1898 & CO.SM
PART OF BURNS McDONNELL

WHITE PAPER / **OPERATIONAL TECHNOLOGY MODERNIZATION**

Strategic considerations for modernizing OT networks

BY Steve Dresie, Dirk Mahling AND Robb Montgomery

IT and OT networks have traditionally been isolated from one another. But bringing the two together offers exponential business value. Understanding the drivers and considering the technical aspects of integration allow for a successful and effective modernized network.

What is OT modernization?

Industrial Control Systems (ICS) are leveraged to support critical infrastructure throughout the world. These systems are the technological backbone for the sustainment of energy, water, transportation, advanced manufacturing and communication systems. ICS devices run on operational technology (OT) networks that typically undergo minimal change from year to year. Reliability is the highest priority for OT networks because an outage disrupts every service that relies on that network.

Historically, information technology (IT) networks and OT networks were isolated from one another. The OT network ran in a physically secure location, disconnected from the outside world, to reduce the likelihood of malicious actions impacting the network's uptime. This segmented network architecture offered a basic level of protection to the control systems due to the nature of access control; only physical access to the environment would yield access to the industrial control systems.

This design, while highly secure, offered few opportunities to streamline operations across multiple sites and limited the advanced features of newer equipment available to organizations. However, many organizations have abandoned the segmented network architecture in favor of an integrated network. This change is often implemented to reduce the administrative burden of managing multiple networks and exploit the advantages of an interconnected system. This wave of integrations is frequently referred to as IT/OT convergence.

OT modernization, then, takes a new perspective on this change by seeking to understand the business value of integrating the IT and OT networks and considering the technical aspects of integration. Placing the business drivers at the front of the discussion allows stakeholders to align on business priorities and reduces the challenges that can arise throughout the project's execution. Thus, an OT modernization project will deliver positive business value as opposed to simply trying to deal with a technology problem.

OT modernization projects delivery positive business value instead of simply trying to deal with a specific technology problem.

Drivers to modernize

OT modernization projects must begin with the examination of the use cases that drive the need to integrate and update the OT network. Every organization is unique, so use cases will be unique. Four key needs tend to rise to the top as the most common drivers to modernize: the need for data, prediction capabilities, decision support and balancing security with operations.

Right data at the right time, at the right level

Data drives business. Access to the right data at the right time allows organizations to make the decisions that grow their business, control their costs and stop issues before they occur. The segmentation of IT and OT networks adds complexity in data exchange and slows system integration, potentially preventing access to the right data. A modernized OT network securely bridges the gap between the IT and OT networks to permit the seamless transfer of data from the OT environment to the IT network where traditional management systems can be used to monitor, audit and analyze operations.

With the ability to move data in a more seamless fashion, a whole new world of systems and capabilities become available. OT systems in the past were seldom able to access systems such as big data platforms, analytics engines, and public and private cloud resources. IT networks can be challenged to assess asset performance data stored in time-series engines, real-time operational status and facility maintenance. An integrated network enhances organizational agility by enabling the exchange of data between technology systems that allow the view of data to widen at the pace required by the business to make decisions.

Historical data drives toward predictive capabilities

In a segmented OT network, data analytics is constrained to the capacity and capability of the local historian. Large-scale analytics systems are often deployed on virtual infrastructure in private or public clouds. In a modernized OT environment, the data exchange between the IT and OT networks enables operational data to be ingested by data lakes or warehouses and then consumed by an analytics pipeline. These tools drive an organization to analyze historical data, unleashing the potential of predictive capabilities not previously possible.

Predictive analytics is often associated with predictive maintenance or asset failure prediction. These are valuable use cases which increase availability of high-value assets and

decrease operational costs. The combination of historical asset information and operational performance with existing business systems opens the door for new possibilities. Predicting holistic business outcomes that combine traditional operational data in combination with business system enables faster decisions and increased business agility. These capabilities are the cornerstones of digital transformation and organizational agility initiatives.

Supporting rapid decision-making

Organizations can gain a greater view of their operations and support decision-making with actionable information gathered by the interconnected systems. This puts the data in the hands of the decision-makers much faster than waiting for a report to be generated and manually disseminated. With business environments changing rapidly, modernized OT environments can enable organizations to keep pace with the changes occurring around them with data-driven decision models.

Instead of focusing on a reactionary operation with visually or manually gathered data, information is gathered for the user and can be used for more detailed analysis through automation tools. This empowers the workforce to make decisions faster and more accurately to maintain operations more efficiently. Giving the workforce more capabilities for decision-making utilizes their historical knowledge of operations without the administrative burden of gathering and documenting information.

Balancing security and operations

To maximize their effectiveness, security controls need to be integrated into everyday processes and procedures; however, this can be more challenging as the complexity of an organization's environment increases. The primary goal of a business is to be profitable and often security is viewed as a hindrance to maximizing profitability. This may be due to the absence of planning, lack of consideration for security requirements during system development, or underestimation of the resources required to identify and address threats. There is no magic formula to determine the right balance between security and operations because the tolerance for risk changes from organization to organization.

The key to optimizing the balance between operations and security is in performing a thorough risk assessment. An evaluation of the risk associated with OT modernization is not immune to this assessment. The risk assessment should clearly define and understand the cost of modernization and help the organization to project the time frame necessary to realize the return on investment. Organizations will also uncover the negative impact or risk of not modernizing its operations. Ultimately, each organization needs to see that the benefits of modernizing outweigh the decision not to.

When to modernize

Understanding the drivers behind OT modernization projects is an important first step. This should be closely followed with an attempt to understand when modernization is appropriate. Just like the business drivers being unique for each organization, so are the indicators of when an organization should begin their modernization effort. There are three key modernization indicators and some warning indicators discussed below.

Modernization to support risk management

Modernization of OT environments can be used to support an enterprise risk management program. The ability to determine what assets are important results in the creation of a strategy for protecting those assets. This is an integral part of risk management. As the National Institute of Standards and Technology (NIST) points out in its Framework for Improving Critical Infrastructure Cybersecurity, every organization is different. Consequently, every organization must tailor its approach to securing its assets to their specific requirements.

In most organizations, OT assets are mission critical but often receive less attention than their IT counterparts. The life cycles of OT assets are typically longer and less tolerant of downtime than IT assets. Additionally, segmented IT and OT networks often preclude a holistic view of asset management.

There can be broad implications to the strategy employed to modernize OT networks. If an organization finds that aging OT infrastructure is presenting a significant risk to its operations, then the mitigation strategy might include a plan to upgrade, replace or decommission outdated assets. When considering a holistic risk management program, modernizing the OT environment can be a major enabler to understanding and reducing the risks facing an organization.

Current technology stack

Like any other technology investment, OT assets must be replaced when they are no longer supported by their manufacturer, no longer function and/or lack the capabilities needed by the organization. When faced with the need to update the existing technology stack, organizations should consider executing an OT modernization project to capitalize on the advanced features of new equipment as well as the benefits of the integrated network.

When examining its existing technology stack, an organization must identify legacy OT assets and applications that may inhibit modernization and integration efforts. These become priority upgrades in the early stages of the modernization effort and pose the greatest opportunity for increased business value early in the process. Organizations must also understand the constraints and requirements of OT systems — such as throughput, processing, timing, etc. — and test how they are impacted due to architecture changes. If the current requirements are not being met, they must enable the architecture to meet or exceed the current demands after modernizing. Most importantly, an organization must understand the flow of data within the environment so as to not affect the required communications streams. Successful modernization will speed up the data delivery and enable the enhanced analytics mentioned earlier.

Cybersecurity considerations

Security incidents have been on the rise since the early 2000s, increasing the focus and attention on the need for securing critical infrastructure around the world. Many of these systems were originally implemented more than 20 years ago, when information security and risk management were seldom considered by most companies or local governments. A successful cyberattack that results in service unavailability could have negative cascading effects on our way of life.

For many organizations with geographically dispersed sites, modernizing the OT environment opens the door to introducing a cybersecurity program for the first time in some locations. OT visibility tools can be implemented across geographic locations and provide a full view of assets, their current health, vulnerabilities, and potential security threats. If an organization lacks visibility and the ability to respond to security threats due to a segmented environment, considering an OT modernization effort will yield a more secure environment as well as operational efficiencies.

Hurdles to Implementation

The life cycle of an OT system pushes the boundaries of conventional wisdom of IT professionals regarding the upgrade of systems. Many OT systems have continued to operate for decades with very little change to the system, while IT is more sensitive and dependent upon software and hardware improvements. The mentality of "if it's not broken, don't fix it," can permeate throughout those responsible for maintaining the OT systems and owning the assets the system controls.

Obstacles to successful OT modernization

- Funding is not available to support the modernization effort.
- System has not reached end of life, or full investment cost not yet realized.
  - Hardware still performing as expected and can be replaced seamlessly on failure.
  - Capitalization of assets not complete.
- Modernization will not result in significant benefits.
  - Speed improvements not an issue.
  - Vendor still fully supports the system.
  - Integration with other data and systems will not realize benefit.
  - New staff can be easily educated on how to operate and maintain system, more so than a modern system.
  - System does not impact regulatory compliance.
  - Mobile technology not desired.
  - Operating costs lower than newer system.
- Other asset upgrades are ongoing, and schedule won't permit additional changes.
- Management perception is that the system is more secure as a legacy system than it would be if it were modernized.

While most of this paper identifies rationale for modernizing an organization's OT environment, modernization may not always be the best decision. This section will identify a few valid reasons not to pursue near-term modernization.

While the above may be valid reasons to hold off on modernization, the inevitable and increasingly rapid march of new technology and regulatory standards makes it impossible to avoid the investment forever.

How to modernize

Internal strategic alignment

The first step to successful modernization is to gain strategic alignment amongst key stakeholders and define clear business objectives. Without precise understanding of the objectives of the modernization, questions will arise throughout the effort concerning direction and value. Defining success upfront and gaining agreement from key decision-makers reduces churn and keeps the effort focused.

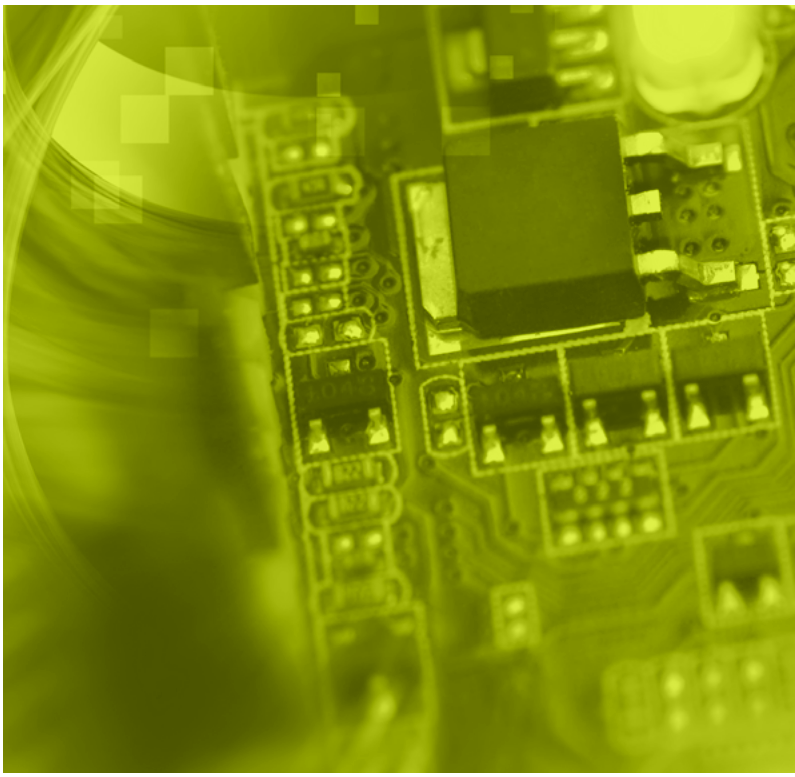
Once a tactical plan is aligned, organizations can execute it to make use of pilot groups and assets. This must be made a priority to gain early wins that show positive business value to validate the decision to modernize. Sticking to the plan even when challenges arise is important, but flexibility allows things to slow down when needed.

Finally, organizations must be willing to engage in difficult conversations and manage conflicts that arise. OT modernization efforts are long-term projects and may span multiple senior leaders. Those in charge must be able to reaffirm the decision to modernize and show the incremental successes that have been won and the business drivers that still hold true. Showing measurable added value through each stage of the project is instrumental in staying the course through leadership changes.

How to start a plan

Organizations can begin an OT modernization effort by compiling of a complete list of assets. Each asset should be tagged based on its business function, processes that leverage it, mission criticality and age. Assets can be grouped logically, such as those that require interaction and have aligned business purposes. To minimize access to certain processes and assets, organizations can define the segregation. A modernized OT environment will maintain a heightened degree of logical segmentation but access to the IT environment is based on the data needed for business processing and analytics.

Next, an organization can choose technologies to implement at an enterprise level that will cascade by process down to the system level. A road map can be created to assist in launching identified technologies segment by segment. Test cases should be robust, and results should convey confidence to stakeholders that the migration will be smooth and yield the desired results. Organizations must regularly revisit the plans to incorporate lessons learned along the way.



Technologies available to support modernization

There are many technologies available to support OT modernization efforts. Virtual Local Area Networks (VLANs) should be set up to virtually segment processes on the OT networks. This will reduce the ability to move laterally between separate OT systems. These VLANs are protected by an outer and inner firewall configuration known as a Demilitarized Zone (DMZ). The firewalls should be from different manufacturers to reduce the likelihood of a single vulnerability bypassing both firewalls. The inner firewall should be configured to only allow the required services to pass into the DMZ. The outer firewall configuration should only allow traffic that is required for the business functions.

To monitor systems inside the OT segments, a centralized logging system needs to be implemented. All OT devices that are capable of transmitting system logs should send them to this centralized logging server. In order to keep up with emerging modernization technologies, the centralized logging server needs to be built on virtualized infrastructure. This will allow for rapid deployment of new technologies with minimal added investment.

Conclusion

OT modernization is about more than just resolving the technical challenges of integrating your IT and OT networks. True modernization requires an understanding of the business needs and requirements that can only be supported by modernizing OT infrastructure. The effort is neither trivial or without its challenges; anchoring decisions on the business value of integrating IT and OT networks will make the decision process more fruitful. Successful modernization will provide increased access to operational data and prediction capabilities that were never possible. Improved real-time data will enhance decision support processes while balancing security and operational demands.

Biographies

Steve Dresie is the managing director of technology consulting at 1898 & Co., part of Burns & McDonnell. With more than 16 years of experience, Steve leads his team to build and implement innovative software solutions across multiple industries, helping clients operating their businesses more effectively and efficiently.

Dirk Mahling is a senior managing consultantat 1898 & Co., part of Burns & McDonnell. Having spent more than 17 years as a technology and consulting executive, Dirk understands regulated environments and their boundaries as well as the importance of using innovative thinking to provide solutions to modern challenges. His work is focused on bringing cost reduction and stakeholder satisfaction to clients.

Robb Montgomery is the director of enterprise systems and integration at 1898 & Co., part of Burns & McDonnell. As a leader in digital transformation, Robert and his group focus on cloud solutions, “internet of things,” data governance and other services. He has more than 25 years of experience in all aspects of IT, with extensive work in complex transformation program management and project delivery.

About 1898 & Co.

1898 & Co. is a business, technology and security solutions consultancy where experience and foresight come together to unlock lasting advancements. We innovate today to fuel your future growth, catalyzing insights that drive smarter decisions, improve performance and maximize value. As part of Burns & McDonnell, we draw on more than 120 years of deep and broad experience in complex industries as we envision and enable the future for our clients. For more information, visit **1898andCo.com**.

11686-OTM-0121