imc 2019
PACIFIC INTERNATIONAL MARITIME CONFERENCE
INTERNATIONAL CONVENTION CENTRE SYDNEY, AUSTRALIA
8-10 OCTOBER 2019

IMC 2019 CONFERENCE FULL PAPER

Enabling Instant Situational Awareness in Naval Bridge Operations

Robert Ventresca
Vice President, Worldwide Marketing
Thinklogical, A Belden Brand
robert.ventresca@thinklogical.com

EXECUTIVE SUMMARY
The proliferation of intelligence, surveillance and reconnaissance (ISR) information has changed the landscape of naval strategic thinking. Real-time analysis of ISR information has influenced the form and function of naval bridge design, transforming the modern bridge into the nerve center for all onboard operations.

STRATEGY OF INFORMATION SUPERIORITY
Defense and intelligence organizations have long been pursuing a strategy of information superiority to defend against a broad range of threats. However, the nature of these threats has changed. Today we need to respond to threats in hours, if not minutes – often without having any advanced warning of what the threat will be

The unpredictability of these threats requires a responsive command and control information gathering workflow that is robust, yet flexible and nimble to meet dynamic mission requirements. Ship commanders are therefore demanding better tools to collect, process, analyze and disseminate this information, leading to instant situational awareness and faster, better-informed decision making

KEY CHALLENGES IN NAVAL SHIP'S BRIDGE DESIGN
But giving that access demanded by commanders is functionally difficult. It requires a highly sophisticated IT architecture and audio-visual infrastructure. Providing access also opens the system to cyber hackers and the insider threat – the threat of accidental or intentional hacking or data breach by an employee or contractor

To manage access and mitigate the insider threat, organizations create information assurance directives to secure the information. These two concepts are in conflict. On the top we want any to any access to improve situational awareness and fulfill the mission – on the bottom, we want to lock down and secure our information – losing it through an insider or cyber event wipes out our strategic advantage.

LEGACY SHIP'S BRIDGE ENVIRONMENT

The other key driver is enhanced operational flexibility. Traditional ship's bridge infrastructures have "siloed" hard-wired workstations, each designed for specific functions. This limits collaborative workflows and increases staffing requirements to support the various dedicated operations. Because these systems are purpose-specific, a fault or failure (or combat battle damage) will render the station inactive and it's function unavailable.

These legacy systems typically use copper-based cabling, which adds weight and is susceptible to electrical emanations that can be "sniffed" or eavesdropped upon. If access to multi-classification networks is required, legacy systems often can't support this capability, or if they do, they either violate standard Information Assurance best practices for data protection due to space limitations or require clumsy manual desktop KVM (keyboard, video, mouse) switches to connect to and move between secure networks.

USS COLE INCIDENT

On 12 October 2000, a suicide bombing by a surface vessel significantly damaged USN Guided Missile Destroyer USS Cole while it was in port in Yemen for refueling. The attack was attributed to Al Qaeda. 17 sailors were killed and 39 injured. The bombing destroyed a mechanical room located below the galley, rendering the ship unseaworthy. [i]

One analyst noted later, "The U.S.S. Cole was a wake-up call for the Navy."[ii]

The incident was a key driver in the U.S. Navy's move towards "mirror-image" redundant fiber-optic based operations, communications and network backbones on new ships and retrofits. Fiber provides speed, bandwidth, reliability, immunity to EMI, and less weight compared to copper cabling systems.

NEXT-GENERATION NAVAL SHIP'S BRIDGE REQUIREMENTS

This is what is driving the need for a next-generation ship's bridge and combat information center infrastructure.

- Achieve information superiority and instant situational awareness through immediate access to critical ISR resources via "any-to-any" switching
- Enable mirror-image redundancy and rapid reconfiguration of command/CIC resources to quickly adapt to dynamic mission requirements
- Simplify management of multiple classifications through a single information assurance (IA) approved AV/IT infrastructure
- Lower total cost of ownership (TCO)

DESIRED END STATE – NEXT GENERATION SHIP'S BRIDGE

Next-generation, fiber-based naval bridges combine a video-enhanced cockpit area for navigation with mirror-image multi-function consoles incorporating an integrated command center and combat information center (CIC). This co-location of multi-purpose systems allows for greater situational awareness and collaboration between those who are driving the ship and those who are operating weapons and sensors.

The new design delivers unparalleled flexibility in how commanders station people on the bridge, providing for as few as two people standing watch on the bridge, replacing up to twelve watch standers typical for naval vessels. Because the integrated command center/CIC and the bridge are co-located, moving personnel takes literarily just a few seconds. With the open architecture of the next-gen design, commanders can re-assign any task to any console available on the bridge, providing a rapid response to the changing tactical needs of the ship.

NEXT-GENERATION SHIP'S BRIDGE INFRASTRUCTURE

In addition to fibre-optic cabling, the underlying infrastructure for secure video and data distribution plays an important role in enabling next-generation ship's bridge and combat information center capabilities. This enabling technology is comprised of two parts:

- Signal Extension (extend KVM - keyboard, video, mouse, USB, peripherals)
    - Moves computers and data sources out of the workspace. This allows for back-racking PCs and data sources in a location away from users
    - All processing and data remain on the source (computer, etc.) for security
- Secure Switching (matrix switching of multiple sources with multiple destinations)
    - Allows for switching of sources from multiple sources (and multiple classifications) on a single infrastructure

SIGNAL EXTENSION

The flexibility of a typical computer system is limited by the length of the cables that connect the computer to the display and peripheral devices, such as the keyboard and mouse. Display and peripheral signaling standards were not designed for lengths of greater than 10-15 feet. Therefore, displays and peripherals need to be located near their computers. And just installing longer cables does not work – the signal degrades and displays just flicker and keyboard and mouse controls don't work reliably.

In order to achieve greater cable lengths, you can use a secure signal extension technology, which allows a user access to a computer from up to 80 kilometers, or 50 miles. This involves installing a Transmitter, which connects to the computer just as the display, keyboard and mouse would in a typical computer system. The Transmitter then sends the video and data over *fiber optic cable* to a Receiver, installed at the user's station. The Receiver connects to the display and peripheral devices, just as they would connect to the computer – but over a significantly greater distance.

Typical commercial audio-visual products are not designed for use in mission critical secure facilities. In a secure infrastructure, the extension system does not modify or touch the signal

or information in any way, to ensure the integrity of the data. It is a stateless device, with no buffers, memory or storage. It strictly transports only the signal from the computer, sending pixels for the display, keyboard strokes and mouse movements. All the data, applications and computing power remain in the computer.

Secure extension technology allows organizations to remove the computers from the user environment. The computers are now moved to a more secure IT friendly environment like a server room. This single step creates all kinds of benefits: reduced heat, reduced noise, better use of space, higher availability, and lower total cost of ownership because they are stored in a more IT friendly environment.

SECURE SWITCHING

Remember that the computers are in a server room, each connected to a Transmitter. These transmitters are now connected to a secure Matrix Switch. On the other side, all the destination workstation desks are connected to the switch via a receiver. The video display, keyboard and mouse at each desk are connected to the receiver. So now, any source can be connected to any destination whenever we want them to be connected.

If a user wants to send what he sees on his display to a video wall, he can do so with a couple of keystrokes. If a user wants to switch from one source to another, he can do so with a couple of keystrokes. If a presenter in a conference room wants to change what is on the video wall, he can do so with a drag and drop on a touch panel. Everything can go everywhere – unless the administrator wants to restrict it – which he can do with a couple of keystrokes. So now, even the classification of a control room can change in just seconds – the administrator simply restricts which sources can be switched to the control room with a couple of keystrokes.

To enable this next-generation C2 infrastructure it required to use a KVM switch with Isolation technology, which reduces or eliminates the need to air gap multiple separate systems to eliminate the chance of crosstalk or data misdirection. Using this isolation technology, a secure matrix switch can ensure that no stream of traffic is ever compromised by another stream; that is, top secret traffic is always isolated from secret, which is isolated from unclassified.

Allowing multiple classifications to flow through a single switch is the only way to achieve any-to-any switching capability in a multiple classification environment, creating a flexible and responsive collaborative workflow and leading to instant situational awareness. It is also typically required that the matrix switch be approved and certified to information assurance accreditations such as NATO NIAPC, Common Criteria EAL4, US DOD DISA JTIC UCR and TEMPEST.

SUMMARY

Through this secure fiber-optic enabling infrastructure technology, the next-generation ship's bridge and CIC can deliver on the intended requirements:

- Achieve information superiority and instant situational awareness through immediate access to critical ISR resources via “any-to-any” switching
    - Access to any potential source of information that might be needed, for an event that is not predictable
    - Flexibility to reconfigure desks, consoles and conference rooms when and as the mission changes
    - Ability to design robust, collaborative and efficient workflows for faster decision making
    - Enable mirror-image redundancy and rapid reconfiguration of command/CIC resources to quickly adapt to dynamic mission requirements
- Simplify management of multiple classifications through a single information assurance (IA) approved AV/IT infrastructure.
    - Dedicated stateless hardware at desk supporting multi-class information sources
    - PCs/sources back-racked and cabling physically separated/air-gapped in IT room
    - USB ports, network cables and hard drives physically isolated from the users for security
    - Reduced staffing
- Lower total cost of ownership
    - Pooling/consolidation of IT and AV infrastructure – less equipment to purchase and maintain
    - Less space, power, cabling, and cooling needed
    - Fiber-optic infrastructure; higher bandwidth, less EMF emanations
    - Future-proof architecture results in longer time between technology refreshes

---

[i] CNN Online article: “USS Cole Bombing Fast Facts” updated March 27, 2019
https://www.cnn.com/2013/09/18/world/meast/uss-cole-bombing-fast-facts/index.html

[ii] Cabling Installation & Maintenance Magazine, August 1, 2001 article: “Fiber-loaded SmartShips testing the waters”
https://www.cablinginstall.com/home/article/16466028/fiberloaded-smartships-testing-the-waters