



ICS
DEFENSE
FORCE

INTEGRATING AI SAFELY IN INDUSTRIAL OPERATIONS

5 OT AI MYTHS THAT CREATE OPERATIONAL RISK



Myth: IT AI policies cover OT.

Reality: OT AI requires engineering approval, defined authority and strict limits on what models may observe, recommend or control.



Myth: Operations will continue normally if AI fails.

Reality: Stale data, corrupted inputs or unsafe outputs can affect safety. Define failure states, manual fallback and tested recovery.



Myth: Updated AI is safe AI.

Reality: Statistical accuracy doesn't ensure safety. Define safety thresholds, human engineering validation with override authority.



Myth: Vendor testing proves an AI system is ready for OT.

Reality: Vendor testing cannot reproduce site-specific equipment, control logic or process conditions. Validate abnormal states and safety scenarios before deployment.



Myth: An approved AI tool is safe to install "out of the box" into OT.

Reality: Use segmentation, least privilege read-only connections. Direct control actions require engineering approval based on cyber-physical consequences.

CONNECT



icsdefenseforce.com