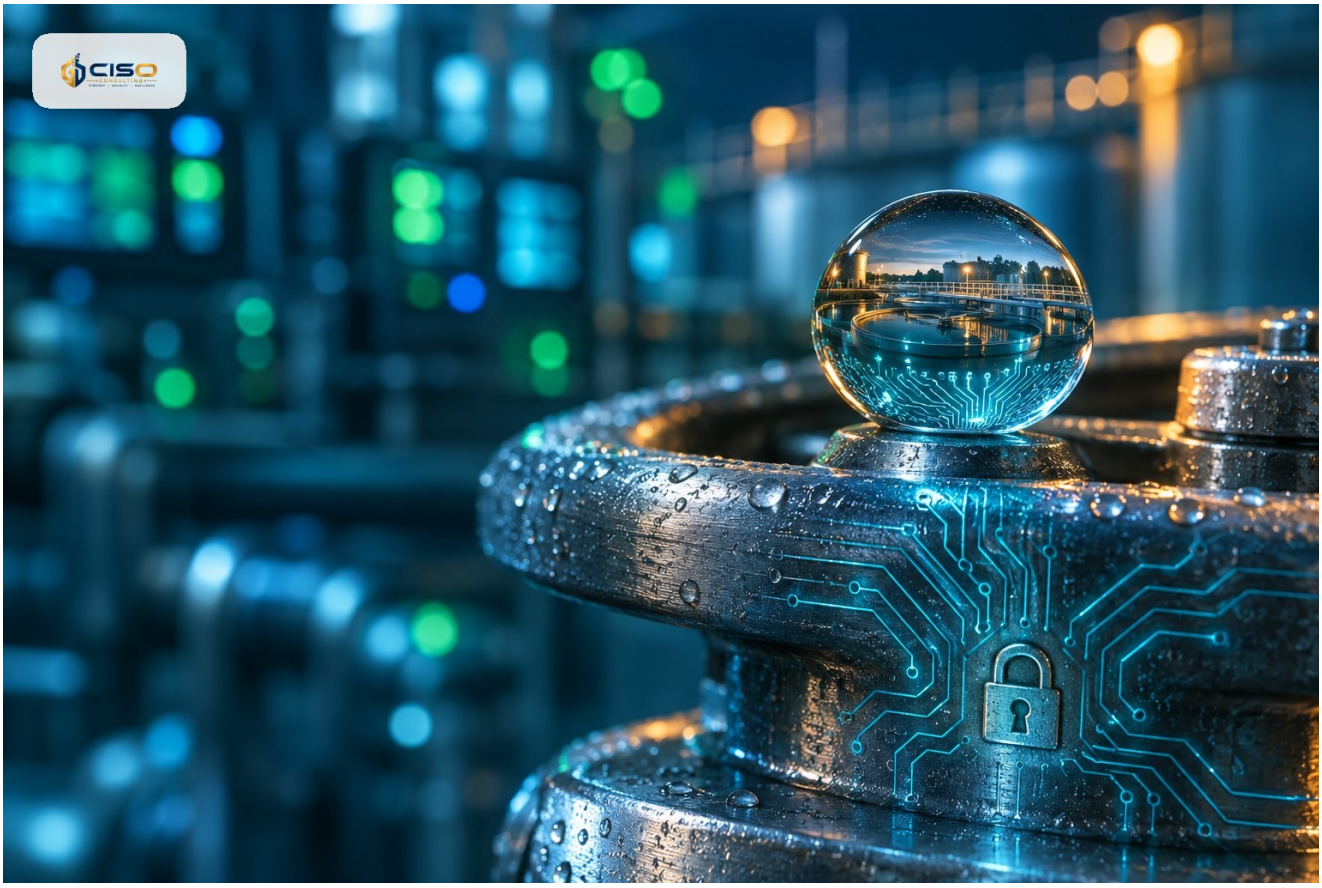
NIST Blog Turns Attention to Securing Water and Wastewater OT Environments



A NIST cybersecurity blog post addresses securing OT in water and wastewater. The text available to us gives only the author's background, so the post itself should be read before acting.

- The NIST post is titled Securing Water and Wastewater Operational Technology Environments.
- The excerpt describes its author, CheeYee Tang, as an electronic engineer at NIST focused on OT cybersecurity research.
- Tang co-authored NIST SP 800-82 and NIST IR 8576, guidance on critical infrastructure and OT cybersecurity.
- The author has over 20 years of experience in product development and embedded systems, and previously led software engineering teams in rail and telecom.

> - The excerpt contains no technical recommendations, so the full post is needed for specifics.

What the source says

NIST has published a cybersecurity blog post titled Securing Water and Wastewater Operational Technology Environments. The portion of the source available to us is the author biography rather than the article's content, so we do not summarise any findings or recommendations here.

The author, CheeYee Tang, is an electronic engineer at NIST working on cybersecurity research for operational technology (OT). Tang co-authored **NIST SP 800-82** and **NIST IR 8576**, both guidance on critical infrastructure and OT cybersecurity. Tang has more than 20 years of experience in product development and embedded systems, and earlier led software engineering teams in the rail and telecom sectors.

Why it matters for Saudi operators

Water and wastewater services depend on OT, and organisations that own, operate or supply such environments in the Kingdom may find the post a useful reference. The author's involvement in SP 800-82 suggests the post is related to that body of guidance, but the excerpt does not state how, so this should be confirmed from the full text.

Suggested approach

Treat this as a prompt to review rather than a call for urgent change. Read the full post, then compare its content with your current OT security programme and with the NCA OTCC controls that apply to you. Record any gaps in your normal risk register and plan remediation through existing governance.

What to do now

1. Read the full NIST post and note any recommendations relevant to your OT environment.
2. Check how it relates to NIST SP 800-82 and NIST IR 8576 if you already use them as references.
3. Compare your water or wastewater OT controls against the applicable NCA OTCC requirements.
4. Log any gaps found in the risk register with an owner and a target date.