



**XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E
TRANSMISSÃO DE ENERGIA ELÉTRICA**

CB/GTL/24

22 a 25 de outubro de 2017
Curitiba - PR

GRUPO - XV

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS- GTL

ANÁLISE DE RISCO E INTERPRETAÇÃO DA NORMA IEC 62443 PARA SISTEMAS DE USINAS HIDRELÉTRICAS

Jéssica Heluany(*)
VOITH DS

Fabio Oliveira
VOITH DS

Leandro Oliveira
VOITH DS

Marcus Hofmann
VOITH DS

Rinaldo Machado
VOITH DS

RESUMO

O objetivo deste informe técnico é contextualizar a importância da implementação de estratégias de segurança cibernética em ambientes de automação industrial, e apresentar resumidamente os aspectos tratados pela norma IEC 62443. Posteriormente será feito um estudo de caso com análise de riscos para alguns sistemas típicos de usinas hidrelétricas evidenciando nas recomendações de solução algumas práticas decorrentes da norma.

PALAVRAS-CHAVE

Segurança Cibernética, IEC 62443, Análise de risco, Infraestrutura crítica, Defesa em Camadas

1.0 - INTRODUÇÃO

A tecnologia mundial está migrando para a 4ª revolução industrial (indústria 4.0), na qual se torna cada vez mais comum o termo *cyber-physical system (CPS)*. *Cyber-physical systems* representam mecanismos controlados por algoritmos, integrados com a internet, e tendo componentes de hardware e de software fortemente interligados. Nesse contexto, os sistemas digitais passam a representar alto risco, visto que a aplicação mais ampla de redes de comunicação Ethernet, wireless, e soluções em nuvem inevitavelmente aumentam a superfície de ataques cibernéticos e, consequentemente, aumentam a probabilidade de ataques bem sucedidos.

Apesar dos mercados apresentarem diferentes características dependentes tanto do ramo de atuação quanto da localização geográfica, tem-se notado uma quantidade crescente de ataques cibernéticos nos últimos anos. Países nos quais a preocupação com a defesa nacional é mais intensa, como os Estados Unidos, possuem diversos órgãos monitorando os incidentes e atuando no sentido de ajudar as organizações a se protegerem. De acordo com relatórios do ICS-CERT (*Industrial Control Systems Cyber Emergency Response Team*) [1] [2], em 2011 a quantidade de incidentes reportados via tickets foi de 204 aumentando para 290 em 2016, ou seja, um aumento de 42%. Levando-se em consideração que nem todos os incidentes são descobertos e reportados, pode-se assumir que as quantidades reais são ainda mais elevadas.

Segundo pesquisa realizada pela IBM e pelo instituto Ponemon [3] [4] com participação de 383 organizações de 12 países, o Brasil é um dos lugares com maior probabilidade de violação de dados, embora o prejuízo resultante seja um dos menores juntamente com a Índia: respectivamente \$100 e \$61 per capita em 2016¹. Considerando as 33 organizações brasileiras que fizeram parte da pesquisa, o custo total devido à violação de dados em 2016 foi de R\$4,31M contra R\$2,64M em 2013 (ver Figura 1). Dados como esses corroboram a preocupação crescente a respeito da segurança de dados independentemente do mercado envolvido sendo que o foco nesse tema deve ser maior quanto maior o impacto relacionado às áreas de saúde, segurança e meio ambiente.

(*) Rua Friedrich von Voit, n° 825 – Prédio P36 – CEP 02.995-000 São Paulo, SP – Brasil
Tel: (+55 11) 3944-6715 – Fax: (+55 11) 3944-4001 – Email: jessica.heluany@voith.com

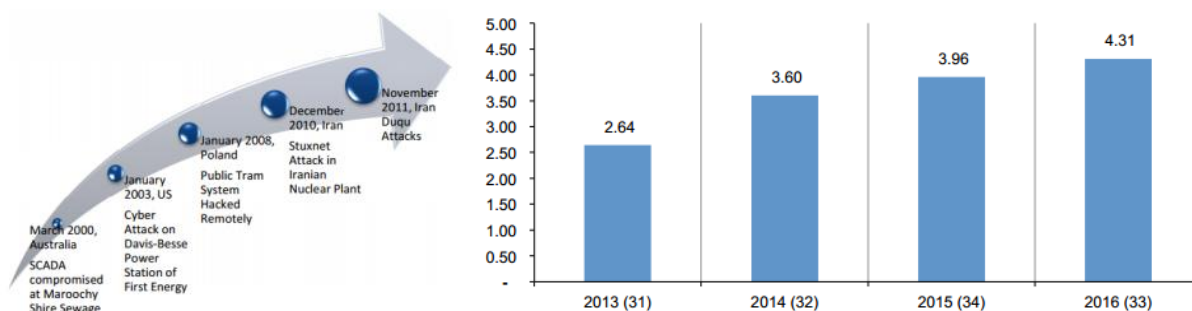


FIGURA 1 – Ataques relevantes no setor energético mundial à esquerda [5], e custo total relativo à violação de dados no Brasil [4], à direita.

Por fazer parte da infraestrutura crítica de um país, o setor elétrico é um alvo provável, sendo necessária a implementação de estratégias de segurança que dificultem ao máximo o acesso não autorizado. No Brasil, aproximadamente 65% da capacidade de geração de energia é proveniente de usinas hidrelétricas, evidenciando a importância de se desenvolver soluções e explorar normas relativas à segurança cibernética. A Estratégia Nacional de Defesa incumbiu o Exército para definir políticas de segurança cibernética, o qual inaugurou, em 2012, o Centro de Defesa Cibernética (CDCiber). O intuito do CDCiber é “orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático” [6]. No entanto, a prática de mercado revela que as empresas do setor energético adotam normas estrangeiras para esse tema.

Nos tópicos a seguir, a norma IEC 62443 será abordada de forma resumida e posteriormente alguns sistemas típicos de usinas hidrelétricas serão avaliados do ponto de vista do risco envolvido. Nas recomendações, são sugeridas soluções aderentes à norma e à tolerância de risco admitida.

2.0 - IEC 62443

A norma ISA/IEC 62443 é derivada da norma ISA 99 e organizada em quatro grupos que abordam os principais temas para a implementação de um programa de segurança cibernética em sistemas de controle industrial. Conforme pode ser visualizado na Figura 2 a seguir, a estrutura organizacional da norma aborda as seguintes áreas: Geral, Políticas e Procedimentos, Sistema, e Componente. Cada uma dessas áreas é composta por uma ou mais partes que detalham um tópico específico.

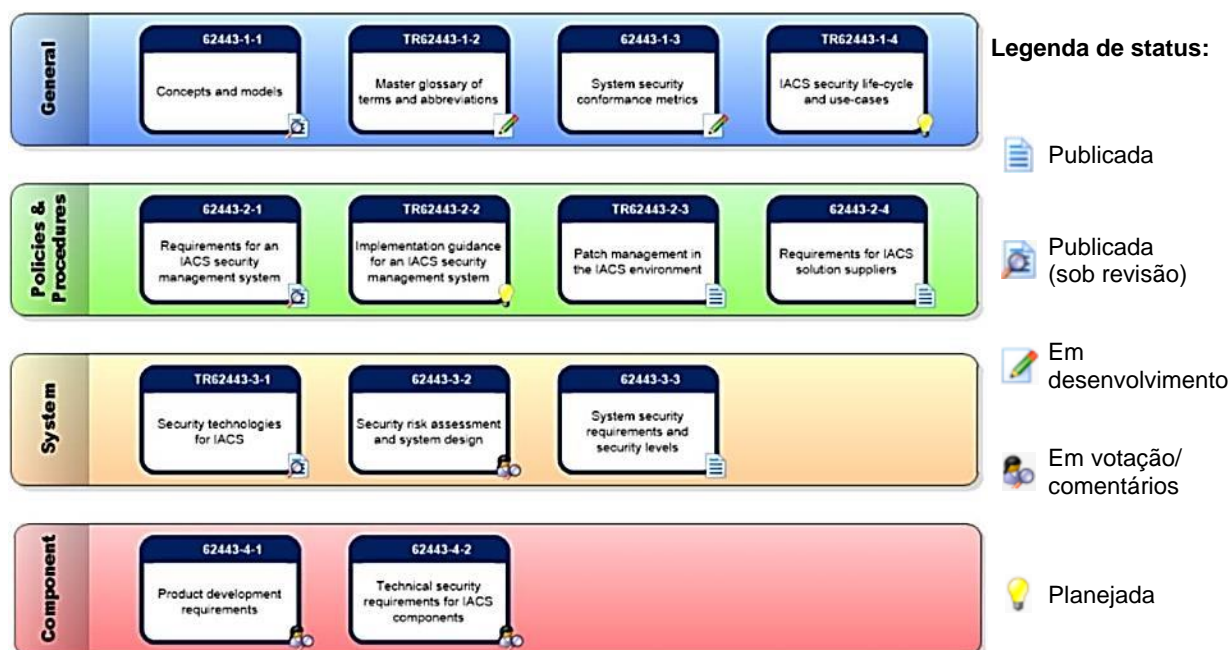


FIGURA 2 – Status dos trabalhos relativos à norma ISA/IEC 62443 [7]

Nota 1. O custo per capita é definido como o custo total pelo tamanho da violação de dados.

2.1 IEC 62443 – Grupo “General”

IEC 62443-1-1 [8]: Essa parte é focada na padronização de terminologias e conceitos com o objetivo de estabelecer a base que será referenciada nos grupos subsequentes. A seguir serão abordadas algumas definições consideradas relevantes para a contextualização deste trabalho.

É importante destacar que os riscos mudam constantemente devido às mudanças nas ameaças e vulnerabilidades que surgem com as evoluções tecnológicas. Sendo assim, qualquer programa de gerenciamento de segurança cibernética deve ser continuamente exercido focando os componentes aplicáveis, ou seja, computadores, redes e todos os dispositivos programáveis.

As ameaças às quais um sistema de controle industrial está submetido podem ser passivas ou ativas, sendo mais comuns as de natureza acidental ou devido a mudanças não validadas. Elas podem ter origem interna, externa ou de causas naturais, e a resposta para estas ameaças pode ser a eliminação de controles ineficazes, transferência do risco, aceitação, minimização, ou desenvolvimento/aplicação de soluções inerentemente seguras.

As ameaças ativas mais comuns se dão através de: destruição física de componentes, escalonamento de privilégios de acesso, negação de serviço, códigos maliciosos (vírus, worms, Trojans), *phishing* (indução a revelação de dados por falsificação de fonte legítima), engenharia social, falsificações de IP, replay, injeção de dados ou via rede de comunicação.

Os requisitos de segurança que devem ser cumpridos incluem controle de acesso, controle de uso, integridade e confidencialidade de dados, restrição de fluxos, disponibilidade de recursos e tempos de resposta a um evento. As contramedidas mais comuns para cumprir com esses requisitos são: autenticação de usuários e computadores, políticas de controle de acesso, detecção de intrusão, mecanismos de criptografia, assinaturas digitais, segregação ou isolamento de recursos, escaneamento contra códigos maliciosos, monitoramento das atividades do sistema, e segurança física dos ativos. Tais contramedidas não eliminam os riscos, mas minimizam a probabilidade de ocorrência que é justamente o foco de uma estratégia de defesa em camadas (*defense in depth*) para evitar os possíveis impactos de uma invasão:

- Roubo, uso indevido ou não autorizado de informações confidenciais
- Publicação de informações para destinatários não autorizados
- Perda de integridade e confiabilidade de dados do processo ou informações da produção
- Perda de disponibilidade
- Transtornos que levem ao comprometimento das funcionalidades do processo
- Danos a equipamentos
- Lesões a pessoas
- Violação de requerimentos legais ou de regulação
- Risco à segurança pública
- Ameaças à segurança da nação

As fases de maturidade de um sistema de gerenciamento de segurança cibernética (CSMS - Cyber Security Management System) são definidas conforme Tabela 1, sendo importante evidenciar que sistemas de uma mesma planta podem estar em estágios diferentes dependendo das prioridades e restrições definidas pelo proprietário.

Tabela 1 – Fases de maturidade de um CSMS [8]

| Fases | Etapas |
|-------------------------|--|
| Conceito | Identificação Conceito |
| Análise funcional | Definição |
| Implementação | Design funcional Design detalhado Construção |
| Operações | Operações Monitoramento de conformidade |
| Reciclagem e eliminação | Eliminação Dissolução |

Para que seja possível o desenvolvimento de um programa de gerenciamento de segurança cibernética, as organizações devem estabelecer políticas e procedimentos que definam como cada tema deve ser tratado dado o critério de tolerância a riscos. As políticas são documentos com os quais as auditorias podem medir conformidade, enquanto os procedimentos definem detalhadamente os passos para as medidas de segurança adotadas. Esses documentos identificam os responsáveis por cada medida e devem ser atualizados constantemente para refletir

mudanças tecnológicas e operacionais. É recomendada a elaboração de uma arquitetura de referência que leve em consideração as zonas de segurança e que atenda aos níveis de segurança (*Security Level – SL*) estabelecidos pela organização, dividindo-os no mínimo em baixo, médio e alto.

2.2 IEC 62443 – Grupo “Policies and Procedures”

IEC 62443-2-1 [9]: detalha como elaborar um sistema de gerenciamento de segurança cibernética (CSMS) partindo de três categorias: análise de risco, endereçamento dos riscos levantados, e monitoramento e melhoria constante. O objetivo não é ser um guia passo a passo, mas sim, servir como ponto de partida que pode ser customizado para atender a necessidades específicas das organizações. Cada categoria é dividida em subcategorias que são detalhadas uma a uma em um dos anexos da norma, com intuito de esclarecer o conteúdo que deve ser abordado e sugerir práticas para implementação.

IEC 62443-2-3 [10]: trata de um conteúdo de extrema importância no contexto de eliminação de vulnerabilidades, mas que pode ser uma fonte de riscos adicionais: gerenciamento de atualizações. É aplicável principalmente aos fornecedores de sistemas de controle industrial e desenvolvedores dos pacotes de atualização que englobam temas relacionados à segurança dos equipamentos. Segundo a norma, as principais atividades relacionadas a esse tema constituem a descoberta de vulnerabilidades, desenvolvimento de atualizações de segurança, distribuição da informação/pacotes obtidos e comunicação constante com os proprietários dos ativos.

IEC 62443-2-4 [11]: especifica requisitos de segurança para fornecedores de serviços relativos a sistemas de controle industrial, os quais podem ser ofertados durante integrações e atividades de manutenção. Tais requisitos devem ser garantidos, seja pelos próprios produtos ou por soluções adicionadas a parte. O anexo A dessa parte da norma define os requisitos em termos de capacidades que um programa de segurança deve prover ao longo da vida útil dos ativos. Assim como nas partes anteriores, as sugestões podem ser customizadas e acordadas entre ambas as partes (fornecedor e proprietário dos ativos). Do ponto de vista de manutenção, embora as atividades iniciem após a implementação da solução, elas incluem aspectos de segurança tanto de forma direta quanto indireta. Fornecedores de manutenção devem participar do levantamento de riscos da planta em questão ou utilizar o existente, e endereçar os riscos nas atividades, seja com pacotes de atualização, upgrades de equipamentos, ajustes em algoritmos de controle, migração de sistemas, ou outras soluções.

2.3 IEC 62443 – Grupo “System”

IEC 62443-3-1 [12]: aborda tecnologias que podem ser utilizadas no mercado de automação industrial a fim de minimizar riscos e vulnerabilidades. Envolve tanto ferramentas, quanto medidas de mitigação e possibilidades de tecnologias diferentes que poderiam ser aplicadas para fins específicos de proteção de dados. Sempre que possível, são apontados pontos fortes e fracos da solução que auxiliam na tomada de decisão sobre a implementação de cada uma.

IEC 62443-3-3 [13]: explora os requisitos de segurança em termos de quatro níveis de segurança (SL1, SL2, SL3, SL4), sendo o SL1 o menos seguro e SL4 o mais seguro. Sistemas com SL1 previnem divulgação não autorizada de informação via espionagem ou exposição casual, e sistemas com SL4 previnem divulgação não autorizada de informação via entidades ativas e altamente motivadas que possuem habilidades específicas de sistemas de controle industrial e que podem utilizar recursos sofisticados em busca das informações.

2.4 IEC 62443 – Grupo “Component”

Conforme pode ser visualizado na Figura 2, as partes desse grupo ainda não foram publicadas, mas abordarão o desenvolvimento de produtos em seus primeiros níveis.

Como atualmente o mundo está passando por uma fase de transição, é normal que boa parte das soluções de segurança não sejam intrínsecas aos equipamentos. No entanto, a tendência é que as novas tecnologias possuam cada vez mais mecanismos intrínsecos de segurança que devem ser desenvolvidos desde o momento da concepção dos componentes.

3.0 - EXEMPLOS DE APLICAÇÕES PARA SISTEMAS DE USINAS HIDRELÉTRICAS

Conforme pode ser observado através do resumo da norma, nela são sugeridas soluções que devem ser adaptadas caso a caso. No contexto de usinas hidrelétricas, comumente a planta é um sistema isolado, o que pode impactar nas decisões das medidas de segurança a serem adotadas nas políticas e procedimentos. Casos nos quais várias usinas podem ser operadas remotamente, através de um Centro Remoto, acabam exigindo uma atenção maior para minimizar a exposição a ameaças. O Departamento de Energia dos Estados Unidos desenvolveu um trabalho sobre transferência segura de dados em sistemas industriais [14] no qual a arquitetura de referência sugerida segue os tópicos da norma IEC 62443.

Nessa arquitetura (Figura 3) foram definidas zonas de segurança em todos os níveis, sendo que entre o nível 1 de Instrumentação, e o nível 3 de Operações (que engloba o sistema supervisório local), existem 4 zonas de segurança que foram divididas de acordo com as funcionalidades dos equipamentos. Nota-se que para as comunicações dos equipamentos de controle industrial com qualquer sistema fora dessa rede, os dados passam por uma DMZ (*Demilitarized Zone*) a fim de segregar a rede de controle (confiável) das redes corporativas ou redes de locais remotos (não confiáveis). Sendo assim, a DMZ contém soluções como Histórico (que pode enviar relatórios para a rede corporativa), antivírus (que deve ter acesso à internet), VPNs (para as comunicações remotas), entre outras.

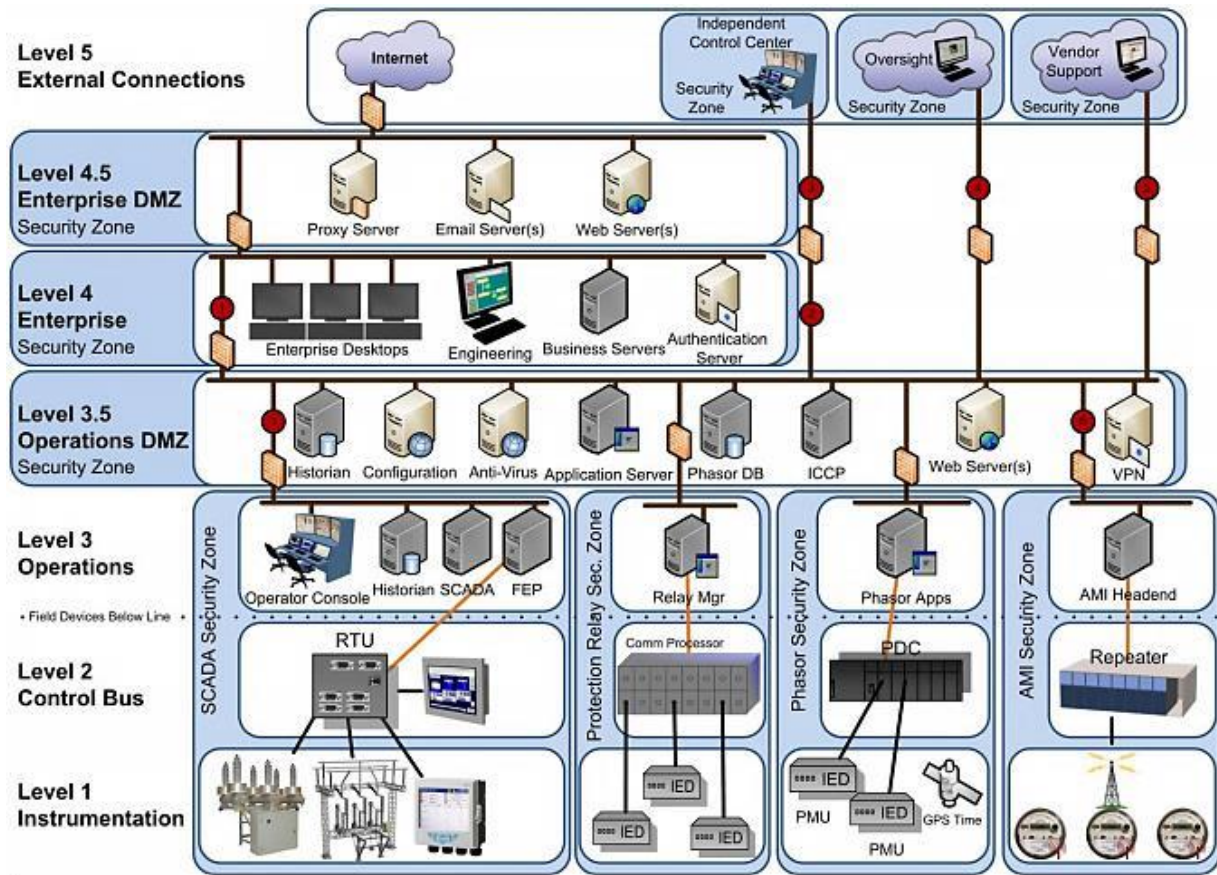


FIGURA 3 – Arquitetura proposta para o SCADA [14]

A seguir, parte dos conceitos expostos neste trabalho serão exemplificados para alguns sistemas de usinas hidrelétricas. O principal foco é a avaliação de risco e as sugestões de solução com base nas consequências que uma ameaça poderia causar.

3.1 Avaliação de Risco

O primeiro passo dessa etapa é a definição da metodologia de avaliação de risco. Vale notar que mesmo análises já existentes que não eram focadas em ameaças cibernéticas, podem ser utilizadas focando cenários nos quais esse tipo de ameaça poderia impedir o bom funcionamento das medidas de proteção [15]. Isso se deve ao fato de que muitas plantas antigas possuem análises focadas em segurança, mas não do ponto de vista de segurança da informação. Apesar de em português utilizarmos sempre a palavra "segurança", em inglês os termos *safety* e *security* distinguem bem esses cenários: enquanto *safety* se refere a riscos diretos ou indiretos a respeito de danos físicos ou de danos à saúde das pessoas, *security* se refere à prevenção de penetração não desejada ou ilegal, acesso inapropriado a informações confidenciais, assim como interferências em sistemas de controle industrial, sejam elas intencionais ou não [16].

Para sistemas cuja consequência de um risco apresenta como severidade o pior caso, idealmente deve-se empregar dispositivos inerentemente seguros. Os exemplos mais comuns de dispositivos inerentemente seguros são: dispositivos de alívio de pressão, trip de sobrevelocidade mecânico, válvulas de *check*, dispositivos de monitoramento de motores, e relés de monitoramento do loop de corrente de instrumentos [15].

Os métodos de avaliação de risco podem ser tanto qualitativos como quantitativos. A Tabela 2 a seguir mostra os principais métodos de cada grupo:

Tabela 2 – Principais métodos de análise de risco [17]

| Métodos Qualitativos | Métodos Quantitativos |
|--|---|
| Listas de checagem (<i>Checklists</i>) | Árvore de eventos (<i>Event Trees</i>) |
| Análise preliminar de Perigos (<i>Preliminary Hazard Analysis - PHA</i>) | Árvore de Falhas (<i>Fault Trees</i>) |
| Revisões E-Se (<i>What-If Reviews</i>) | Análise de Modo e Efeito de Falha (<i>Failure Modes and Effects Analysis - FMEA</i>) |
| Revisões de Perigo e Operabilidade (<i>Hazard and Operability Reviews - HAZOP</i>) | Análise de Camadas de Proteção - semiquantitativa (<i>Layers of Protective Analysis - LOPA</i>) |
| Análise gravata borboleta (<i>Bow-Tie Analysis - BTA</i>) | Análise de nível de integridade de segurança (<i>Safety Integrity Level - SIL – Analysis</i>) |
| Diagrama Espinha de Peixe (<i>Fishbone</i>) | |

Para a avaliação dos sistemas propostos, foi utilizada a metodologia HAZOP com as definições evidenciadas na Tabela 3:

Tabela 3 – Critérios para classificação de Probabilidade, Severidade, e Risco

| Severidade (S) | | Probabilidade (P) | | | Risco (R) | |
|----------------|---|-------------------|----------------|---|----------------|---|
| Pior Caso | 1 | ≥ 95% | Quase certeza | 1 | Alto | 1 |
| Severo | 2 | ≥ 75% | Muito provável | 2 | Moderado | 2 |
| Grave | 3 | ≥ 25% | Chances iguais | 3 | Baixo | 4 |
| Moderada | 4 | ≥ 5% | Pouco provável | 4 | Negligenciável | 5 |
| Mínima | 5 | < 5% | Remota | 5 | | |

3.1.1 Sistema de Proteção

O sistema de proteção de uma usina hidrelétrica comumente é composto por diversos relés de proteção e apenas um dispositivo para configuração, que geralmente é um computador dedicado com as licenças adequadas de cada fornecedor. É um sistema de extrema importância para a proteção dos ativos da usina, e por isso foram recomendadas soluções de defesa em camadas que vão desde o nível físico, com o estabelecimento de um perímetro de segurança, até as configurações específicas de *hardening* do dispositivo de configuração e características da rede de proteção.

Tabela 4 – Avaliação de risco HAZOP para os dispositivos de proteção com parâmetro guia Ação (do dispositivo)

| Desvio | Causas | Consequências | S | Salvaguardas | P | R | Recomendações |
|-------------|--|--|---|---|---|---|---|
| Ação errada | -Erro de parametrização -Falha interna -Falha de instalação | -Operação indevida -Perda de geração/receita -Penalidades -Impacto para o SIN | 2 | -Relés redundantes -Projeto com transformadores de medição adequados -Fonte de alimentação redundante -Procedimentos de testes para comissionamento e manutenção | 5 | 4 | <i>Hardening</i> do computador de configuração: -Configurar apenas serviços do Windows efetivamente utilizados -Configurar serviços de firewall -Configurar apenas portas TCP/IP efetivamente utilizadas -Criar perfis de usuários com segregação de acesso |
| Sem ação | -Erro de parametrização -Falha interna -Falha de instalação -Falha de alimentação | -Ausência de operação -Avarias na máquina (perdas materiais / pessoais) -Perda de geração/receita -Penalidades -Impacto para o SIN | 1 | -Relés redundantes -Projeto com transformadores de medição adequados -Fonte de alimentação redundante -Procedimentos de testes para | 5 | 3 | Rede: -Separação das redes de controle e proteção - <i>Hardening</i> dos dispositivos de rede Físico: - Delimitar acesso físico ao computador |

| | | | | | | |
|--|--|--|------------------------------|--|--|--|
| | | | comissionamento e manutenção | | | |
|--|--|--|------------------------------|--|--|--|

Entende-se por *hardening* um conjunto de ações que visam incrementar as configurações de segurança de um determinado hardware ou software, a fim de eliminar vulnerabilidades conhecidas e, por vezes, provenientes do próprio fabricante em função da gama de clientes e aplicações que cada fornecedor deve atender. Uma vez implementada tal metodologia, é necessária uma estratégia de testes bem como procedimento detalhado de instalação e remoção das configurações.

3.1.2. Sistema de Sincronismo

A solução mais recorrente para o sincronismo das unidades geradoras consiste em um sincronizador automático e um *check* de sincronismo. Esses dispositivos possuem sistemas que permitem a equalização da velocidade e da tensão, pois são recebidos os sinais de frequência do gerador, frequência do sistema, tensão do gerador e tensão do sistema (inclusive com os valores de fase). Ou seja, se o dispositivo for configurável por rede e algum desses sinais for corrompido para um valor forçado que leve a um sincronismo errado, a máquina pode sofrer graves consequências. É mais um exemplo de sistema crítico para o qual a solução tecnológica adotada deverá apresentar o menor risco possível e atender a requisitos de defesa em camadas idealmente alinhados com a norma IEC 62443.

Tabela 5 – Avaliação de risco HAZOP para os dispositivos de sincronismo automático com parâmetro guia Ação (do dispositivo)

| Desvio | Causas | Consequências | S | Salvaguardas | P | R | Recomendações |
|-------------|--|--|---|--|---|---|--|
| Ação errada | -Falha de instalação -Erro de parametrização -Falha interna -Falha de alimentação | -Avarias na máquina -Avarias nas estruturas de fixação -Impacto no SIN | 1 | -Relé de sincronismo e <i>check</i> - sincronismo -Sincronismo manual | 5 | 1 | -Utilizar modelos com parametrização no display do equipamento, e não via rede -Utilizar dispositivos que não tenham Sistema Operacional, que seriam passíveis de atualizações e acessos via rede |

3.1.2 Regulador de Velocidade Hidráulico

Geralmente, cada unidade geradora possui um sistema redundante para a detecção de sobrevelocidade, sendo o primeiro incorporado no regulador digital e o segundo um dispositivo elétrico ou mecânico. Caso o segundo dispositivo seja elétrico, idealmente deve-se implementar fonte de alimentação redundante e supervisioná-la no diagrama de trips. Já a solução com o pêndulo mecânico é inerentemente segura, pois mesmo que o regulador seja invadido e que o sinal seja inibido, o pêndulo vai atuar e impedir que a máquina seja danificada.

Nesse caso, a solução inerentemente segura elimina a necessidade de várias camadas de proteção (*defense in depth*), mas exige manutenção constante para garantir a correta atuação do pêndulo caso ocorra sobrevelocidade ou disparo da unidade geradora.

Tabela 6 – Avaliação de risco HAZOP para o regulador hidráulico com parâmetro guia Velocidade e aplicação exclusiva para sobrevelocidade (do eixo)

| Desvio | Causas | Consequências | S | Salvaguardas | P | R | Recomendações |
|------------|--|---|---|---|---|---|---|
| Muito alta | -Falha de operação do regulador de velocidade -Falha de sistema -Falha na válvula de entrada | -Vibrações -Avarias na estrutura do eixo -Desbalanceamento da máquina | 2 | -Detecção de sobrevelocidade no regulador digital - Detecção de sobrevelocidade através de pêndulo mecânico -Projeto contempla operação nessa | 4 | 2 | -Dada a importância desse sistema e a facilidade de implementar uma solução inerentemente segura, recomenda-se a utilização do pêndulo mecânico |

| | | | | | | | |
|--|--|--|--|-----------------------------|--|--|--|
| | | | | condição por tempo limitado | | | |
|--|--|--|--|-----------------------------|--|--|--|

4.0 - CONCLUSÃO

Através da contextualização do cenário atual de ataques cibernéticos e da tendência de que os mesmos aumentem ao longo dos próximos anos, enfatiza-se a importância de se considerar requisitos de segurança cibernética desde o momento da concepção das soluções de automação, sejam elas para plantas novas ou que sofrerão modernização.

A fim de esclarecer os cuidados que devem ser tomados, esse informe explorou resumidamente uma das normas mais recorrentes sobre esse tema: a IEC 62443. Espera-se ter elucidado como ela pode auxiliar no planejamento de um programa de gerenciamento de segurança cibernética para usinas hidrelétricas. Além disso, também é importante destacar que a definição das zonas e consequentemente dos requisitos de segurança deve estar baseada em análises de risco, e a divisão pode ser tanto física quanto lógica. No item 2.4 deste informe foram elencadas as principais técnicas de avaliação de risco mantendo os nomes em inglês para facilitar a procura por informações adicionais. A definição das zonas de segurança é importante porque ajuda a limitar a solução tecnológica que será empregada, a qual deve ficar muito clara para possibilitar uma comparação igualitária dos fornecedores.

Destaca-se que o responsável por definir a arquitetura de referência, políticas e procedimentos, e nível de tolerância a riscos é o próprio dono dos ativos, visto que ele que arcará com os possíveis impactos de um ataque. Neste sentido, a integração entre equipes no âmbito da organização é fundamental, ou seja, as equipes responsáveis pelos ativos na usina hidrelétrica e as equipes de tecnologia da informação especializadas em segurança da informação, administração de redes e gestão de infraestrutura, devem estar alinhadas. Tais equipes devem considerar requisitos de segurança cibernética, não só em novas implementações, mas também nas mudanças executadas nas usinas ao longo do tempo.

Por fim, os exemplos de avaliações de risco HAZOP para os sistemas de proteção elétrica, sincronismo, e regulador hidráulico (sobrevelocidade) buscaram exemplificar todo o conteúdo abordado e como o seguimento à norma pode ajudar nas recomendações de solução. Com isso, espera-se auxiliar trabalhadores do setor energético no entendimento da norma IEC 62443, na elaboração dos seus programas de gerenciamento de segurança cibernética e, consequentemente, nas tomadas de decisão sobre as soluções que serão requeridas para modernizações e plantas novas.

5.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ICS-CERT YEAR IN REVIEW 2013 – Industrial Control Systems Cyber Emergency Response Team
- [2] ICS-CERT MONITOR – NOV/DEC 2016 - Industrial Control Systems Cyber Emergency Response Team
- [3] 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS - Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC – June 2016
- [4] 2016 COST OF DATA BREACH STUDY: BRAZIL - Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC – June 2016
- [5] CYBERSECURITY FOR INDUSTRIAL AUTOMATION & CONTROL ENVIRONMENTS - Protection and Prevention Strategies in the Face of Growing Threats – A Frost & Sullivan White Paper in Partnership with Schneider Electric – April 2013
- [6] POLÍTICA CIBERNÉTICA DE DEFESA (MD31-P-02) – Ministério da Defesa - 2012
- [7] ISA99 COMMITTEE WIKI - Status of the various work products in the ISA/IEC 62443 series of IACS standards and technical reports – Disponível em: <http://isa99.isa.org/ISA99%20Wiki/Home.aspx>

- [8] IEC/TS 62443-1-1 - INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY – Part 1-1: Terminology, concepts and models – Edition 1.0 2009-07
- [9] IEC 62443-2-1 - INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY – Part 2-1: Establishing an industrial automation and control system security program– Edition 1.0 2010-11
- [10] IEC TR 62443-2-3 - SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS – Part 2-3: Patch management in the IACS environment – Edition 1.0 2015-16
- [11] IEC 62443-2-4 - SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS – Part 2-4: Security program requirements for IACS service providers – Edition 1.0 2015-16
- [12] IEC/TR 62443-3-1- INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY – Part 3-1: Security technologies for industrial automation and control systems– Edition 1.0 2009-07
- [13] IEC 62443-3-3 - INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY – Part 3-3: System security requirements and security levels– Edition 1.0 2013-08
- [14] SECURE DATA TRANSFER GUIDANCE FOR INDUSTRIAL CONTROL AND SCADA SYSTEMS – Prepared for the U.S. Department of Energy under Contract DE-AC05-76RL01830 Edition 1.0 2013-08 – September 2011
- [15] EDWARD M. MARSZAL - ISA InTech - Security Process Hazard Analysis Review - Determining security level requirements – March/April 2016
- [16] THE ROCKY RELATIONSHIP BETWEEN SAFETY AND SECURITY – Best practices for avoiding common cause failure and preventing cyber security attacks in Safety Systems – ABB – 2012
- [17] SAFETY AND SECURITY REVIEW FOR THE PROCESS INDUSTRIES - Application of HAZOP, PHA, What-IF and SVA Reviews - 4th Edition - Dennis P. Nolan - 2014

6.0 - DADOS BIOGRÁFICOS



Jessica Barbosa Heluany(*)

Nascida em São Paulo/SP, 1988

Engenheira Eletricista graduada em 2014 pela Escola Politécnica da USP – São Paulo/SP

Engenheira Trainee

Voith Digital Solutions, desde 2015



Fabio Oliveira

Nascido em São Paulo/SP, 1974

Bacharel em Sistemas de Informação graduado em 2005 pela UNIP – São Paulo/SP

Coordenador de Segurança da Informação

Voith Digital Solutions, desde 2008



Leandro Oliveira Silva

Nascido em Sinop/MT, 1981

Engenheiro Eletricista graduado em 2005 pela UFSC – Florianópolis/SC

Head de Serviços e Upgrades

Voith Digital Solutions, desde 2012



Marcus Hofmann

Nascido em São Paulo/SP, 1972

Engenheiro Eletrotécnico graduado em 1996 pela FAAP – São Paulo/SP

Projetos Especiais

Voith Digital Solutions, desde 2002

Rinaldo de Paula Machado



Nascido em São Paulo/SP, 1971

Engenheiro Eletricista graduado em 2001 pela USJT – São Paulo/SP
Engenharia de Aplicação

Voith Digital Solutions, desde 2002