UTILIZANDO ZONAS E CONDUÍTES DE SEGURANÇA EM UM PROJETO DE REDES DE TA ORIENTADO A PREMISSAS DA SEGURANÇA DA INFORMAÇÃO[1]

Leandro Pfleger de Aguiar[2]
Marcelo Ibrahim Soares[2]

Resumo

Com a publicação de normas e padrões de segurança da informação específicos para ambientes de automação industrial, o desafio tornou-se a sua interpretação e implementação na prática sem desrespeitar as restrições e heterogeneidade pertinentes a este ambiente, Grande parte das tentativas de implementação de segurança ocorrem através de projetos de rede, com pequenas etapas que deixam de considerar o investimento em segurança com a visão de gestão de riscos inaceitáveis para o negócio. Este trabalho descreve, sob a ótica de projeto, sobre como transformar recomendações de normas como a ISA 99 e NIST SP-800 em resultados práticos em termos de implementação de segurança, mesmo quando isto é feito como uma etapa de um projeto de rede, destacando em especial as recomendações para a definição de zonas e conduítes de segurança que permitem que segmentos inseguros convivam com segmentos com sistemas críticos de forma controlada e racional. Os resultados apontam para um alinhamento estratégico dos stakeholders do projeto, com uma melhora geral da integração do Representante de Segurança Corporativo, equipe de automação e fornecedores, e orientação dos investimentos aos reais objetivos corporativos de gestão dos riscos.

Palavras-chave: Segurança da informação; Zonas e conduítes; Segmentação de redes; Redes de automação.

USING ZONES AND CONDUITS IN THE DESIGN OF A INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS NETWORK BASED ON INFORMATION SECURITY PREMISSES

Abstract

After the publication of Standards and Guidelines specific for Industrial Automation and Control Systems Security, the greatest challenge for managers became how to interpret and deploy those best practices without disregarding the restrictions and heterogeneity of this complex environment. Several attempts to implement security projects take place through network design projects. These are usually based on steps that do not consider information security as Risk Management task. This paper describes, from a design perspective, about how to transform guidelines and best practices proposed by standards such as ISA 99 and NIST SP-800 into practical benefits in terms of security implementation, even when it is done as a stage of a simple network project. Special recommendations for the establishment of Zones and Conduit, a recently proposed concept by ISA99, will be highlighted, allowing an implementation in which secure and insecure systems are allowed to live together in a controlled and rational way. The expected results point to a better strategic alignment of project stakeholders, with an overall improvement in the relationship between the Organization´s Security Representative, automation staff, and suppliers.

Key words: Cyber security; Zones and conduits, Network segmentation; Control systems network.

[1] *Contribuição técnica ao 13° Seminário de Automação de Processos, 7 a 9 de outubro de 2009, São Paulo, SP.*

[2] *Chemtech – A Siemens Company*

1 INTRODUÇÃO

Um Sistema de Gestão de Segurança da Informação, seja para o Ambiente Corporativo ou Industrial, tem por objetivo proteger os seus recursos mais importantes, o que inclui Hardware, Software, Equipamentos e, obviamente, Informação. Por meio da seleção e aplicação dos mecanismos de proteção adequados, a organização pode proteger os seus recursos tangíveis e intangíveis, seus empregados, sua reputação e demais recursos financeiros e físicos. A lógica da segurança da informação deve ser observada como uma relação de equilíbrio entre custo e risco. A segurança perfeita nunca poderia ser efetivamente alcançada, sendo os custos de implementação e manutenção, e as perdas de funcionalidade conseqüências diretas desta direção, tornando-a impraticável. O processo de desenvolvimento de um sistema seguro requer, portanto, uma revisão contínua de aspectos financeiros, para garantir que o custo dos controles não venha a exceder os benefícios resultantes. A segurança deve ser proporcional à severidade, probabilidade e extensão dos potenciais danos a serem evitados. Investir na Segurança de Informação é uma prática inteligente, pois conduz à identificação das medidas de segurança necessárias para evitar a concretização de ameaças no ambiente cibernético e permite uma melhoria no conhecimento sobre os sistemas existentes, o que resulta em outros benefícios para a sua operação.

Os requisitos de segurança para cada organização são particulares e dependem de diversos fatores, que incluem a arquitetura de sistemas, relacionamento com fornecedores e clientes e da própria cultura organizacional. Isto faz com que não exista uma única seqüência de procedimentos que possa se adaptar a todo tipo de empresa. Entretanto, existe uma série de boas práticas, já consagradas, que fornecem diversas diretivas que podem conduzir ao desenvolvimento de um ambiente efetivamente seguro. Transformar estas boas práticas, entretanto, em uma implementação de segurança eficaz, concisa e condizente com as necessidades reais de segurança de uma organização não é uma tarefa simples. Muito do que é feito em termos de segurança nos projetos reais envolvendo ambientes industriais é embutido em projetos de rede apenas como pequenas etapas e os stakeholders nem sempre são capazes de lidar com os aspectos de integração e comunicação para gerar resultados práticos positivos.

Este trabalho apresenta uma visão prática do uso do conceito de Zonas e Conduítes dentro de um projeto de redes orientado a premissas de segurança da informação. Será destacado, sob uma ótica de implementação, como este conceito pode ser utilizado para tratar a questão da segurança de maneira racional e alinhada com a ISA99, mesmo nos casos em que a segurança é tratada como uma etapa do projeto.

1.1 Os Projetos de Segurança na Automação

Mesmo na TI (TI – Tecnologia da Informação), por um bom tempo, a segurança foi tratada como um acessório em projetos de Rede. Após uma sucessão de incidentes pelo mundo envolvendo transações eletrônicas e uso indevido da informação, de fato, houve uma grande preocupação com a segurança da informação que trafegava pelas redes de computadores. A visão moderna de Gestão Riscos, porém, trouxe o benefício do reconhecimento de que a segurança vai muito além dos ativos de comunicação, envolvendo as pessoas e o ambiente interno e externo, por exemplo.

As normas e padrões evoluíram e a maturidade para a visão de riscos também já alcança os ambientes industriais, mas a visão de execução dos projetos permanece. É muito comum a segurança ser tratada como elemento opcional de projetos de rede, o que é compreensível, considerando este histórico e o pouco tempo de vida das normas de segurança específicas para a TA. Dentro da própria ISA 99 há, por vezes, contextualização e argumentação fortemente baseados em seqüências e elementos que lembram aspectos de um projeto de redes ethernet, levando a crer que este sentimento do profissional de TA está, de fato, enraizado.
A informação na TA é usada para garantir a disponibilidade dos processos e é este o foco que a segurança industrial deve assumir. Não importa como os projetos são estruturados, desde que o seu conteúdo seja coerente com os riscos que devem ser tratados para garantir esta disponibilidade. Há, contudo, uma necessidade de amadurecimento para que a segurança deixe de ser acessório e incorpore os elementos necessários a tratar em um sistema de gestão de segurança da informação bem estruturado, ainda que isto seja feito dentro de um projeto de rede.

1.2 O Fracasso dos Projetos

A implementação da segurança de um Sistema tendo como base o projeto da Rede não seria um problema, desde que houvesse um tratamento adequado da questão, respeitando todos os elementos essenciais a considerar no planejamento de controles. Há uma grande distância entre o modelo ideal de projeto, com todas as alternativas de controle possíveis, o modelo ofertado pelos fornecedores com suas soluções *turn-key*, e um modelo balanceado com os controles e restrições para minimizar riscos não aceitáveis ao negócio. Projetar esta solução de maneira ponderada, atendendo aos desejos de todos os *stakeholders* é um verdadeiro desafio, já que não há roteiro para um projeto que atinja este objetivo de maneira calculada e previsível. Cada participante atua fortemente na defesa de interesses muito particulares e coordenar os esforços torna-se fator chave para o sucesso do projeto.

Um dos elementos deste projeto é, certamente, o representante da Segurança da Informação da empresa, cargo normalmente desempenhado pelo CSO – *Chief Security Officer*. Na maior parte dos casos, este representante é um profissional vinculado e contratado pela TI, segmento que, indiscutivelmente, despertou mais cedo o interesse pela segurança da informação e possui maior maturidade, em relação à TA, no seu tratamento (razão pela qual dificilmente os projetos de segurança envolvem TI e TA simultaneamente). Se de um lado há, por parte da TA, falta de maturidade em relação à segurança cibernética, e uma visão de que a segurança é um elemento de restrição de funcionalidades, do outro há, por parte da TI e do CSO, falta de entendimento de características de processo e das necessidades dos sistemas de controle. Inevitavelmente, surgem dificuldades no diálogo Segurança de Informação (TI) x TA. Este *stakeholder* compreende os requisitos de segurança da organização e tende a conduzir corretamente o tratamento dos riscos inaceitáveis para o negócio, mas a sua visão muitas vezes restrita do processo industrial, enfraquece seus argumentos, impedindo-o de sustentar uma posição de rigidez no projeto. Um outro *stakeholder* que influencia nos resultados é o time de automação, com profissionais que compreendem bem o

processo industrial e sistemas de automação e controle, razoavelmente[1] bem as tecnologias de TI, mas que possuem um conhecimento insuficiente acerca da importância dos aspectos de gestão dos serviços de TI desempenhados pela TA, especialmente da gestão da segurança da informação. Quase sempre as suas decisões são guiadas pela filosofia de oposição a qualquer mudança em sistemas funcionais, restringindo a visão proativa de gestão de riscos necessária e impedindo-o de trabalhar com alguns riscos necessários do projeto para evitar catástrofes futuras.

O fornecedor ou provedor de soluções de automação também se enquadra neste contexto de projeto e constitui num papel altamente relevante. Apenas recentemente os grandes fabricantes decidiram incluir em seus times, profissionais de segurança da informação capazes de embutir aspectos de segurança essenciais em suas soluções. Como conseqüência, o que temos, na prática, instalados nos parques industriais, são soluções com pouco ou nenhum controle. Há falta de flexibilidade, especialmente nas soluções fechadas, soluções que não se integram às arquiteturas e boas práticas e, por fim, como estratégia de defesa, argumentos contrários ao investimento em segurança.

Muitos projetos fracassam em implementar controles de segurança efetivamente adequados pois o resultado da interação entre estes stakeholders não é bom. Quem entende de segurança não é capaz de convencer a quem tem autonomia e a conseqüência é o baixo retorno do investimento com controles fracos. Para resolver a questão, não basta, entretanto, a presença de um integrador ou mediador imparcial. Como não há um conjunto definido de boas práticas que sirva para todos os casos, é importante que o integrador tenha alternativas para os casos em que um controle não é aplicável, é importante que tenha conhecimento sobre os padrões, normas e regulatórios e, acima de tudo, é importante que saiba correlacionar estes conhecimentos com cada situação em particular para atribuir controles bem dimensionados.

2 PROJETO DE REDES BASEADO EM PREMISSAS DE SEGURANÇA DA INFORMAÇÃO

Uma solução de integração que endereça os problemas mencionados é a adoção de uma filosofia de projeto de rede que seja orientada por premissas de segurança da informação. Ao invés de conduzir uma etapa de segurança focada na escolha dos ativos para a segurança da rede, orienta-se o processo para o que realmente deve tratar: a Gestão de Riscos capaz de vincular as necessidades funcionais inerentes a todo processo industrial com o tratamento adequado das ameaças existentes.

Segundo a ISA,(1) um erro comum ao tratar a segurança industrial é tratar os sistemas individualmente, sem considerar o conjunto como um todo. Ao decidir pelo tratamento baseado em probabilidades e efeitos associados a todos os riscos, é possível identificar com mais clareza as concessões com baixo ou nenhum impacto no resultado final do projeto. Aplicar atualizações do sistema operacional pode ser uma prática desejável para todas as estações, mas uma concessão aceitável seria flexibilizar a necessidade de atualizações para um sistema em particular que pode

---

Este argumento se sustenta na afirmação de que as tecnologias de TI na TA são apenas um meio para a viabilização dos processos industriais e de que, na prática, há pouca preocupação em gestão proativa, orientação a serviços e ROI, por exemplo, aspectos tratados com severidade por gestores.

operar *off-line* e que ofereceria, portanto, menor probabilidade de incidentes. Este é um exemplo simples em que a insistência na adoção de um controle com baixo resultado prático custaria um esforço pouco vantajoso, negativo para o projeto. A flexibilização, no entanto, não precisa ser entendida apenas como relaxamentos na necessidade de controles. É aceitável que o processo de *login/logoff* ao sistema Scada seja tratado com relaxamento em uma sala de controle quando este processo oferece risco (por exemplo, o risco de esquecimento da senha em casos de urgência), mas considerando que o acesso ao sistema por qualquer pessoa (incluindo as não autorizadas) presente na sala seria facilitado, é necessário aumentar o rigor no controle e registro de entrada e saída ao ambiente, uma troca justa e com bom resultado.

Ao mesmo tempo em que conhecer e adotar alternativas pode criar soluções de sucesso, esta prática, quando mal interpretada, pode se transformar em uma justificativa para manter tudo como está. Existe uma linha de fronteira a partir da qual concessões tornam-se negligência ao tratamento de riscos pertinentes ao projeto que precisa ser conhecida, o que pode ser solucionado com um projeto baseado em Premissas de Segurança da Informação. A questão que persiste, entretanto, é, como transformar este conhecimento em resultados práticos em termos de implementação que permitam que segmentos inseguros convivam com segmentos com sistemas críticos de forma controlada e racional?

3 ZONAS E CONDUÍTES

O conceito de zonas e conduítes de segurança foi introduzido oficialmente no documento ANSI/ISA-99.01.01,[(2)] o trecho da norma que apresenta os conceitos principais, os modelos e a terminologia relacionada à segurança da informação em ambientes industriais. Após ser aplicado diretamente como solução para o problema da Segmentação de Rede, o conceito vem sendo expandido desde então como ferramenta para uma fase do processo de avaliação de segurança proposto para todo o sistema de gestão. A proposta é associar os sistemas de automação a zonas e qualificar os níveis de segurança (*SAL – Security Assurance Level*) dentro do processo de análise de conseqüências/riscos executando esta atividade com base nas zonas definidas. Ao agrupar sistemas com mesmos níveis de criticidade e outras características similares, estamos reconhecendo a heterogeneidade e permitindo tratamento diferenciado. Uma vez definidos os níveis de segurança aplicáveis para cada zona, este modelo se transforma em um framework que pode ser reutilizado à medida que os novos sistemas e requisitos se assemelham. Há também a possibilidade de relacionamento com métricas de segurança, já que diferentes setores ou segmentos poderiam se relacionar a diferentes metas em termos de segurança.

A definição de sistemas de automação através de Zonas e Conduítes podem ser feitas em projetos novos, nos quais a rede de TA está sendo definida desde o princípio, e também em projetos de adequação de ambientes existentes. Faz parte das atividades de implementação de um sistema de gestão de segurança industrial a execução de pequenos projetos de mitigação, onde o nível de segurança alvo determinado através da análise de risco e da política de segurança seria transformado em níveis qualificados e específicos para cada zona. No caso de um projeto desenvolvido como (ou dentro de) um projeto de Rede, a definição dos sistemas em termos de zonas pode ser embutida nas etapas de levantamento de

requisitos de segurança com abrangência e foco maiores, permitindo conclusões muito mais racionais sobre controles necessários à rede.

O esquema da Figura 1 destaca as etapas essenciais a executar dentro do projeto para definir os sistemas de automação em termos de Zonas e Conduítes. O foco desta sequência não é apresentar as etapas para o estabelecimento de um programa de gestão da segurança, mas sim, tratar de um ponto específico dentro deste processo que é a segregação dos sistemas (e não necessariamente da rede apenas) utilizando Zonas e Conduítes (razão pela qual nem todas as etapas de construção do programa são apresentadas[2]). Na norma, estas etapas se encaixariam dentro das fases de Avaliação e Desenvolvimento.

Figura 1. Etapas para definir os sistemas de automação em termos de zonas e conduítes.

Em um projeto de adequação ou de mitigação é possível que a Política de Segurança da Informação da empresa já esteja definida. Considerando que a política estabelece os princípios básicos que dão as direções para a organização em termos de segurança, é provável que seja necessária a criação de normas e procedimentos adicionais que tratem das particularidades da TA após a definição das Zonas e Conduítes, mas os elementos chave já estarão escritos. As premissas que serão utilizadas devem ser fortemente embasadas na política, já que as metas do projeto e da empresa devem estar alinhadas.

A determinação dos níveis de tolerância ao risco são altamente dependentes do que a organização é capaz de absorver em relação à concretização de ameaças. Estes valores estão intimamente ligados com impactos financeiros e aspectos

_____

De fato, a própria norma ANSI/ISA-99.02.01 afirma que a definição do framework é uma tarefa a ser cumprida por quem vai implementar, sem, no entanto, descrever sobre como isto deve ser feito.

intangíveis que podem ser de difícil acesso, o que pode exigir uma participação maior de contato com o nível estratégico. A tolerância será utilizada no momento da estipulação dos níveis de segurança alvos para cada zona, o que já faz parte de uma análise custo-benefício. Naturalmente, o esforço para mudar uma arquitetura de um fornecedor de uma solução fechada não faria parte desta análise de custo, mas, na prática, o que ocorre são conflitos que resultam em relaxamento excessivo da segurança, razão pela qual este aspecto deve ser considerado.

Determinar os sistemas de automação pode aparentar ser a etapa mais simples para sistemas já em funcionamento, mas a realidade é que nem sempre estes sistemas são documentados ou de fácil compreensão. Além disso, tecnologias legadas podem oferecer a maior restrição ao uso de controles de segurança, razão pela qual se transformarão no maior desafio para o projetista. É necessário um levantamento de possíveis controles homologados e restrições conhecidas ao uso de controles (exemplo: softwares Scada costumam não operar com quaisquer versões e configurações de ferramentas de proteção contra código malicioso).

Uma vez conhecidos os sistemas e as suas características, já é possível iniciar o ciclo de determinação das zonas que abrigarão cada grupo de sistemas. Este processo deve ser feito seguindo o fluxograma e requisitos definidos na ISA 99. Há requisitos que definem, por exemplo, que o nível de segurança atribuído à zona será sempre o nível correspondente ao menor nível do sistema que ele abriga. A avaliação de riscos pode entrar como insumo, caso este processo já tenha sido realizado e documentado, ou ser realizada durante o processo. Avaliar riscos utilizando uma abordagem orientada a ativos pode não ser muito simples em uma planta nova. Neste caso, uma alternativa pode ser utilizar a análise baseada em cenários, em que os riscos são estruturados com base em possíveis incidentes e não em ativos e suas vulnerabilidades. Ao final desta etapa, as bases para a segregação da rede estarão concluídas, embora as tecnologias que o farão ainda não.

Para que a escolha do nível de segurança alvo de cada zona possa ser iniciado, deve-se ter em mãos as contra-medidas possíveis, as práticas de base escolhidas e, principalmente, a lista de premissas elaborada. O esquema abaixo ilustra exemplos de cada um destes elementos:

Tabela 1. Grupos de contra-medidas, práticas de base e premissas

Grupos de Contra-Medidas	Práticas de Base Possíveis	Premissas
Segurança Física e do Ambiente	• Controle do ambiente com Alarme; • Controle do ambiente com CFTV; • Barreira eletrônica de entrada e saída com dispositivo de autenticação de dois fatores; • Instalação de fontes redundantes de energia para o ambiente; • Uso obrigatório de de paredes de alvenaria e portas reforçadas; • Adoção de Normas de Acesso físico complementares; • ...	• Todas as conexões em áreas internas e externas devem ser protegidas contra danos ambientais; • Ambientes contendo sistemas de supervisão e controle devem ter acesso restrito a funcionários com autorização de acesso ao sistema; • ...
Segmentação da Rede	• Segregação física (ativos e passivos) e lógica; • Segregação apenas lógica com VLANs e ACLs; • Posicionamento na DMZ; • Segregação lógica com firewall e monitoramento de tráfego anômalo; • ...	• Sistemas instrumentados de segurança devem ser isolados; • Toda comunicação não essencial deve ser proibida; • Sistemas críticos de controle devem ser segregados fisicamente e logicamente; • ...
Controle de Acesso: autenticação	• Autenticação de um fator: Usuário/Senha; • Autentitação de dois fatores: Usuário/senha/Token; • Requisitos mínimos de complexidade de senhas; • Controle de MAC Address para conexão do dispositivo; • Adoção de normas de controle de acesso lógico complementares • ...	• Usuários remotos devem utilizar autenticação “forte”; • Todos os sistemas devem possuir mecanismos de autenticação; • Sistemas não críticos devem adotar requisitos de complexidade de senha; • Todo o acesso deve ser registrado em log;
Outros Grupos...	Outras Práticas ...	Outras Premissas ...

Com o conhecimento das características dos sistemas, criticidade e restrição ao uso de controles é possível iniciar a atribuição dos níveis de segurança para cada zona, o que servirá de entrada para o passo final, a escolha dos controles apropriados. A ISA 99 recomenda que esta atribuição seja feita em um primeiro momento de maneira qualitativa e depois, com a inclusão de métricas, de maneira quantitativa[3] a partir da qualificação inicial.

Ao cumprir com todas estas etapas, a equipe do projeto terá à disposição insumos precisos para que os ativos e passivos de rede sejam projetados com perfeita adequação às necessidades de segurança. A seqüência de execução ou ordem de precedência não são necessariamente relevantes já que todo o processo deve ocorrer de forma iterativa (há pontos de decisão e controle que podem se aplicar[4]).

---

[3] *A descrição detalhada deste processo de conversão será apresentada na norma ISA-99.03.02.*

[4] *Na página 122 da norma ANSI/ISA-99.02.01–2009 há um fluxograma que apresenta o processo de atribuição do nível de segurança na fase de avaliação dentro do ciclo de vida do modelo de nível de segurança.*

4 ADEQUANDO O PROJETO DA REDE

Nos itens anteriores pôde-se observar os aspectos e questões mais relevantes para implementação da segurança cibernética no ambiente de TA, e verificar que é possível tratar a questão da segurança, mesmo dentro de um projeto de Rede. Contudo, é necessário tratar ainda sobre como encaixar este método dentro do que já é praticado por quem está conduzindo um projeto. A fim de exemplificar como o conceito Zonas e Conduítes pode ser utilizado como ferramenta no projeto de sistemas de segurança, destacamos nesta seção o seu uso inserido dentro de uma metodologia de projeto para redes de automação convencional.

O processo usual de projeto de Redes TA inicia-se, normalmente, com um levantamento de necessidades e objetivos da Rede e uma verificação da situação da atual do ambiente. Dentre as premissas que conduzem este projeto (Figura 2) em todas as suas ações, dos levantamentos à especificação propriamente dita, a segurança figura dentre requisitos como escalabilidade, disponiblidade, performance, gerenciabilidade e preço, assumindo um papel secundário. Em geral, quando esta etapa de levantamento é executada, faltam procedimentos estruturados que auxiliem os projetistas a levantar corretamente os requisitos de segurança, já que muitos dos aspectos mencionados na Figura 1 não são considerados. Quando chega-se à fase de projeto, nas etapas seguintes, a visão de requisitos de segurança é apenas suficiente para enxergar funcionalidades muito particulares nos ativos de rede, restringindo-se a recomendações sem relação com níveis de risco.

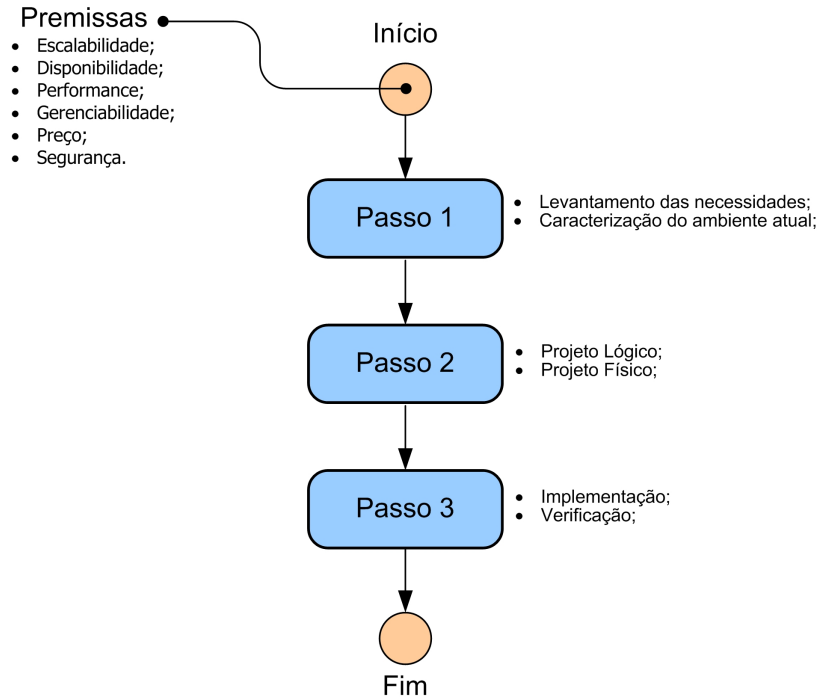

Figura 2. Processo usual de desenvolvimento de redes de automação.

Este fluxo de trabalho, estruturado em Início, Meio e Fim, constitui, aparentemente, uma metodologia de projeto bem estruturada. Entretanto, observando em detalhes, é possível identificar os *gaps* de desenvolvimento que o tornam sujeito a falhas no tratamento da segurança.

Para solucionar os problemas associados a este tipo de estratégia, um esquema de um projeto baseado em premissas de segurança da informação pode

ser observado na Figura 3Erro! Fonte de referência não encontrada.. Este fluxo consiste, basicamente, naquele apresentado na Erro! Fonte de referência não encontrada. com a inclusão, dentro do seu fluxo básico, dos aspectos relativos ao processo de definição das zonas e conduítes. A primeira modificação consiste na introdução de iteratividade ao processo. Além do fluxo básico Começo, Meio e Fim, temos agora um fluxo contínuo de desenvolvimento que pode, ao contrário da metodologia usual, se adaptar à detecção tardia de requisitos. Observa-se também que, as etapas de Levantamento e Projeto encontram-se associadas ao projeto das Zonas e Conduítes (é sugerida, inclusive uma alocação das tarefas), assegurando que o conhecimento obtido com a execução destas etapas será utilizado nas decisões de projeto da rede, sejam elas decisões relacionadas aos aspectos físicos ou lógicos da rede em si, ou dos sistemas que nela serão executados. Como conclusão, o projeto baseado em premissas de segurança da informação passa a ter a segurança com um foco muito mais centrado em objetivos que serão compatíveis com as metas da organização, e não mais apenas com metas de um projeto de redes.

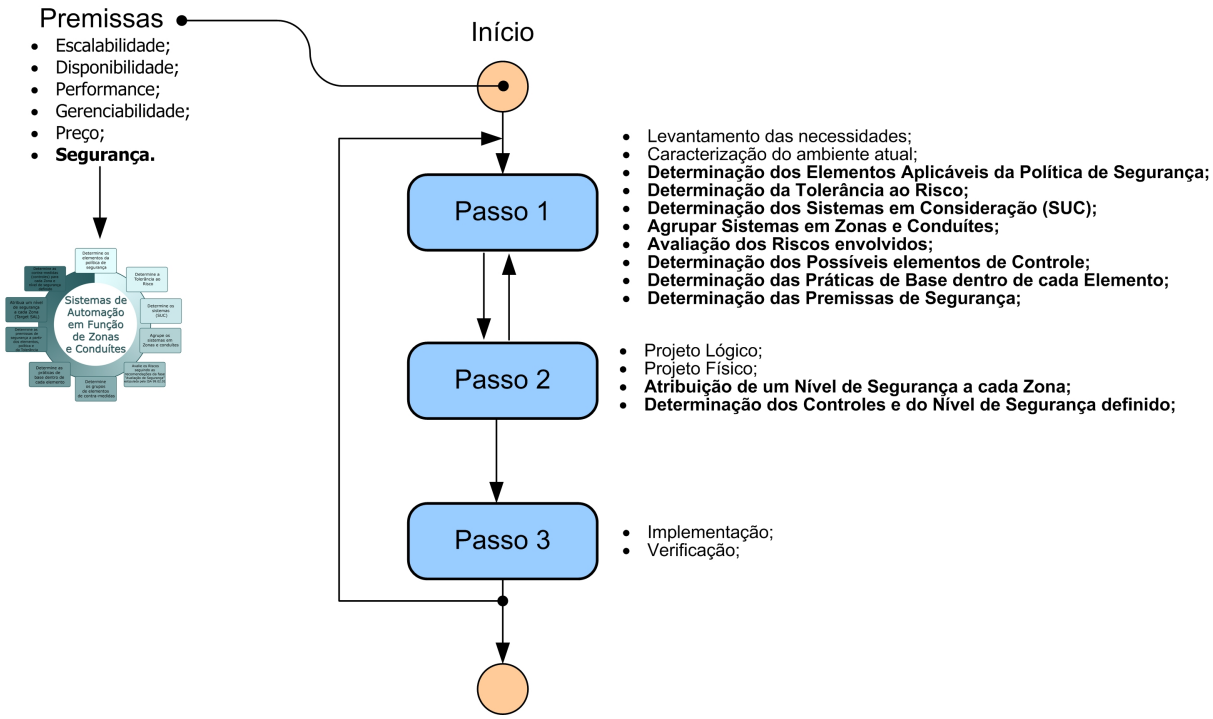

Figura 3. Projeto baseado em premissas de segurança da informação.

5 PROJETANDO COM ZONAS E CONDUÍTES DE SEGURANÇA

No item anterior foi possível entender sobre como embutir as recomendações da ISA 99 para a definição dos sistemas de automação em termos de Zonas e Conduítes dentro de um projeto de rede usual. É importante entender também, em detalhes, dentro do processo de segmentação, como que tecnicamente isto ocorre.

A definição de Zonas, como já mencionado, procura propor que, para sistemas industriais, torna-se inviável ou mesmo impraticável, aplicar o mesmo nível de segurança a todos os componentes. A solução seria, portanto, agrupar ativos, informações, ou aplicações que possuem requisitos de segurança semelhantes em uma mesma área, ou zona. Uma zona pode ser definida em um sentido físico, agrupando ativos em uma mesma localização física, ou lógica, com a criação de

segmentos virtuais confiáveis ou não. É possível ainda que existam subzonas, o que possibilitaria uma segurança em multicamadas com requisitos de segurança crescentes, a chamada defesa em profundidade (*Defense in Depth*).

Um dos aspectos mais importantes relacionados ao conceito de Zonas está ligado à forma como deve ser realizada a comunicação com outras zonas, já que elas possuem fronteiras e seus elementos devem deixar entrar e sair dados em seu perímetro. Esta comunicação pode se dar das mais diferentes formas, incluindo a comunicação virtual com a troca de mensagens entre diferentes sistemas, movimentos de pessoas, como funcionários, fornecedores e visitantes, movimento de produtos e insumos e tantos outros, mas a idéia é que haja mecanismos de controle capazes de assegurar a proteção de cada zona. Para lidar com esta necessidade é que foi estabelecido um conceito complementar, definido como conduítes de Segurança.

Assim como ocorre para as zonas, os conduítes podem assumir um aspecto lógico, com a definição de rotas de pacotes, ou mesmo físico, como um corredor, capaz de possibilitar a comunicação entre diversas salas. Oficialmente, a ISA define um conduíte como sendo um grupo de elementos de comunicação que protegem a segurança do canal que este contém.(3) Percebe-se então que um conduíte pode ser pensado como uma zona com características particulares, cuja sua função é agrupar, não ativos, mas a comunicação entre zonas. Da mesma forma, como ocorre nas zonas, os conduítes também podem ser considerados confiáveis ou não. Conduítes responsáveis pela comunicação intrazona normalmente são considerados confiáveis, como, por exemplo, a comunicação entre um servidor Scada e um PLC em uma zona denominada Zona de Controle. Conduítes responsáveis pela comunicação interzonas através de perímetros que não possuam os requisitos mínimos de segurança, devem garantir a comunicação segura fim a fim, como, por exemplo, um protocolo de criptografia que permita a comunicação segura em uma rede não confiável.

Estes conceitos podem ser compreendidos mais facilmente através da Figura 4. Neste exemplo estamos tratando de zonas e conduítes de comunicação lógica da rede, mas o conceito é válido também para a segurança física, onde poderíamos tratar os aspectos de acesso às salas de controle/operação, por exemplo, diferenciando-as dos demais ambientes e tratando do controle sobre quais pessoas são autorizadas a acessar tais ambientes. Pode-se observar que áreas diferentes do processo produtivo foram definidas como subzonas da Zona Rede TA, com uma subzona destinada a cada área de produção (A, B e C). Os conduítes possibilitam a comunicação dentro de cada zona e entre as diferentes zonas. Equipamentos ou sistemas com características e, principalmente (na TA), restrições semelhantes, são agrupados em zonas independentes. Há, por exemplo, uma zona separada para os equipamentos de controle, como os PLCs. Problemas como pacotes mal formados ou tempestades de pacotes – *packet storms* (problemas muito comuns que advém, normalmente de mal funcionamento de equipamentos) que ocorram num segmento seriam confinados a este segmento, garantindo a operação dos demais setores da rede.

Em termos de segmentação de rede, as zonas podem ser implementadas através de segmentação física (com switches, roteadores etc.) independentes para cada segmento, ou lógica, através de tecnologias como as VLANs (redes virtuais). Cada zona pode recomendar ou exigir determinada técnica, dependendo da criticidade e do impacto em caso da concretização de uma ameaça. Os conduítes de comunicação ativa entre zonas diferentes podem ser implementados através de

dispositivos de Firewal ou de listas de controle de acesso (ACLs), suportadas pela maior parte dos switches ethernet no caso em que o roteamento é possível.
O uso de Zonas e Conduítes de segurança resulta em uma implementação natural do conceito de Defesa em Profundidade, citado anteriormente. Um ataque originado através da Internet, por exemplo, teria que passar por diversas barreiras de segurança antes de chegar aos sistemas de controle, resultando na segurança multicamadas defendida pela ISA.[5]

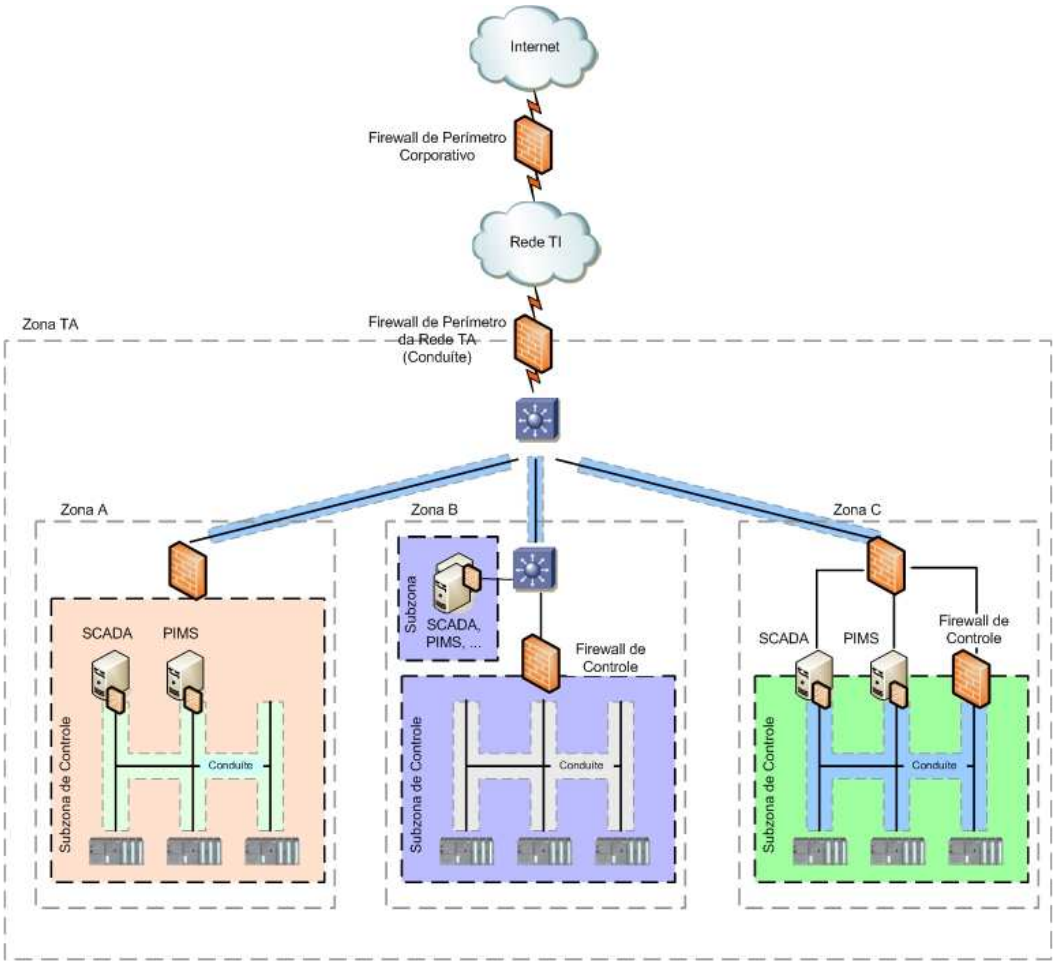

Figura 4. Exemplo de zonas e conduítes.

FIREWALL DE CONTROLE

Alguns fabricantes têm defendido o uso de um firewall exclusivo para a proteção das redes de controle: o firewall de controle. Trata-se da implementação do conceito de conduítes de comunicação ativa, ainda que os fabricantes não declarem este conceito explicitamente.

O Firewall de controle é responsável pela segregação da Rede de Controle das demais redes da unidade, sendo capaz de regular o tráfego entre esta rede, que possui características substancialmente diferentes do restante da Rede, dos demais segmentos menos ou igualmente críticos. Através da implementação de um equipamento exclusivo é possível aumentar os níveis de controle acerca do que

---

Este conceito também já foi introduzido (a partir de discussões oriundas da TI) em outras normas destinadas a segurança de sistemas de automação como o Guia [(4)] do NIST para Sistemas Industriais (Guide to Industrial Systems Security - NIST), e consiste em garantir uma maior segurança para o sistema através da definição de mecanismos de segurança sobrepostos, de tal forma reduzir os efeitos de uma fraqueza em um dos controles de segurança.

ocorre nestas redes, já que, tipicamente, firewalls possuem funcionalidades avançadas como a detecção e bloqueio de alguns tipos de ataques. Com o firewall de controle cria-se também uma alternativa para a realização do acesso remoto de forma mais segura, um problema recorrente em projetos de redes industriais.

6 CONCLUSÃO

Zonas e Conduítes são mecanismos interessantes para promover a segurança em redes de automação. Este é um tema que está sendo discutido intensamente dentro dos grupos de trabalho da ISA 99 e evoluiu de uma técnica de segregação de redes para uma excelente alternativa para avaliar as necessidades e propor controles adequados ao nível efetivo de exposição aos riscos. Por se tratar de uma solução altamente focada nos casos práticos de sistemas de TA, é possível tratar com precisão as recomendações da ISA 99, mesmo nos casos em que a segurança é tratada como um elemento de um projeto de rede.

Por oferecer soluções para que segmentos inseguros convivam com segmentos seguros de maneira controlada, a orientação dos projetos à premissas de segurança e Zonas e Conduítes oferece uma solução para a questão recorrente da falta de entendimento entre equipes de automação, fornecedores e o representante da área de segurança da informação corporativa.

Tecnicamente, além dos benefícios já expostos, Zonas e Conduítes continuam a solucionar a questão da segregação das redes. O seu uso fornece uma alternativa viável e robusta para promover a segurança da automação, não apenas em relação às ameaças que podem vir do mundo externo como a internet, mas de ameaças que podem surgir dentro da própria TA. Além de evitar problemas resultantes da concretização de ameaças identificadas, a correta segregação melhora a organização geral do projeto, facilita a manutenção e a resolução de problemas, reduzindo futuros custos com paradas.

Vale ressaltar que, mesmo a execução de um projeto bem sucedido não dispensa a necessidade do estabelecimento de um sistema de gestão da segurança da informação, integrado com a visão estratégica da empresa de gestão de riscos e melhorado continuamente. Assim como os sistemas de TA, é esperado que a segurança evolua, acompanhando a tecnologia e a evolução e surgimento de novas ameaças, incutindo no dia-a-dia da gestão de TA, a gestão dos riscos que são inaceitáveis para o negócio.

REFERÊNCIAS

1 ANSI/ISA-99.02.01-2009 – Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

2 ANSI/ISA-99.00.01-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models

3 dISA-99.03.02 – Security for Industrial Automation and Control Systems: Target Security Assurance Levels for Zones and Conduits

4 NIST – National Institute of Standards and Technology. *Special Publication 800-82 – Guide to Industrial (ICS) Control Systems Security*.