White paper
Public

The bridge to possible

Enabling DoD Maintenance, Repair, and Overhaul (MRO) Transformation through Industry 4.0 and Smart Manufacturing

Author: Todd Bower, Systems Architect, U.S. Navy Account Team, Cisco

The bridge to possible

About the Author

Todd Bower
Systems Architect

Todd Bower is a Systems Architect for the U.S. Navy Account team at Cisco Systems, Inc.

He works with the U.S. Navy to assist maintenance, repair, and overhaul (MRO) activities and organizations in the digital transformation of their networks.

This includes identifying mission requirements, providing technical guidance on the future direction of technology, and assisting in aligning solutions and implementation strategies.

Contents

List of Figures

The bridge to possible

What you'll learn

Network

How to connect machines and control systems with secure and standards-based industrial networks to improve operations, margins, quality, and safety.

Workforce

How to empower the workforce with innovative tools for faster problem solving and seamless collaboration.

Security

How to protect your industrial assets from cyberthreats to ensure the continuity and safety of shipyard operations.

Abstract

In the digital age, manufacturers succeed when they are connected, agile, and secure. Technology is leading the way as manufacturing and related industries embrace the fourth industrial revolution, also known as Industry 4.0.

Underpinning Industry 4.0 is a digital transformation that is sweeping across the manufacturing, mining, oil and gas, transportation, and other associated industries. It is modernizing their operations and helping them achieve greater insight and efficiencies. The transformational roadmap enacted by these industry leaders can be adapted to provide a secure platform that transforms Navy Shipyard MRO operations—delivering significant mission benefits for the U.S. Navy.

This paper will demonstrate:

- How to connect machines and control systems with secure and standards-based industrial networks to improve operations, margins, quality, and safety
- How to empower the workforce with innovative tools for faster problem solving and seamless collaboration
- How to protect your industrial assets from cyberthreats to ensure the continuity and safety of shipyard operations.

If properly implemented, technology can enable digital transformation to deliver on these three key functional capabilities. The results can drive increased effectiveness and efficiency in shipyard operations. This includes hyper awareness, informed decision making, and the ability to execute more quickly.

With the advent of Industry 4.0 and more connected devices and workers, a significant amount of data is generated where the ability to manage and analyze the data is a key differentiator to enable success.

Introduction

Timely deployment of the U.S. Navy's warships is directly linked to the operational efficiency of public shipyards and their ability to complete scheduled work on time, with the requisite quality, and at cost. The productivity and throughput at the four public shipyards are directly linked to the Navy's ability to meet operational requirements around the world.

Similar to the public shipyards, the manufacturing industry is critical to the U.S. and is responsible for one-third of the gross domestic product of our nation. The manufacturing industry has experienced multiple revolutions (mechanization through water and steam power) to mass production and assembly lines driven by electrical machines. The current revolution, which started around 2011, takes what was started with the use of computers and automation, enhancing it via fusion of the cyber and physical worlds. This is driven by increased value and performance achieved through smart autonomous systems powered by data, machine learning, and wireless mobility. This revolution is known as the fourth industrial revolution or Industry 4.0.

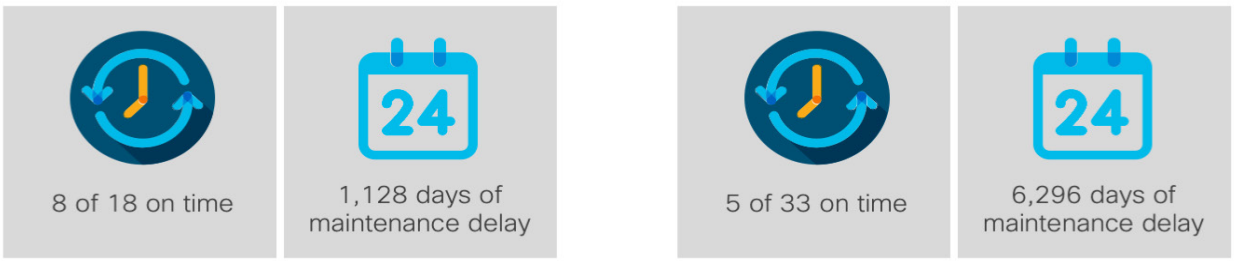
The Navy and its public shipyards must revolutionize and digitally transform by using the methods of success found in Industry 4.0. This transformation starts with the intelligent networking of machines and processes via Information Technology (IT) systems as its foundational platform. The Navy's public shipyards can leverage such platforms in a way similar to the manufacturing industry. By doing so they can achieve advances in automation, advanced robotics, artificial intelligence, and enhanced reality that make production more efficient, improve quality, and enhance safety.

The IT platform can also be expanded to reach the entire workforce using Wi-Fi 6 and 5G cellular service. And it can do so securely by leveraging Zero Trust Security Architecture and an intent-based network for configuration and management. A secure, resilient, flexible IT platform is essential to optimization of shipyard infrastructure and processes. By properly collecting and aggregating all the data generated from an IT platform, the Navy can then apply analytics and management solutions that let them better understand their data and, more importantly, turn that data into an actionable asset. By deploying a modern network the Navy can enable a connected workforce and all the effeciences that result; from the artisan to the expert, as well as provide additional access to backend office applications.

Industrial Automation

In the digital age, naval shipyards have fallen behind in modernizing their processes for use as a tool to keep up with the increasing demand for maintaining, overhauling, and repairing ships in the fleet. This is reflected in the findings from GAO report GAO-20-588, that indicates the Navy's four shipyards completed 38 of 51 (or 75 percent) of maintenance periods late for aircraft carriers and submarines with planned completion dates in fiscal years 2015 through 2019. This equaled a combined total of 7,424 days of maintenance delay. For each maintenance period completed late, the shipyards averaged 113 days late for aircraft carriers and 225 days late for submarines. **Figure 1** presents a summary of the maintenance delays at Navy Shipyards for Fiscal Years 2015 through 2019.

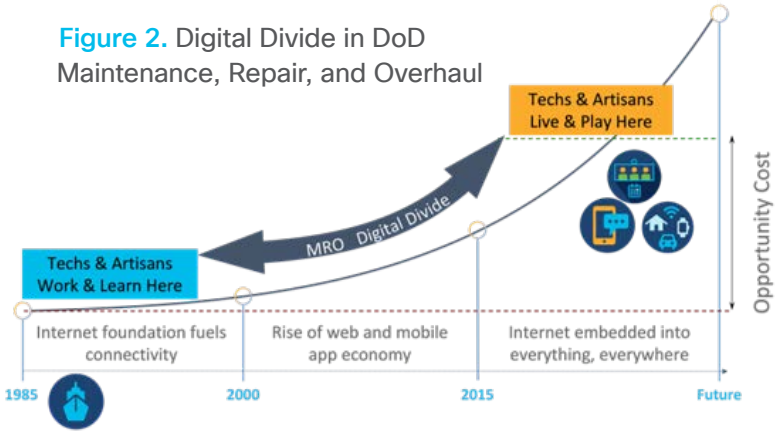
Figure 1. FY15 through 19 Maintenance Delays at U.S. Navy Shipyards



Source: GAO analysis of Navy data (text);U.S. Navy/T. Nguyen (aircraft carrier), U.S. Navy/D. Amodo (Submarine). GAO-20-588-6123P001.

Currently, there is a digital divide in the Department of Defense (DoD) MRO sector. The technicians and artisans live with current technology at home, outside of the workplace. This includes real-time video calling and messaging. But at work they're using outdated and far older (and slower) methods of communicating with their peers, higher management, and experts. **Figure 2** shows how the digital divide occurs at Navy Shipyards.

Figure 2. Digital Divide in DoD Maintenance, Repair, and Overhaul



Every day a ship is not ready to deploy, it is not part of the force defending the nation from ever growing global threats in the sea and in the air presented by adversaries. Performing MRO on a ship at a timely pace is a key part to the defense of our nation. Industry 4.0 sees technology as a major and innovative driving force for leading the manufacturing industry to experience significant business results. Creating ubiquitous network coverage across a shipyard is an important move forward in enabling the workforce. But leveraging the same network design to provide coverage across **all** shipyards provides a seamless infrastructure that is critical in enabling the IT workforce to provide multiple steps forward in connectivity, collaboration, and insight for the Operation Technology (OT) workforce.

There are various benefits from modern connectivity that can be deployed at a shipyard using wired and wireless networking to include Wi-Fi 6, 5G Cellular and beyond, Bluetooth Low Energy (BLE), and Long-Range Wide Area Network (LoRaWAN). These networks must be secured with Zero Trust Architecture and implemented and managed with intent-based networking for micro/macro-segmentation and automation.

Growing enterprise networks with wireless technology is a simple and logical step to enable the workforce to close the digital divide with collaboration and access to network services and information. Wi-Fi 6 offers a more consistent and dependable network connection for all clients, Internet of Things (IoT), and all apps (especially voice and video when compared to prior Wi-Fi standards). In addition, as wireless demands increase and include more IoT devices, Wi-Fi 6 can handle more data across the air than previous Wi-Fi standards. When combined with intent-based networking, IT departments can automatically separate and secure wireless IoT devices from the enterprise network.

Wi-Fi 6 operates in the 2.4 GHz and 5 GHz shared Industrial, Scientific, and Medical (ISM) frequency bands and is backwards compatible with all previous iterations of Wi-Fi standards. Existing Wi-Fi devices will be able to work on any newly installed Wi-Fi 6 access points across the enterprise installation. As a result, any devices that currently operate on Wi-Fi will be able to connect and any new devices that are able to connect natively via Wi-Fi 6 will experience the benefits of the new standard.

When compared to the previous Wi-Fi 5 standard, Wi-Fi 6 delivers a more consistent and dependable network connection that will deliver speeds up to four times faster with four times the capacity for data. Wi-Fi 6 also delivers reduced latency, greater reliability, and better power efficiency. Wi-Fi 6 also offers improved security with Wi-Fi Protected Access 3 (WPA3). WPA3 offers enhanced security for open Wi-Fi networks with encryption of unauthenticated traffic, robust password protection against brute-force dictionary attacks, and superior data reliability for sensitive information with 192-bit encryption. The increased security should help to assure previously hesitant IT departments to begin considering a deployment of Wi-Fi 6 to modernize their network and workforce. The quadrupling of throughput is achieved by using Orthogonal Frequency-Division Multiple Access (OFDMA) to achieve higher spectral efficiency as well as Multiuser Multiple-Input Multiple-Output (MU-MIMO). OFDMA is a type of frequency-division

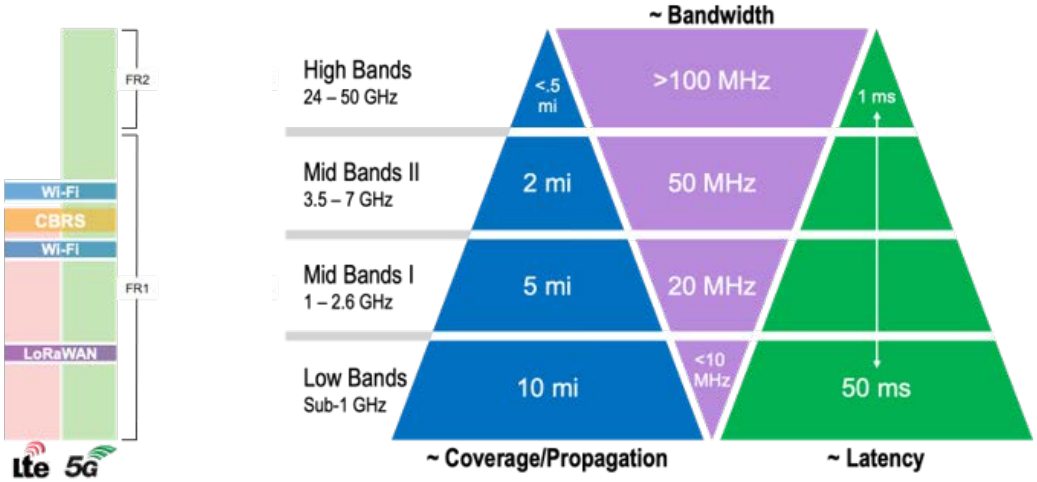
multiplexing that can use subcarriers more efficiently when it comes to transporting data. Wi-Fi 6 communicates in parallel with compatible devices, where previous standards could only communicate with one device at a time. This increased capacity is essential since the number of wireless devices on networks is expected to grow rapidly as IoT device deployments expand in the coming years.

Deploying Wi-Fi 6 will enable the workforce and create many advantages for them and the IT department. Allowing multiple workers to be able to connect on the same network provides increased convenience over a wired connection and enables mobility for the workforce to continue to work anywhere to include connecting to a remote expert on demand if needed. The potential for increased productivity for the workforce only grows as more Wi-Fi 6 access points are deployed.

In addition to deploying Wi-Fi 6, a private cellular 5G network can provide added coverage at a shipyard installation. When considering 5G and Wi-Fi 6, it is not an "either or" situation, but more of how they work together in a heterogenous network. A 5G network can be used to augment a Wi-Fi 6 network and provide coverage in areas that are hard or expensive to reach with Wi-Fi or in areas where mobility coverage is needed. 5G is the first cellular radio technology designed specifically with business and IoT applications in mind. The new capabilities of 5G make it an attractive option beyond public networks, especially private network applications.

While Wi-Fi operates on shared ISM spectrum, 5G operates on licensed private and shared spectrum in a specific geographic area. This makes 5G a viable private network option for doing business in an area where shared ISM spectrum is a concern, or where users want to maintain control over the Radio Frequency (RF) environment ensuring dedicated spectrum is available for their use. 5G networks also provide wider coverage areas, have reliable handovers for mobility use cases, and allow for cellular security that can be built on top of a Zero Trust Architecture. In addition, network slicing enables 5G network to be partitioned into virtual networks that can be tailored to specific operational and application needs.

Figure 3. Mobile Broadband Spectrum



The 5G mobile broadband spectrum is broken into two different frequency ranges. Frequency range 1 (FR1) operates from 450 MHz to 6 GHz. Frequency range 2 (FR2) operates in the band from 24.25 GHz up to 52.6 GHz. As with any type of radio system, the higher the frequency the greater the ability to support high data-transfer speeds. However, at higher frequencies, the signal propagation or distance traveled is greatly reduced. This distinction requires an understanding of the end-use case and requirements to be able to provide the best environment to satisfy the needs of the network. **Figure 3** gives a general overlook at the 5G mobile broadband spectrum and tradeoffs in terms of coverage/propagation, bandwidth, and latency.

The three main pillars of 5G are:

- Ultrareliable Low-Latency Communication (URLLC)
- Massive Machine-Type Communication (mMTC)
- Enhanced Mobile Broadband (eMBB).

URLLC allows a network to be optimized for processing volumes of data with minimal delay, on the order of 10 ms today and 1 ms in the near future. Ultralow latency is critical for time sensitive and mission-critical process applications. mMTC enables support for network access of sensing, metering, and monitoring devices. This along with 5G's broad reach make it an ideal technology for IoT applications. eMBB supports high data rates with broad coverage enabling surveillance, quality control, and Augmented Reality/Virtual Reality (AR/VR) applications.

Even as a new and emerging technology, 5G is here today and there is a breadth of devices currently available on the market that utilize it. They make up a diverse ecosystem of devices that can be deployed to connect the Operational Technology (OT) workforce to the IT network, closing the digital divide. Devices range from fixed wireless access points, routers and gateways, smartphones and tablets, and AR/VR and remote expert endpoint devices. **Figure 4** shows some of the devices that are currently available to operate in a 5G network.

Figure 4. Ecosystem of Devices and Uses

The mobility aspect of 5G is important because it enables fast hand off between antennas that can provide the infrastructure needed for Automated Guided Vehicles (AGV) in warehouses and for parts movement. Combined with URLLC, real-time control of automated process and robotic control is within reach of most facilities. This is seen as a forward movement path in the future for the manufacturing industry.

Modern manufacturing environments generate an enormous amount of data. This data, produced by the manufacturing process itself, is essential to track. However, there are other aspects of manufacturing and MRO—the people, material, equipment, and other assets—that can also be leveraged to generate data that can improve efficiencies, reduce downtime, and improve worker safety. Historically, knowing where an asset was at certain moment, typically when scanned, was sufficient to support operations. But in the modern manufacturing environment, knowing where an asset is in real-time or near real-time, is essential.

Asset tracking is a powerful capability for MRO that can provide several benefits across the enterprise for the U.S. Navy.

Asset tracking is a powerful capability for MRO that provides several benefits across the enterprise. First, knowing the location of key parts, support equipment, tools, hand-held devices, and other inventory (and, perhaps people) gives the workforce and supervisors real-time visibility to minimize the time spent looking for assets while also providing operational data to optimize processes and workflows. Second, asset tracking increases worker safety by enabling real-time alerting in lone worker or hazardous conditions, and by establishing geofencing capabilities. And third, asset tracking data ingested into an inventory system enables more thorough loss prevention.

There are several technologies that enable the asset tracking use case. Wireless access points can deliver ultraprecise hyper-location services that leverage a combination of Wi-Fi and Bluetooth Low Energy (BLE). Additionally, Radio Frequency Identification (RFID) technology, in concert with Wi-Fi, can enable location of tagged devices with high accuracy. Cellular technologies can also transport data from sensors affixed to assets. Each technology has strengths and weaknesses and should be evaluated against use-case specific criteria. Things to consider include, but are not limited to, the type and number of assets being tracked, the distance it might travel, the available spectrum, the total cost of ownership, and any environment-specific requirements (for example, intrinsic safety).

LoRaWAN, a low-power, low-cost, wide area networking protocol, is designed to wirelessly connect battery operated things to the network in very large areas or assets in transit between sites. This technology extends the asset tracking capability across long distances or very large outdoor spaces. For example, assets could be tracked between MRO sites or from suppliers to shipyards and depots with Global Positioning System (GPS) accuracy. LoRaWAN also enables use cases other than asset tracking, like condition monitoring. Sensors can be deployed to monitor warehouse environmental conditions (temperature, humidity, light/sound levels, etc.), detect leaks, observe occupancy, and even monitor machine and equipment condition. The LoRaWAN protocol was built with security top of mind and uses several capabilities to ensure that the data broadcasted is secure. Using LoRaWAN to track assets, monitor physical infrastructure, and provide data into environmental conditions will provide immediate benefits to MRO operations by answering questions in real-time, such as “where is this material?” and “where is that asset?” It can also provide the data necessary to optimize processes and operations at the macrolevel.

An improved and modern network with ubiquitous connections available anywhere can simplify shipyard infrastructure by enabling a unified approach. Expanding this unified approach across all public shipyards will provide return on investment at a greater scale versus deploying a unique solution at each shipyard. Adding wireless and mobility will expand seamless roaming for users and IoT devices regardless of the underlying network technology. And with an IoT network, smart buildings can begin to digitize workspaces and prepare for the future.

As networks begin to expand beyond wired connections to include more workers and IoT connecting via wireless, cybersecurity has never been more important to the Navy. This is especially so for MRO organizations as they begin the journey to modernize through the convergence of IT and OT. Fortunately, adopting a Zero Trust Architecture (ZTA) can enhance the security posture of network deployments, from wired to wireless.

As the workforce grows and continues to access a variety of information (sensitive and not) it is important to implement a strong security posture based on a ZTA to determine appropriate levels of access to the network, based on identity. Organizations that have switched to a Zero Trust framework that identifies, segments, and continuously monitors all devices have ensured that internal resources remain secure, and that data, applications, and intellectual data stay safe.

A Zero Trust approach means automatically assuming that anything outside or inside the network perimeter cannot be trusted and must be verified before granting access to the network. To implement Zero Trust, it is important to identify not only who, but what devices are connecting to the network. This includes operating systems, services, applications, IoT devices, and machines. Once this information is known, then policies, architectures, and access controls can be created so that when an endpoint or user connects to the network, it is granted access based on identity rather than just IP address. Implementing Role-Based Access Controls will give in-depth visibility into such factors as identity, location, type of connection, business function, job role, and device type (see **Figure 5**).

Figure 5. ZTA Security and Identity Based Contexts

To extend Zero Trust Security to industrial networks, IT should be aware of endpoint visibility, compliance, network segmentation, and threat detection response. Endpoint visibility is achieved by gaining detailed visibility of what is connected to the network. This is imperative to understand what is being protected as well as continuously verifying the identity and understanding the operational variables of each device. Many organizations today struggle to operate with up-to-date asset inventory. Endpoint compliance is needed since many industrial assets may contain software vulnerabilities that must be identified to properly plan corrective measures. The IT and OT team must work together to manage the volume of devices that can be present, mitigating any issues and correcting them where applicable.

Most industrial devices have been developed without the security found on enterprise hardware. Once an IoT device has been granted access, it should be added to an industrial zone as defined by ISA99/IEC-62443, and with calls out for isolating devices with micro- and macro-segmentation. With ZTA, communications are continuously monitored to detect malicious traffic and abnormal behavior. Anomalous events are reported with the appropriate context for fast response and remediation without impacting operations. For example, if an IoT device or machine monitoring port tries to access the internet where it previously never had, this is cause for alarm and inspection. These types of events are detected over time as net flows are captured and analyzed with Artificial Intelligence and Machine Learning (AI/ML) to determine the anomalous behavior.

Today's modern networks are being used to connect people, devices, application, sensors, and machines at an increasing rate to help streamline and modernize workflow. There is increasing complexity with connecting things together, as well as the need to require enhanced security that can keep data segregated, as needed, to comply with security policies. An intent-based network can simplify complexity in the network space while providing more time for IT innovation. It does this by improving network visibility, analytics, and automation while providing faster threat detection and containment, continuous security compliance, and reduced downtime. The improvements in reduced time and effort to manage and maintain the network will provide real value to the MRO process by freeing up resources to focus on the mission at hand and future innovation.

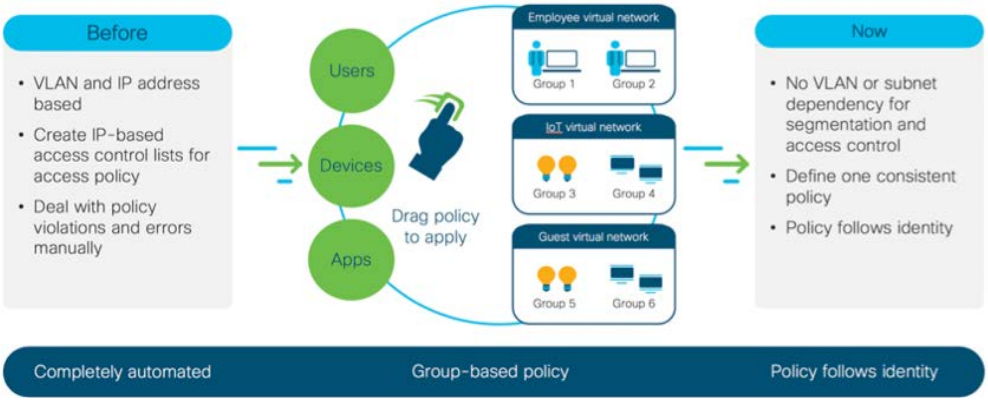
In order to reinforce security within the network, access control to create identity-based segmentation is the first step. This allows network operators to secure people and things through automatic segmentation without redesigning the network. The next step to reinforce security on the network is with the Zero Trust Security model using automated policy-based segmentation. This allows for secure access to the network and for all devices, including IoT, to be able to gain access to the network only where needed. Using AI-driven security with endpoint analytics, IT network administrators will be able to gain visibility to endpoint devices via AI/ML to further secure the network.

Intent-based networking is available on wired and wireless networks. Using the above-mentioned networking technologies with intent-based networking and ZTA, IT can securely connect workers throughout a campus, base, port, or any type of installation. Intent-based networking allows IT to capture and translate intention into policies that the network can act on by installing these policies across the physical and virtual network using network-wide automation. The intent-based network integrates with other IT and business systems and applications to quickly adapt to new application and service requirements, reduce risk, operate efficiently, and support exceptional customer experience. Being able to quickly and securely deploy network policies to end users is part of an IT transformation that will enable speed and accuracy toward the completion of the mission.

Intent-based networking centers around software defined access to deliver a network configuration that has the intelligence and automation to meet the mission requirements. This is achieved through a centralized controller that automates the translation of mission or business intent into network configurations and security policies. **Figure 6** illustrates how this model works.

No longer are IT teams required to manually configure network devices while trying to translate IP addresses into mission alignment. Translating IT data into mission intent is becoming way too complex, error-prone, and time consuming of a task. Software defined access automates user-access policy implementation so organizations can ensure the right policies are established for any user or device, with any application across the network.

Figure 6. Identity and Security Policy



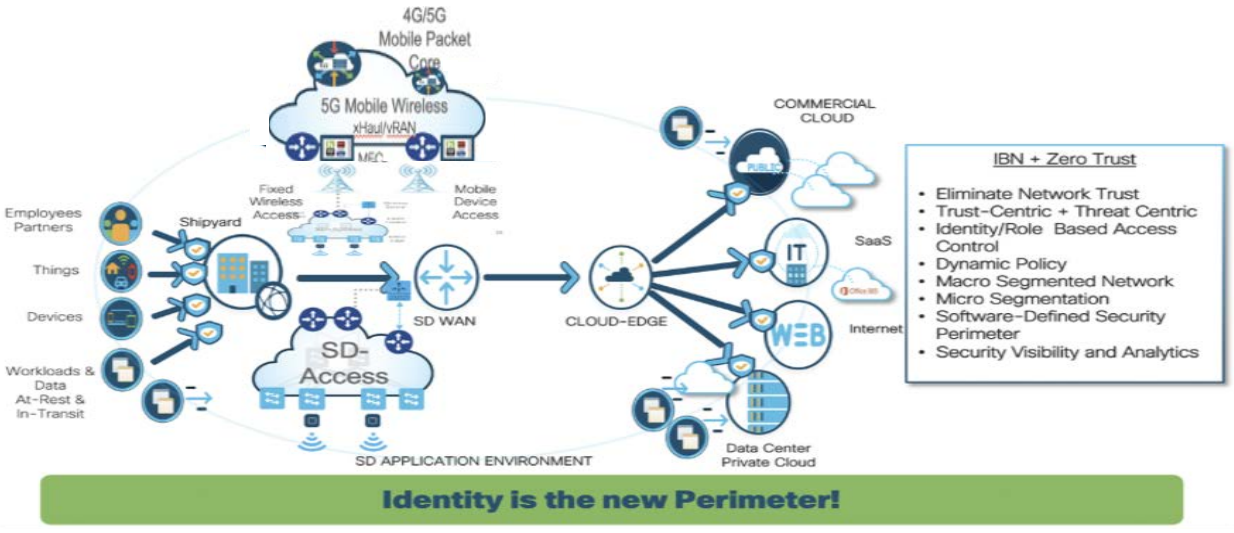
This is accomplished with a single-network fabric across the Local Area Network (LAN) and Wireless Local Area Network (WLAN) which creates a consistent user experience anywhere without compromising security. Centralized network control then leverages advanced analytics and machine learning to provide user, network, and application health scores to proactively modify the networks intent to enhance user experience and productivity. This continuous feedback loop allows for constant optimization of the network to better facilitate mission success with minimal human interaction required during operation.

Software defined access enables software defined segmentation capabilities that can simplify and accelerate implementation, sensing, and enforcement of a consistent security policy across both IT and OT networks. Macro- and micro-segmentation policies can be centrally defined and implemented throughout the network. Segmentation policies now follow users wherever they go on the network and whether they connect via wired or wireless because access policies are based on identity, not location or mode of accessing the network. By basing classification on "identity" rather than IP addresses, end-to-end policy changes may be implemented centrally and propagated efficiently across the entire network. Modification of users, applications, operating systems, and more can be changed at the endpoint level and propagated across the entire network, greatly simplifying access control and segmentation management.

The IT network is the foundation for network transformation, and it all begins with automation. Intent-based networking enables IT to work smarter and drive business outcomes with software defined networking by leveraging Network Operations (NetOps), Artificial Intelligence Operations (AIOps), Security Operations (SecOps), and Development Operations (DevOps) within the network.

NetOps can increase scale by providing business resiliency, continuity, and quick time to add value of the network. AIOps will enable improved performance by reducing Operating Expenses (OPEX) through faster root cause analysis and increasing IT visibility and observability. SecOps leads to improved security by automating enforcement of security policies on network infrastructure as well as endpoint visibility, classification, and grouping. DevOps will improve service delivery with Application Programming Interface (API)-based automation workflows and early issue detection and integration with third party platforms through enhanced notification channels. Combining these operational methods with increased automation and detection throughout the network will provide IT departments the ability to continue enabling business efficiency while driving innovation forward.

Figure 7. Navy Shipyard Network of the Future



With the convergence of IT and OT networks, the network must be able to connect and manage enterprise end devices and Internet of Things (IoT) devices from a centralized node. Most IoT devices are not designed with security in mind, so being able to use intent-based networking to classify devices as they are identified on the network will allow for network segmentation and policy enforcement to provide additional security throughout the enterprise. Embracing and using IoT devices can help enable mission readiness and reduce workload and complexity for teams across the workforce. **Figure 7** shows how all of the technologies of Wi-Fi, cellular, IoT, ZTA, and intent-based networking combine to create the network to lead the workforce and close the digital divide, providing speed and excellence while transforming the way IT and OT work together to deliver for the Navy.

Data Management

The manufacturing industry has turned to data analytics for three key reasons; to improve operational efficiency, gain real-time production visibility, and lower operating and maintenance costs. Just as in the manufacturing industry, data collection and management are critical to improved analytics in ship maintenance. The goal of transforming maintenance, repair, and overhaul operations drives the need for data capture, analysis, and sharing in real time. Data analytics will enable operators to obtain valid performance data across functions and sites that will improve efficiency, maximize equipment up time, and optimize employee performance. The network will enable data collection and visualization at scale across sensors, equipment, sites, functions, and operations. A distributed compute architecture from the edge to the cloud empowers this, allowing processing where it makes a difference and best supports optimized operations.

It is key to ensure adequate data extraction, transformation, sharing, and governance from data center to the edge to clouds. In manufacturing, validated designs, such as Converged Plantwide Ethernet (CPwE) and Networking and Security in Industrial Automation Environments, help ensure reliable data management in industrial environments. Since ship maintenance can vary significantly from one evolution to another, it is important to look to manufacturing industry examples that showcase the necessary agility to perform shipyard availabilities in an uncertain environment.

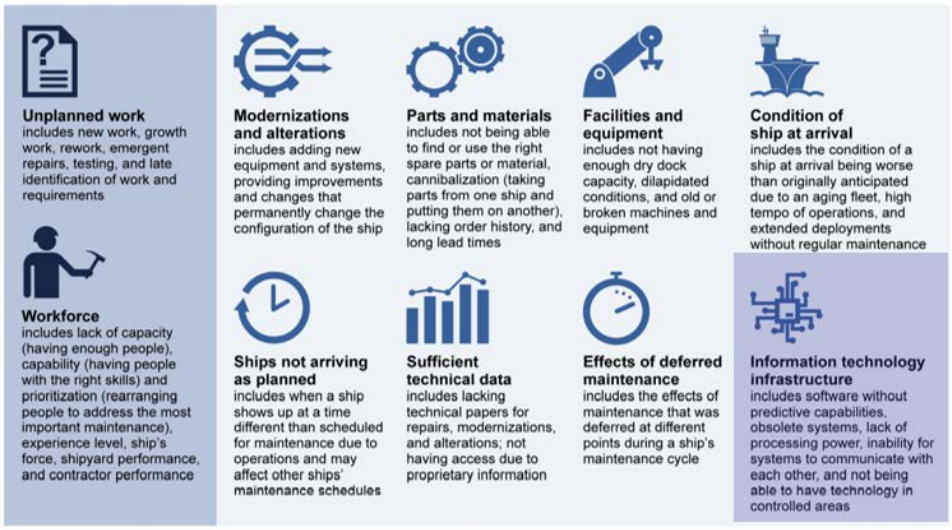
Case study: Daimler Trucks North America. They required not just cost control but also the agility to deliver customization of products they manufactured. Daimler upgraded its Western Star production facility network to better coordinate this flexibility. Their optimized network was based on the Converged Plantwide Ethernet validated design and leveraged Wi-Fi connectivity throughout their plant. Their enhanced network enabled reliable communications, real-time visibility to confirm product configurations, and analytics that delivered visibility of supply status from the warehouse to factory. Leveraging a combined IT and automation network enabled real-time data visibility analytics across their operation and increased security and IT reliability. Data is now transmitted securely to key personnel and applications to enable them to make better and faster decisions. Software defined networking also allowed remote troubleshooting and improved management and automation.

The same advances can be delivered in the Navy's Maintenance and Modernization operations. Leveraging a network such as this can allow data silos to be broken down to allow maximum return on Navy's software investments in Enterprise Asset Management, Product Lifecycle Management, and Enterprise Resource Planning, etc.

Connected Worker

Per fiscal year 2022 (FY22) budget documents, Navy plans to employ 20 percent of its civilian workforce in direct support of ship maintenance. Such a robust workforce requires an equally robust IT infrastructure. An August 2020 Government Accountability Office (GAO) report [GAO-20-588] identified both workforce and IT infrastructure being in the ten factors contributing to shipyard maintenance delays for aircraft carriers and submarines (see **Figure 8**). Yet the IT infrastructure at each of the four public shipyards continues to be nonstandard and disaggregated.

Figure 8. Factors Contributing to Shipyard Delays per GAO Analysis in GAO-20-588



A modern and connected network enables collaboration across a connected workforce. A connected workforce enables completion of critical shipyard tasks such as resource loading of industrial equipment and human resources, drafting and updating project integrated master schedules, remote troubleshooting communications, and supporting a variety of maintenance software tools and processes.

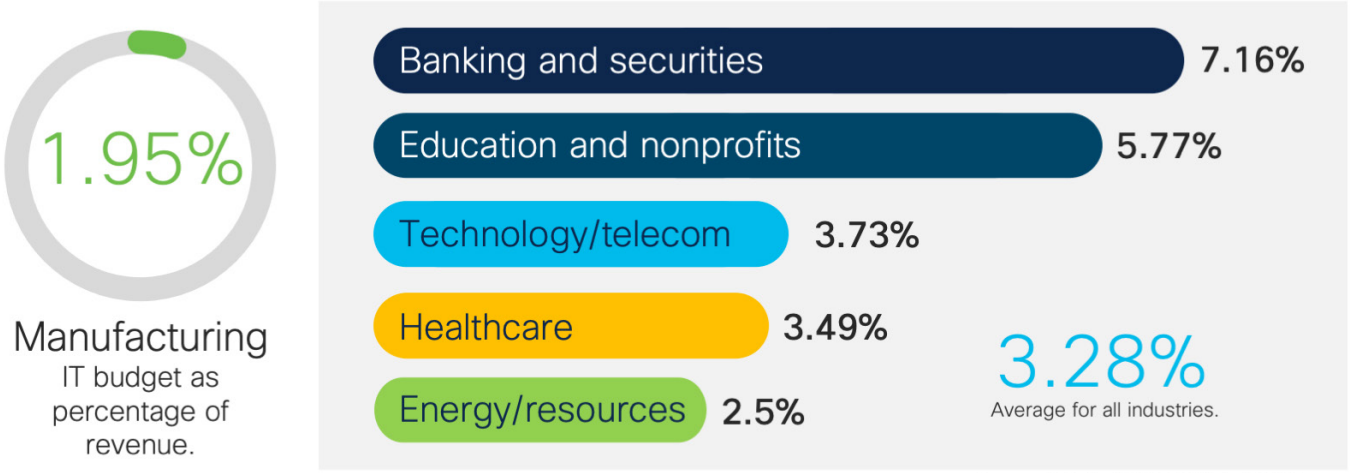
As aforementioned, Wi-Fi 6 and 5G technology gives sailors, whose shipboard network is often disconnected during maintenance availabilities, the ability to continue supporting their contribution to ongoing maintenance activities. For example, a Wi-Fi 6 or 5G network available from the ship or assigned berthing barge enables ship's forces and shipyard workers an onsite ability to request, modify, and approve work items, coordinate tasking, and provide remote monitoring and troubleshooting.

A side benefit is that the network provides the sailors and shipyard workers a means to keep up with their qualifications and certifications from any location within the shipyard. These technologies open the possibilities to connect and segregate shipyard workers, ship's forces, and remote subject matter experts to enhance and streamline work at shipyards to create new, efficient, knowledge sharing improvements to modernize ship maintenance and worker experience.

Prioritizing IT Investment

A recent study by Deloitte, "Technology Budgets: From Value Preservation to Value Creation," compared IT budget expenditures to revenue for a variety of industry sectors. It was noted that IT investments spanned from around 1.5 percent to 7 percent of revenue depending on the nature of the industry (see **Figure 9**).

Figure 9. IT Budget as a Percentage of Revenue



Source: Deloitte 2016-17 Global CIO Survey.

Arguably, shipyards do not have "revenue" per se, and they may be considered at the lower end of the spectrum for IT spending. Using the Navy's annual ship maintenance budget of approximately $12.5B, a 2-percent lower-end estimate would result in an expected IT budget of $250M annually, which is likely far less than what Navy has invested in IT for our public shipyards and supporting activities.

The bridge to possible

Enabling mission success for the Department of Defense

At Cisco, we know what mission success means. As a leading partner with the Department of Defense (DoD), Cisco is delivering next-generation technologies that enhance operational readiness against ever-evolving and more complex global threats. This includes leveraging industry-leading and DoD compliant solutions that connect, secure and automate to accelerate digital transformation in secure DoD-cloud environments.

That's why we understand there are new weapons in America's arsenal that yield tremendous untapped power our nation can leverage for our defense:

- The DoD network as a weapons system
- Data as a strategic asset operationalized.

As a result, we're poised at the tip of the spear, empowering our nation's military with mission ready solutions for:

- Secure cloud computing
- Software-defined networking
- Analytics
- Artificial intelligence
- Automation
- Real-time video collaboration
- Cybersecurity.

To enable your mission, visit: cisco.com/go/DoD.

The Power of Connecting Shipyads

With an IT transformation roadmap standardized across the four public shipyards, the Navy can identify and prioritize the segments of the network that would more quickly provide value to the workforce and realize a return on investment in the network. Applying a near-term capital investment into the network can help the shipyards and their workforce in their path toward modernization and returning to on-time delivery of ships back to the fleet.

Conclusion

Naval Shipyards have an opportunity to drive operational improvements into their production systems and assets through convergence and digitization by leveraging the new paradigms in Industry 4.0.

Shipyards need a unified enterprise and industrial network that is agile and handles growth and change intuitively, by constantly adapting to the enterprise while also constantly protecting against cyberthreats. IT and OT leaders in manufacturing understand that success in the digital era means working together to converge and upgrade networks and create an environment that links IT and OT (building automation systems, control systems, machinery, etc.) to drive improved productivity.

Manufacturing has become a technology-driven industry and the U.S. Navy can apply lessons learned from manufacturing to optimization of shipyard infrastructure and processes. The result of this digital transformation will be new opportunities to improve operational efficiency, increase productivity, accelerate decision making, maintain compliance, and increase fleet readiness.

References and Bibliography

GAO report: GAO-20-588

Deloitte, 2016-2017 Global CIO Survey, N=747: "Technology Budgets: From Value Preservation to Value Creation"

Appendix: Acronyms

AGV	Automated Guided Vehicles
AI/ML	Artificial Intelligence and Machine Learning
AIOps	Artificial Intelligence Operations
API	Application Programming Interface
AR/VR	Augmented Reality/Virtual Reality
BLE	Bluetooth Low Energy
CPwE	Converged Plantwide Ethernet
DevOps	Development Operations
DoD	Department of Defense
eMBB	Enhanced Mobile Broadband
FR1	Frequency range 1
FR2	Frequency range 2
GAO	Government Accountability Office
GPS	Global Positioning System
IoT	Internet of Things
ISM	Industrial, Scientific, and Medical
IT	Information Technology
LAN	Local Area Network
LoRaWAN	Long-Range Wide Area Network
mMTC	Massive Machine-Type Communication
MRO	Maintenance, Repair, and Overhaul
MU-MIMO	Multiuser Multiple-Input Multiple-Output
NetOps	Network Operations
OFDMA	Orthogonal Frequency-Division Multiple Access
OPEX	Operating Expenses
OT	Operation Technology
OT	Operational Technology
RF	Radio Frequency
RFID	Radio Frequency Identification
SecOps	Security Operations
URLLC	Ultrareliable Low-Latency Communication
WLAN	Wireless Local Area Network
WPA3	Wi-Fi Protected Access 3
ZTA	Zero Trust Architecture