SEGURANÇA DA INFORMAÇÃO NOS AMBIENTES DE AUTOMAÇÃO DA ARCELORMITTAL TUBARÃO ALINHADA A UM DIRECIONAMENTO CORPORATIVO[1]

Leandro Rodrigues Ramos[2]
Antônio Carlos Aguiar Gagno Junior[3]

Resumo
Arcelor e Mittal Steel, durante o processo de fusão, herdaram mais de 100 políticas com quase 700 padrões de segurança. Evidências nos mostram que uma alta porcentagem (80% a 90%) de falhas de segurança poderiam ter sido evitadas por meio da implementação de um conjunto simplificado de controles. Seguindo esta linha de raciocínio, uma política contendo um conjunto de 16 controles de segurança da informação foi definida a nível global. Entretanto é de conhecimento que existem diferenças operacionais críticas entre TI e TA que influenciam diretamente na medição destes controles. Este trabalho tem por objetivo mostrar como um modelo corporativo de gestão da segurança da informação vem sendo aplicado de forma sinérgica em cenários de automação. Este modelo possibilita a medição do nível de segurança no contexto industrial, dando visibilidade à alta gestão de riscos no ambiente e proporcionando o compartilhamento de melhores práticas orientadas a um baseline simplificado de controles adaptados para automação.
Palavras-chave: Segurança; Automação; Controles.

INFORMATION SECURITY UNDER THE PROCESS AUTOMATION ENVIRONMENT OF ARCELORMITTAL TUBARAO ALIGNED WITH A CORPORATE LEVEL DIRECTIVE

Abstract
Arcelor and Mittal Steel have inherited over 100 policies, with almost 700 security standards. Publishing evidence shows that a high percentage (80%-90%) of security breaches could have been avoided through the implementation of simple controls. Following this line of reasoning a small set of 16 baseline IT security controls has been defined at group level. However there are critical operational differences between IT and PA that influence how specific measures should be applied. This paper aims to show how a corporate security information model has been applied synergistically under process automation scenarios. This model enables measurement of the security level in the industrial context, giving visibility of risks to the top management and sharing best practices oriented to a simplified baseline of security controls adapted for process automation.
Key words: Security; Automation; Controls.

[1] *Contribuição técnica ao 17° Seminário de Automação e TI Industrial, 24 a 27 de setembro de 2013, Vitória, ES, Brasil.*

[2] *Bacharel em Ciência da Computação. Especialista Desenvolvimento em Automação e Instrumentação. ArcelorMittal Tubarão. Tubarão, ES, Brasil.*

[3] *Engenheiro Eletricista. Especialista Desenvolvimento em Automação e Instrumentação. ArcelorMittal Tubarão. Tubarão, ES, Brasil.*

1 INTRODUÇÃO

Durante os últimos anos, sistemas de automação e controle industrial eram suportados por uma infraestrutura que envolvia computadores isolados bem como sistemas operacionais e redes proprietárias. Na literatura,[(1)] os acrônimos ICS (*Industrial Control Systems*) ou IACS (*Industrial Automation and Control Systems*) são utilizados para referenciar estes sistemas que de uma forma geral podem ser divididos em diferentes tipos de software e hardware:

- Sistemas SCADA (*Supervisory Control and Data Aquisition*) ou DCS (*Distribution Control Systems*);
- Interfaces Homem-Máquina (IHM);
- Controlador Lógico Programável (*PLC – Programmable Logical Controller*);
- Sistemas de otimização de processos e modelos matemáticos.

A Figura 1 nos dá uma visão dos diferentes níveis hierárquicos de automação e informação com seus respectivos ICS/IACS. Esta ilustração foi utilizada pela comunidade global de Automação da ArcelorMittal como referência para as fronteiras de atuação na medição do nível de conformidade dos controles de segurança em suas respectivas plantas.

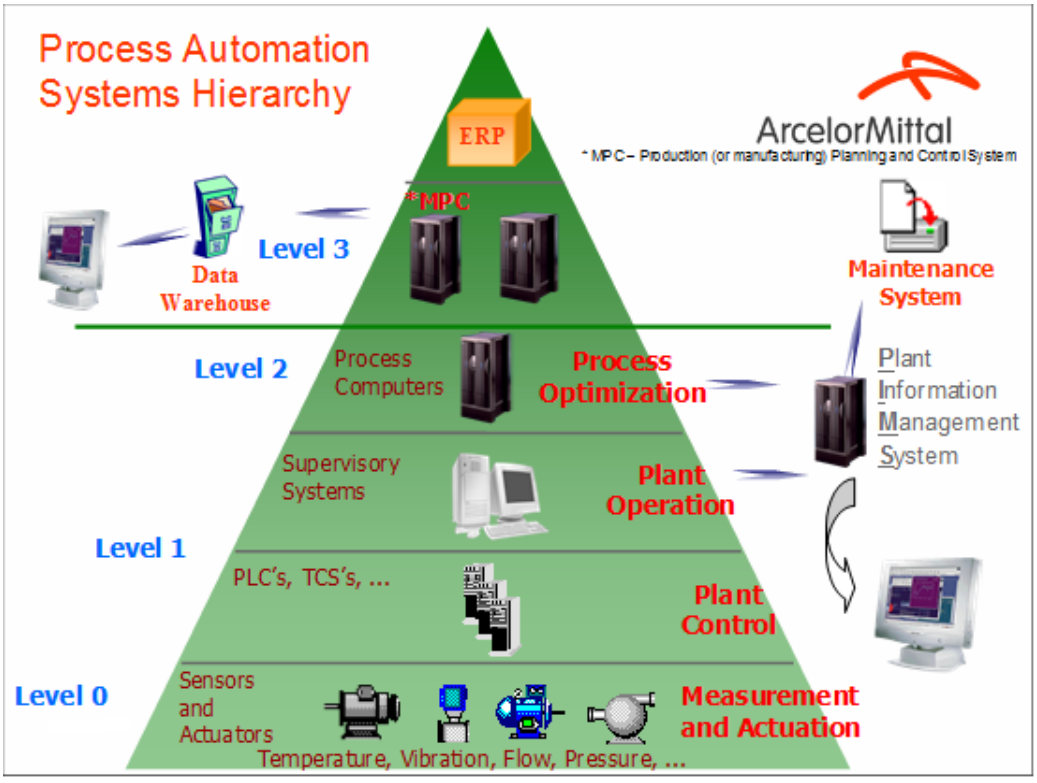

Figura 1. Níveis hierárquicos dos sistemas de automação e controle.

Atualmente, sabemos que tecnologias abertas e de conhecimento comum estão sendo cada vez mais utilizadas em sistemas de automação e controle. ICS já não é mais um equipamento individual, isolado e com hardware e software especializado. Sistemas que historicamente eram operados em redes separadas com protocolos proprietários, começaram a ser migrados para redes padrões (Ethernet/IP) e até mesmo expostos à Internet para simplificar a gestão de ativos, bilhetagem e operações de suporte remoto. Originalmente os ICS eram intrinsicamente seguros, portanto não foram concebidos levando em consideração requisitos segurança. À

medida que estes sistemas são expostos, problemas de segurança que eram mascarados por uma superfície de ataque restrita, começam a se manifestar. Segundo dados da OSVDB (*Open Source Vulnerability Database*)[(2)] apenas 76 vulnerabilidades foram divulgadas em sistemas SCADA de 2008 a 2010. Entretanto, após o descobrimento do *worm* Stuxnet em plantas nucleares do Irã (2010), o foco em avaliar a segurança de sistemas SCADA aumentou consideravelmente. Em 2011, foram 164 vulnerabilidades divulgadas em sistemas SCADA e o número cresceu novamente para 191 em 2012,[(3)] representando uma porcentagem de 768% de aumento quando comparado com os números de 2008 (Figura 2).

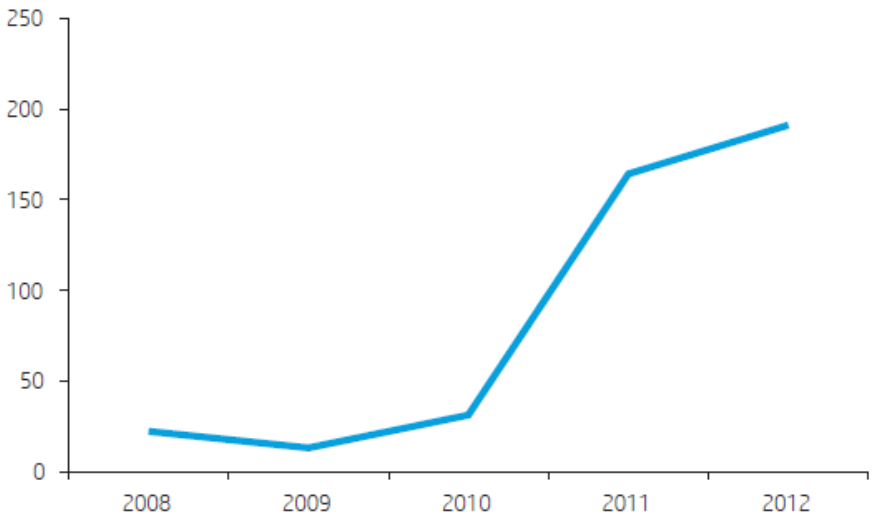

Figura 2. Vulnerabilidades SCADA divulgadas pela OSVDB, 2008-2012.

Em outras palavras, sem a devida proteção, estes sistemas se tornam alvos fáceis. Segundo informações do ICS-CERT (*The Industrial Control Systems Cyber Emergency Response Team - US*) dos aproximados 191 incidentes de segurança reportados no ano fiscal de 2012, 41% foram no setor de energia. Destes incidentes, 23 foram resultados de campanha de e-mail (*fishing-spam*) orientados a um ICS específico, enquanto alguns foram resultados de dispositivos USBs utilizados por administradores de sistemas. O relatório ainda indica vários sistemas de controle com endereços IP diretamente conectados à Internet com diversas vulnerabilidades exploráveis via web. Mecanismos de busca especializados como o *Shodan Computer Location Service* também estão facilitando a vida dos agressores. Uma equipe de pesquisadores de uma universidade em Berlim (*Free University Berlin*) reportou ao ICS-CERT que utilizaram o Shodan para descobrir milhares dispositivos inseguros que usam SCADA e outros sistemas de controle industrial. Um mapa de risco denominado IRAM (*Industrial Risk Assessment Map*) foi desenvolvido baseado no Shodan e integrado ao *Google Earth.* Este mapa nos dá uma visualização geográfica global de sistemas SCADA pelo mundo que são acessíveis via internet.
Levando em consideração esta nova realidade, a comunidade de automação da ArcelorMittal iniciou um programa de segurança com o objetivo elevar o nível de segurança dos sistemas de controle e redes localizadas nas áreas industriais da companhia. Trabalhando de forma sinérgica com as iniciativas de segurança de TI, inicialmente avaliando o nível de conformidade dos controles de segurança TI dentro do contexto industrial, com as devidas adequações e complementando com controles de segurança específicos de para os sistemas industriais de automação.

2 MATERIAS E MÉTODOS

Arcelor e Mittal Steel, durante o processo de fusão, herdaram mais de 100 políticas com quase 700 padrões de segurança. Evidências nos mostram que uma alta porcentagem (80% a 90%) de falhas de segurança poderiam ter sido evitadas por meio da implementação de um conjunto simplificado de controles. Seguindo esta linha de raciocínio, uma política contendo um conjunto de 16 controles de segurança foi definida a nível global. No escopo de TI, planos de ação foram definidos objetivando atingir 100% de aderência a esta política, sendo suportados pelo negócio e endereçados em todos os segmentos. Em 2011 a comunidade de Automação da ArcelorMittal, lideradas por Burns Harbor e ArcelorMittal Tubarão, iniciou um programa de segurança levando em consideração uma série de motivadores:

- Recentes tentativas de ataque aos sites da ArcelorMittal fez surgir novas frentes de segurança lideradas por comitês de risco. Destacaram também a necessidade de se criar controles de segurança efetivos para os ambientes de TA;
- Os sistemas de automação da ArcelorMittal estão cada vez mais conectados às redes corporativas utilizando de recursos e ferramentas padrões de ambientes de TI;
- Aumento nas tentativas de intrusão em grandes corporações, por motivações diversas, podendo afetar a produção e reputação da empresa.
- Protocolos abertos chegaram às redes de automação e controle (Ethernet Industrial, TCP/IP e outros);
- A plataforma Windows já é uma realidade para diversos sistemas de controle. Isto significa que umas séries de ameaças que antes eram endereçadas somente no âmbito de máquinas corporativas são agora ameaças potencias para o ambiente de produção.

O trabalho inicial baseou-se inicialmente em melhores práticas de TI (*baseline* de 16 controles). A proposta era definir um conjunto mínimo de requisitos objetivando garantir um nível de segurança apropriado para os sistemas de automação e controle e suas respectivas redes localizadas nas áreas industriais da empresa. Entretanto é de conhecimento que existem diferenças operacionais significativas entre TI e TA que influenciam diretamente na medição destes controles. O desafio na aplicação deste *baseline* é que as melhores práticas de TI nem sempre podem ser aplicadas em sistemas de automação sem gerar impactos na execução dos mesmos. Como exemplo, o uso de antivírus e ferramentas de gestão de *patches* usualmente impactam as aplicações pelos quais eles foram designados a proteger. Neste caso, nosso desafio é encontrar uma maneira de tornar estes ambientes de automação e controle o mais seguro possível, minimizando impactos.

2.1 Controles de Segurança Consolidados para Automação

Benchmarks foram realizados globalmente pelo grupo ArcelorMittal tentando identificar e medir a aplicabilidade do *baseline* proposto pela TI nos diferentes níveis de Automação. Analisando a compilação dos resultados percebemos que muitos destes controles foram considerados aderentes e com base nestes mesmos resultados o grupo decidiu seguir em frente considerando os 16 controles como um direcionador inicial para se definir controles de TA. Para um melhor entendimento e

visibilidade segregaram estes controles em diferentes níveis de automação, sendo considerados três níveis:

- Controle de Planta N0/N1 (*Plant Control Level*) – PLCs, *Smart Cameras*, DCS e TCS.[*] Em geral: medição, sensoriamento, acionamentos, controladores em tempo real, sensores, atuadores fazendo uso de redes industriais (*fieldbus)*;
- Supervisórios N1/N2 (*Supervisory Level*) – IHMs, SCADA. Em geral: dispositivos de operação de planta, acessando equipamentos N0-N1 através de drivers e protocolos específicos;
- Otimização N2 (*Optimization Level*) – Equipamentos que executam modelos matemáticos, estações de engenharia.[**] Em geral: dispositivos de otimização de processos e modelos matemáticos, bancos de dados industriais, interfaces com sistemas N3, PIMS, acessando dispositivos N1 através de redes não proprietárias (Ethernet/IP) ou redes industriais.

Mudanças e simplificações foram feitas nos controles (e sub-controles relacionados) devido aos requisitos e restrições específicas existentes no ambiente industrial. A Tabela 1 nos dá uma visão macro destes controles e a aplicabilidade dos mesmos nos três diferentes níveis de automação propostos.

Tabela 1. Sumário dos 16 controles de segurança e aplicabilidade em TA

IT Baseline Security Controls		Applicability		
Code	**Description**	**Plant Control**	**Supervisory**	**Optimization**
LSC001	Antivirus	**N.A.**	Applicable	Applicable
LSC002	Security Patches	**N.A.**	Applicable	Applicable
LSC003	Out-of-Support Systems	Applicable	Applicable	Applicable
LSC004	Internet Access Points	**N.A.**	**N.A.**	**N.A.**
LSC005	Network connection with third parties	**N.A.**	**N.A.**	**N.A.**
LSC006	Wireless installations	Applicable	Applicable	Applicable
LSC007	Network access	Applicable	Applicable	Applicable
LSC008	Identification, Authentication and Passwords	Applicable	Applicable	Applicable
LSC009	Default passwords	Applicable	Applicable	Applicable
LSC010	User access rights	Applicable	Applicable	Applicable
LSC011	User exit procedure	Applicable	Applicable	Applicable
LSC012	Backups	Applicable	Applicable	Applicable
LSC013	Security incidents	Applicable	Applicable	Applicable
LSC014	Remote access	**N.A.**	**N.A.**	**N.A.**
LSC015	Data protection	**N.A.**	**N.A.**	**N.A.**
LSC016	Logs	Applicable	Applicable	Applicable

Para uma primeira abordagem, estas simplificações foram necessárias com o intuito de mitigar maiores impactos em sistemas legados. No nível de controle de planta, por exemplo, devido à variabilidade de dispositivos, é extremamente complexo de se forçar uma política de senhas (tamanho de senha, complexidade, tempo de expiração etc.). Alguns controles foram considerados como não aplicáveis ou que deveriam ser endereçados pelas equipes de TI. Na ArcelorMittal Tubarão, a segurança de perímetro (Ex: Firewalls de Internet) e controle de acesso remoto para os colaboradores e parceiros (Ex: VPNs) passam obrigatoriamente pelo crivo de processos e tecnologias gerenciadas pela TI. Já no nível de supervisório, por exemplo, os 16 controles foram reduzidos para 12 controles. A Tabela 2 extrai um trecho do documento *ArcelorMittal Baseline PA Security Controls,*[4] criado por consenso pela comunidade de automação e que oficializa os controles de segurança de TA no grupo.

[*] TCS (*Technological Control System*) se refere a equipamentos específicos utilizados por alguns fornecedores (SMS, VAI), baseados no sistema operacional Vx Works com interfaces VMIC.

** Estações de engenharia, utilizadas na configuração de dispositivos N1, foram endereçadas no nível de otimização devido a similaridades com os equipamentos de otimização (Software e Hardware).

Tabela 2. Controle LSC001 – Antivírus

	Control	Sub Controls	Guidance
1	**Antivirus**	**Requirements** **Devices running Windows Operation System (Servers and Terminals)** All local disks are effectively protected (Including removable media). All connectable storage devices/media (CD, DVD, USB keys, external disks) are effectively protected. Users are not allowed to disable these protections, nor to change the anti-virus policy. The signature file is updated at least on a **daily** basis. A scan is planned to be launched **during operational areas maintenance** or during accorded windows **Optional Recommendations** **Autorun** The "autorun" functionality is disabled for removable equipement/media such as CD, DVD, USB keys, external disks. **Process Automation Policy** A specific and "lighter" Antivirus policy should be implemented for Process Automation, trying to minimize perturbations on critical systems and handling exceptions relevant to this environment (Example: Exclude scans on core folders of InTouch supervisory).	Virus scan on internet browsing or e-mail systems should be implemented by IT. They are already in charge of Internet Access security and also own the messaging servers. When we say "lighter", is to minimize performance impacts on critical systems, avoiding "heavier" policies like: automatic full scans, checking all kind of file extensions, enabling very sensitive heuristics, checking for virus only on write IO operations (heavy IO servers) etc.

É importante frisar que muitos destes controles são aderentes a elementos existentes nas normas ISA-99/01/02, consideradas como a principal referência para a segurança da informação em sistemas de automação.

2.2 Medições do Nível de Conformidade dos Controles de Segurança

Com um *baseline* de segurança para automação proposto, o próximo passo foi medir efetivamente o nível de conformidade dos controles de segurança nas diversas plantas do grupo. Um comitê global foi criado e uma estratégia de medição foi definida pelo mesmo.

Um ponto único de contato (*SPOC – Single point of contact*) foi definido em cada unidade de negócio. Este usuário chave ficou como responsável em conduzir o programa de segurança em sua respectiva planta, fazendo a interface com o comitê global e coordenando o cronograma e as medições locais. Recomendou-se que representantes das principais áreas operacionais (Aciaria, Laminação, Redução, etc.) deveriam ser eleitos e para cada área, três papéis deveriam ser considerados:

- *Sponsor* (Gerente ou Gerente de área): Quem deve "comprar" a iniciativa para aquela área, mobilizando seu time e tentando identificar usuários chaves para apoiar na medição dos controles de segurança.
- Especialista em sistemas de controle e supervisório: Possui uma visão horizontal dos principais sistemas de controle e supervisórios relacionados aos processos de sua área.
- Especialista em sistemas de otimização: Possui uma visão horizontal dos sistemas de otimização relacionados aos processos da sua área.

Dependendo da complexidade/estrutura de cada unidade, os papéis 2 e 3 poderiam ser representados por um único especialista. Para os papéis 2 e 3 foi recomendado que os gerentes elegessem, se possível, profissionais com perfil ou conhecimentos de TI. Isto facilitaria um melhor entendimento dos controles de segurança associados à sua área/processo de atuação. Três questionários foram criados e distribuídos, de forma a mensurar o nível de conformidade dos controles de segurança:

- *Q1 - PA Security Controls Assessment - Plant Control Level Questionnaire;*
- *Q2 - PA Security Controls Assessment - Supervisory Level Questionnaire;*
- *Q3 - PA Security Controls Assessment - Optimization Level Questionnaire.*

Os especialistas eleitos ficaram como os responsáveis para preencher os questionários, levando em consideração o nível de conformidade em suas respectivas áreas. Isto nos dá uma visão localizada de quais áreas estão em situação crítica, podendo catalisar projetos emergenciais. O SPOC da planta consolida os questionários locais, reportando os resultados para o comitê global e gerando um índice de conformidade para a sua unidade de negócio. O comitê global consolida os resultados de todas as unidades, tendo uma visão do nível de conformidade da organização. A Figura 3 nos dá uma visão consolidada deste processo.

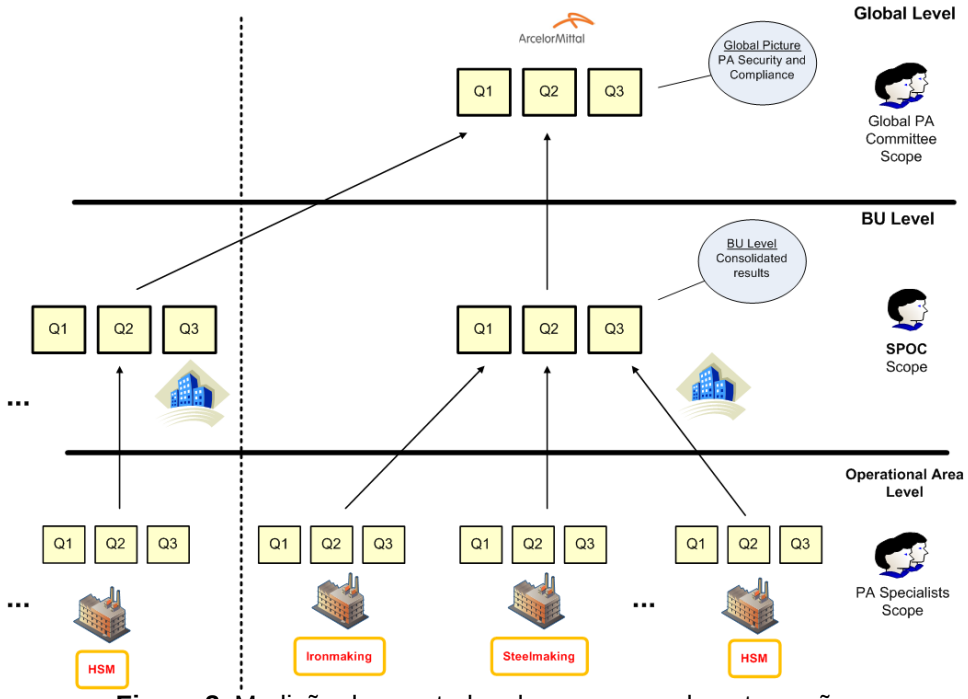

Figura 3. Medição dos controles de segurança de automação.

3 RESULTADOS

Mediante estas análises, um conjunto de iniciativas e projetos foram iniciadas na ArcelorMittal Tubarão objetivando aumentar o nível de conformidade em relação aos controles de segurança propostos.

3.1 Segregação das Redes de Informação e Processo

Na ArcelorMittal Tubarão foi criado um *backbone* de redes exclusivo para os sistemas N2 (Figura 4). Um anel de alto desempenho (10 Gbits) foi criado interligando os principais sites industriais. Sendo devidamente isolado do *backbone* de TI por intermédio de firewalls CISCO ASA 5585X-SSP10, configurados em cluster para garantir *uplinks* redundantes entre redes N2 e N3.[5] A topologia em anel associada a equipamentos CISCO proporcionou a configuração de protocolos de alta resiliência como o CISO-REP (*Resilient Ethernet Protocol*) que garante tempos de convergência na faixa de 50ms em cenários de falha.

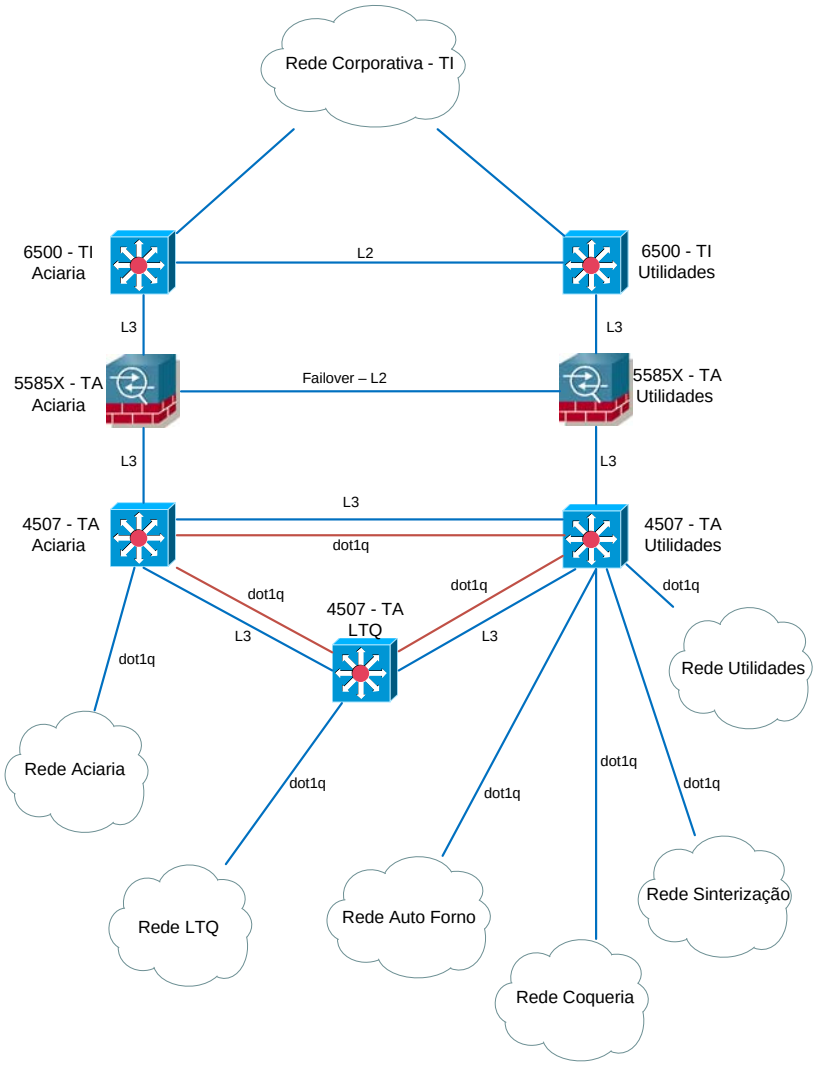

Figura 4. Novo *backbone* de Automação N2 – ArcelorMittal Tubarão.

Os firewalls instalados reduzem a superfície de ataque às possíveis ameaças provenientes das redes corporativas locais de TI que por sua vez estão conectadas às diversas redes corporativas do grupo através da ArcelorMittal *Global WAN*.

3.2 *Active Directory* Dedicado para Ativos de Automação

O *Active Directory* (AD) é um diretório de autenticação que pode ser integrado aos sistemas industriais, provendo mecanismos para a gestão centralizada de usuários e equipamentos. Dentre as suas características e benefícios citamos:

- Gestão centralizada de senhas, com políticas específicas para Automação (tamanho de senha, prazo de expiração, complexidade, etc.). Promovendo conformidade ao controle LSC008;
- Configuração de GPO (*Group Policy Objects*): Controla o que os usuários podem e não podem fazer em equipamentos Windows de forma centralizada (Ex: bloqueio de acesso a dispositivos USB). Este recurso vem sendo utilizado de forma efetiva no projeto de *Thin Clients* que está em produção na ArcelorMittal Tubarão;

- Serviços básicos de rede como o *Network Policy Server* (RADIUS) facilita a configuração de protocolos de segurança como o 802.1x em switches industriais, garantindo que somente dispositivos autorizados podem ser conectados à rede (conformidade com o controle LSC007).

3.3 Gestão de *Patches* e Antivírus

Active Directory e GPO facilitaram a implementação de um processo de gestão centralizado de *patches* de segurança para ambientes Windows, utilizando a ferramenta WSUS (*Windows Server Update Services*). O WSUS possibilita a gerência e distribuição de atualizações e *hot-fixes* de segurança para terminais e servidores com sistema operacional Windows. Os administradores possuem controle total de quais patches podem ser aplicados e quando devem ser aplicados. Os equipamentos são classificados e as atualizações priorizadas mediante uma matriz de risco [5] onde impacto no processo e nível de exposição são avaliados (Figura 5).

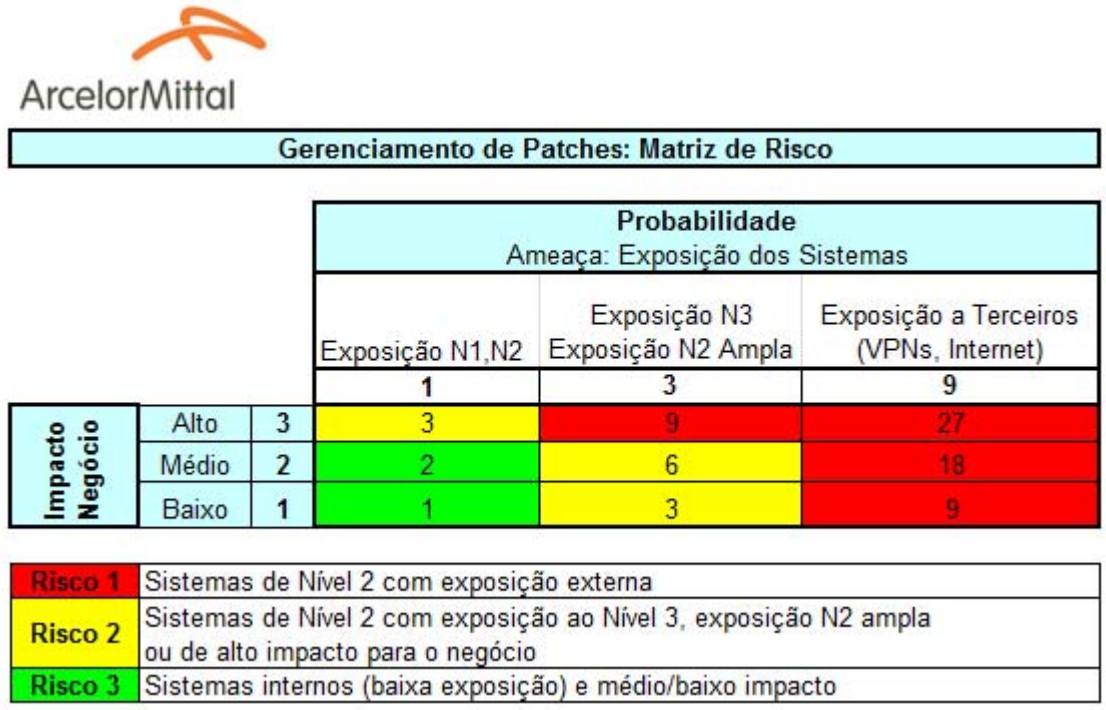

Figura 5. Gestão de *patches* e análise de risco.

Uma topologia de servidores de antivírus também foi implantada, baseada no produto McAfee ePO 4.6. Com uma política afinada para ativos de automação, minimizando perturbações e impactos, vem proporcionando cobertura a equipamentos de N1 e N2 na ArcelorMittal Tubarão, reduzindo drasticamente os incidentes relacionados à contaminações de vírus.

3.4 Controles de Segurança em Sistemas N1

Utilizando a referência de uma planta de nível 1 com 11 sistemas supervisórios, 26 estações de trabalho, 42 controladores, foi observado nos últimos 36 meses a ocorrência de 8 incidentes, sendo três de contaminação por vírus em estações, duas por falha e travamento devido à não atualização do sistema operacional Windows XP, outras duas por falha de infraestrutura como perda do link de rede de dados e

uma ultima com causa não identificada. Para reduzir essas vulnerabilidades, foram implementadas medidas como:

- Implantação de antivírus em todos os servidores e estações de trabalho Windows;
- Política de atualização dos sistemas operacionais, conforme a disponibilidade e parada da planta;
- Segregação das redes de nível 1 separando-as das redes de nível 2 e nível 3, de forma a não permitir acesso irrestrito como anteriormente;
- Desativação (*shutdown*) de todas as portas dos switches de nível 1 e de nível 2 sem uso, e ativação controlada e gerenciada, com registro de logs de forma centralizada;
- Implementação de bloqueio de mais de um endereço MAC em cada porta dos switches de nível 1 e de nível 2 ativadas, com registro de log e alarmes com controle e gerenciamento centralizado;
- Implementação de política de segurança (GPO) padrão em todas as estações de trabalho e servidores, impedindo acessos privilegiados e instalação de mídias removíveis.

Com essas ações, os incidentes foram reduzidos a zero nos últimos 12 meses, porém ainda existem pontos de vulnerabilidades a serem tratados.

4 CONCLUSÃO

Entre os principais aspectos verificados, na avaliação da segurança da informação no ambiente industrial, foi a existência de sistemas sem atualização, alguns descontinuados pelo fabricante e até mesmo sem suporte. Isto se dá devido ao compromisso com a continuidade do negócio, o que leva à adoção de soluções consolidadas e a uma forte restrição quanto à disponibilidade para mudanças. Fatores estes que tornam a implementação da segurança da informação no ambiente de TA diferente das implementações em TI. Este compromisso entre a segurança e a garantia da continuidade operacional, torna necessária a homologação prévia de soluções e a monitoração contínua dos sistemas.

Ainda fazendo uma análise entre os dois ambientes, de TI e de TA, para a segurança da informação, constatou-se com os resultados já obtidos na ArcelorMittal Tubarão que, uma ação efetiva é a segregação entre as duas áreas, liberando acessos apenas onde se faz estritamente necessário. Ficou claro que o bloqueio de acessos e de funcionalidades muitas vezes traz mais benefícios que custos às restrições impostas.

Outro aspecto verificado foi a possibilidade de compartilhar entre TI e TA, os controles de segurança. Isto evidencia a oportunidade de sinergia entre a segurança da informação no ambiente de TI e de TA, havendo assim uma necessidade de estudo conjunto, sempre avaliando os sistemas como um todo, as interferências e oportunidades para os dois ambientes.

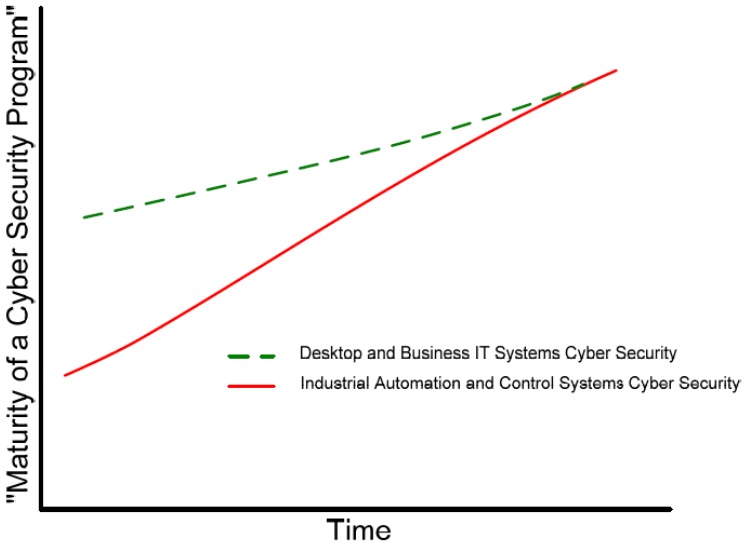

Figura 6. Convergência dos programas de segurança de TI e TA (ISA–99.00.01–2007)

A ISA-99[6] preconiza que as organizações de TI e TA devem sempre trabalhar em conjunto alinhando suas habilidades e conhecimento para endereçar a segurança da informação. O objetivo final é um programa de segurança maduro e convergente (figura 6), integrando todos os aspectos de segurança da informação, incorporando equipamentos e sistemas corporativos, bem como sistemas de automação e controle.

REFERÊNCIAS

1 ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems. Disponível em: <http://www.isa.org/Template.cfm?Section=Standards&template=/Ecommerce/ProductDisplay.cfm&ProductID=9665>. Acesso em: 25/05/2013.

2 Open Source Vulnerability Database. Disponível em: < http://osvdb.org/>. Acesso em: 25/05/2013.

3 White paper - HP 2012 Cyber Risk Report. Disponível em: <http://h30458.www3.hp.com/media2.php/PDF/EZINE_APR/2012CyberSecurityReport4AA4-5495ENW.PDF> Acesso em: 25/05/2013.

4 ArcelorMittal Baseline PA Security Controls v1.13, 2013.

5 Padrões Técnicos e Padrões de Empresarias da ArcelorMittal Tubarão para Segurança da Informação, 2011.

6 ANSI/ISA-99.00.01-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models. Disponível em: http://www.isa.org/Template.cfm?Section=Standards&template=/Ecommerce/ProductDisplay.cfm&ProductID=9657>. Acesso em: 25/05/2013.