistemas de controle compartilham muitas semelhanças com os sistemas corporativos da TI, mas são tecnicamente, administrativamente, e funcionalmente mais complexos e únicos. As redes nos sistema de controle têm hoje todo o risco das modernas tecnologias de TI, sem a capacidade de aplicar ou gerenciar controles de segurança disponíveis para departamentos de TI corporativos. Neste tópico do relatório pretendemos discutir os mecanismos de defesa disponíveis e como a aplicação das normas e padrões da TI corporativa podem contribuir para aumento da segurança neste ambiente industrial, que é a fonte de dados para o sistema PIMS.

4.2 Riscos e Ameaças

Para entender o contexto de riscos e ameaças vale discutir alguns equívocos associados à segurança em um sistema de controle industrial:

- Os sistemas de controle industrial estão em rede física separada e independente. Muitos sistemas de controle, baseados em softwares do tipo SCADA, foram construídos originalmente em redes isoladas, levando os gestores de TI a considerar que estes sistemas não poderiam ser acessados através da rede corporativa ou de pontos de acesso externos. Infelizmente, esta é apenas uma crença! Na realidade com a necessidade de se integrar os dados de automação nos sistemas corporativos, muitos usuários têm feito ligações diretas entre as redes corporativas e de controle de forma direta, sem considerar a segurança das informações. Muitas vezes esta ligação é feita ligando-se na mesma máquina duas placas de rede, cada uma ligada em uma rede, sem um total conhecimento e gerenciamento dos riscos. O problema dessas ligações é que estas máquinas oferecem potenciais furos de segurança para ambas as redes, principalmente na rede de automação onde os aplicativos raramente consideram estes fatores de segurança.
- As conexões entre os sistemas de controle industrial e a rede corporativa são protegidas por fortes controles de acesso. As redes de automação são construídas na maioria das vezes, com a premissa de que é isolada (como mencionada acima) e de que o acesso é feito fisicamente e localmente. Deste modo não é gasto muito tempo se preocupando com questões de controle de acesso, sendo o mesmo feito através de um usuário único, com uma senha padrão (normalmente de baixa complexidade) focando apenas em diminuir a chance de acessos físicos às estações em questão. Como resultado, os controles desenhados para proteger os sistemas industriais de acesso não-autorizado são usualmente mínimos.

Ocorre que muitas vezes a segurança é comprometida por um funcionário de dentro da empresa, conectado à rede e que através de um notebook ou até mesmo sua máquina de trabalho, introduz, involuntariamente, o aplicativo malicioso na rede.
Outro grande complicador é que, considerando a necessidade de atendimento rápido nas redes industriais, os nomes dos principais equipamentos e sistemas facilitam aos invasores a identificação da localização das informações críticas como firewall1, historiador1, dns-primario.[3]
Através da estratégia de uso de firewalls internos e sistemas de detecção de intrusos, junto às políticas fortes de definição de senhas, altamente recomendadas, alguns poucos fornecedores de sistemas de controle industrial conseguem proteger seus dados.

4.3 Redes de Controle e Rede Corporativa

A rede de controle industrial é responsável pela comunicação entre as consoles de operação e os dispositivos de controle. Também alguns componentes de nível 3, como sistemas PIMS e MES, podem estar ligados a este barramento. No caso do PIMS, todo o processo de aquisição e coleta dos dados é realizado nesta rede devido à sua alta disponibilidade e proximidade dos equipamentos de campo. O padrão de meio-físico mais utilizado neste tipo de rede é o Ethernet. Praticamente todos os grandes fabricantes de equipamentos de automação já possuem este padrão implementado. Normalmente fazem parte desta rede os seguintes equipamentos ou sistemas: DCS (*Distributed Control Systems*), PLC (*Programmable Logic Controllers*) e SCADA (*Supervisory Control and Data Acquisition System*). Podemos dividir os equipamentos em duas redes: rede de informação e rede de controle. A rede de informações é formada pelos computadores do SCADA (servidor

e/ou clientes), os coletores do PIMS e outros sistemas como MES. Já a rede de controle restringe-se ao SCADA e CLPs ou SDCDs.

A rede corporativa ou rede de escritório abriga os serviços de uso geral dos funcionários da corporação acessados normalmente via intranet. Os principais serviços são o correio eletrônico e os pacotes de gestão de negócios. A rede de escritório está normalmente conectada à internet e os seus procedimentos de transferência de dados consomem largura de banda significativa, causando um efeito negativo sobre o tempo de resposta da rede. O comportamento de uso da banda é bastante variado e sofre constantes alterações em função de quais atividades ou operações estão sendo realizadas pelos usuários. Devido à sua visibilidade e acessibilidade, a rede corporativa é mais vulnerável a invasões por meio do uso de ferramentas de uso público.

A arquitetura mais adequada para a implantação do PIMS, onde os dois ambientes são interligados, visa isolar o sistema de controle da rede corporativa através de combinações apropriadas de firewalls e DMZ (rede de perímetro). É importante configurar os firewalls para bloquear as conexões de entrada e limitar as conexões de saída permitindo somente os acessos necessários para as operações, aumentando a dificuldade para um invasor externo explorar outras vulnerabilidades. Sem a proteção de uma DMZ e firewalls cuidadosamente configurados, a invasão é possível até mesmo por atacantes pouco qualificados.

As redes de controle e corporativa devem estar preferencialmente separadas fisicamente, entretanto em muitos casos podem estar fundidas em uma rede única. Apesar de comum, esta topologia apresenta alguns inconvenientes:

- o tráfego na rede de controle é de natureza diversa do tráfego na rede corporativa, caracterizando-se por mensagens curtas e muito frequentes.; e
- o tráfego da rede corporativa é em geral representado por arquivos maiores transmitidos com baixa frequência.

Os requisitos de desempenho e segurança das duas redes também são diferentes. Embora este tipo de topologia seja muito utilizado, quando não existir a separação física é obrigatório a separação lógica em VLANs para segmentar cada tipo de tráfego.

4.3.1 Firewall

O Firewall é um recurso utilizado para controlar o tráfego de dados entre um computador e Internet/rede, e vice-versa. Eles podem tanto filtrar os pacotes baseados em regras, como também atuar no controle de aplicações (*Proxy*).

O objetivo é permitir a transmissão e a recepção SOMENTE de dados autorizados. O Firewall garante que somente computadores conhecidos troquem determinadas informações entre si e tenham acesso a determinados recursos. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail da rede), enquanto outros são bloqueados por padrão, por terem riscos elevados.

Existem firewalls baseados na combinação de hardware e software e baseados somente em software. Estes equipamentos estão cada vez mais sendo utilizados devido ao aumento na sofisticação dos ataques, principalmente se consideramos os ataques às empresas, conforme pode ser observado no gráfico da Figura 4.

ISSN 2237-0234

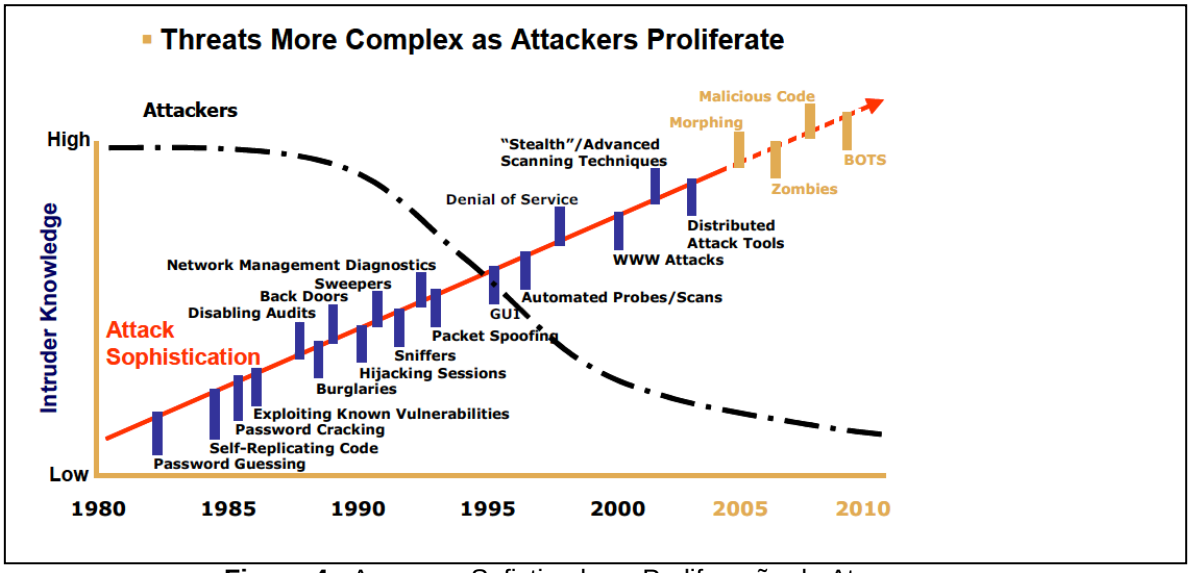

Figura 4 - Ameaças Sofisticadas x Proliferação de Ataques.

Neste cenário, para integração entre as redes industrial e corporativa, a segurança cibernética deve ser uma prioridade, portanto, tornando imperativo o uso dos firewalls. A implantação de firewalls impõe muitos desafios para a comunicação baseada em OPC e, consequentemente em DCOM[4], pois a tecnologia requer uma quantidade de portas de comunicação para operar.
As redes industriais e corporativas quando têm a tecnologia adequada e são configuradas e mantidas corretamente, podem coexistir muito bem.
Recomendamos fortemente consultar o fornecedor ou integrador local dos sistemas de controle para identificar todo o tráfego entre o sistema de controle ou supervisão e a DMZ, além da equipe corporativa de TI, cuja especialização pode facilitar o uso e configuração destes recursos de rede.

4.3.2 DMZ – Zona desmilitarizada

A DMZ (*Demilitarized Zone*) ou Rede de Perímetro permite definir uma fronteira, lógica ou física, em torno de um conjunto de ativos de informação e implementar as medidas necessárias para evitar a troca de informação não autorizada nestes ativos. Os firewalls representam as soluções mais comuns de proteção de perímetro, podendo realizar inspeção e filtragem de pacotes de dados, analisando as diversas camadas até o nível da aplicação. É um conceito usado para implementar um segmento de rede isolado e protegido. De uma maneira bem geral, a DMZ é uma rede entre 2 redes protegida por firewall, cuja função é garantir maior segurança de uma rede contra a invasão externa. Pode ser entendida como uma "camada" a mais de firewall. Caso algum invasor consiga explorar uma vulnerabilidade a sua ação ficará bastante restrita.
Como a rede de perímetro protege a rede interna é recomendada a instalação do servidor ou servidores (aplicações, web, antivírus) do PIMS nesta rede.
A política de segurança aplicada em uma DMZ (Figura 5) é geralmente a seguinte:

- *Tráfego da rede externa (intranet) para o DMZ autorizado*: neste caso os clientes da rede corporativa, via intranet, podem ter acesso ao servidor do PIMS e consequentemente a seus dados. Também o servidor do PIMS centralizado poderá acessar dados do servidor local do PIMS;

- *Tráfego da rede externa (intranet) para a rede interna (processo) proibido*: neste caso os clientes da rede corporativa, via intranet, não têm acesso aos dados diretamente das ilhas de informação, ou seja, os sistemas SCADA e SDCDs ficam protegidos do acesso externo;
- *Tráfego da rede interna (processo) para o DMZ autorizado*: neste caso, unicamente os coletores de dados têm autorização para enviar os dados coletados ao servidor do PIMS, ficando as demais máquinas impedidas do acesso;
- *Tráfego da rede interna (processo) para a rede externa (intranet) autorizado*: neste caso, as máquinas da rede corporativa que forem instaladas em pontos da rede interna poderão ter acesso à intranet;
- *Tráfego do DMZ para a rede interna (processo) proibido*: neste caso, vírus e outros softwares "mal intencionados" que forem instalados não têm acesso à rede interna, exceto aqueles especificamente relacionados como a atualização de assinatura dos antivírus; e
- *Tráfego do DMZ para a rede externa (intranet) recusado*: neste caso, vírus e outros softwares "mal intencionados" que forem instalados não têm acesso para envio de dados ou até mesmo infecção ou auto-instalação através da rede corporativa.

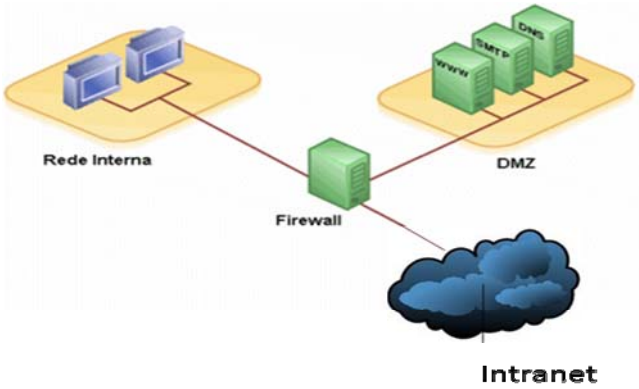

Figura 5 – Arquitetura de uma DMZ.

4.4 Antivírus

Os vírus são programas capazes de se inserir em outros arquivos ou programas e usá-los para reproduzir-se, executar alguma tarefa e também transmitir informações.(2) Estes programas assumiram várias formas e são encontrados nas seguintes formas: vírus, *worms* e cavalos de tróia (trojans).
Para proteger o ambiente computacional destas ameaças é necessária a instalação de um antivírus. Um bom antivírus deve: identificar e eliminar a maior quantidade possível de vírus e outros tipos de malware; analisar os arquivos que estão sendo obtidos pela Internet; verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e "pen drives", de forma transparente ao usuário; procurar vírus, cavalos de tróia e outros tipos de malware em arquivos anexados aos e-mails; criar, sempre que possível, uma mídia de verificação (disquete ou CD de boot) que possa ser utilizado caso um vírus desative o antivírus que está instalado no computador; atualizar as assinaturas de vírus e malwares conhecidos, pela rede. A maioria dos antivírus tem oferecido proteção com

muita eficiência, mas todos eles exigem atualizações frequentes para lidarem com novos softwares mal-intencionados.
Toda solução antivírus profissional fornece um mecanismo rápido e descomplicado para garantir que as atualizações para os arquivos de assinatura requeridos — arquivos que contêm informações usadas por programas antivírus para detectar e lidar com software mal-intencionado durante uma verificação e que são regularmente atualizados por fornecedores de aplicativos antivírus — sejam fornecidas ao computador cliente o mais rápido possível. No ambiente corporativo, normalmente, há uma prática de atualização diária, que em alguns casos não se aplica ao ambiente de controle de processo, sendo indicada a instalação de uma máquina dedicada para teste e homologação das vacinas na rede de automação. A partir desta máquina, somente após o teste é que se deve proceder à atualização das demais máquinas da rede de controle de processo. Recomendamos configurar a ferramenta de automatização, deste processo de atualização, fornecida pelos fornecedores de antivírus do mercado.
É muito importante manter o antivírus e suas assinaturas sempre atualizados!
Porém, tais atualizações têm seus próprios riscos de segurança, pois os arquivos de assinatura são enviados do site de suporte do antivírus para o aplicativo host (normalmente pela Internet). Por exemplo, se o mecanismo de transferência usado para obter o arquivo for o FTP, os firewalls de perímetro da organização devem permitir esse tipo de acesso ao servidor FTP na Internet. Verifique se o seu processo de atualização é seguro o suficiente para atender aos requisitos de segurança do ambiente da rede de automação.
Mesmo executando todos os procedimentos de proteção do ambiente é muito importante definir uma estratégia de "backup" dos dados do servidor PIMS bem como uma rotina de verificação do conteúdo salvo.

5 CONCLUSÃO

Embora nenhum dos cuidados aqui discutidos seja particularmente revolucionário, o objetivo das práticas é garantir o acolhimento das necessidades mínimas de segurança, de tal maneira que o ambiente seja menos suscetível a ataques comuns do Windows, mas que ainda permita que todas as aplicações OPC e seus clientes possam funcionar normalmente.
Isso é muitas vezes mais difícil do que deveria ser por dois motivos. Em primeiro lugar, alguns requisitos para a operação OPC estão em desacordo com boas práticas de segurança do Windows. Em segundo lugar, um número de fornecedores de OPC, não todos, parece ignorar uma série de especificações do Windows DCOM e suas exigências.[5]
A segurança da maioria dos produtos de software tem melhorado significativamente nos últimos anos. Isto é especialmente verdadeiro para Microsoft Windows e vários produtos OPC. A utilização do padrão OPC-UA também vem ajudar significativamente a reduzir os esforços de segurança e reduzir os riscos atualmente enfrentados pela indústria.
Além da prevenção é muito importante possuir um plano de contingência para o caso de algo dar errado e a rede de automação ser infectada. É essencial ter ferramentas de backup automatizado instaladas além de redundância nos servidores críticos da rede de automação. A experiência mostra que o processo de desinfecção de uma rede de automação contaminada é bastante oneroso, complexo e quase

sempre depende da colaboração dos fabricantes para o sucesso, o que torna o processo lento e muito caro.
Abaixo apresentamos algumas práticas que podem ajudar a garantir um ambiente mais robusto e menos vulnerável para integração de sistemas da TA e TI.

5.1 Políticas de Segurança para implantação do PIMS

Algumas considerações importantes para o gerenciamento de contas no PIMS:

- adote políticas de gerenciamento de conta refletindo as melhores práticas convencionais de TI;
- substitua nomes padrões sempre que possível, pois estes geralmente são definidos nas documentações do sistema e podem ser extraídos dos códigos binários dos executáveis; e
- estabeleça políticas de senhas garantindo a complexidade de senha apropriada e proíba senhas curtas ou fáceis de adivinhar.

5.2 Liberação de Acesso para os Usuários

A liberação de acesso aos dados do PIMS pode ser feita através de 03 (três) mecanismos:

- *conexão confiável ou Trust*: Permite o acesso aos dados do PIMS sem a necessidade de uma interface para validação de usuário e senha. A configuração do *Trust* define qual máquina ou grupo de máquinas e usuários terão acesso aos dados do PIMS automaticamente após serem ligadas. Podem ser configurados trusts para uma máquina específica (coletor de dados) ou para todas as máquinas definidas dentro de um *range* de endereços Ips, por exemplo, todas as máquinas de uma subrede local.
- *usuário interno do PIMS*: Permite o acesso aos dados do PIMS através de usuários locais, reconhecidos apenas pelas ferramentas nativas do PIMS. Pode ser definido um usuário padrão com acesso somente de leitura aos dados do PIMS para conexão padrão de todos os clientes, e quando necessário trocar o usuário para outro com maiores níveis de permissão;
- *integração como Microsoft Active Directory (AD)*: permite o acesso aos dados do PIMS através do logon do Windows, ou seja, os usuários da rede corporativa são mapeados para o sistema PIMS e configurados em grupos de acesso que definem as suas permissões e restrições aos dados.

5.3 Melhores Práticas para Homologação e Liberação de Atualizações de Antivírus

Abaixo listamos alguns cuidados importantes no processo de atualização de antivírus na rede de processo:

- mantenha as máquinas de automação sem acesso à internet definindo um servidor de antivírus localizado em um ambiente protegido e através do qual se faz a busca na internet das atualizações;
- se existirem servidores web na automação, por exigência da arquitetura dos sistemas de supervisão e controle implantados, faça um endurecimento nas regras de segurança para estabelecer um nível mínimo de permissões de acesso.
- não permitir acesso a email nas máquinas de processo;

- na medida do possível, manter a atualização dos *patches* e atualizações dos sistemas operacionais e ferramentas do ambiente (SCADA e outros aplicativos), reduzindo a exposição a ataques associados às vulnerabilidades conhecidas. Patches são frequentemente liberados em resposta a estas vulnerabilidades publicamente identificadas.(6)
- remova ou desative os serviços desnecessários nos servidores do sistema de controle e nas estações de operação.
- evite o compartilhamento de arquivos entre as máquinas de processo e os servidores do PIMS;
- mantenha um *backup* atualizado (automatizado) com cópias regulares;
- mantenha sempre que possível uma imagem (*ghost*) da máquina com a última configuração válida;
- monitore o espaço em disco e sempre mantenha espaço disponível para as atualizações; e
- instale as atualizações primeiramente em uma máquina com o ambiente similar ao do processo para testes e validação das atualizações. Somente após uma etapa de monitoramento e validação faça a atualização para as demais máquinas da rede de processo. Em caso de utilização de várias tecnologias de controle (SCADA, SDCDs, CLPs) é interessante testar em cada ambiente!

REFERÊNCIAS

1 SEIXAS, Constantino. PIMS - Process Information Management System - Uma introdução, Universidade Federal de Minas Gerais, 2002.

2 BARBOSA, Heber Almeida. Detecção de Intrusão em Redes de Automação Industrial; Programa de Pós-Graduação em Informática. Universidade Federal do Espírito Santo, 2006

3 STOUFFER, Keith. Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, 2011.

4 HONEYWELL, Whitepaper. Guide OPC Consideration for Network Security., 2011.

5 BRITISH, Whitepaper, Columbia Institute of Technology. OPC Security Whitepaper #3 Hardening Guidelines for OPC Hosts. Byres Research, 2007.

6 FINK, Raymond K. Lessons learned from cyber security assessments of SCADA and Energy Management Systems, 2006.