IT'S HIP TO BE EQUIPPED

Increase value and update functionality by merging and modernizing IT and OT environments.

Operational technology (OT) networks that run industrial control systems for critical infrastructure historically have been isolated from information technology (IT) networks. The two networks have traditionally remained segregated, resulting in reduced impacts on operational systems from malicious actions against the IT network.

IT environments in this design are regularly updated, taking advantage of new features and capabilities. However, OT environments are commonly left behind, increasing the likelihood of reduced resiliency, increased technology debt and new cyber vulnerabilities on the OT network.

This creates a range of issues for critical infrastructure owners and operators. Without a way to support or use aging systems affordably, organizations lose the ability to protect critical assets or gain new business insights.

Leveraging the value of digitization means making effective use of data no matter where it lives. In many organizations, this means harnessing the value of data in OT environments for the first time.

To do so, the OT network must be modernized and integrated with the IT network. Connecting these systems requires considerable planning, but successful execution yields reductions in operational expenditures, new ways to serve customers, and opportunities to create new revenue streams through existing assets, better data management and analytics.

"A modernized, integrated IT/OT environment allows you to extract the data from the OT environment and leverage it in your IT environment," says Kevin Fuller, managing director of security and risk consulting at 1898 & Co., a business, technology and security solutions consultancy, part of Burns & McDonnell. "All the fun stuff you want to do with data — build better methodologies, utilize data analytics, form classifications, and improve business continuity and threat protection — begins with a modernized OT environment."

INFORMATION TECHNOLOGY

Undertaking such a program begins with a well-formulated strategy centered on business cases that drive real value.

It's important to establish the business value and the strategy's return on investment to garner organizational buy-in that withstands leadership changes.

"What are the goals of the organization?" asks Dirk Mahling, a principal consultant at 1898 & Co. "You must meet the strategic goals of the company — which likely include operational expenditure reduction through innovation. Having a robust business justification is paramount to supporting successful IT/OT network modernization and convergence."

Once the value of the program is solidified, applying a plan-build-run methodology charts the way forward.

EXPLORE HOW IT/OT CONVERGENCE PROVIDES SUBSTANTIAL BUSINESS VALUE.
burnsmcd.com/TwoBecomeOne

In the last decade, organizations that maintain critical infrastructure have moved toward a security-by-design model, embedding security into the physical design of their networks. Carefully considering each piece of a system is important in this model, informing which assets must be secured, which data flows are most critical and what network behaviors are accepted.

Redundancies and safeguards also must be considered during this process to increase network reliability and resiliency.

It is important to understand how system changes will impact regulatory compliance as the program progresses. All industries have regulations to follow; meeting those requirements is one vital step on the way to future success.

Whether the planning phase uncovers the need for new security measures or updated software and hardware for the entire system, the build phase relies on adaptable execution. Geopolitical, regulatory and administrative changes will influence the process, making flexibility key.

Keeping organization leaders informed during the planning phase minimizes the impact of changes during the build phase. Because of the program's broad impact, support groups — such as IT, security, engineering and operations staff — should receive continued communication and training.

The most significant piece of the run phase relies on attitude changes within the organization. Existing technology debt creates a gap in staff knowledge, meaning operators must be trained to use the new systems. Maintaining system relevancy requires constant updating; staff will need a mindset of change to avoid further technology debt. A shift in operations and maintenance cost is necessary to achieve this, likely changing the expenditure model of the organization.