PROJETO E IMPLEMENTAÇÃO DA INFRAESTRUTURA DE AUTOMAÇÃO NA VSB ADOTANDO AS MELHORES PRÁTICAS DAS NORMAS ISA-99 E ITIL[1]

Diego Melo [2]
Ana Alda Gomes Tavares [3]
Raphael Muniz [4]
Luciano Souza [5]
Turíbio Tanus Salis [6]
Nathália Rocha [7]
João Pimenta [8]

Resumo

A infraestrutura tem um papel relevante no sucesso dos projetos tanto de TI quanto de TA. Uma estrutura bem projetada favorece a gestão e a realização de atividades que vão desde a gerência de ativos até o desenvolvimento de sistemas. O projeto da infraestrutura de automação da VSB é um caso de sucesso na utilização das normas e melhores práticas em termos de segmentação, segurança e gerenciamento centralizado. O projeto contou com equipamentos de ponta típicos de ambiente de TI associados à equipamentos industriais como PLCs, IHMs e estações de sistemas de supervisão. O projeto da infraestrutura de automação da VSB buscou fundamentalmente garantir a alta disponibilidade dos serviços e equipamentos, disponibilizar a informação obedecendo às normas de segurança, interligar os sistemas de produção de toda a usina possibilitando a integração dos dados, e ainda buscou favorecer o gerenciamento centralizado dos processos e ativos. A concepção do projeto se baseou em normas técnicas e nas melhores práticas de mercado, por exemplo, a ISA-99 e ITIL. Atualmente a infraestrutura de automação conta com 1200 ativos entre PLCs, IHMs, Coletores, Servidores, Supervisórios, Switches, Firewalls, Access Points Wireless, entre outros.

Palavras-chave: Infra estrutura de automação; Rede de automação; Sistemas industriais; Segurança da informação.

DATA INTEGRATION COMING FROM HETEREOGENEOUS AND DISTRIBUTED DATA BASES BY USING PROCESS PORTAL AND ETL

Abstract

Infrastructure has an important role in the success of IT projects either as TA. A well- designed structure favors the management and execution of activities since asset management until systems development. The project of VSB automation infrastructure is a success story in the use of standards and best practices in terms of segregation, security and centralized management. The project has advanced equipment typical IT environment associated with industrial equipment such as PLCs, HMIs and SCADA systems stations. The design of VSB automation infrastructure sought primarily to ensure high services availability, available of information obeying safety rules, interconnect production systems throughout the plant enabling the integration of data, and sought favor the centralized essets and process management. The project was based on technical standards and best market practices, for example, ISA-99 and ITIL. Nowadays the VSB automation infrastructure has 1200 devices such PLCs, HMIs, Collectors, Servers, Supervisory station, Switches, Firewalls, Wireless Access Points, among others.

Key words: Data Integration; ETL;, Processes portal; Datawarehouse.

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

[2] *Esp. em Redes de Computadores, Ana. Automação. VSB – Vallourec e Sumitomo Tubos do Brasil. Jeceaba, Minas Gerais, Brasil.*
[3] *Analista de Automação. VSB. Jeceaba, Minas Gerais, Brasil.*
[4] *Analista de Automação. VSB. Jeceaba, Minas Gerais, Brasil.*
[5] *Esp. Em Redes de Computadores, Ana. de Automação. VSB. Jeceaba,Minas Gerais, Brasil*
[6] *Msc. Eng. Elétrica, Ana. de Automação. VSB. Jeceaba, Minas Gerais, Brasil.*
[7] *Analista de Redes de Computadores. VSB. Belo Horizonte, Minas Gerais, Brasil.*
[8] *Analista de Redes de Computadores. VSB. Belo Horizonte, Minas Gerais, Brasil.*

1 INTRODUÇÃO

O projeto de infraestrutura e segurança da informação para a rede de automação da VSB, tem por objetivo implementar um sistema capaz de melhorar as características e necessidades presentes na automação, e ao mesmo tempo atenuar os riscos associados a ameaças e vulnerabilidades. Isso ocorre devido a grande evolução e crescimento em alta velocidade da área tecnológica da informação, e por consequência a área de automação.

Para garantir a segurança e integridade da tecnologia de automação, um conjunto de políticas, normas e procedimentos específicos para a rede de automação foram criados, devido ao fato de que, inicialmente, os sistemas desenvolvidos para a automação eram isolados das redes de informação (TI Coorporativa), faziam uso de protocolos proprietários e utilizavam software e hardware especializado. Desde então, este cenário mudou, as soluções proprietárias começaram a ser substituídas por soluções baseadas em protocolo IP, já utilizadas pela Tecnologia da Informação e o uso destas soluções permitiu que a conectividade entre as áreas da corporação fossem aumentadas. A integração trouxe novas possibilidades para a redes de automação, como a implementação de Sistema Operacional Windows, Protocolos abertos de comunicação, redução no custo de implementação das tecnologias, maior integração de sistemas, etc.

Porem as soluções de segurança desenvolvidas para a Rede TI não foram projetadas para lidar com as características particulares da automação, e tiveram um tratamento diferenciado antes da sua implementação. Dentre as principais diferenças incluem-se a possibilidade de altos índices de paradas de produção, elevadas perdas financeiras e produtivas, risco à vida humana e agressão ao meio ambiente.

Para darmos inicio ao projeto de infraestrutura de automação da VSB, recursos tecnológicos de última geração foram utilizados para garantir a segurança e disponibilidade dos negócio. Com esse intuito será apresentado neste descritivo de forma sucinta o método utilizado pela VSB, e também a arquitetura lógica e física do ambiente de automação. Assim como a utilização de algumas das melhores práticas de segurança já consolidadas no mercado.

2 MÉTODOS UTILIZADOS

A VSB possui um projeto de infraestrutura de automação que contempla a adoção das melhores práticas no ambiente de Tecnologia de Automação. Tomamos como referência para a elaboração dos procedimentos de gestão de serviços da rede de TA, órgãos normativos utilizados na elaboração de todos os procedimentos de gestão, voltados especificadamente para automação. Tendo como foco principal a ISA-99 dentro dos conceitos de automação. O Quadro 1 descreve algumas das normas utilizadas como base na elaboração do projeto de infraestrutura de redes de automação:

Quadro 1. Normas técnicas utilizadas pela VSB

ITIL v2	IT Infrastructure Library
ITIL v3	IT Infrastructure Library
ISO/IEC 20000	Information technology – Asset Management
ISO/IEC 7498-4	Information technology – OSI Model Management
ISA 99	Manufacturing and Control Systems Security
dISA-99.02.01	Establishing a Industrial Automation and Control Systems Security Program
The Complete Guide to IT Service Level Agreements	Livro que estabelece o conceito de SLA. Autor: Adrew Hiles

3 DEFINIÇÃO DA TOPOLOGIA LÓGICA

Foram definidas algumas premissas durante a elaboração do projeto lógico da rede. Estas premissas do projeto lógico asseguram os principais objetivos da infraestrutura em termos de disponibilidade, performance, segurança, escalabilidade e gerenciabilidade necessários aos sistemas de TA. Todas as decisões de projeto e o detalhamento das topologias são justificados por tais premissas. Os seguintes aspectos foram considerados para a elaboração das premissas:

- padrões de projeto de redes;
- normas internacionais de segurança da informação para o ambiente industrial;
- recomendações e padrões de projeto de fornecedores;
- premissas e restrições pertinentes ao ambiente de TA;
- requisitos de sistemas específicos de TA;
- padrões de projeto de TI.

A seguir apresenta-se as premissas e os principais fatores que justificam sua adoção.

3.1 Separação das Redes de TI e TA

As redes de TI e TA devem ser totalmente segregadas. Esta segregação deve ser física (com equipamentos não compartilhados) e lógica (com perímetros lógicos de rede bem definidos). Esta é uma recomendação de normas de TA justificada pelo fato de que a TI está em contato com o ambiente externo (ex. Internet) e, portanto, está exposta a maiores riscos advindos desta característica.
Para garantir a separação um ponto único de comunicação da TA com o ambiente externo e todo o tráfego é filtrado e monitorado através de um dispositivo de firewall. Esta recomendação é explicitamente ditada pela norma ISA SP99, que trata de segurança da informação no ambiente industrial.

3.2 Controle de Tráfego de Entrada e Saída de TA

Uma boa prática adotada para garantir a segurança da rede foi minimizar o número de regras no firewall que permitem a comunicação direta entre as redes de TI (ambiente externo) e TA. Esta é uma recomendação do “Guia de Segurança para Sistemas Industriais de Controle”, publicado pelo NIST, e da norma ISA SP99. Para isso foi criado uma DMZ (Zona Desmilitarizada) onde foram posicionados todos os servidores que fazem comunicação com o ambiente externo.

3.3 Segregação de Redes para Sistemas que Não se Comunicam

Sistemas que não se comunicam foram separados em redes distintas. A segmentação lógica foi feita através da criação de VLANs (Virtual Local Area Network, “redes lógicas”) e também por meio de redes física, utilizando equipamentos/recursos diferentes para determinada conjunto da rede, onde o recurso de VLANS não foi possível. O critério de decisão para o uso de segregação física e lógica deve-se ao nível de criticidade dos sistemas, segurança, disponibilidade e performance. Assim, uma rede (lógica ou física) de um determinado sistema não gera tráfego na rede de outro sistema que não comunicam entre si.

3.4 Segregação Física/Lógica das Redes de Controle (Nível 1)

A rede de controle ou, rede nível 1, é a rede considerada de maior criticidade para a automação, já que a sua indisponibilidade implica diretamente na parada da produção. Desta forma, todas as redes de controle foram criadas de forma isolada, física e logicamente, das outras redes cujos equipamentos e sistemas não comunicam entre si. Ou seja, a rede de um determinado sistema/equipamento não gera tráfego na rede de outro sistema/equipamento com o qual não comunica.

3.5 Rede Totalmente Gerenciada

A rede de automação da VSB permite o gerenciamento contínuo dos ativos (incluindo ativos de nível 1 como PLCs, IHM e remotas) de forma centralizada. Os ativos pertencentes às diversas áreas do processo produtivo podem ser monitorados de forma centralizada. Ativos como servidores e estações críticas também são monitorados e gerenciados. Alguns equipamentos de controle como PLC´s não permitem a gerência através de protocolos de gerenciamento mais estruturados como o SNMP ou RMON. Neste caso, a gerência ainda ocorre através do protocolo ICMP. A funcionalidade de Gerenciamento da Rede de Automação ainda prevê:

- *Gestão de Serviços:* um modelo de processos para gestão de serviços está sendo implementado para garantir a gerência de falhas, performance, segurança, contabilização e configuração, considerando características específicas do tipo do ambiente, sistemas e pessoas.
- *Central de Serviços:* existe também um ponto a partir do qual a gerência de toda a rede pode ser praticada. Neste local, uma plataforma de gerência faz o controle de todos os ativos de rede ethernet instalados. Para isto foi criada uma sub-rede lógica de gerência, permitindo toda a comunicação com toda a rede de TA de forma controlada e segura.
- *Serviços de Gerência Compartilhados:* na camada core da rede foram instalados servidores de serviços de gerência que foram compartilhados entre as áreas de processo. Servidores como o “Console Gerenciador de Antivírus” e o “gerenciador de ativos” (inventário) permitindo um controle centralizado dos ativos de TA com regras e restrições de acordo com recomendações de normas de TA e o modelo de gestão de serviços definido.

3.6 Alta Disponibilidade

A rede de automação foi implementada de forma a separar os ativos e sistemas em diferentes níveis de disponibilidade, uma vez que há requisitos diferentes para cada nível. As seguintes premissas foram adotadas para garantir a disponibilidade adequada aos diversos equipamentos e sistemas, principalmente aos de alta disponibilidade:

- *Redundância do Core:* redundância dos core's para os serviços compartilhados e na conexão com o ambiente externo (TI). Assim, o núcleo da rede (core) possui redundância em dois datacenters: CPD principal e CPD de contingência;
- *Redundância no nível de distribuição:* os switches do nível de distribuição tem a função de agregar os equipamentos da camada inferior, provendo acesso ao núcleo da rede e conectividade a servidores críticos para a disponibilidade do processo. Havendo assim redundância de equipamentos neste nível;
- *Redundância no cabeamento:* redundância na conexão física dos cabos entre os níveis de core e distribuição e entre os níveis de distribuição e acesso para redes de acesso críticas (ex. redes de clientes SCADA). As rotas de cabos são projetadas para garantir caminhos alternativos distantes entre si;
- *Convergência rápida no nível 1:* a convergência (chaveamento) para equipamentos ou links redundantes em caso de falha, nas redes de controle, ocorre de forma rápida, com o objetivo de evitar perda de dados. Para que isto, somente tecnologias de convergência rápida (inferior a 1 segundo) poderão ser utilizadas nas redes de controle.

  Observação: há protocolos que operam em topologias de anel que atendem a este requisito. Para uma topologia em anel com tecnologia Cisco é utilizado o protocolo REP (Resilient Ethernet Protocol), que garante um tempo de convergência entre 50 e 250ms.

3.7 Independência de Serviços da TI

A rede de automação provê, sempre que possível, seus próprios serviços de rede, mantendo-se independente dos serviços de TI. Dessa forma, serviços como patch management, asset management, serviço de diretórios (active directory) e servidor de antivírus são independentes e específicos para a rede de TA.

3.8 Serviço de Autenticação, Autorização e Contabilização Integrado para Switches e Roteadores

A autenticação nos switches e demais equipamentos de rede foram projetados de forma integrada com o serviço de diretórios do Active Directory, possibilitando assim, um controle adequado da autenticação, autorização e auditoria nestes equipamentos. Para isto foi criada conectividade para o serviço de autenticação, autorização e contabilização (AAA) na camada core, a partir de todos os switches da rede.

4 MODELO HIERÁRQUICO

O modelo de referência adotado para estruturar a rede de automação da VSB é o modelo hierárquico adaptado. Buscando atender ás premissas das normas ISA S99

e S95 o modelo adotado na VSB contempla a inclusão de um nível de rede referente às redes de controle.
O Modelo Hierárquico é amplamente utilizado em todo o mundo na concepção de projetos de rede de médio e grande porte. Grandes redes podem ser consideravelmente complexas, envolvendo múltiplos protocolos, configurações e diversas tecnologias como é o caso da VSB. A hierarquização, ou a divisão em camadas, faz com que vários problemas de performance, segurança e escalabilidade sejam minimizados e até mesmo completamente evitados. Sistemas de redes hierárquicos permitem identificar facilmente onde um recurso pode ser alocado, sua função na rede e sua interação com demais equipamentos. Muitos dos fabricantes sugerem, atualmente, um modelo de três camadas, cada qual dedicada a uma função específica. Pelos motivos acima supracitados, este modelo foi o escolhido para a implantação da rede da VSB. A rede implementada procura seguir todas as recomendações deste modelo, desde a função de cada uma das três camadas até a forma de encaminhamento do fluxo de dados.

4.1 Core

Por definição o Core é a camada da rede responsável pelo intercâmbio de dados de forma rápida e confiável. Na rede de automação da VSB esta é a camada onde todas as áreas de produção e os servidores comuns a essas áreas estão conectados. Além disso, nesta camada é realizada a interface com outras redes como a da TI, para acesso a internet (casos estritamente e ponderadamente permitidos), comunicação com o sistema MES ou qualquer outro serviço disponibilizado pela TI. Nesta camada está conectada a Central de Serviços TA (CTA), responsável por realizar todo monitoramento e gerência dos ativos da rede TA da VSB. Para garantir plena disponibilidade e continuidade aos serviços de automação, algumas características da camada Core devem ser enfatizadas:

- A rede de TA da VSB possui dois DataCenters onde são utilizados equipamentos idênticos para garantir a replicação dos recursos e serviços, gerando redundância.
- Para cada área de automação (centros de distribuição) temos dois links, gerando uma redundância para a comunicação, sendo um link conectado ao DataCenter Principal e outro ao DataCenter Contingência.
- Os switches Core, são ligados entre si, garantindo que no caso de falha de um link de comunicação de uma determinada área com algum destes switches, os serviços de rede não serão interrompidos.
- Os servidores comuns a todas as áreas serão ligados junto aos switch Core de contingência e switch Core principal.
- O core da rede possui dois firewalls de perímetro, responsáveis pela comunicação entre as redes de TA e mundo externo, incluindo a TI. A convergência entre eles se dá através do protocolo OSPF.
- Os únicos acessos à rede externa a da TA (Rede de TI) são através da DMZ (Zona desmilitarizada), que é ligada ao firewall de perímetro para garantir segurança contra possíveis ataques (nessa zona encontram-se servidores como o do Antivírus e WSUS que precisam de atualizações e por isso o acesso a rede externa se faz necessário) e alguns servidores das áreas que precisem se comunicar com o MES da TI.

- Ligado ao switch Core do DataCenter Contingência temos o sistema de backup. Este sistema é composto de um servidor de backup, uma tape library ligada a ele e dois storages, cada ligado a um switch Core.

A Figura 1 mostra a estrutura da camada do CORE, com os dois firewalls de perímetro, dois switches core (cada um em um DataCenter), os servidores comuns e as ligações com a DMZ (Zona Desmilitarizada onde os servidores podem ter acesso a rede de TI “Internet”), Central de TA e a rede da TI.

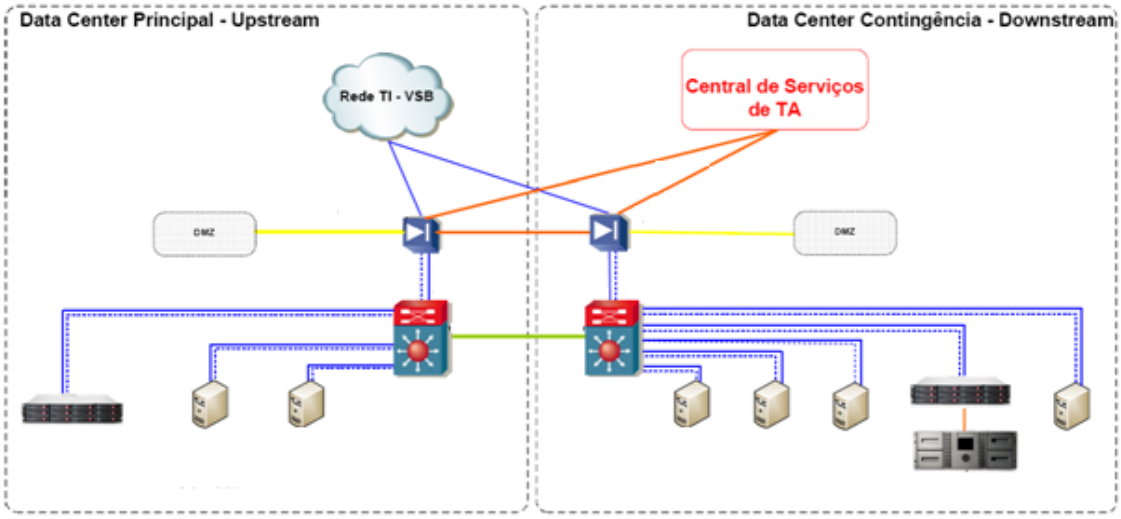

Figura 1: A Camada CORE da rede da VSB.

4.2 Distribuição

Por definição a camada de Distribuição tem como principal função, prover roteamento, políticas de segurança e acesso ao Core. Algumas tarefas executadas nessa camada são:

- Implementação de ferramentas como listas de acesso (ACLs) e filtragem de pacotes;
- Redistribuição entre protocolos de roteamento (OSPF), incluindo roteamento estático;
- Roteamento entre VLANs (Virtual Local Area Network).
  Cada uma das áreas da TA possui na distribuição quatro switches Layer 3 operando em stack (empilhados), conectados aos dois switches Core da rede através de dois links de 10Gbps cada, garantindo maior disponibilidade dos recursos e serviços da rede.
  Esses switches da Distribuição estarão instalados fisicamente dentro dos DataCenters da seguinte forma:
- DataCenter Principal: Equipamentos da Aciaria e Redução
- DataCenter Contingência: Equipamentos da Laminação , OCTG e Q+T (Downstream I e Downstream II)
  A figura 2 mostra a estrutura da camada de Distribuição de cada área, assim como as ligações entre os switches de distribuição e os switches core. Essas ligações são feitas através de uma rede Dummy.

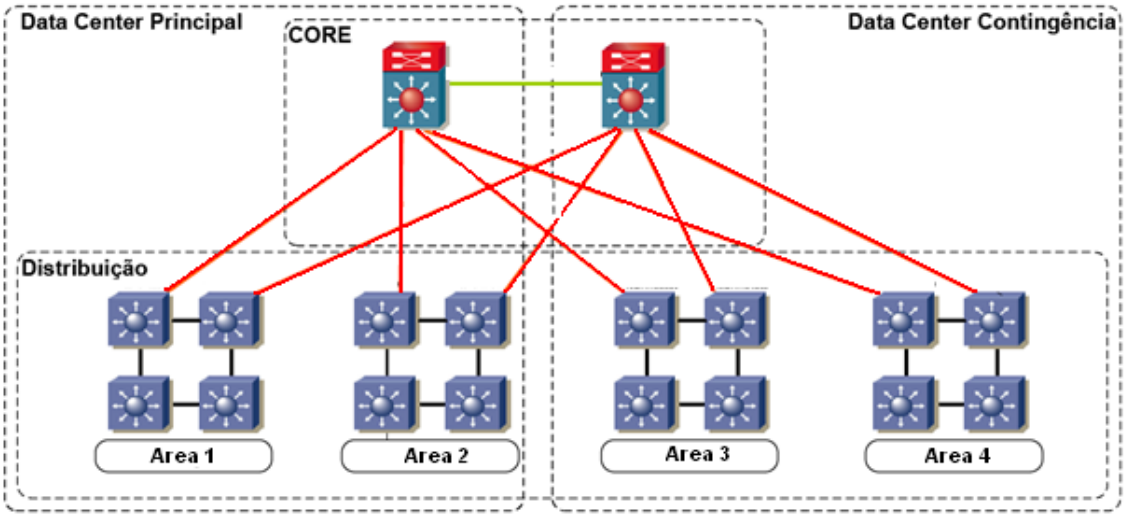

Figura 2: Camada de distribuição.

4.3 Acesso

Provê acesso à rede para usuários nos segmentos locais. Esta camada freqüentemente usa apenas hubs e switches.

4.3.1 Rede Nível 2

A camada de acesso nível 2 controla o acesso de grupos de usuários aos recursos da rede. Grande parte dos recursos que os usuários precisarão, estarão disponíveis localmente.

Algumas tarefas que foram consideradas na camada de acesso:

- implementação de políticas de acesso à rede e segurança;
- criação de diferentes domínios de colisão (separação em vlans);
- conectividade dos grupos de trabalho com a camada de distribuição.

O acesso nível 2 é composto basicamente pelos sistemas de supervisão da planta, que inclui os servidores SCADA, clientes SCADA, clientes nível 2 e outras estações como as estações de engenharia/manutenção. Algumas considerações importantes relacionadas à rede TA da VSB:

- os links entre o acesso e o '*nível de distribuição*' de cada uma das áreas são redundantes;
- cada link é conectado a um switch de distribuição distinto, garantindo conectividade ao core mesmo em caso de falha de um switch da distribuição.

4.3.2 Rede Nível 1

Em razão dos níveis de criticidade para os equipamentos pertencentes à rede de controle, um conjunto de premissas foi definido para o modelo desta rede:

- as redes são segregadas física e logicamente. Assim, PLC´s ou grupos de PLC´s que não possuem necessidade de comunicação mútua estão separados em redes distintas (com switches e VLAN´s separadas);
- existe conexão redundante entre a rede de controle e o nível de Distribuição;
- os equipamentos de rede de controle garantem alta disponibilidade e, em casos de operação em ambiente hostil, equipamentos próprios são utilizados, tais como switches industriais CISCO IE3000 e módulos específicos para ambientes com altas temperaturas e poeira.

Nas redes em anel da Aciaria e Redução o protocolo REP (Resilient Ethernet Protocol) está configurado para evitar que ocorram loops na camada de Enlace da rede. O REP tem tempo de convergência entre 50ms e 250ms.
As redes de controle são segregadas fisicamente das demais redes através de um firewall de controle, localizado entre os switches que realizam roteamento dessas redes (layer 3) e o switch de distribuição de sua respectiva área. A segregação lógica entre as redes de controle de uma determinada área é realizada através de ACLs aplicadas nos switches que realizam roteamento das mesmas.
Sendo assim, equipamentos pertencentes a uma mesma rede de controle possuem conexão direta entre si, sem roteamentos, para que não ocorram atrasos ou perdas na comunicação.

4.4 Redes de Engenharia

A Vlan de engenharia é dedicada às estações de engenharia/manutenção. Estas estações geralmente fazem acesso tanto à rede de controle nível 1, quanto à rede nível 2. Desta forma a permissão de comunicação das vlans de engenharia com as redes nível 1, são feitas nos firewalls de controle para garantir a segurança dessa comunicação. Em cada área foi criada uma rede de engenharia, ou seja, redes de engenharia de áreas diferentes não comunicam umas com as outras, assim como não se comunicam com redes de controle de áreas diferentes da sua.

4.5 Rede Central de Serviços TA

Para obter uma gestão confiável e protegida, foi implementada uma estrutura em que por uma vlan de gerência trafegam todas as informações de gestão e é possível monitorar e fazer intervenções em toda rede de TA. É objetivo desta estrutura proporcionar a gestão de todos os ativos da rede da VSB, incluindo equipamentos como switches (layer 2 e layer 3), firewalls e plcs. Todos estes dispositivos terão uma vlan de gerência (e consequentemente um IP) associados a ele. Como forma de garantir maior segurança a rede, a rede da Central de Serviços TA estará conectada diretamente ao Firewall de perímetro, uma vez que através dessa rede todos os ativos da rede de TA podem ser acessados.
Um bom gerenciamento da rede pode ajudar a VSB a alcançar os objetivos de disponibilidade, performance e segurança desejados. O processo de gerenciamento da rede verifica se os objetivos e premissas do projeto da rede foram alcançados e ainda mostrar resultados que não puderam ou foram percebidos anteriormente.
Os processos de gerenciamento a serem adotadas para a rede de automação da VSB têm como referência o ITIL e a ISO/IEC

4.6 Redes de Backup

Devido à grande quantidade de servidores granularizados e com volume de dados de backup relativamente pequeno, a solução de armazenamento mais adotada pela VSB é a do tipo NAS (Network Attached Storage), na qual o dispositivo de armazenamento estão conectado diretamente à rede. Para garantir a segurança e o desempenho da rede, dispositivos (switches e transceivers) com links de alta capacidade (10Gbps) de processamento (throughput) foram criados. O tráfego de dados de backup foi segregado dos dados de produção logicamente, utilizando uma

VLAN exclusiva e cada servidor de dados gera os dados de backup através de uma interface de rede exclusiva.
No Core da rede de TA existem links exclusivos para o tráfego de backup entre os switches e os firewalls de perímetro. Esses links não podem ser utilizados para o tráfego de produção e em caso de falha a comunicação de backup. Estes links serão restabelecidos quando o link for reativado, ou seja, o tráfego de backup nunca usará os links de comunicação da produção como meio.

5 SEGURANÇA

Os controles de Segurança da Informação planejados para o projeto foram adotados em conformidade com as recomendações das seguintes normas internacionais:

- *ISA-99.02.01*, Establishing an Industrial Automation and Control Systems Security Program;
- *ANSI/ISA-TR99.00.01-2007,* Security Technologies for Industrial Automation and Control Systems;

5.1.1 DMZ

Para minimizar a criação de regras diretas entre a TA e o perímetro externo, foi criada uma DMZ entre as redes de TI e TA, contendo os componentes (servidores) que fazem acesso ou que são acessados pelas duas redes. Nesta topologia o firewall possui três interfaces, sendo uma para a conexão com a TI, outra para a conexão com o switch Core da TA e por fim, outra para a DMZ.
Neste caso não havendo comunicação direta entre sistemas das redes de TI e TA, garantindo maior segurança para os sistemas. Assim, o fluxo de dados é representado conforme mostrado na Figura 3.

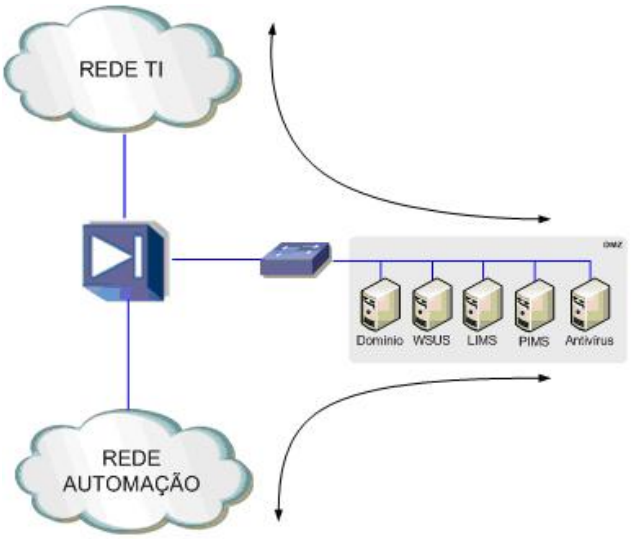

Figura 3 - Fluxo de dados na DMZ.

5.1.2 Firewall

- **Firewalls de Perímetro**

São os Firewalls localizados no Core da rede e que realizam a conexão entre a rede da Automação da VSB, da TI da VSB, da Central de serviços TA e da DMZ onde estão localizados os servidores que farão acesso a rede externa a da Automação.

As regras criadas nesses dois Firewalls são bem restritivas, permitindo apenas que as comunicações extremamente necessárias sejam autorizadas, através de IP de origem e destino, protocolo e porta de destino da comunicação.Para criação de novas regras nos Firewalls de perímetro, devem ser analisadas por quais interfaces o tráfego entra no Firewall, a fim de determinar a regra necessária a ser criada. É importante lembrar que as regras são feitas de forma mais restritiva possível e nunca é utilizado um destino (ou origem) indefinido (“any”). Uma vez feita essa análise, a configuração deve ser realizada no Firewall localizado no DataCenter Principal e replicada manualmente para a interface correspondente no Firewall localizado no DataCenter Contingência, pois em caso de falha de um dos Firewalls, o tráfego da rede de TA (exceto o tráfego da rede da DMZ que se encontra atrás do firewall de perímetro onde houve a falha) será encaminhado para o outro Firewall de Perímetro.

- **Firewalls de Controle**

O firewall de controle é um equipamento de pequeno porte, desenvolvido com o propósito de proteger redes críticas de outros segmentos de redes. É uma prática sugerida para garantir a segurança das redes de controle. O firewall de controle garante que os equipamentos destas redes serão isolados ao mesmo tempo em que permite que eles sejam controlados e monitorados pelas ferramentas de gerência da rede. O firewall de controle será ligado entre o switch de distribuição e o switch nível 1, nas topologias sugeridas, como mostrado na Figura Figura 4: Firewall de Controle. Estações de engenharia ligadas em um switch de acesso poderão acessar a rede de nível 1 passando pelo switch de distribuição, firewall de controle, switch nível 1 e finalmente atingindo o PLC ou estação cliente. Esta conexão é justificada, pois:

- O acesso das estações de engenharia ao nível 1 é eventual;
- Esta conexão não é critica e, se essa comunicação falhar por causa do firewall, por exemplo, o processo produtivo não será afetado.bAs rotas para acesso as redes de controle foram inseridas de forma manual nos firewalls de controle. Além dessas rotas temos uma rota default apontando para o ip da rede Dummy utilizado pelo switch de distribuição. A figura 4 mostra o esquema do Firewall de controle.

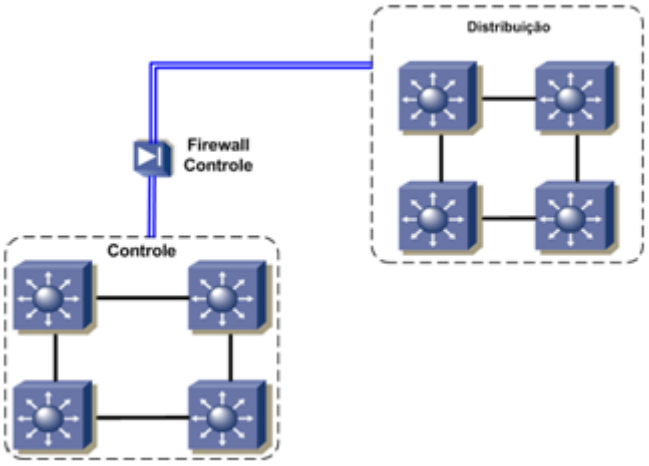

Figura 4: Firewall de Controle.

5.1.3 VLANS

Para aumentar o nível de segurança da rede de automação da VSB, aproveitando as tecnologias adquiridas com os Switches, foram criadas VLANS.

As VLAN's (Virtual Local Area Network) são formas de segmentar logicamente a rede, agrupando em um mesmo domínio de broadcast as estações/sistemas que compartilham as mesmas características. Dessa forma, o desempenho pode ser otimizado, já que o fluxo de dados passa a ser bem definido e ainda garante-se a independência e controle de cada um dos sistemas.

Os principais objetivos a serem alcançados com a segmentação em VLANS são:

- Segmentação de problemas por área/sistema: problemas que ocorrem em uma área não serão repassados para as outras áreas. As divisões nos níveis de automação facilitam a criação de VLANs e consequentemente o gerenciamento e resolução de problemas.
- Diminuição dos domínios de broadcast: Broadcast são comuns e necessários em toda rede ethernet, muitas aplicações requerem o broadcast para funcionar apropriadamente. Como não é possível eliminar os broadcasts de uma rede ethernet, é recomendado que os seus domínios sejam claros e não muito grandes para que minimize o impacto dos mesmos na performance e carga da rede e dispositivos.
- Diminuir o tráfego de multicast em portas que não são endereçadas;
- Facilitar a organização e o gerenciamento;
- Aumentar a segurança: uma rede que não implementa VLANs não tem a devida preocupação com segurança. Uma possível vulnerabilidade em uma sub-rede pode atingir a rede como um todo.

6 GERENCIAMENTO DE MUDANÇA

As mudanças no ambiente de TA podem ser resultado de problemas identificados ou mesmo de iniciativas que buscam benefícios aos negócios, como redução de custos, ampliação de serviços e consequentemente melhoramento dos serviços prestados. O Gerenciamento de Mudanças tem como meta garantir que as mudanças no ambiente de TA ocorram sem causar impacto no negócio da empresa.

6.1 Descrição do Processo

O Processo de Gerenciamento de Mudanças é responsável por decidir e coordenar as mudanças, não tendo como objetivo a execução das atividades propriamente dita. A implementação é realizada por uma equipe técnica responsável pela área da mudança, como a área de redes, sistemas indstriais, hardware, programação de CLP entre outras. O processo tem como objetivo controlar as mudanças para que elas sejam implementadas de forma segura e eficiente, no que se refere ao custo e com um mínimo de riscos para os serviços disponibilizados.

O processo do Gerenciamento de Mudanças inclui as seguintes atividades:

- Registro e classificação (Criar e registrar a Requisição de Mudança-RDM);
- Aprovação (Revisar e avaliar a Mudança);
- Coordenar o desenvolvimento;
- Acompanhar o resultado dos testes de homologação (caso não seja possível, necessário justificativa);
- Autorização e implementação;
- Avaliação e encerramento (Revisar e encerrar).

6.1.1 Registro e classificação

O Registro de classificação possui informações para a tomada de decisão, tais como categoria, impacto, custo, razão da mudança, pessoas envolvidas, plano de rollback entre outras informações. Grande parte dessas informações são submetidas a análise do Comitê de Mudanças. Estas informações também serão utilizadas para extrair o relatório gerencial que servirá de base para uma análise posterior à mudança. Também é importante alocar a prioridade para cada mudança para definir a agenda de mudanças programadas.

6.1.2 Autorização e implementação

Após passar pela fase de desenvolvimento, as mudanças são testadas antes de ir para o ambiente de produção. Após o resultado dos testes a mudança fica autorizada a ser implantada. Dependendo da urgência e do impacto da mudança, a fase de testes pode ser ignorada.

6.1.3 Implementação

O Gerenciamento de Mudanças deve garantir que as mudanças sejam implementadas seguindo um programa e cronograma previamente definido que é acompanhado pelo processo de gerenciamento de mudança. A execução da implementação não é de responsabilidade deste processo, ele apenas o coordena. O processo de Gerenciamento de Liberações poderá ser coordenado pelo processo de Gerenciamento de Mudanças, pois as mudanças acabam gerando novos releases de software ou de hardware. Diagrama de Impacto ou risco deve ser apresentado antes da implementação e avaliação dos testes.

6.1.4 Avaliação e encerramento

O Gerenciamento de Mudanças avaliará todas as mudanças implementadas após até uma semana após a implementação. Esta revisão se chama Revisão Pós Implementação (RPI). O processo de Gerenciamento de Problemas também poderá acompanhar este processo, visto que o Controle de erros tem esta atividade no seu escopo. Esta revisão serve para verificar se a mudança trouxe os resultados esperados, ou se houver algum problema ou ineficiência, ações devem ser tomadas para a correção. A mudança deve ser formalmente encerrada após o aceite do cliente.

6.1.5 Mudanças emergenciais

Caracteriza-se como mudança emergencial, a necessidade de alguma alteração com criticidade alta no ambiente de produção que não possa aguardar o processo normal descrito acima. Geralmente são necessidades de correção de graves problemas, com impactos significativos no negócio da empresa. Para que se tenha condições de tratar essas solicitações de forma adequada, se faz necessário a criação de um Comitê Consultivo de Mudanças Emergencial, ou Comitê de Emergência (CCM/CE). Nesse caso, é necessário identificar uma configuração menor com autoridade para tomar decisões emergenciais. Este comitê sempre será formado pelo Gerente de Mudanças, os Engenheiros responsáveis pela implementação da Mudança e o gerente da área onde a mudança será aplicada. Nesse comitê também será discutido todos os prováveis impactos da mudança e também o processo de rollback caso aconteça alguma falha durante a implementação, assim como o planejamento para implementação, porém, com mais agilidade, objetividade e a prioridade que uma mudança emergencial demanda. O

processo de acompanhamento após a implementação se mantém conforme o procedimento para acompanhamentos de demandas não emergenciais.

6.1.6 Fluxograma de solicitações de mudança no ambiente de automação da VSB

A Figura 5 mostra o fluxo de atividades referentes à solicitações de mudança no ambiente de automação da VSB.

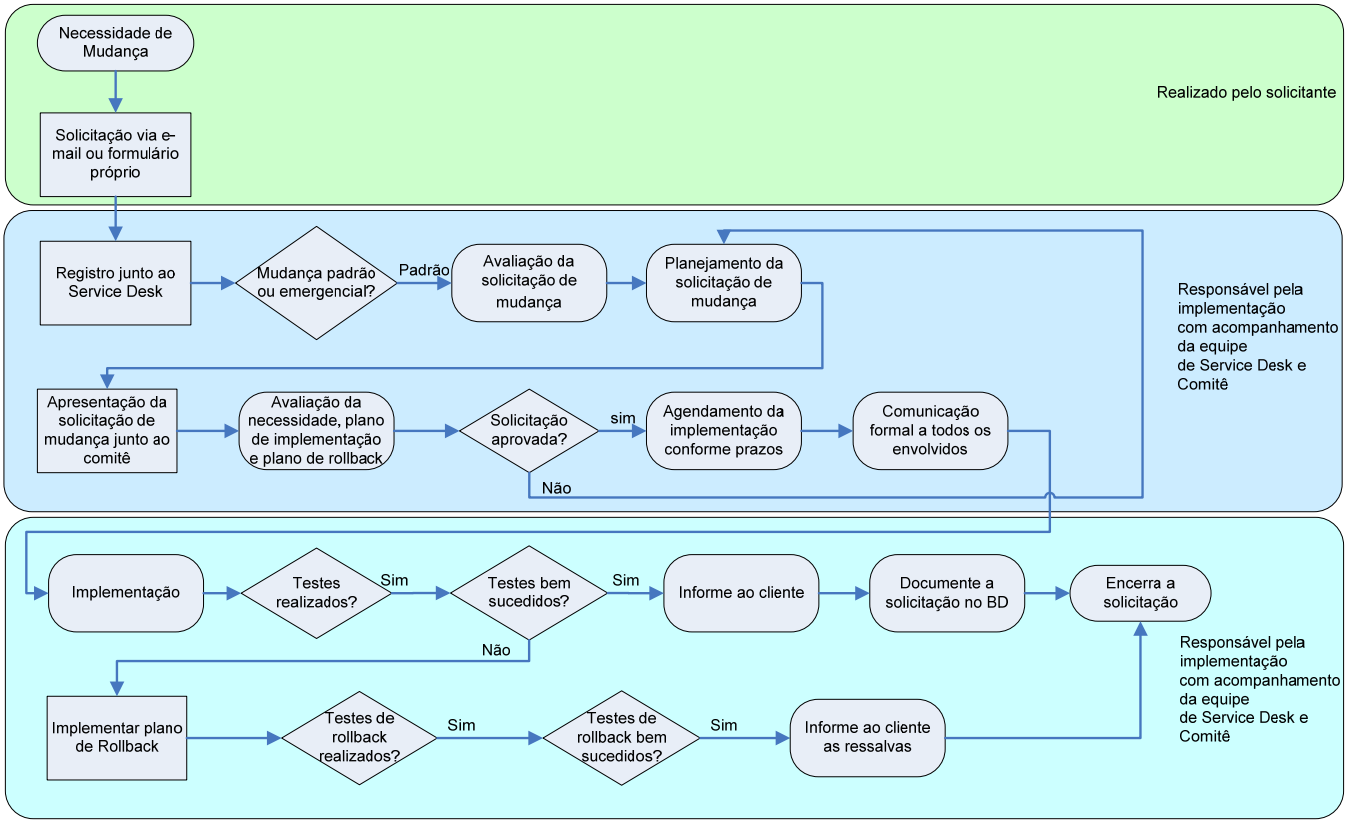

Figura 5: Fluxograma de solicitações de mudança no ambiente de TA da VSB.

6.1.7 Comitê de Controle de Mudanças (CCM)

É um grupo responsável pela avaliação do impacto das mudanças. Este grupo é composto de várias pessoas técnicas e até mesmo os clientes das atividades, que fornecerão assessoria ao Gerente de Mudanças sobre quais mudanças devem ser aprovadas e auxiliarão na programação das mudanças.

Possíveis membros do CCM:

- O Gerente de Mudanças
- Cliente(s);
- Gerente(s) Usuário(s);
- Representante(s) de Grupo de Usuários;
- Engenheiros de desenvolvimento/manutenção de aplicações (quando apropriado);
- Consultores, especialistas e técnicos;
- Equipe de serviços (se necessário);
- Equipe de serviços administrativos (quando as mudanças afetam as instalações);
- Representantes dos contratantes ou de terceiros (se necessário - por exemplo, em situações de outsourcing).

7 RESULTADOS: A INFRAESTRUTURA DE TECNOLOGIA DA AUTOMAÇÃO EM NÚMEROS

Abaixo é apresentada uma lista que exemplifica os números dos ativos no ambiente de automação da VSB.

Quadro 2. Quantitativo de equipamentos e sistemas VSB

Tipo de Ativo	Descrição	Quantidade
Access Point Wireless	Pontos de Acesso (rádios) e antenas correspondentes Indoor e Outdoor de diferentes marcas a modelos	**73**
Coletores	Dispositivos móveis (hand helds) utilizados em campo	**9**
Estações Clientes	Estações de operação de diferentes sistemas de automação, com Sistema Operacional Micrososft Windows XP, Vista ou Windows 7	**271**
Estações de Engenharia	Workstations utilizadas para desenvolvimento e testes pelos engenheiros	**27**
Firewalls	Firewalls dos Modelos Cisco ASA5550 ou ASA5505	**16**
IHM	Interface Homem Máquina – dispositivos utilizados para operação em campo, com sistema operacional proprietário ou Micrososft	**37**
Impressoras	Impressoras Laser ou Jato de Tinta, de rede ou conectadas diretamente a computadores/servidores	**32**
Notebooks de Manutenção	Notebooks utilizados para manutenção em campo ou pelos engenheiros e analistas de Automação	**10**
PLC	Controladores Lógicos Programáveis	**219**
Servidores	Servidores com Diferentes Aplicações (listadas posteriormente), com sistema operacional Microsoft Windows 2003, 2008, 2008 R2 ou Linux	**106**
Storage	Storages HP StorageWorks 4400 Scalable NAS File Services, com Windows Storage Edition e HP Data Protector	**9**
Tape Library	Library HP MSL 4048	**1**
Switches	Switches Cisco de Modelos Catalyst 3750, 4507, 2960 e Switches Industriais Cisco Modelo IE3000	**197**
UPS	Unidade de Fornecimento de Energia de Diferentes Fabricantes e Modelos	**14**
Outros serviços		
Controlware	Sistema Controlware	

CMS	Controle de Versões de Lógica de Controle GE Fanuc Proficy™ Change Management (CMS)
LIMS	Sistema LIMS – Laboratory Information Management System
PIMS	Plant Information Management System
WEB Portal de Relatórios	Techsteel/VSB – Repositório Relatórios WEB
WEB Portal de Processos	Techsteel/VSB – Aplicações para integração e análise de dados dos processos.
Serviços de Rede	Antivírus Symantec; Tz0 – Inventario; DNS Microsoft; DHCP Microsoft; Active Director Microsoft; HP Data Protector Backup; Acronis Image; Zabbix Monitor VPN Connection

8 CONCLUSÃO

O projeto de implantação de segurança e infraestrutura da VSB foi bem sucedido em garantir a segurança e a integridade, em conjunto com as políticas, normas e procedimentos específicos criados para a rede de automação. Com a mudança do mercado e o atual cenário tecnológico as soluções proprietárias de automação, passaram a ser substituídas por comunicações baseadas em protocolo IP, já utilizadas pela Tecnologia da Informação. O continuo uso destas soluções facilitam ainda mais o aumento da comunicação entre maquinas de operação e ativos computacionais. Desta forma o ambiente de automação está cada vez mais próximo de um ambiente de TI. Para isso a VSB adotou as normas de mercado como ISA-99, ITIL, CobiT, entre outras para que seus processos fossem criados de maneira segura e em conformidade com o cenário atual. O aumento da qualidade dos serviços da tecnologia da automação de forma segura, passam a ser essenciais e orientados aos negócios da empresa. Pois cada vez mais a empresa passa a ser dependente dos serviços de automação para atingir seus objetivos corporativos. Acredita-se que com todo esse investimento e tecnologia adotada na área de automação, a VSB atinja a excelência na parte de comunicação e segurança desse seu maior bem, pessoas e tubos .