ESTUDO DE CASO DA IMPLANTAÇÃO DA NORMA ANSI/ISA99 NA UTE DO ATLANTICO – THYSSENKUPP CSA SIDERÚRGICA DO ATLANTICO – TKCSA[1]

Flavio José da Silva[2]
Valeria Farias Alves[3]

Resumo
Diante da evolução tecnológica e da necessidade de troca de informações entre os diversos departamentos, a integração entre as redes de automação industriais e corporativas são vitais. Para que esta troca de informação aconteça de forma segura, se faz necessária a implantação de medidas de segurança para garantir integridade, confidencialidade e disponibilidade dos sistemas. As redes de automação industriais contemplam todos os sistemas de controle e supervisão utilizados em processos como energia, petróleo e gás e contemplam todos os itens utilizados para automatizar, monitorar e controlar. De forma a apoiar os processos relacionados à segurança da informação em redes industriais, foi desenvolvida a norma ANSI/ISA99 (*Security for Industrial Automation and Control Systems*) direcionando quanto às melhores práticas, de forma a tornar o acesso e controle das informações mais seguro e confiável. Este trabalho visa apresentar o estudo de caso da Thyssenkrupp CSA quanto a implantação da norma ANSI/ISA99 na rede de automação da UTE do Atlântico. A termoelétrica foi comissionada em dezembro de 2010 e em janeiro de 2011 teve sua operação comercial oficializada. O ambiente de automoção foi recebido com seis redes que operavam de forma isolada, o que impedia a gestão, controle e troca de informações de forma centralizada. Para realizar o processo de Gestão da Segurança foi adotada a norma ANSI/ISA99.
Palavras-chave: Segurança; Integração; Controle.

CASE STUDY OF THE IMPLEMENTATION OF THE STANDARD ANSI/ISA99 IN THE UTE ATLANTICO - THYSSENKUPP CSA SIDERURGICA DO ATLANTICO - CSA

Abstract
Front of the e technological changes and the need for exchange information between the various departments, the integration between automation networks, industrial and corporate networks are vital. For this exchange of information happen safety, it is necessary to implement safety measures to ensure integrity, confidentiality and availability of the systems. The networks include all industrial automation control systems and supervision used for process, such as energy, oil and gas, and include all items used to automate, monitor and control. In order to support the process related to information security in industrial networks, the standard ANSI/ISA99 (Security for Industrial Automation and Control Systems), was developed to directing on the best practices, to make access and control of information security and reliable. This paper explain about the study case of Thyssenkrupp CSA as the deployment of standard ANSI/ISA99 in network automation on UTE do Atlântico. The Power Plant was commissioned in December 2010 and started the commercial operation in January 2011. The automation environment was received with six networks that operated in isolation way, difficult the management, control and exchange information. To carry out the management process safety the standard ANSI/ISA99 was adopted.
Key words: Security; Integration; Control.

[1] *Contribuição técnica ao 17° Seminário de Automação e TI Industrial, 24 a 27 de setembro de 2013, Vitória, ES, Brasil.*
[2] *Tecnólogo em Mecatrônica, Coordenador de Automação da Termoelétrica da Thyssenkrupp CSA, Rio de Janeiro – RJ, Brasil.*
[3] *Mestranda em Tecnologia, Especialista em TI da Termoelétrica da Thyssenkrupp CSA, Rio de Janeiro – RJ, Brasil.*

1 INTRODUÇÃO

A Segurança da informação se refere à proteção de informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto para informações corporativas quanto pessoais. Tal segurança não está relacionada a apenas sistemas computacionais, mas também ao aspecto físico do ambiente, onde devemos controlar também os acessos de pessoas a salas e departamentos específicos.
Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição, desde que devidamente autorizado.
O ativo mais valioso para uma organização ou pessoa é a informação. Este grande diferencial competitivo então deve estar disponível apenas para as pessoas de direito. Elaborar e garantir critérios que protejam estas informações contra fraudes, roubos ou vazamentos é o grande desafio da Gestão de Segurança da Informação.
O complexo ecossistema formado por processos de negócio, pessoas e tecnologia devem ser geridos de forma a garantir os atributos da segurança da informação, que são confidencialidade, integridade, disponibilidade e autenticidade.
Muito se tem falado em segurança da informação para a área de tecnologia da informação, porém com o avanço tecnológico, a preocupação com segurança, não se limita apenas as redes de TI, mas também as redes industriais, pois estas redes passaram a operar com protocolos ethernets, softwares com aplicações web e banco de dados de uso comum.
Para os itens relacionados a tecnologia da informação, a tríade da segurança, obedece a seguinte ordem: confidencialidade, integridade e disponibilidade. Já para os sistemas de automação e controle, o item prioritário é a disponibilidade, seguida da integridade e confidencialidade, pois em um caso de falha, vidas estarão em risco e não somente informações:

Figura 1. Prioridade TI e TA.

Considerando a indisponibilidade de alguns sistemas de automação e controle, catástrofes de valores monetários imensuráveis podem ocorrer, levando a perdas de vidas, equipamentos entre outros.
Para garantir a continuidade do negócio de uma organização é preciso assegurar que cada membro deste ecossistema esteja em conformidade com normas internas criadas pela própria organização e normatizações externas, nacionais e

internacionais. Por este motivo a termoelétrica da TKCSA adotou o uso da norma ANSI/ISA99 como balizador para aos assuntos relacionados a Segurança.
Através desta norma, controles e segmentações especificas para rede de automação e controle são sugeridos, segmentando em níveis diferenciados, de acordo com a função de cada equipamento, definido para cada nível o controle mais apropriado, conforme sua criticidade e impacto.
A norma ANSI/ISA99 busca direcionar quanto à prevenção de acessos ilegais ou não autorizada de agentes externos as informações contidas nas redes de automação e sistemas de controle, que contemplam computadores, ativos de redes, sistemas operacionais, aplicações e outros equipamentos programáveis.

2 VISÃO GERAL DA TERMOELÉTRICA

A UTE do Atlântico está fisicamente instalada dentro com complexo siderúrgico da Thyssenkrupp CSA (TKCSA) e utiliza gás de processo gerado pelo alto forno e vapor proveniente da Coqueria.
A Termoelétrica é composta por três unidades geradoras de energia, GT11, GT12 e ST18. As duas primeiras, operando com gás do Alto Forno (BFG) e a ST18, operando com vapor oriundo da Coqueria e dos gases quentes recuperado na caldeira de recuperação acoplado as turbinas a gás.
A termoelétrica foi gerenciada e projetada pelos engenheiros internos e construída através de um contrato do tipo *Turn Key*, onde um fornecedor Europeu foi o responsável pela construção, montagem e comissionamento. Todo o processo de construção civil, projetos de fabricação das turbinas foi realizado pela empresa contratada, sob a supervisão da equipe interna da TKCSA.

2.1 Redes Industriais da Termoelétrica

A termoelétrica é composta por seis redes de controle, onde temos equipamento de nível 1, 2 e 3, contemplando computadores, switches, impressoras e PLCs.
Tais redes foram entregues após o comissionamento, operando de forma isolada e sem gestão. São compostas por softwares e equipamentos de fabricantes distintos, cada uma com uma função específica. São elas:

Quadro 1. Redes da Termoelétrica

Rede	Descrição
WTP – Water Treatment Plant	Tratamento da Água
Egatrol	Controle das turbinas a gás
Disturbance Record	Analise de distúrbios elétricos
Depp/Amodis	Historiador (Turbinas)
Alspa	Controle da turbina a vapor e auxiliares
Controladores	Rede de controladores (PLC)

Além das redes acima mencionadas, existem as comunicações com o mundo externo, que contempla a conexão com os órgãos de controle, como a ONS [Operador Nacional do Sistema e CCEE (Câmera de Comercialização de Energia Elétrica)].
As redes operavam de forma isolada e sem nenhum tipo de gestão sob os equipamentos. Diante deste cenário, se fez necessário um estudo da melhor forma de integração e controle do ambiente de automação, considerando as melhores práticas utilizadas pelo mercado, onde foi identificada como melhor solução a

adoção da norma ANSI/ISA99 como direcionadora para todos os processos de controle relacionados à Segurança.

3 ETAPAS DO PROCESSO DE IMPLANTAÇÃO DA ANSI/ISA99

O passo inicial para a implantação da norma foi realizar o treinamento de alguns membros da equipe responsável pela estruturação. Após o treinamento, foi iniciado o levantamento do “cenário atual”, onde foram identificados os pontos de melhoria e as primeiras etapas do processo de controle e gestão do ambiente. Foram respondidas questões do tipo:

- Qual será o escopo do projeto de segurança?
- Quais interfaces deverão ser protegidas?
- Que tipos de controles deverão ser implementados?
- Quais são os maiores pontos vulneráveis?
- Quais itens da norma poderão ser aplicados em nosso ambiente?

A partir desta análise foram iniciados os processos de ajuste no ambiente.

3.1 Protegendo as Interfaces

Após o levantamento detalhado das interfaces das redes de automação, sejam entre elas, entre a rede corporativa e redes externas, foram definidas as segmentações e proteções através de firewall, seguido o conceito de “Conduítes”, conforme descrito na norma.

Através da segmentação, podemos obter o controle e liberação do acesso entre as redes, onde é possível observar o comportamento de cada segmento e prevenir que anomalias em determinado segmento seja propagado para todas as redes.

Controles relacionados à detecção de intrusos são utilizados para a detecção dos acessos.

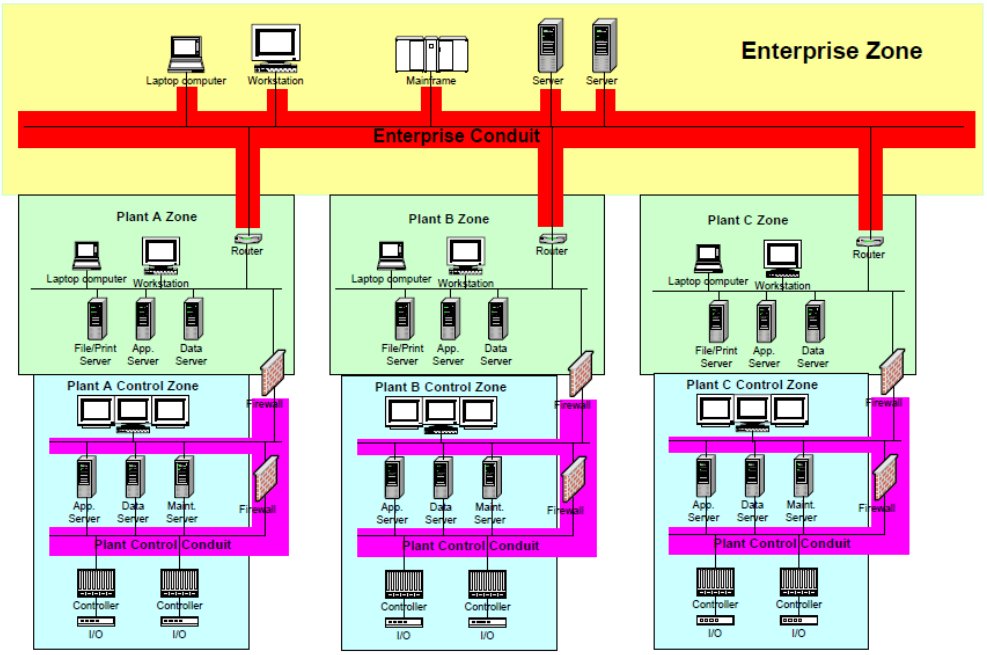

Figura 2. Interfaces de rede.

3.2 Controlando Usuários e Acessos

Após a segmentação, a segunda etapa foi tratar o controle de acesso local aos equipamentos, de forma a garantir controle centralizado e histórico das ações.
Através da instalação do Active Directory, foi possível realizar o controle de acesso de todos os usuários, criando logins de acesso com permissões específicas, de acordo com a função de cada usuário.
Através desta ferramenta foi possível a implementação nas estações SCADA, de políticas de controle, como bloqueio de portas USB, evitando assim o uso de pen drives e disco externos nas máquinas de automação. Assim como, a implementação de um console de gerenciamento de antivírus, onde podemos ter em tempo real a situação da estação, tais como informação a versão do antivírus que está sendo utilizada, versão da vacina e histórico das infecções.
Destacando que grande parte dos ataques sofridos pelas organizações são internos, é de extrema importância o controle de acesso tanto físico quanto lógicos aos sistema SCADA.

3.2.1 Criação de DMZ

Para um melhor controle, uma DMZ (Zona Desmilitarizada) foi criada. Nesta DMZ estão instalados os servidores responsáveis pela realização do backup de dados dos sistemas. Dois servidores, instalados fisicamente em locais distintos, são responsáveis por esta tarefa. Na mesma DMZ encontra-se também o servidor responsável pela gerencia da rede e monitoramento de tráfego.

3.2.2 Analisando logs de equipamentos

Foi implementado software para o monitoramento e gestão dos ativos de redes, entre eles, switches industriais, roteadores e servidores. Com este software é possível ter um base line da rede e em caso de anomalias dos sistemas, alertas são disparados, para que ações sejam imediatamente iniciadas.
Auditorias constantes são realizadas nos logs dos equipamentos, com o objetivo de identificar tentativas de ataques ou tentativas de acessos não autorizados.

3.2.3Controle de Acesso físico

Como os sistemas de automação e controle estão diretamente ligados ao processo, a perda de informações ou a invasão de sistemas, podem causar além de perda de dados, perda de vidas, perda de produção, danos ambientais dentre outras.
Medidas de controle físico foram adotadas de forma a prevenir e controlar os acessos as áreas criticas e que possuem informações e sistemas que requerem confidencialidade. Em algumas áreas a integridade física das pessoas, foi um dos principais itens motivadores para o controle de acesso.

3.3 Melhoria Continua

O processo relacionado à gestão da segurança da informação é contínuo, por este motivo temos em nosso planejamento ações direcionadas a atualizações tecnológicas e busca de ferramentas mais eficientes que estejam alinhadas com as melhores práticas do mercado.
Dentre as melhorias a serem implementadas esta o uso de White list nas estações SCADA e a instalação de equipamentos, baseando-se na “proteção em

profundidade" (*defense in delph*) em pontos estratégicos dentro das redes de automação.
Com a implementação e atualização constante dos recursos, podemos minimizar os impactos e tornar o ambiente mais seguro e protegido.
A busca de consultorias externas, com foco exclusivo no tema, agregam grande conhecimento e visão para a equipe interna, proporcionando assim atualização constante do conhecimento e atualização quanto as práticas adotadas por empresas de mesmo seguimento (*benchmarking*).
Treinamentos internos são realizados de forma a introduzir internamente entre os colaboradores da termoelétrica, assuntos relacionados a segurança da informação, mencionando os passos seguros para atuação e divulgando forma de proteção do ambiente.

4 RESULTADOS

A integração entre os diversos níveis de rede relacionadas a automação e controle industrial, proporciona inúmeros benefícios, entre eles, uma grande visibilidade da cadeia produtiva em tempo real, onde podemos ter a visão dos processos, status dos equipamentos e atividades em execução.
Através dos controles seguros na norma ANSI/ISA99, pode-se observar a maturidade do processo de gerenciamento de risco (*Risk Management*). Através da gestão implementada, alguns incidentes são identificados antes mesmo que o usuário perceba. Como exemplo, a identificação de máquinas com comportamentos suspeitos onde ações corretivas podem ser implementadas antes mesmo de haver a queda total dos serviços, pois apesar da redundância, se não houver um monitoramento, podemos ficar sem as duas estações (*hot stand by*) inesperadamente.
Diante de uma infecção ocorrida, através das ferramentas de gestão foi possível rastrear e identificar qual o usuário foi responsável pela contaminação, o tipo de vírus que infectou o sistema e a sua origem. A atuação foi realizada antes que qualquer problema maior fosse manifestado.

5 CONCLUSÃO

As normas técnicas são ferramentas poderosas para organizações de todos os tamanhos, apoiando a inovação, controle e o aumento de produtividade. Os custos e riscos do negócio podem ser minimizados, os processos internos racionalizados e a comunicação melhorada. A normatização promove a interoperabilidade de forma segura e eficaz. Através da utilização de normas as empresas buscam a sua liderança no mercado, criam vantagens competitivas e desenvolvem as melhores práticas do mercado.
Com a adoção da norma ANSI/ISA99 vários benefícios podem ser adquiridos, entre eles:

- manter a disponibilidade, integridade e confidencialidade dos sistemas de controle e automação e seus componentes;
- redução de impactos operacionais através de controles de acessos das pessoas aos ambientes, sistemas e equipamentos diversos que compõem o processo;
- a redução dos riscos relacionados a incidentes de segurança;

- facilidade na rastreabilidade de incidentes, de forma a atuar de forma mais rápida e efetiva;
- proporciona um monitoramento em tempo real do ambiente;
- reduzir riscos relacionados à integridade física, tanto das máquinas e informações quanto das pessoas.

Os itens listados acima constituem um ganho que não pode ser mensurado, pois as perdas diretas, como perda de ativos, reposição de equipamentos e as perdas indiretas, como o tempo de parada do processo produtivo, retrabalho, danos a imagem e perda de vidas, que podem ocorrer como resultados de falhas relacionadas a segurança da informação são imensuráveis. Face a este cenário, a análise e controle de todas as vulnerabilidades deve ser mitigada, de forma a tornar os sistemas cada vez mais seguros e confiáveis.

A análise dos riscos, considerando a probabilidade do acontecimento versus as perdas provenientes, deve ser detalhadamente avaliada, de forma a serem definidas as formas de controle e proteção. Em alguns casos, a tolerância ao risco é considerada, pois formas de controle não podem, por algum motivo, serem implementadas, porém deve ser algo declarado e de conhecimento da direção.

O processo de avaliação da maturidade dos riscos de segurança é normalmente acompanhado e medido pelas organizações, fornecendo direcionamento e estratégicas de atuação para a corporação como um todo e não apenas para departamentos específicos e tende a oferecer uma visão real do status da empresa, quanto aos seus riscos, controle, ações planejadas.

É de grande importância a criação de políticas internas que esclareçam e difundam o tratamento da segurança da informação, pois este processo depende principalmente das pessoas, de suas ações seguras e conscientes.

Agradecimentos

A todos os colaboradores Thyssenkrupp CSA que contribuíram diretamente ou indiretamente na implementação da norma ANSI/ISA99 no departamento da termoelétrica da Thyssnekrupp CSA e ao consultor Marcelo Branquinho que muitos nos auxiliou e continua nos auxiliando em nossa caminhada rumo à segurança de nosso ambiente.

BIBLIOGRAFIA

1 Código de Prática para Gestão de Segurança da Informação - NBR ISO/IEC 27002; 2005
2 Security for Industrial Automation and Control System ANSI/ISA99, Part 1: Terminology, Concepts and Models; 2007
3 BAYRES, ERIC. Understanding Depp Packet Inspection for SCADA Security – White Paper, Dezembro 2012
4 CLARKE, RICHARD A.; KNAKE, ROBERT. Cyber War: The next threat to National Security and what to do about. Editora Ecco – 2010
5 KRUTZ, RONALD L. Securing SCADA Systems. Editora Wiley. Novembro 2005.
6 MITNICK, KEVIN; SIMON, L. A arte de Enganar. Editora Makron Books – 2003.
7 WEISS, JOSEPH. Protecting Industrial Control Systems from Electronic Threats. Editora Momentum Press. 2010