Plataformas de Inteligência Artificial vão dominar o mundo?

Uma análise crítica a partir da segurança cibernética de infraestruturas críticas

Autores: Marcelo Branquinho & Plataforma Safer
Data: 03 de agosto de 2025

Resumo

O artigo propõe uma reflexão crítica sobre a aplicação da Inteligência Artificial (IA) em infraestruturas críticas, como plantas industriais, subestações de energia, refinarias e sistemas de bombeamento. Ele argumenta que, embora a IA represente avanços significativos, sua autonomia total em decisões operacionais nesses ambientes é tecnicamente inviável e normativamente inaceitável.

A principal preocupação não está na IA em si, mas na delegação de funções críticas sem supervisão humana, o que pode comprometer a integridade e a segurança dos sistemas. Em setores regulados por normas como a IEC 62443, o NIST SP 800-82r3 e a RO-CB.BR.01 do ONS, decisões automatizadas devem ser sempre validadas por operadores humanos, com rastreabilidade e governança robusta.

A IA deve ser usada como ferramenta de apoio analítico, jamais como substituto da decisão humana. A segurança cibernética, nesse contexto, exige uma abordagem estruturada, com forte base em governança, ética e normas técnicas, sendo papel dos SOCs industriais garantir esse equilíbrio entre tecnologia e responsabilidade.

Keywords: Inteligência Artificial, Infraestruturas Críticas, Segurança Cibernética Industrial, IEC 62443, NIST SP 800-82r3, RO-CB.BR.01, Governança, SOC Industrial, Confiabilidade Operacional, Decisões Automatizadas, Supervisão Humana, Resiliência Cibernética, Tecnologia Operacional (TO)

POWERED BY SAFER

Introdução

O crescimento acelerado da Inteligência Artificial (IA) nos últimos anos tem gerado debates acalorados e, por vezes, polarizados sobre o seu impacto na sociedade, na economia e na autonomia humana. Em um extremo, há o temor de que as máquinas venham a "controlar" ou "dominar" as decisões humanas, assumindo funções que hoje são delegadas exclusivamente à racionalidade e ao julgamento técnico de pessoas. No outro extremo, surgem expectativas elevadas sobre a capacidade da IA de revolucionar setores inteiros, solucionando problemas complexos, otimizando processos e promovendo ganhos de escala e eficiência impensáveis até pouco tempo.

Entretanto, quando o olhar se volta para o contexto das **infraestruturas críticas**, como redes elétricas, sistemas de abastecimento de água, refinarias, plantas industriais ou estações de bombeamento, a discussão adquire contornos mais graves e específicos. Nesses cenários, qualquer erro decisório pode provocar não apenas perdas financeiras ou reputacionais, mas também impactos reais sobre a vida humana, o meio ambiente e a soberania nacional. A IA, nesse contexto, não pode ser encarada apenas como um avanço tecnológico, mas sim como uma variável sensível dentro de uma equação de risco. A aplicação de IA em sistemas industriais exige cuidados redobrados com ética, confiabilidade, auditabilidade e, sobretudo, governança clara. É neste ponto que este artigo se propõe a aprofundar a análise, com foco nas exigências técnicas, normativas e operacionais que envolvem a utilização segura e eficiente da IA em ambientes críticos, especialmente dentro de centros de operações de segurança cibernética (SOCs).

A IA vai controlar tudo? Não — e nem deve

A ideia de que a IA se tornaria autônoma a ponto de dominar sistemas industriais ou tomar decisões críticas é tecnicamente infundada e

normativamente inaceitável. Para que uma IA possa tomar decisões complexas de forma autônoma em ambientes industriais, ela precisaria não apenas entender o contexto operacional e físico em tempo real, mas também antecipar consequências multivariadas de suas ações, o que ainda está fora do escopo da tecnologia atual. Além disso, sistemas de IA não possuem consciência situacional ou ética; suas decisões são guiadas por padrões aprendidos, o que os torna suscetíveis a erros quando enfrentam cenários fora do treinamento.

Modelos de IA, sejam eles baseados em redes neurais profundas, machine learning supervisionado ou algoritmos de correlação de eventos, operam a partir de dados e regras delimitadas por humanos. Ou seja, o modelo aprende com base em dados históricos, que por si sós não garantem previsibilidade ou confiabilidade absoluta em situações operacionais dinâmicas. Quando se trata de infraestruturas críticas, qualquer margem de erro pode ser catastrófica, e confiar cegamente em algoritmos sem a devida validação humana compromete a segurança e a resiliência do sistema.

O perigo, portanto, não reside na IA em si, mas na delegação irrestrita de funções críticas sem mecanismos de supervisão, validação e responsabilização. Em vez de substituir operadores humanos, a IA deve atuar como um reforço inteligente, oferecendo apoio analítico, identificando padrões e fornecendo recomendações, sempre com a possibilidade de intervenção humana. Esta abordagem preserva a integridade operacional e garante que as decisões estejam alinhadas com normas técnicas, valores éticos e princípios de responsabilidade institucional.

Ambientes industriais exigem controle rigoroso de alterações operacionais, rastreabilidade de decisões e previsibilidade de ações. Normas como a **IEC 62443**, o **NIST SP 800-82r3** e diretrizes como a **RO-CB.BR.01** do ONS impõem que toda decisão automatizada que possa impactar a continuidade operacional deve ser submetida à

validação humana. Assim, é essencial compreender que o papel da IA deve estar subordinado a um arcabouço de governança robusto.

Em ambientes como subestações de energia, plantas de cloro-soda ou estações de bombeamento, qualquer falha provocada por uma decisão automatizada errada pode causar prejuízos ambientais, financeiros ou mesmo riscos à vida humana. Portanto, é não apenas desejável, mas obrigatório, que a IA atue como **copiloto inteligente** e **não como piloto autônomo**.

IA como copiloto: o modelo ideal para ambientes industriais

O papel da IA em um centro de operações de segurança cibernética é funcionar como um multiplicador de capacidades analíticas, fornecendo suporte decisório em tempo real e ampliando a capacidade da equipe de responder com agilidade a potenciais incidentes. A IA consegue processar grandes volumes de eventos gerados por ativos industriais, redes de controle e dispositivos de acesso remoto, classificando-os em níveis de criticidade e relevância com base em padrões históricos e comportamentais.

Entre suas funções mais relevantes, destacam-se a capacidade de detectar desvios de padrão em protocolos industriais, a identificação de atividades incomuns em redes segmentadas, a sugestão de respostas com base em playbooks de segurança e a priorização de eventos conforme o impacto previsto sobre os processos industriais. Essa habilidade é fundamental para lidar com a complexidade crescente dos ambientes de tecnologia operacional, onde milhares de eventos podem ocorrer simultaneamente e a resposta a um falso positivo pode comprometer a estabilidade da operação.

Por exemplo, em uma instalação de transmissão de energia, a IA foi empregada para analisar continuamente os fluxos de dados entre controladores e equipamentos de campo. Durante uma madrugada, detectou-se um comportamento atípico de leitura e escrita em

registradores que normalmente não sofrem alteração fora do horário de expediente. A IA correlacionou este padrão com registros anteriores de anomalias semelhantes e sinalizou o evento com alta prioridade. A equipe do SOC investigou e constatou que uma estação de trabalho havia sido acessada por um colaborador externo fora da janela autorizada, permitindo a rápida contenção do incidente.

Em outro cenário, numa planta industrial do setor químico, o sistema de IA identificou múltiplas alterações simultâneas em arquivos de configuração e aumento no tráfego de rede em portas tipicamente não utilizadas naquele ambiente. A IA sugeriu que esse comportamento se assemelhava a padrões de movimentação lateral usados por malwares do tipo ransomware. A equipe, alertada, optou por isolar o segmento afetado, conter o possível vetor de infecção e revisar imediatamente os acessos e permissões naquele setor.

Apesar de todo esse apoio, a IA jamais deve tomar decisões críticas de forma autônoma. Toda ação sugerida deve ser validada manualmente por operadores devidamente treinados, respeitando critérios técnicos, normativos e contextuais. A manutenção de registros de auditoria, a rastreabilidade de todas as etapas e a supervisão contínua são pilares que garantem que a IA seja um aliado estratégico e seguro, e não um risco operacional. Essa abordagem fortalece a confiabilidade dos SOCs e assegura que decisões de alto impacto permaneçam sob controle humano.

Normas e diretrizes: o limite claro do uso da IA em ambientes operativos críticos

As principais normativas de segurança cibernética para sistemas industriais são categóricas em limitar a autonomia plena de sistemas baseados em Inteligência Artificial em ambientes de infraestrutura crítica, pois tal autonomia conflita diretamente com os princípios de resiliência, confiabilidade e responsabilidade operacional. A norma

IEC 62443-3-3, por exemplo, estabelece que "medidas de segurança devem ser implementadas para garantir que apenas ações autorizadas e controladas sejam permitidas nos sistemas industriais" (SR 1.1 e SR 5.2). Essa exigência implica que qualquer processo automatizado, como os conduzidos por IA, deve possuir restrições e ser passível de supervisão humana. Além disso, a IEC 62443-4-2, no requisito CR 2.1, demanda que alterações no comportamento de dispositivos e aplicativos sejam sujeitas a processos de validação, teste e auditoria.

Complementarmente, o NIST SP 800-82r3, no item 6.2.2, reforça que sistemas de controle industrial (ICS) operam em ambientes onde o tempo de resposta humano é fundamental e que, por isso, a automação com IA deve sempre manter o operador humano no centro das decisões, inclusive nas respostas a incidentes automatizadas. A publicação enfatiza que "a presença humana é essencial para mitigar o risco de decisões incorretas baseadas em dados incompletos ou em padrões de comportamento que ainda não foram totalmente compreendidos".

Já a diretriz RO-CB.BR.01 da ONS, voltada ao setor elétrico brasileiro, determina que todos os acessos, comandos e alterações operacionais devem ser auditáveis, previamente autorizados e realizados de forma a garantir o controle pleno das ações nos sistemas de automação da cadeia de operação do SIN. Isso exclui a possibilidade de um sistema baseado em IA executar comandos de forma não supervisionada ou sem rastreabilidade.

Portanto, essas normas e diretrizes formam uma base sólida que deixa claro: a IA pode ser uma ferramenta poderosa para análise, correlação e recomendação, mas jamais deve operar de forma autônoma em processos industriais críticos sem a devida validação e autorização humana.

A **IEC 62443-4-1** define que qualquer alteração em software, incluindo sistemas de IA, deve ser auditável, validada e testada. A **IEC 62443-3-3**

exige que medidas de controle sejam atribuídas a cada nível de segurança e que sistemas críticos sejam segregados de redes administrativas e públicas. O **NIST SP 800-82r3** destaca a necessidade de supervisão humana nas operações de resposta a incidentes automatizadas.

Na prática, a aplicação desses princípios implica que:

- A IA pode sugerir respostas, mas não executá-las sem validação.
- A comunicação entre zonas (conduítes) deve ser monitorada por ferramentas com IA, mas controlada por regras estáticas.
- Toda ação precisa ser logada, rastreada e revisada.

Considerações finais

A visão de que a IA vai dominar o mundo não resiste à análise técnica e normativa em ambientes industriais. Embora a IA represente uma evolução importante na capacidade de análise, correlação e previsão de incidentes, ela deve ser vista como uma aliada estratégica, e não como uma entidade capaz de assumir o controle decisório de forma autônoma. A segurança cibernética de ambientes operacionais exige um entendimento profundo do contexto, da criticidade dos ativos, da lógica de operação de processos industriais e das consequências de ações automatizadas. Essas camadas de interpretação e responsabilidade ainda são inatingíveis por qualquer sistema automatizado, por mais sofisticado que seja.

É possível e desejável utilizar IA para melhorar a segurança, a eficiência e a resposta a incidentes. A IA pode ser empregada para identificar padrões anômalos de comportamento em redes industriais, correlacionar eventos dispersos em múltiplos domínios, e sugerir respostas baseadas em conhecimento acumulado. No entanto, essas sugestões devem ser sempre validadas por operadores humanos que compreendem o ambiente de forma holística, levando em consideração aspectos técnicos, operacionais e organizacionais. O papel da IA, portanto, é de copiloto: ela fornece dados relevantes,

antecipa riscos e recomenda ações, mas quem define o rumo, aplica os comandos e responde pelas consequências continua sendo o ser humano.

É inaceitável que a decisão final sobre sistemas críticos seja delegada a um sistema autônomo porque isso comprometeria os princípios de governança, responsabilidade e rastreabilidade exigidos por normas como a IEC 62443 e o NIST SP 800-82r3. Em caso de falhas ou incidentes, deve estar claro quem autorizou cada ação, com base em qual contexto e sob quais premissas. Apenas o ser humano pode assumir essa responsabilidade de forma legítima. Por isso, em vez de buscar substituir operadores e analistas, o uso de IA deve estar voltado para elevar suas capacidades, reduzir sua carga cognitiva e permitir decisões mais ágeis, conscientes e seguras.

O caminho seguro é aquele em que IA e operadores humanos atuam em sinergia. A IA amplia a visão, mas é o humano que escolhe a direção. Nesse modelo, ganhamos em produtividade sem comprometer a segurança, e construímos plataformas de defesa mais resilientes, confiáveis e alinhadas às boas práticas internacionais.

Assim, a resposta à pergunta "Plataformas de IA vão dominar o mundo?" é clara: **não, desde que os humanos continuem dominando a IA.**