



**Grupo de Estudo de Sistemas de Informação e Telecomunicação para Sistemas Elétricos-GTL**

**A metodologia EPRI para avaliação de riscos cibernéticos nas infraestruturas críticas e sua relação com a norma IEC 62443-2-1**

**LUIZ AUGUSTO KAWAFUNE CAMPELO(1);**  
**OSI(1);**

**RESUMO**

O objetivo deste trabalho é discorrer sobre a metodologia desenvolvida pela EPRI (Electric Power Research Institute) para mapeamento de riscos cibernéticos de um conjunto de componentes, produzindo os denominados CSDS (Cyber Security Data Sheet).

Estes documentos mostrarão ao usuário os riscos cibernéticos associados a componentes, estratégias de mitigação e vulnerabilidades residuais (que não podem ser mitigadas pelo próprio componente), com interpretação mais simplificada do que as classificações CVE (Common Vulnerabilities and Exposures).

Os CSDS podem ser integrados ao CSMS (Cyber Security Management System) previsto na norma ISA/IEC 62443-2-1 sendo uma importante ferramenta de avaliação de riscos dada a sua escalabilidade.

**PALAVRAS-CHAVE**

Cibersegurança, Vulnerabilidades, CSDS, EPRI, TAM

**1.0 - INTRODUÇÃO**

Quando falamos sobre segurança cibernética, normalmente nos recordamos de técnicas, tecnologias, ferramentas, incidentes e equipamentos ou sistemas para monitoramento. Nos últimos anos, a segurança cibernética tem ganho mais destaque nas empresas do setor, ainda mais pelo fato da necessidade de uma integração antes não vista entre os sistemas de IT (Information Technology) e OT (Operational Technology).

Com esse novo universo de aplicações, o que chamamos de "superfície de ataque" aumenta exponencialmente, dadas as características dos sistemas de IT (Information Technology) e OT (Operational Technology). E, por consequência, o trabalho das equipes responsáveis pela segurança cibernética das empresas aumenta no mesmo passo em que estas tecnologias convergem.

Este universo de aplicações e sistemas, que possuem suas próprias características (e, como todo componente de software, possui vulnerabilidades conhecidas e/ou ainda não conhecidas), introduzem elementos de risco em toda a infraestrutura. Risco este que deve ser apropriadamente mensurado e tratado.

A norma ISA/IEC 62443-2-1 estabelece que um Programa de Segurança para Sistemas de Controle Industriais deve contar com um CMMS (Cyber Security Management System) basicamente composto de três elementos: Políticas de Segurança, Contramedidas para mitigação de vulnerabilidades e Mecanismos de Implementação.

Entretanto, a norma define que as metodologias utilizadas para cumprir com seus requisitos são arbitrários, ou seja, devem ser escolhidos pela organização.

Para abordar este tópico a EPRI (Electric Power Research Institute) introduz sua metodologia de avaliação e mapeamento de riscos cibernéticos produzindo os chamados CSDS (Cyber Security Data Sheet) que utilizam os mesmos conceitos observados no padrão OSHA 3514 (Occupational Safety and Health Administration) – Material Safety Data Sheet, utilizados pela indústria química e considerada uma das normas de referência para esta indústria.

A metodologia da EPRI (Electric Power Research Institute) utiliza o conceito de mitigação de vulnerabilidades em núcleos bem definidos, gerando como resultado o que chamamos de “Vulnerabilidades Residuais” que são vulnerabilidades que não podem (por quaisquer razões, sejam limitações do sistema ou infactibilidade mediante requisitos de negócio) ser mitigadas utilizando recursos do próprio sistema, mas que poderiam ser mitigadas, por exemplo, quando utilizados recursos do sistema ao qual ele interage ou se integra.

## 2.0 - A NORMA ISA/IEC 62443

A ISA/IEC 62443 é uma série de normativas que definem procedimentos para desenvolver Sistemas Industriais de Automação e Controle sob estritas métricas de segurança cibernética. Estas normas são voltadas para os usuários finais, integradores de sistemas, profissionais de segurança cibernética e fabricantes de Sistemas de Controle Industriais. (1)

Estes documentos foram originalmente lançados como ANSI/ISA-99 ou ISA 99 pelo fato de terem sido criados pela Sociedade Internacional de Automação (International Society of Automation – ISA) e lançados publicamente pelo Instituto Americano de Padrões Nacionais (American National Standards Institute – ANSI). Em 2010 estes conjuntos de normas foram numerados como ANSI/ISA-62443 com o intuito de alinhar a numeração da documentação ISA e ANSI com a Comissão Internacional Eletrotécnica (International Electrotechnical Commission – IEC). (1)

A Figura 1 mostra as categorias que fazem parte da norma ISA/IEC 62443. Todas as normas e relatórios técnicos estão organizados em quatro categorias gerais chamadas **Geral**, **Políticas** e **Procedimentos**, **Sistemas** e **Componentes**.

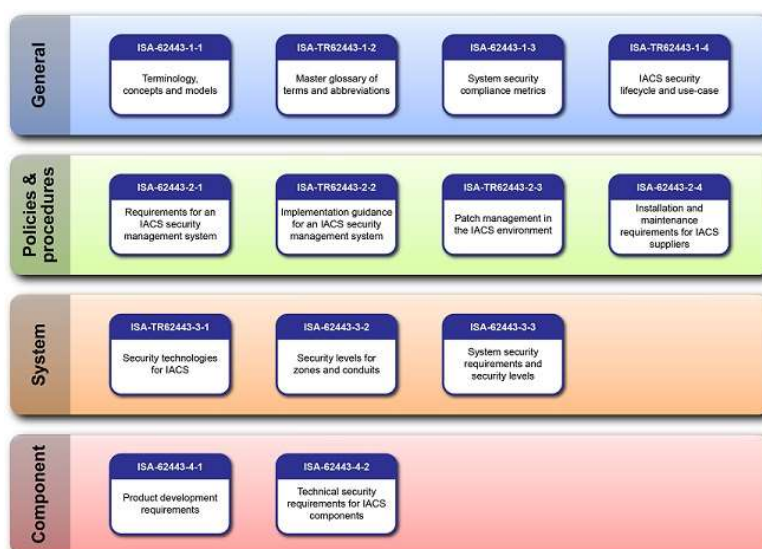


FIGURA 1 – A estrutura da norma ISA/IEC 62443

### 2.1 A norma ISA/IEC 62443-2-1

O capítulo 2-1 da norma ISA/IEC 62443 versa sobre o estabelecimento de um programa de segurança cibernética em ambientes industriais. Muito do exposto neste capítulo tem forte ligação com as normas ISO 27001 e ISO 27002 (International Organization for Standardization – ISO) no sentido de que utiliza uma metodologia de avaliação e mitigação de riscos baseada em análise e posterior documentação em mapas de risco dedicados.

Este programa de segurança é denominado CSMS (Cyber Security Management System) que é composto de três grandes tópicos, a saber (2):

- Análise de Riscos
- Tratamento de Riscos
- Melhoria Contínua

Esta estruturação da norma é mostrada na Figura 2, abaixo.

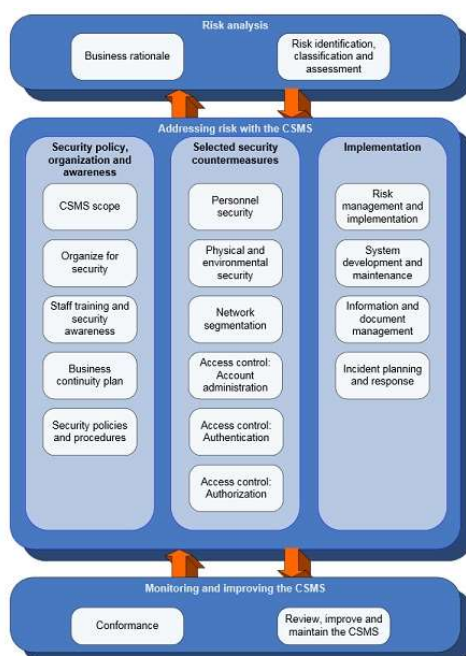


FIGURA 2 – Estruturação da norma ISA/IEC 62443-2-1

No tópico de Análise de Riscos, a norma divide o processo em dois tópicos adicionais:

- *Lógica de negócio*: Identificar os objetivos e restrições do negócio quando se aborda a questão de segurança.
- *Identificação, classificação e tratamento dos riscos*: Identificar os riscos cibernéticos, priorizar as vulnerabilidades baseadas em **factibilidade** e **severidade**, assim como as consequências de uma falha. A organização deve escolher uma metodologia de análise e aproximação para o problema.

No tópico de Tratamento de Riscos, a norma divide o processo em três tópicos adicionais:

- *Política de Segurança, Organização e Conscientização*: Compreende etapas como definição de escopo, equipes, treinamento e conscientização e plano de continuidade que serão agregados a um conjunto de políticas e procedimentos. É importante contemplar neste plano não somente a organização como seus clientes, parceiros e fornecedores.
- *Contra-medidas de Segurança*: São o conjunto de medidas para assegurar a presença de barreiras de segurança, sejam físicas ou virtuais.

- **Implementação:** Conjunto de medidas que envolvem a execução e a manutenção das políticas e programas de segurança cibernética.

No tópico de Melhoria Contínua, a norma divide o processo em dois tópicos adicionais:

- **Conformidade:** Garantir que o CSMS (Cyber Security Management System) de uma organização é seguido por todos, estabelecendo-se métricas de avaliação de sucesso e medidas corretivas em casos de não-conformidades.
- **Revisão, Manutenção e Atualização/Melhorias:** Definir procedimentos e recursos para o processo de revisão/manutenção/melhoria do CSMS (Cyber Security Management System) de uma organização. Este processo deve contemplar desde a revisão dos riscos aceitáveis até o processo de feedback dos usuários finais, objetos das políticas.

Esta estruturação macro define o programa de segurança cibernética em âmbito industrial sugerido pela norma. Embora muitos aspectos estejam bem definidos no escopo da ISA/IEC 62443-2-1, como podemos observar no tópico de Análise de Riscos, a norma deixa em aberto qual a metodologia que deve ser adotada pela organização para realizar esta análise.

### 3.0 - A METODOLOGIA EPRI PARA ANÁLISE DE RISCOS CIBERNÉTICOS

#### 3.1 Sobre a EPRI

A EPRI (Electric Power Research Institute) é uma organização que realiza pesquisa, desenvolvimento e projetos para benefício do público dos Estados Unidos e internacional. É uma organização não-governamental independente focada em geração e entrega de eletricidade, colaborando com as empresas do setor elétrico para melhorar a qualidade e a confiabilidade assim como diminuir o impacto ambiental do setor. (3)

#### 3.2 Motivação: A normativa OSHA 3514

A OSHA (Occupational Safety and Health Administration) foi criada em 1970 para garantir condições seguras dos trabalhadores por meio da publicação de normativas, treinamento, capacitação e assistência. (4)

A OSHA 3514 é uma normativa que requer ao fabricante, distribuidor ou importador de materiais químicos fornecer os SDS (Safety Data Sheet) que contenham informações de todos os componentes químicos perigosos das substâncias e quais são as ações ou pré-requisitos para mitigar potenciais efeitos perigosos no manuseio delas. A norma especifica 16 seções com informações desde a identificação do componente até as medidas de primeiros socorros e contenção de danos. (5) A Figura 3 mostra um exemplo de um SDS (Safety Data Sheet).

10 a 13 de novembro de 2019  
Belo Horizonte - MG


2. HAZARDS IDENTIFICATION	
Classified according to the criteria of the Globally Harmonized System of Classification and Labeling of Chemicals (GHS), OSHA Hazard Communication Standard (29 CFR 1910.1200) and the Canadian Controlled Products Regulations.	
<b>Hazard Classification</b>	
<b>Health Hazards</b>	
Carcinogenicity	Category 1A
Specific Target Organ Toxicity - Repeated Exposure	Category 2 (Lung, Bone)
<b>Label Elements</b>	
<b>Hazard Symbol:</b>	
<b>Signal Word:</b>	Danger
<b>Hazard Statement:</b>	May cause cancer. May cause damage to organs (Lung, Bone) through prolonged or repeated exposure.
<b>Precautionary Statement</b>	
<b>Prevention:</b>	Obtain special instructions before use. Do not handle until all safety precautions have been read and understood. Use personal protective equipment as required. Do not breathe dust/fume.
<b>Response:</b>	If exposed or concerned: get medical advice/attention if you feel unwell.
<b>Storage:</b>	Store locked up.
<b>Disposal:</b>	Dispose of contents/container to an appropriate treatment and disposal facility in accordance with applicable laws and regulations, and product characteristics at time of disposal.
<b>Other hazards which do not result in GHS classification:</b>	Electrical Shock can kill. If welding must be performed in damp locations or with wet clothing, on metal structures or when in cramped positions such as sitting, kneeling or lying, or if there is a high risk of unavoidable or accidental contact with workpiece, use the following equipment: Semiautomatic DC Welder, DC Manual (Stick) Welder, or AC Welder with Reduced Voltage Control.  Arc rays can injure eyes and burn skin. Welding arc and sparks can ignite combustibles and flammable materials. Overexposure to welding fumes and gases can be hazardous. Read and understand the manufacturer's instructions, Safety Data Sheets and the precautionary labels before using this product. Refer to Section 8.  The welding fume produced from this welding electrode may contain the following constituent(s) and/or their complex metallic oxides as well as solid particles or other constituents from the consumables, base metal, or base metal coating not listed below:
<b>Substance(s) formed under the conditions of use:</b>	

FIGURA 3 – Exemplo de SDS (Safety Data Sheet)

A forma como são analisados e classificados os riscos dos componentes químicos na OSHA 3514 são considerados referência para a indústria no mundo. Por que não usar este formato com outros tipos de risco, como o cibernético?

### 3.3 A metodologia EPRI

A EPRI (Electric Power Research Institute) desenvolveu uma metodologia para identificação e mitigação de vulnerabilidades chamada TAM (Technical Assessment Methodology) que consiste em uma verificação com escopo bem definido das vulnerabilidades presentes em um sistema (seja ele um software ou uma rede completa de automação) utilizando o conceito de “Sequência de Exploração” (Exploit Sequence). (6)

Para que uma Sequência de Exploração seja caracterizada, ela necessita da definição de três fatores:

- Um “Objetivo de Exploração” (Exploit Objective)
- Um “Caminho de Ataque” (Attack Pathway): Um caminho físico ou lógico que um atacante pode utilizar para ações diretas ou acesso a dados críticos.
- Um “Mecanismo de Exploração” (Exploit Mechanism): Mecanismo específico que pode ser utilizado a partir de um dado Caminho de Ataque.



FIGURA 4 – Determinando a existência de uma Vulnerabilidade Residual

Uma Sequência de Exploração mapeada resulta no que chamamos de “Vulnerabilidade Residual” (Residual Vulnerability) conforme a Figura 4. Note que, quaisquer componentes de hardware e software possuem Vulnerabilidades Residuais que devem ser mitigadas. Na classe de vulnerabilidades residuais está incluído o conceito de “Insecure by Design”. Note que, uma Vulnerabilidade Residual não necessariamente é uma falha de software.

Como pode ser observado, esta metodologia analisa sistemas desde o ponto de vista de suas Superfícies de Ataque. Após realizar o mapeamento e verificação das Vulnerabilidades Residuais presentes em um sistema, se tem visibilidade suficiente para aplicar os chamados Métodos de Controle (Security Control Method) que sejam mais efetivos para mitigar estas Vulnerabilidades Residuais.

#### 3.4 O conceito de “Existem Meios” (Means Exist)

A metodologia da EPRI (Electric Power Research Institute) usa o termo “Existem Meios” (Means Exist) como elemento definidor de um Objetivo de Exploração. Em outras palavras, diz-se que “Existem Meios” se, há um Caminho de Ataque e um Mecanismo de Exploração para se alcançar um Objetivo de Exploração. De forma contrária, portanto, se não há um Caminho de Ataque e um Mecanismo de Exploração, não há Objetivo de Exploração a ser alcançado.

#### 3.5 Mecanismos de classificação de vulnerabilidades

Como já foi mencionado na seção 3.4, para que um ataque seja possível, “Meios Existem” para que um determinado Objetivo de Exploração seja bem-sucedido, ou seja, uma combinação de Caminho de Ataque com Mecanismos de Exploração.

Baseado nesta premissa, a EPRI (Electric Power Research Institute) classifica a caracterização da superfície de ataque dos sistemas de acordo com as informações mostradas na Tabela 1, abaixo.

Vetores de Ataque		Classes de Objetivos de Exploração	
1. Redes Cabeadas 2. Redes Wireless 3. Interfaces Portáteis 4. Acesso Físico 5. Cadeia de Suprimentos	<b>Ação Direta</b>	1. Desabilitar 2. Desabilitar Temporizado 3. Negação de Serviço 4. Malware	
	<b>Manipulação de Dados Críticos</b>	1. Roubo 2. Alteração 3. Em Repouso 4. Em Trânsito	1. Dados de Processo 2. Configuração/Aplicações definidas pelo fabricante 3. Configuração/Aplicações definidas pelo usuário 4. Dados de Segurança 5. Configuração/Aplicações de Segurança definidas pelo fabricante 6. Configuração/Aplicações de Segurança definidas pelo usuário

TABELA 1 – Caracterização das Superfícies de Ataque



Das informações da Tabela 1, podemos destacar:

- São definidos 5 Vetores de Ataque que podem gerar diversos Caminhos de Ataque.
- Os Objetivos de Exploração são classificados em Ação Direta (com 4 classes de ações adicionais) e Manipulação de Dados Críticos (com 6 classes de dados adicionais).
- A Manipulação de Dados Críticos ainda possui 4 cenários adicionais possíveis: Roubo, Alteração, Em Repouso e Em Trânsito.
- Desta forma, temos **28 possíveis Objetivos de Exploração** utilizando um dos **5 Vetores de Ataque**, que caracterizam um Caminho de Ataque.

Esta forma de classificação, embora inicialmente pareça grande, é significativamente menor que a árvore de vulnerabilidades utilizada pelo CVE (Common Vulnerabilities and Exposures) que é um dos métodos mais utilizados para análise e classificação de vulnerabilidades. A Figura 5 faz uma comparação entre a quantidade de classificações utilizadas pelo CVE (é uma imagem parcial uma vez que a árvore completa não caberia numa imagem) e as classificações da EPRI (Electric Power Research Institute).

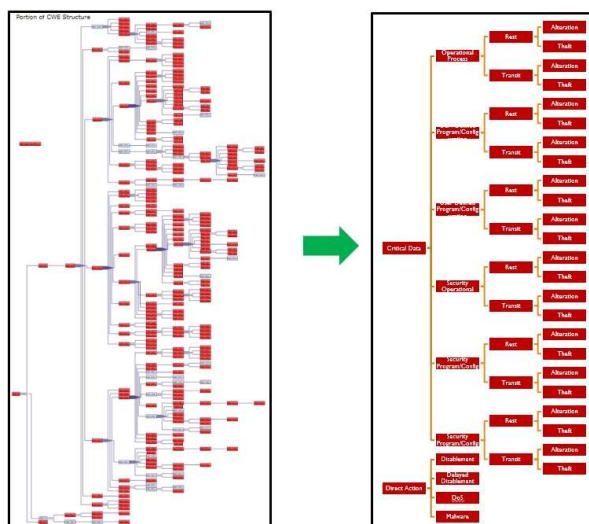


FIGURA 5 – Comparação de árvores de vulnerabilidades: CVE (esquerda) e EPRI (direita)

### 3.6 Resultado: Os Cyber Security Data Sheet (CSDS)

Os CSDS (Cyber Security Data Sheet) são documentos onde são listadas todas as Vulnerabilidades Residuais detectadas em um sistema e seus Métodos de Controle. A organização dos CSDS (Cyber Security Data Sheet) é composta pelos documentos listados na Figura 6, abaixo.

CSDS Organization	
Step 1: Attack Surface Characterization	Work Product
Part 1a: Asset Characteristics	MS-Word document
Part 1b: Target Installation Configuration and Data Flow	
Part 1c: Attack Pathways	MS-Excel spreadsheet
Part 1d: Exploit Mechanisms for Applicable Classes of Exploit Objectives	MS-Excel spreadsheet
Step 2: Engineered Security Control Method Identification, Efficacy, and Allocation	
Part 2a: Engineered Security Control Method Identification and Efficacy	MS-Excel spreadsheet
Part 2b: Engineered Security Control Method Allocation	MS-Excel spreadsheet

FIGURA 6 – Organização dos CSDS (Cyber Security Data Sheet)

A partir desta documentação inicial, a metodologia segue um fluxo de quatro passos como mostrado na Figura 7. Os passos 1, 2 e 3 são necessários e o passo 4 é opcional.

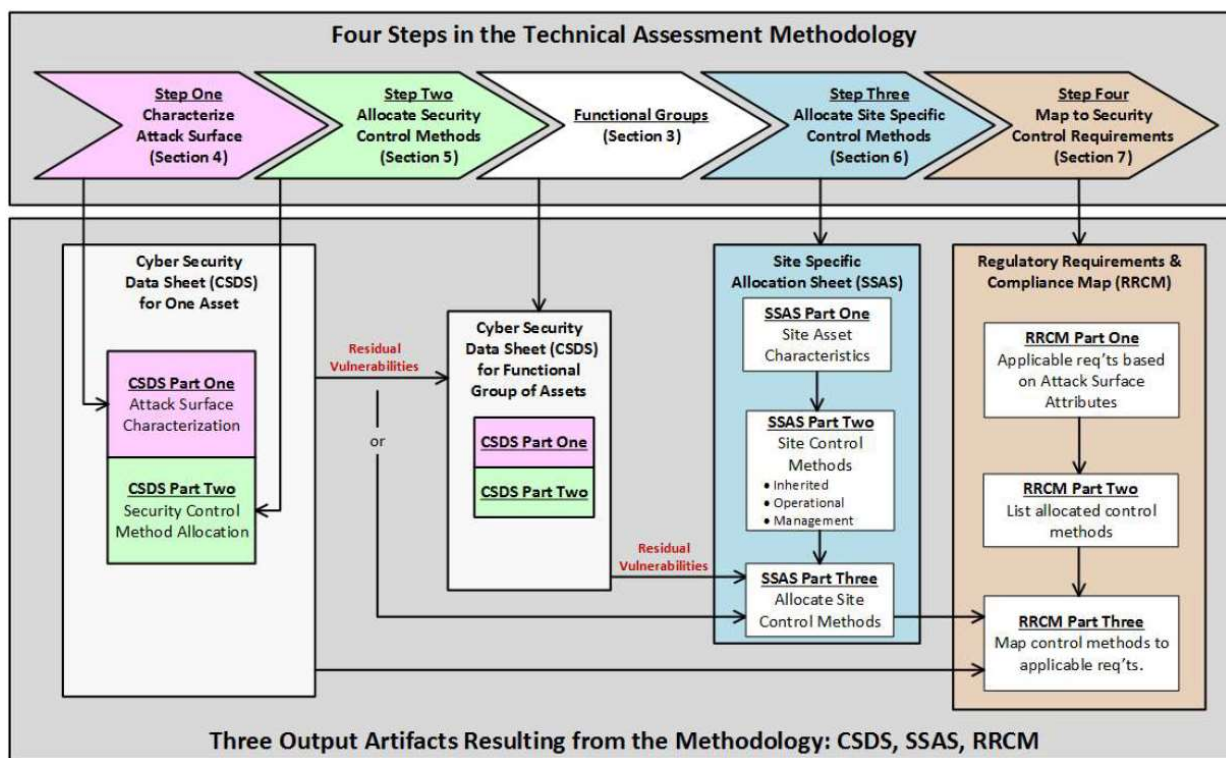


FIGURA 7 – Passos da metodologia TAM (Technical Assessment Methodology)

No passo 3, após a caracterização da superfície de ataque e a alocação de Métodos de Controle para um determinado componente, uma composição de CSDS (Cyber Security Data Sheet) existentes pode ser feita (em termos de Grupos Funcionais) e Métodos de Controle adicionais podem ser aplicados (o chamado Site Specific Allocation Sheet – SSAS) para o conjunto, onde as Vulnerabilidades Residuais de um componente podem ser mitigadas quando interagem com outros componentes dos Grupos Funcionais.



No passo 4, pode-se utilizar os CSDS (Cyber Security Data Sheet) e os SSAS (Site Specific Allocation Sheet) gerados para mapear requisitos regulatórios ou normas de segurança cibernética nos chamados RRCM (Regulatory Requirements & Compliance Map). Por exemplo, na IEC 62443-2-1, no tópico de Tratamento de Riscos, a norma solicita que sejam definidas e implementadas Contramedidas de Segurança que são, basicamente, as alocações dos Métodos de Controle quando se detecta uma Vulnerabilidade Residual num CSDS (Cyber Security Data Sheet). A Figura 8 mostra uma parte da documentação gerada como resultado após a aplicação da metodologia.

CSDS Part 1d: Applicable Technical Vulnerability Classes and Associated Exploit Mechanisms						
Technical Vulnerability Class		Description		Applies?	Applicable Attack	Mechanism to Exploit Vulnerability Class and Notes
Vulnerability Classes Associated with Direct Action Against the Component						
Component Enable/Disablement-Immediate		Means exist to immediately initiate or halt component operation.		YES	A1, A2	A1.1 - Disconnect power supply. A2.1 - Actions via the faceplate that can take manual control or take the SLC out of service.
Component Disablement- Delayed		Means exist to degrade support systems or the environment for component operations, eventually resulting in component disablement.		NO		There is no mechanism to trigger a delayed action.
Denial of Service (DOS)		Means exist to interfere with the normal operation of the component by presenting false demands for component interaction at a component digital port.		NO		Flooding the SLC with HART signals will not interfere with its operation.
Malware		Means exist to inject or install unauthorized and undetected program content on the component that does not constitute an alteration of existing authorized program content.		NO		Only firmware files can be loaded into memory per the manufacturer.
Vulnerability Classes Associated with the 6 Critical Data Types						
Operational Process Data	Theft	In Transit	Means exist to access and record operational process data while being transmitted to or from the component, including process variables, control signals, process element state information, alarms, and process data logs. Transmission includes digital data communication and the use of portable storage media.	YES	A1	A1.1 - A HART device "listening" on the loop can record the HART signal.
		At Rest	Means exist to access and record operational process data while stored on the component, including process variables, control signals, process element state information, alarms, and process data logs.	YES	A1	A1.1 - A HART capable device can access the SLC to read and download process data.
	Alteration	In Transit	Means exist to alter operational process data while being transmitted to or from the component, including process variables, control signals, process element state information, alarms, and process data logs. Transmission includes digital data communication and the use of portable storage media.	NO		Operational process data is transmitted via the 4-20 mA signal and is not digital in this data flow.
		At Rest	Means exist to alter operational process data while stored on the component, including process variables, control signals, process element state information, alarms, and process data logs.	NO		The process data cannot be changed on the SLC.

Figura 8 - Exemplo de um CSDS

Em síntese, os CSDS (Cyber Security Data Sheet) têm, como característica principal, a escalabilidade. A partir de um ou mais documentos gerados, pode-se criar um novo documento customizado para a infraestrutura de rede de Automação e Controle de uma organização usando os CSDS (Cyber Security Data Sheet) dos componentes individuais como ponto inicial.

Outro ponto importante é que esta documentação pode ser gerada tanto pelas organizações como por fabricantes, onde os fabricantes podem prover as organizações com os CSDS (Cyber Security Data Sheet) para os seus produtos e as organizações, de posse dos mesmos, pode construir seu próprio CSDS (Cyber Security Data Sheet), mapeando os riscos e aplicando os Mecanismos de Controle conforme regras e necessidades de negócio.

#### 4.0 - CONCLUSÃO

Como parte do estabelecimento de políticas de segurança cibernética, o mapeamento e tratamento de riscos é, certamente, a tarefa mais complexa e, muitas vezes, tediosa para as equipes de segurança cibernética das organizações.

Utilizando a árvore do CVE (Common Vulnerabilities and Exposures) no momento de analisar as vulnerabilidades de um sistema, ou conjunto de sistemas, os analistas de risco cibernético podem levar intermináveis horas, indo cada vez mais fundo nas classificações do CVE e, em muitas vezes, especialmente para o caso das redes de Automação e Controle, levando a análise de potenciais vulnerabilidades que sequer são aplicáveis a realidade destas redes, num ciclo de análise quase que interminável.

A metodologia desenvolvida pela EPRI (Electric Power Research Institute), utilizando uma aproximação de escopo definido, facilita o trabalho de fabricantes e especialistas das organizações pois, além de simplificar e limitar o escopo de análise, esta análise pode ser granularizada em componentes de hardware/software e ser utilizada como documentação de base em análises mais amplas, a partir da integração entre diversos componentes e equipamentos.

Os CSDS (Cyber Security Data Sheet) provêm visibilidade das Vulnerabilidades Residuais de um sistema às organizações que podem, de maneira muito mais racional e proativa, direcionar seus investimentos em segurança cibernética, priorizando os ativos mais críticos e atendendo a requisitos de negócio. Além disso, por conta de sua granularidade, os CSDS são mais resilientes a mudanças nas superfícies de ataque em decorrência de modernizações, substituições ou adição de ativos uma vez que, para cada uma destas operações, ao invés de se revisitar toda a superfície de ataque, revisita-se apenas os pontos onde houveram modificações.

Da mesma forma, do ponto de vista dos fabricantes, os CSDS (Cyber Security Data Sheet) podem prover informações importantes acerca das características dos seus produtos e possibilitar melhorias, inclusive, no ciclo de desenvolvimento das aplicações em termos de segurança.

Obviamente, a metodologia não existe em si própria mas age como um elemento que auxilia a aplicação correta dos mecanismos de controle presentes em diversas normativas como NIST (National Institute of Standards and Technology), NERC/CIP (North American Reliability Corporation/Critical Infrastructure Protection), ISA/IEC 62443, entre outras possíveis. Desta forma, a metodologia serve como subsídio para planejamento, execução e manutenção de programas de segurança cibernética para o setor.

#### 5.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) WIKIPEDIA. Cyber Security Standards - [https://en.wikipedia.org/wiki/Cyber\\_security\\_standards](https://en.wikipedia.org/wiki/Cyber_security_standards)
- (2) INTERNATIONAL SOCIETY OF AUTOMATION. Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program - ANSI/ISA-62443-2-1 – 2009
- (3) ELECTRIC POWER RESEARCH INSTITUTE. About EPRI - <https://www.epri.com/#/about/epri?lang=en-US>
- (4) OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION. About OSHA - <https://www.osha.gov/about.html>
- (5) OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION. Hazard Communication Standard: Safety Data Sheets - <https://www.osha.gov/Publications/OSHA3514.html>
- (6) GEDDES, B., THOW, M. EPRI Technical Assessment Methodology: Vulnerability Identification and Mitigation (3002008023)



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

10 a 13 de novembro de 2019  
Belo Horizonte - MG

4306  
GTL/23

## 6.0 - DADOS BIOGRÁFICOS



Luiz Augusto Kawafune Campelo  
Engenheiro Eletricista – UNICAMP 2008

Engenheiro Eletricista com 10 anos de experiência no setor elétrico, tendo atuado como Engenheiro de Automação e Controle em projetos de geração de energia no Brasil e no exterior. Na OSIsoft exerce a função de Engenheiro de Sistemas, especialista em Segurança Cibernética para a América Latina e atua, principalmente, com empresas do setor elétrico do Brasil e da América do Sul.

Membro do Comitê de Segurança Cibernética da Associação Brasileira da Internet das Coisas (Abinc)

Membro do Grupo de Trabalho do Cigré (D2) em Segurança Cibernética para o setor elétrico.

Membro do Comitê de Smart Cities da Associação Brasileira da Internet das Coisas (Abinc)