

Inside ExxonMobil's live rollout of open process automation

By Len Vermillion

Distributed control systems (DCS) that run chemical plants or refineries have traditionally been a closed box. They use one vendor's hardware, one vendor's software, and one vendor's roadmap. That's been going on for decades. At YNOW2026, Yokogawa's User Conference & Exhibition, ExxonMobil Systems Engineer Toriano "Tito" Jackson stood in front of attendees and described what happens when a company decides to break that box open on a live production unit.

Jackson's session *Open Process Automation (OPA) in Practice: How We Modernized a Live Chemical Plant and What We Learned* was less a product pitch than a field report. Jackson has

spent 16 years as a control systems engineer at ExxonMobil facilities around Baton Rouge, La., the last four of them implementing and now maintaining an OPA system built in collaboration with Yokogawa. He was candid that the transition was not, in his words, "a cakewalk."

"I can talk about OPA and my experience all day long," Jackson told the audience. "But it wasn't easy at first."

OPA explained

For attendees unfamiliar with the standard, Jackson broke down OPA in plain terms. It's a vendor-neutral, standards-based control architecture designed to end the proprietary lock-in that has

defined DCS and programmable logic controller (PLC) markets for generations. Under a traditional DCS, a plant's control hardware, engineering software and human-machine interfaces (HMIs) typically all come from a single supplier. So upgrades, replacement parts and new capabilities are constrained by that vendor's product cycle and pricing.

OPA, developed through the Open Process Automation Forum (OPAF), instead defines open interfaces and a common standard, called O-PAS, so that controllers, input/output modules and software from different suppliers can be mixed within a single system. Jackson's analogy for the audience was simple: it should work the way a USB

“The best answers come through real operational experience, not a lab.”

—Toriano "Tito" Jackson,
Systems Engineer, ExxonMobil



02

drive works when plugged into any laptop.

“With OPA standards, you have that mindset with the products, and you should be able to plug and play with anything,” he said.

The system’s key elements, he noted, are interoperability, modular plug-and-play hardware and cybersecurity built into the architecture rather than bolted on afterward.

A founding partnership

ExxonMobil brought the original demand for an open standard to the industry in 2016, frustrated by the total cost of ownership and inflexibility built into closed control systems. Yokogawa joined as one of the forum’s founding member companies, committing its own engineers to technical and administrative leadership roles within OPAF as the standard took shape.

The relationship became concrete when Yokogawa was selected as ExxonMobil’s system integrator to move OPA from test-bed concept to the first field trial on an operating Gulf Coast production unit. It’s the same collaboration, refined over roughly a decade of joint research and pilot work, that Jackson now maintains day-to-day.

Minimizing disruptions

Jackson described a project built around minimizing disruption. The plant’s legacy DCS cabinets were swapped out during a planned outage window, with the physical cutover to the new system completed in roughly one to two weeks. They were replaced by a much smaller

control room built around industrial PCs and remote I/O rather than dedicated proprietary controller hardware.

Economics were part of the motivation for the transition, he said. Legacy DCS controllers, according to Jackson, can run \$10,000 apiece, and when they fail, replacement or repair often means shipping a board back to a single manufacturer with no competitive alternative. The industrial PCs used in the OPA build, by comparison, cost closer to \$1,800.

Removing vendor lock-in, he said, let the facility make hardware decisions based on what the plant needed rather than what one supplier happened to offer.

Lessons learned

Jackson didn’t gloss over the rough patches. Early in the deployment, roles were blurred. As the resident systems engineer, he found himself fielding calls not just on control-system issues but on instrumentation and field problems that operations and application engineers used to route elsewhere.

In one incident, routine maintenance on a Windows-based virtual machine caused an operator to briefly lose control of the console. The scare was resolved without any product loss, but Jackson said it underscored how essential constant communication between operations, engineering and vendors becomes in an open architecture. The facility also ran one operator through months of firsthand training during the buildup so that person could then train colleagues once the system went live.

The team’s first major system upgrade was bumpy, with intermittent loss of console control traced to software that hadn’t been fully burned in on the test bed before deployment. Since then, Jackson said operations have smoothed

out considerably to the point that he described going months without a first-hand intervention.

Real-world stress test

Roughly a year and a half into live operation, Jackson pointed to fewer cable failures, a sharp drop in support calls and a clean result from a third-party vulnerability assessment as results of the project. Testers found one critical firmware issue that the team had, in fact, already scheduled to patch.

He also described weathering multiple full-power outages, including one that knocked out grid power to the surrounding area for about six hours. The plant’s uninterruptible power system kept the OPA platform running throughout, with battery capacity to spare.

For Jackson, that kind of unplanned, real-world stress test carries more weight than any demonstration. “The best answers come through real operational experience,” he said, “not a lab.”

Jackson closed by summarizing the payoff as he’s seen firsthand, including architectural flexibility, reduced dependence on any single supplier, a stronger cybersecurity posture and a control system built to absorb innovative technology rather than resist it.

He was careful to point out that the benefits he discussed are specific to his own plant’s experience, and there’s no guarantee every plant would see the same results. So, operators should consider their goals and ability to withstand rough patches in the transition before proceeding. ∞