# ESTUDO SOBRE A TÉCNICA DE HAZOP NA ANÁLISE DE RISCOS DA CIBERSEGURANÇA INDUSTRIAL

**Bruno Santos Junqueira[1]**; **Tuane Lisboa Silva Paixão**[2] **Ruy Carvalho de Barros**[3]
[1] Bolsista; de Pesquisa, Desenvolvimento e Inovação– PD&I; bruno.junqueira@fbter.org.br
[2] Bolsista; de Pesquisa, Desenvolvimento e Inovação– PD&I; tuane.paixao@fbter.org.br
[3] Formação; Universidade Federal da Bahia; Salvador-BA; ruy.barros@fieb.org.br

**RESUMO**

As avaliações de riscos têm sido uma prática bem estabelecida desde a década de 90 para ajudar as organizações a identificar e gerenciar os riscos industriais. No entanto, as avaliações de segurança, por padrão, não abordam o risco relacionado à segurança cibernética. Para entendermos e avaliarmos efetivamente os riscos cibernéticos operacionais e relacionados à segurança de processos, é necessário avaliar vulnerabilidades, ameaças e consequências. Neste contexto, o objetivo deste artigo é um estudo comparativo de compatibilidades da metodologia de HAZOP, na IEC 61882[1], no contexto da cibersegurança industrial, suas regras básicas e a correlação dos requisitos empregados na norma de IEC 62443[2].

**PALAVRAS-CHAVE:** Cibersegurança; HAZOP; IEC 62443; IEC 61882.

## 1. INTRODUÇÃO

As avaliações de riscos (AR) são fundamentais na cibersegurança industrial para a geração de um plano estratégico, sendo através dela que serão verificadas quais ameaças e vulnerabilidades estão presentes nos seus sistemas de controle e automação industriais (SCAI), podendo interferir no bom funcionamento de processos e operações dentro de uma organização, onde há o emprego de tecnologias de automação (TA). Na ISO 31000[3] são três as etapas básicas do processo de AR: a identificação de riscos, a análise e a AR propriamente dita, que permitirão qualificar e quantificar os riscos e assim gerenciá-los, priorizando a prevenção e a mitigação ou como estratégia alternativa, a realização da transferência de riscos de eventos e incidentes indesejados para compartilhar impactos e responsabilidades e assim realizar o tratamento destes riscos. Dessa forma, a AR é importante para ajudar na tomada de decisões de governança e para a definição do orçamento destinado a proteção dos ativos da organização.

Existem diversas metodologias de AR na cibersegurança, estas se dividem em ativos ou são baseadas em cenários. As abordagens de segurança buscam identificar as vulnerabilidades ou as fragilidades no SCAI que permitam ataques cibernéticos bem-sucedidos[4]. Aliada a cada metodologia podem ser empregadas técnicas diferentes. Geralmente estas possuem como propósito, dentro do contexto da cibersegurança industrial, o desenvolvimento de um programa de cibersegurança. O objetivo final da AR é endereçar respostas para cada risco encontrado, mesmo que essa resolução seja aceitar o risco [5].

As técnicas de AR também podem ser classificadas por seu direcionamento a processos ou a operações. Aquelas que são direcionadas a processos, por exemplo a *Hazard and Operability Studies* (HAZOP) e a Failure Mode and Effects Analysis (FMEA), classificadas como técnicas de *Process Hazards Analysis (PHA)*, visam identificar possíveis problemas com antecedência, para manter uma produção operante, e existe uma necessidade de prevenção contra acidentes tais como incêndios, explosões ou a liberação de resíduos e rejeitos em indústrias dos mais diversos segmentos, tais como a indústria de óleo e gás, siderúrgica, química e petroquímica, de papel e celulose.

Um aspecto importante na norma IEC 62443[2] para este estudo é se a técnica de HAZOP suporta uma AR de alto nível. Esse tipo de AR é usado para determinar os riscos com maiores impactos na saúde, meio ambiente e segurança (SMS), em caso de uma falha em um componente ou sistema. A AR de alto nível acontece através do monitoramento, análise crítica, acompanhamento da execução e efetividade dos planos de gestão de riscos, direcionados para os riscos mais importantes. A AR de alto nível serve para uma futura integração de resultados de avaliações de vulnerabilidade detalhadas, e também para o fornecimento de guias para tratar os riscos mais impactantes, possibilitando assim uma maior capacidade de mitigação do risco.

A cibersegurança industrial entra nesse contexto para prevenir e mitigar possíveis incidentes em que os controles de processos são tomados ou desativados através de um acesso não autorizado ou ataque. O presente artigo busca analisar e comparar a compatibilidade da técnica de HAZOP para sua aplicação na cibersegurança industrial, utilizando o guia da IEC 61882[1] através de uma verificação dos procedimentos e similaridades das regras básicas da técnica tomando como base os requisitos impostos pela norma IEC 62443[2].

## 2. METODOLOGIA

Selecionar a técnica de AR para uma organização é uma tarefa muito subjetiva, baseada no número de problemas, porém, a premissa de que risco é uma combinação de uma determinada probabilidade de um evento e as consequências deste ocorrerem é comum para as mesmas. Considerando a abordagem sistemática, disciplinada e documentada do HAZOP, ela foi selecionada para a realização deste estudo.

Apesar do HAZOP ser uma técnica qualitativa de riscos, é possível ser realizada uma análise do tipo estática; neste tipo de análise, informações estatísticas referentes ao ambiente de risco são coletadas através de entrevistas e questionários. Posteriormente, poderão servir como um parâmetro para definir quantitativamente o nível de risco de um determinado evento ou incidente utilizando uma matriz de riscos, que é uma tabela onde se calcula o produto entre impactos e probabilidade de cada risco, seguindo os procedimentos da IEC 60300-3-9 *Dependability management - Part 3: Application guide - Section 9: Risk analysis of technological systems* [6].

Os requisitos de AR na IEC 62443[2] deste estudo foram obtidos de consultas à norma e da tabela *Analysis of risk identification, classification, and assessment in IEC 62443*[7]. Para realizar uma comparação com esses requisitos extraídos da IEC 62443[2], foi feita uma pesquisa exploratória através da observação de compatibilidades nos tópicos das normas citadas neste estudo que guiam a aplicação do HAZOP e a AR na cibersegurança industrial, com uma posterior discussão das compatibilidades, feita pelos autores do presente artigo, por meio da identificação de ações e padrões comuns ou convergentes, explicitados através da tabela 1, na coluna compatibilidade, obtidos através da comparação dos requisitos da norma de cibersegurança industrial com os procedimentos de aplicação da técnica de HAZOP inseridos na norma IEC 61882 *Hazard and operability studies (HAZOP studies) - Application guide*. Essa norma forneceu orientações sobre a aplicação da técnica e sobre o procedimento de estudo do HAZOP, incluindo definição, preparação, sessões de análise, documentação e acompanhamento dos resultados. Dessa forma, utilizando como base estas duas normas, foi possível identificar compatibilidades entre o que está imposto pela IEC 62443[2] e o que é feito através desta técnica.

## 3. RESULTADOS E DISCUSSÃO

As análises dos requisitos para realização de uma AR da IEC 62443[2] e o procedimento da técnica de HAZOP levaram à identificação de diversas similaridades entre estas. Observou-se que alguns pontos comparados não foram apresentados com a mesma sintaxe e que a tradução de algumas sentenças dos textos nas normas apontou concordâncias através de termos similares. Considera-se que foi possível realizar uma análise da efetividade do uso desta técnica, pois dentro do guia do HAZOP foram encontrados diversos textos que apontam ações por meio de artifícios equivalentes aos que são propostos na IEC 62443 para a realização da AR. Construiu-se uma tabela para apresentar os resultados, onde se identificou requisitos, procedimentos e as suas respectivas compatibilidades, dispostas na coluna de compatibilidades.

Tabela 1. Requisitos da IEC 62443 e procedimentos da técnica HAZOP compatíveis

| Ação | Requisito IEC 62443 | Procedimentos IEC 61882 | Compatibilidade |
|---|---|---|---|
| Selecionar avaliação | Estabelece que a AR deve identificar e priorizar riscos baseada em ameaças à segurança, vulnerabilidades e consequências relacionadas aos ativos do SCAI. | Entre os objetivos de identificação de HAZOP temos os problemas operacionais, incluindo efeitos na qualidade de um produto. | Pode-se afirmar que existe uma compatibilidade na escolha de HAZOP, pois os problemas de segurança em programas de sistemas eletrônicos podem ser classificados como operacionais. |
| Fornecer | A organização deve fornecer participantes na atividade de AR com treinamento na metodologia, antes de começar a identificar os riscos. | O líder do estudo deve ser treinado e possuir experiência em HAZOP. Um representante da manutenção, um usuário do sistema e caso seja um sistema próprio, o projetista, também participam da análise. | Existe uma clara convergência nesse ponto, é importante que haja participantes da organização para que as análises sejam mais aprofundadas. |
| Executar | Uma AR de nível alto deve ser realizada para entender as consequências financeiras e de SMS de um evento com alta probabilidade e impacto. | Nesse procedimento são documentados detalhes dos perigos e problemas operacionais em conjunto com detalhes de provisões para a sua prevenção. | HAZOP não possui explicitamente uma referência à uma análise de nível alto, mas trabalha com detalhes dos riscos identificados juntamente com detalhes de mitigações. |
| Identificar | A organização deve identificar os vários SCAIs e coletar dados sobre os dispositivos para caracterizar a natureza do risco à segurança e agrupar os dispositivos em sistemas lógicos. | HAZOP é particularmente útil para identificar pontos fracos nos sistemas envolvendo o fluxo de materiais, pessoas ou dados, ou um número de eventos ou atividades em uma sequência planejada ou os procedimentos que controlam essa sequência. | É possível afirmar que o critério de identificação da IEC 62443 é atendido, pois utilizando HAZOP consegue-se coletar dados dos ativos que poderiam ser utilizados de forma maliciosa e caracterizar os riscos de cada sistema. |

| | | | |
|---|---|---|---|
| Integrar | Os resultados das AR cibernéticos, físicos e de SMS devem ser integradas para entender o risco geral dos ativos. | HAZOP é uma metodologia de identificação de perigos que considera as partes do sistema individualmente e examina metodicamente os efeitos dos desvios em cada parte. Às vezes, um risco sério envolverá a interação entre várias partes do sistema. | Uma desvantagem no uso de HAZOP identificada é a falta de integração dos resultados para uma análise crítica do risco geral dos ativos. |
| Conduzir | As AR devem ser conduzidas através de todas as etapas do ciclo de vida da tecnologia incluindo desenvolvimento, implementação, mudanças e retirada. | Os estudos com HAZOP são uma das ferramentas estruturadas de AR mais adequadas nos últimos estágios do projeto detalhado para examinar as instalações operacionais e quando as alterações nas instalações são feitas. | HAZOP é aplicável aos diferentes ciclos de vida na cibersegurança de um SCAI, podendo ser aplicada nas fases de conceito, projeto, instalação, operação e desativação. |
| Documentar | A metodologia de AR e os resultados da AR devem ser documentados. | A força principal do HAZOP é que ela apresenta uma abordagem sistemática, disciplinada e documentada. Para obter todos os benefícios de um estudo HAZOP, ela deve ser adequadamente documentada e seguida. | Devido a sua abordagem, HAZOP é bem qualificada para ser empregada na cibersegurança industrial. |
| Manter | Registros de avaliação de vulnerabilidades atualizados deve ser mantido para todos os ativos compreendendo o SCAI. | Um dos estilos de registro de HAZOP é o por exceção, esse envolve o registro apenas dos perigos e problemas de operabilidade identificados juntamente com as ações de acompanhamento | O estilo de registro de HAZOP é viável para documentar as vulnerabilidades. |

Fonte: Elaboração do Autor

## 4. CONSIDERAÇÕES FINAIS

Foi possível observar a convergência das normas para o tratamento dos requisitos de segurança de processos e de cibersegurança. Ambas se traduzem em custo, impacto e riscos significativos para todos os segmentos industriais e, em particular, de infraestruturas críticas, tais como energia e telecomunicações. O ataque cibernético pode efetivamente ser tratado, no âmbito da segurança de processos, como uma causa potencial de falha, juntamente com outros fatores, tais como o erro humano, as falhas nos sistemas de controle, na instrumentação e nos equipamentos em geral. Este estudo preliminar demonstrou compatibilidades significativas entre os requisitos da IEC 62443[2] para uma AR da cibersegurança industrial utilizando os procedimentos da técnica de HAZOP na IEC 61882[1]. Faz-se necessário o prosseguimento dos estudos, objetivando um maior detalhamento dos requisitos e na estruturação de uma abordagem que caracterize adequadamente as ameaças cibernéticas como riscos de processos e as contramedidas sistêmicas às vulnerabilidades, como barreiras de segurança de processos. Isto tornará possível integrar as medidas de tratamento que consigam prevenir ou mitigar os riscos. Conclui-se que a técnica de HAZOP possui uma potencial aderência em termos de sua aplicabilidade para o tratamento dos riscos cibernéticos, como evento impactante na segurança de processos industriais.

## 5. REFERÊNCIAS


[1] STANDARD, British. **BS IEC 61882 Hazard and Operability Studies (HAZOP Studies)-Application Guide**. 2001.

[2] INTERNATIONAL ELECTROTECHNICAL COMMISSION. IEC 62443-2-1:**Establishing an industrial automation and control system security program**. 2010.

[3] ABNT. **Gestão de Riscos – Princípios e diretrizes**. NBR ISO 31000. Associação Brasileira de Normas Técnicas. 2009.

[4] BAYBUTT, P. **Sneak Path Security Analysis (SPSA) for Industrial cyber security**. Intech, v. 51, n. 9, set. 2004.

[5] BRANQUINHO, Marcelo Ayres et al. **Segurança de Automação Industrial e SCADA**. Elsevier Brasil, 2014.

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION et al. **IEC 60300-3-9: 1995 Risk Management: Part. 3 Guide to Risk Analysis of Technological Systems**. IEC: Geneva, Switzerland, 1995.

[7] DAVAADORJ, NYAMBAYAR; KOSHIJIMA, ICHIRO. **SAFETY AND SECURITY INTEGRATION FOR THE PRODUCTION INDUSTRY UNDER THE RESILIENCE MATRIX**. WIT Transactions on The Built Environment, v. 174, p. 203-211, 2018.