AMERICAN WATER WORKS ASSOCIATION AND WEST YOST: HOW CONSEQUENCE-DRIVEN CYBER-INFORMED ENGINEERING (CCE) HELPED US TO BE MORE RESILIENT

THURSDAY: SESSION 4, TRACK 1

SESSION CHAIR

Tim Klett, Idaho National Laboratory

SPEAKER

Andrew Ohrt, West Yost Associates

SESSION ABSTRACT

Consequence-driven Cyber-informed Engineering (CCE) is a methodology developed by Idaho National Laboratory (INL). To-date it has been applied to protect facilities within the Nuclear and Energy sectors from cyber attacks. West Yost is working with INL to adapt this methodology to the water sector. This methodology assumes that if a SCADA system is targeted by a persistent and capable threat actor, it will be compromised. Based on this assumption, the West Yost team designs SCADA systems in such a way that a utility will still be able to confidently carry out its mission of delivering drinking water to customers, even if the SCADA system is compromised.

This design approach includes use of modern automation, but with such things as hard-wired controls (i.e. Hand/Off/Auto switch) to allow for control in the absence of automation or mechanical backstops that physically prevent a compromised control system to result in damage to physical assets. As an example, if well flushing valves are currently wired for control from the PLC, they may not be functional if the SCADA system were compromised.

This approach may be similar to design approaches already implemented in a City's systems. CCE builds on these existing approaches and allows for a consistent approach to prevent over-reliance on automation during design and subsequent operation.