Self-Defense Test Ship Remote Combat System Operation

Rick R. York and Kirk L. Bateman

The Combat System Remote Control System (CSRCS) was designed and developed by APL to provide remote control capability for the weapons, sensors, and control elements on the U.S. Navy's Self-Defense Test Ship. These components comprise all of the combat system elements currently used by the Navy for ship self-defense. The CSRCS incorporates custom hardware and software with a variety of commercial computer platforms and operating systems to provide real-time control of the shipboard systems via console-representative graphical user interfaces at a land-based control site. It enables the Navy to safely conduct live firing tests of ship self-defense systems on a sea test range.

REQUIREMENT FOR A REMOTE-CONTROLLED TEST SHIP

On 10 February 1983, while conducting weapons testing and training in the Norfolk area, USS *Antrim* (FFG 20) was struck by a target drone that skipped off the surface of the water. The accident caused a fire in the wardroom and in the electronic spaces. A civilian instructor aboard the ship was killed. To prevent similar accidents, the Navy imposed restrictions on test exercises that prohibit target vehicles from approaching within 2.5 nmi of a manned ship.

This restriction created an impasse to testing short-range weapon systems first addressed by the Rolling Airframe Missile (RAM) Block I acquisition program. In 1986, during RAM developmental test/operational test (DT/OT) planning, the Navy recognized that not all of the required tests could be conducted on a manned ship. The final acquisition decision for the RAM Block I system depended on demonstrated capability against a set of threats, which included low-altitude, supersonic anti-ship cruise missiles. Tests involving most of the specified targets could have been conducted on either a Fleet ship or an existing test ship, but it was impossible to conduct a realistic test against a supersonic target while keeping the target 2.5 nmi from the ship. To maintain the safe distance, a target would either have to fly in a straight line toward a 2.5-nmi offset point or fly toward the ship and turn toward an offset point. In either case, it would look like a crossing target to the RAM. Because of the RAM's relatively short engagement range, realistic—i.e., radially inbound—target profiles would require a much closer approach to the ship than was allowed.

To resolve the conflicting requiremements of conducting close-in engagements while ensuring personnel safety, the Commander Operational Test and Evaluation Force recommended creation of a remote control test ship. In 1987, the Chief of Naval Operations selected a decommissioned ship, formerly USS *Decatur* (DDG 31), and designated it the Self-Defense Test

Ship (SDTS). Funding was allocated for conversion in FY1989, and by the end of FY1994 the ship was ready to support test operations.

Although the SDTS was initially conceived as a test platform for RAM, the Phalanx Close-In Weapon System (CIWS) Block IA and Block IB programs and the Evolved Seasparrow Missile (ESSM) program have had similar requirements to conduct tests against low-altitude, high-speed targets. The SDTS has thus subsequently evolved into a test platform for all ship self-defense systems.

The first planned use of the SDTS was the DT/OT of the AN/SWY-2 combat system, which combines RAM with the Mk 23 Target Acquisition System (TAS). APL and the Naval Surface Warfare Center (NSWC), Corona Division (formerly Naval Warfare Assessment Station), were jointly tasked to develop a remote control system (RCS) for the AN/SWY-2. APL developed the control system, and NSWC developed the communications link connecting the shipboard elements to the remote elements. However, the AN/SWY-2 RCS was never used on the SDTS. Development was completed, but RAM testing was delayed in order to eventually test it in connection with the Ship Self-Defense System (SSDS) Mk 1.

In the meantime, the first actual use of the SDTS was in support of two phases of CIWS testing during 1995 to 1997. The first phase was to test a software modification to the Block IA system, and the second was to test the Block IB system. APL developed RCSs for CIWS and the AN/SLQ-32(V)3 electronic countermeasures system for those tests.

RAM testing began on the SDTS in 1998. The test configuration included RAM, CIWS, AN/SLQ-32(V)3, the AN/SPS-49A radar, and SSDS Mk 1. APL developed remote control capabilities for the radar and SSDS and fielded the previously developed remote control elements for the remaining systems. In the RAM test configuration, the combined data throughput requirements of the remote control elements exceeded the throughput capability of the original communications link, so it was replaced with a new higher-capacity link, also developed by NSWC. The RAM Block I DT/OT was successfully conducted on the SDTS from September 1998 to November 1999.

Currently, the SDTS is being used to support ESSM testing. The system configuration for the ESSM firings includes a Rearchitectured NATO Seasparrow Missile System (RNSSMS), CIWS, AN/SPS-49A radar, TAS, SSDS, and the Multi-Sensor Integration and Tracking System (MSITS). The MSITS has no operator interface and therefore does not require remote control. The TAS RCS, initially developed as part of AN/SWY-2 test preparation, was put into service along with the other existing remote control elements. The only new remote control element that had to be developed for the ESSM DT/OT configuration was the RNSSMS RCS, which APL fielded in early 2000. The first ESSM test firing on the SDTS was conducted on 4 April 2000. Eleven more firings are planned.

CONCEPT OF OPERATIONS

The SDTS is berthed at Port Hueneme, California, and maintained and operated by NSWC, Port Hueneme Division. Test operations are conducted at the Naval Air Warfare Center (NAWC), Weapons Division Sea Test Range, near San Nicolas Island, which is one of the Channel Islands about 56 nmi south of Port Hueneme. The SDTS does not have a permanently assigned crew. For aircraft tracking and firing exercises that do not involve a safety hazard, the SDTS is manned with a small crew of NSWC personnel and contractors. With the ship manned, tracking exercises are performed under local and remote control to test the tracking capability and operation of the various sensors and to verify remote control procedures and operation of the RCS before an unmanned test event. The ship operates unmanned only during firing exercises that would present a safety hazard to personnel onboard.

Figure 1 shows the SDTS concept of operations. During remote operations, ship propulsion and steerage are controlled from the NAWC Range Operations Center at Point Mugu via a control system developed by NAWC. This system is based on the Hulk Integrated Target System, which has been in use for several years for remote control of surface targets on the sea range. The sensor and weapon elements and associated instrumentation are controlled from the Surface Warfare Evaluation Facility (SWEF) at NSWC, Port Hueneme Division. Voice and data communication between the SDTS and SWEF is provided by a secure digital telecommunications link. Separate analog links are used to transmit several channels of video from the ship to the remote control sites at NAWC's Range Operations Center and SWEF.

The communications link includes antenna sites at San Nicolas Island and on Laguna Peak at the Pacific Missile Test Center, Point Mugu. The San Nicolas Island site is used when the ship is on the outer test range, west of the Channel Islands, where the firing tests are conducted. The Laguna Peak site is used when the ship is either in port or operating on the inner test range, which is the area between the coast and the Channel Islands.

The SDTS is not a target ship. During firing exercises it tows a target barge (Fig. 2) at a distance short enough to allow realistic target presentations but far enough to minimize risk to the ship.

REMOTE CONTROL APPROACH

The remote control elements for the various sensors and weapons on the SDTS are collectively known as

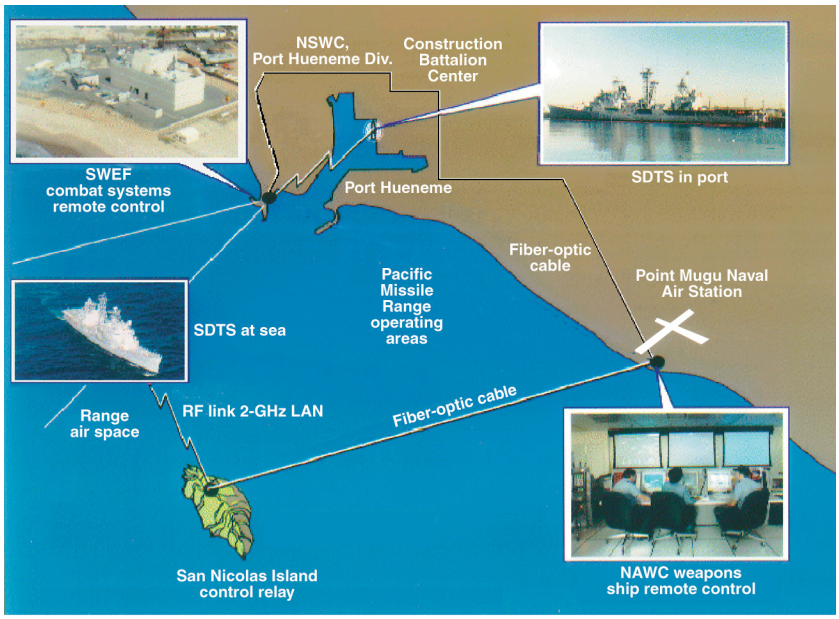

Figure 1. SDTS concept of operations. The ship operates from Port Hueneme, California. Weapons and sensors are remotely controlled from the Surface Warfare Evaluation Facility (SWEF), and propulsion and steering are remotely controlled from the Naval Air Warfare Center (NAWC). Communication between the ship and the remote control sites is provided by radio and fiber-optic cable.

the Combat System Remote Control System (CSRCS). However, largely because of the sequential way in which these elements were developed, they are actually a collection of loosely coupled subsystems. Each is capable of operating independently of the others, and they can be used in any combination required.

The remote control subsystems typically consist of a remote control panel (RCP) at SWEF and a remote control interface unit (RCIU) on the ship. The RCPs are software emulations of selected sets of system controls and status indicators running on UNIX workstations. The RCIUs provide the physical interfaces to the combat system elements through custom-built cabling and circuit boards. When a system is placed under remote control, the RCIU retrieves status from the system and passes it to an RCP. In addition, the RCIU receives commands from the RCP and executes control of the system accordingly. Each RCIU and its associated RCP exchange status and control information via the network communications link by message passing using Internet Protocols (IPs). This generalized approach to remote control is shown in Fig. 3.

The RCPs are implemented as X-Windows Graphical User Interface (GUI) applications running on UNIX workstations. There are no actual consoles or control panels at SWEF. Each RCP simulates to some extent the console or local control panel of the system it is controlling. For example, the RAM RCP simulates the RAM weapon control panel (WCP). The TAS RCP includes simulations of the TAS console and the system status panel (SSP). The RCPs invoke X-Windows routines to create a graphic representation of the actual console or control panel (buttons, status indicators, track symbology, and textual message display) on the workstation. System operation is entirely point-and-click. Thus, operators familiar with the system require no special training to operate it remotely other than how to invoke the RCP from a pulldown menu.

Figure 2. The SDTS tows a target barge during tests to minimize the likelihood that the ship will be hit.

The specific control provided by each RCP is dependent on the particular system and on test requirements. It is usually not necessary to provide every system control feature to a remote operator; however, the control features provided are typically a large subset of the control features available on the actual system console or control panel. In many cases, the RCP also provides control features not available to the local system operator. Some RCPs also provide control of ancillary equipment or instrumentation associated with the system under control. For example, the CIWS RCP primarily simulates the CIWS local control panel but also includes numerous controls for CIWS-related instrumentation.

The only consoles not simulated are the SSDS and RNSSMS consoles since they are AN/UYQ-70 consoles—basically, UNIX workstations in rugged chassis. The SSDS and RNSSMS console functions are already implemented as X-Windows GUIs. Remote control of these systems was accomplished by simply redirecting the X-Windows displays from the actual consoles to workstations at the remote site.

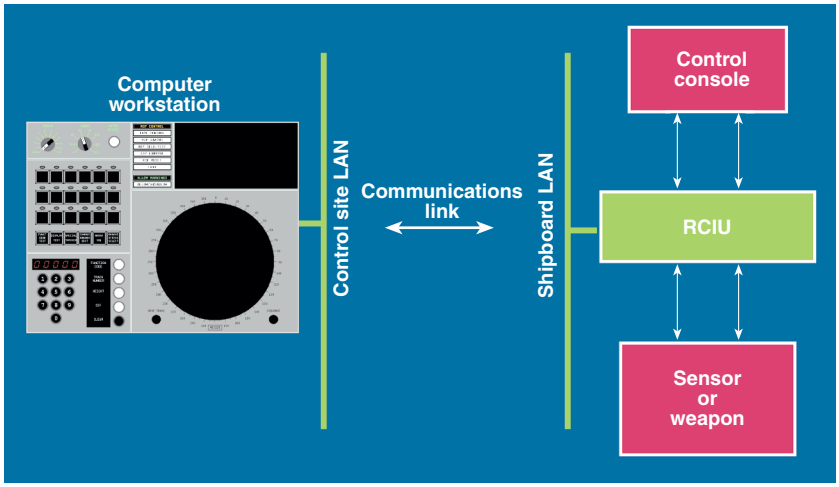

Figure 3. The remote control approach provides a console emulation at the remote site communicating with an RCIU connected to the system under control aboard the ship.

The RCIUs are VMEbus systems having 4 to 12 VME cards, depending on the application. Each RCIU contains an MVME-167 single-board computer hosting a Motorola 68040 microprocessor and associated circuitry. The microprocessor runs the VxWorks real-time operating system and serves as the controlling interface to the functions in the RCIU. The other cards are custom or commercial interface cards designed specifically to control one of the system interfaces.

Generally, the RCIUs are interposed between actual system consoles or control panels and the system elements to which the consoles or control panels are normally connected (Fig. 3). They contain switching circuitry that allows them to be switched in or out of the interface. When remote control is selected, the RCIU is switched in line and takes over control of the interface. The sensor or weapon element is then controlled by the RCP for that system. When local control is selected, the RCIU is bypassed so that the sensor or weapon element is controlled, as usual, by the actual console or control panel.

SYSTEM DESCRIPTION

The main components of the CSRCS are several UNIX workstations, RCIUs, and remote control power switches. Figure 4 shows the CSRCS components and their locations aboard the SDTS or at the remote control site. An infrastructure consisting of Ethernet hubs, radios that provide a connection between the ship and shore site, and cryptologic equipment to ensure a secure radio link underlies and supports the CSRCS. The infrastructure provides a secure and reliable Ethernet connection between the control site local area network (LAN) and the shipboard LAN.

The RCPs (e.g., Fig. 5) run on Sun workstations. Because development of the CSRCS spanned several years, the workstations are of several models: Ultra 1, SPARC 20, and SPARC 2. Two of the workstations, an Ultra 1 and a SPARC 2, are located aboard the SDTS; the remainder are located at SWEF. Other than the TAS display, the RCPs can run on any of the Sun workstations. The TAS display must be run on the SPARC 2 computers because the application uses calls to SunView, a toolkit supporting interactive, graphics-based applications running within windows. SunView is supported by the operating system (SunOS 4.1.3_U1) on the SPARC 2 but not by the newer operating system (Solaris 2.5.1) on the SPARC 20 and Ultra 1 workstations.

The Ultra 1 workstation aboard the ship serves as a software development system and as a host to each RCIU. The Ultra 1 software development tool includes a cross-compiler, linker, loader, a tool for building GUIs, and various UNIX tools (e.g., vi editor and perl) that are essential to the development environment. As a host to the RCIUs, the workstation contains the bootup scripts, operating system kernel, and executable application code for each unit. When an RCIU is powered up or rebooted, the boot code, residing in read-only memory installed on the microprocessor board, causes it to log on to the host workstation and download the operating system kernel and the application code.

The CSRCS also includes five HP workstations that serve as surrogates for the AN/UYQ-70 SSDS and RNSSMS consoles aboard the ship. Two of these—the Sensor Supervisor (SSUP) and the Weapon Supervisor (WSUP)—are used as the remote SSDS consoles. The remaining three accommodate two remote RNSSMS tracker/illuminator consoles (TICs) and one RNSSMS supervisor (SUP) console.

Each system (weapon or sensor) under control of the CSRCS has an associated RCIU. Some systems have ancillary equipment that is also controlled through the RCIU. Each RCIU is mounted in a rack near the equipment under control. The placement of each RCIU is necessitated by limitations on the length of cables connecting the RCIU and the equipment under control.

The RAM RCIU is connected to the missile system via an adjunct PC-based interface unit developed by Raytheon. This unit, in turn, is connected to the RAM WCP. The RAM system RCP has an additional interface to its data extraction (DX) PC, which provides control of the RAM DX capability. Remote control of the DX PC is accomplished using Virtual Network Computing (VNC), a free software product developed

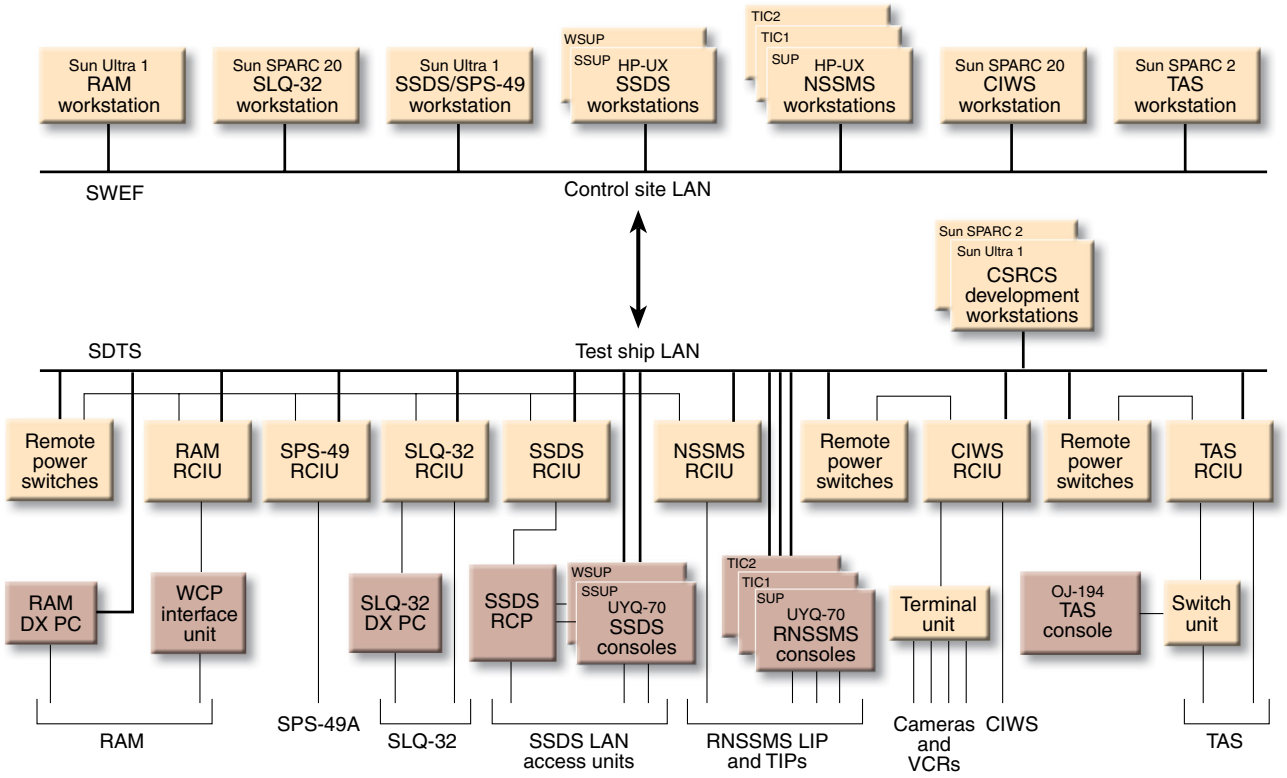

Figure 4. Block diagram of the CSRCS. Shipboard and remote site components and their connectivity are shown.

by the Olivetti and Oracle Research Laboratory that displays the screen image from the DX PC, operating in a Windows environment, on a Sun workstation at the remote site.

In a slightly different configuration, the SLQ-32 RCIU is connected between the SLQ-32 digital display processing unit, which is the console, and the digital processing unit (DPU) and also between the DPU and the SLQ-32 power rack. The DPU/console interface is a digital serial interface with a unique protocol. When remote control is selected, switching circuitry in the RCIU connects the DPU to interface circuitry that relays the console interface messages between the DPU and the RCP. The RCIU is also connected, via an Ethernet stub, to the SLQ-32 DX PC. The SLQ-32 RCP includes control for the DX PC and the SLQ-32 electronic countermeasures system.

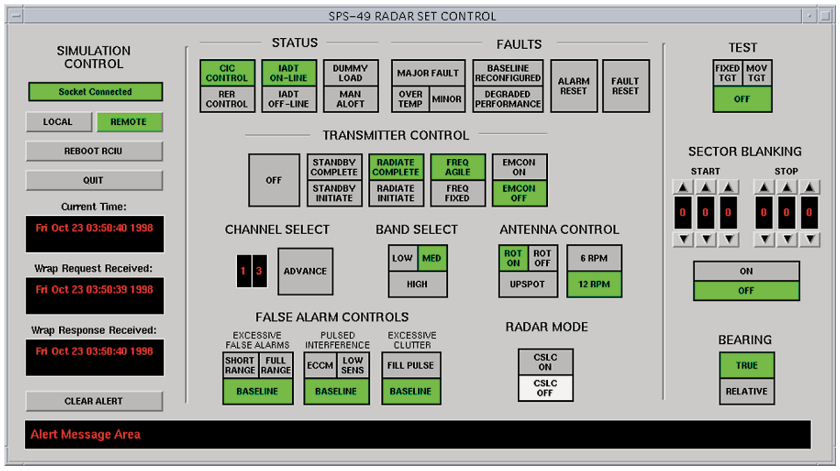

Figure 5. The SPS-49 RCP simulation contains many of the controls and indicators available on the shipboard console.

The SPS-49 RCIU is connected between the radar's signal data processor (SDP) and radar set control (RSC) cabinets. The SDP drives the indicators on the RSC and reads the RSC front panel buttons and switch states. When the RCIU is off or in local mode, the signals from the SDP pass through the RCIU directly to the RSC. When the RCIU is in remote mode, the signals from the SDP are switched from the RSC to a set of custom interface cards inside the RCIU. Relays on the interface cards, which can be set and cleared from the SPS-49 RCP (Fig. 5), emulate the buttons and switches on the front panel of the RSC. Other circuitry detects the states of the indicator signals, which are displayed on the RCP.

The CIWS RCIU includes a custom interface card supplied by Hughes Missile Systems (now Raytheon). It is connected to the CIWS Weapon Control Group computer

via a system bus, which is also used for the interfaces with the SSDS and the CIWS data collection system. The interface card transfers data between the CIWS bus and the VME bus, allowing the Weapon Control Group computer and the control processor in the RCIU to exchange commands and status. In addition to controlling the CIWS radar and gun, the RCS controls a thermal imager and several cameras and VCRs used to monitor and record CIWS engagements. The cameras are connected to a video channel-select switch, which is also controlled via the RCP.

The TAS is controlled through two separate units: an AN/UYA-4 console and an SSP. The console has an interface to the TAS computer and provides for the display and control of system functions controlled by the TAS computer program. The SSP interfaces with the TAS SDP and controls a small set of radar functions not controlled by the computer. The TAS RCIU is connected to the console interface through an external Navy Tactical Data System switch unit and to the SSP through custom-switching circuitry. The TAS RCP includes simulations of the console and the SSP on a single workstation.

Remote control connections to the SSDS and RNSSMS are different from the other systems. The RCIUs for these systems do not connect to the consoles. Instead, the consoles are connected directly to the shipboard LAN via the onboard Ethernet ports of their internal processors. HP workstations, acting as remote X-Windows clients, provide remote display and control of these systems. In addition, the SSDS and RNSSMS include system elements not controlled by the consoles, for which RCIUs and RCPs are required.

The CSRCS also has a DX capability for monitoring and troubleshooting its applications. The DX system resides in a separate chassis connected to the system network. Although it is not typically used during test operations, the DX system can record messages sent to it by the RCIUs. These time-tagged messages are available for off-line analysis and can aid in troubleshooting problems that might arise in the CSRCS.

REMOTE DISPLAY TECHNIQUES

The use of the network communications link allows great flexibility in implementing remote display and control systems. Any remote display technique that can be implemented on an Ethernet connection can be implemented between the SDTS and the remote control site, constrained only by data throughput limitations. Three different techniques have been implemented on the SDTS. In the technique used with the RCIUs and RCPs, display and control are implemented in two separate software applications which communicate using standard IPs. The SSDS and RNSSMS consoles use remote X-Windows. The VNC software for the RAM DX PC is based on a remote frame buffer approach. Several commercial and public-domain software packages are available for this purpose, but they are generally only applicable to Windows-based PCs.

The selection of a particular technique for each of the RCSs was driven primarily by considerations of network bandwidth use and difficulty (cost) of implementation. The network communications link has an ample throughput capacity of about 6 Mbits/s (four T1 telecommunication lines). Even so, its purpose is to support real-time operation of weapon systems, so it is important to restrict usage to well within the theoretical limitations in order to minimize network collisions and latent message delivery. Only the messages sent from the ship to the remote site need to be considered in determining throughput. The amount of data sent from the remote site to the ship, consisting mainly of operator controls, is relatively insignificant.

The RCIU/RCP approach is used most often. It requires the least amount of data to be exchanged. In this approach the messages sent from the ship to the remote site contain only the information to be displayed. The RCP has all of the information and instructions for displaying the data. In the remote X-Windows approach, the control panels are generated by the shipboard console, and the data sent from the ship to the remote display include the instructions for drawing the panels. This is usually a much larger volume of data, but the approach is used for the SSDS and RNSSMS because of the difficulty of hosting those display applications at the remote site. The remote frame buffer approach is very simple and inexpensive to implement, and because the commercial software used to implement it is designed to work over telephone modems, it does not require much data throughput. However, because these applications are designed for low data rates, they typically update the displays only once per second, which is insufficient for real-time control of the combat system. Consequently, they are used only for control of instrumentation, which is not time critical.

The RCIUs and RCPs exchange messages through a standard client-server protocol using Transmission Control Protocol (TCP)/IP sockets. The RCIUs act as the socket servers. Upon initialization, they wait for a request for a socket connection from their associated RCP client. After a socket is established, the RCIU and RCP communicate by exchanging predefined status and control messages. This message exchange is facilitated by packages of message passing and socket-handling software routines known as common socket handlers. One set of socket-handling routines, which runs under the VxWorks real-time operating system, was developed for use with all of the RCIU software. Another set, which runs on the Sun workstations, was developed for use with all of the RCP applications. Each

RCIU application will accept only one client application, so it is impossible for two instantiations of an RCP to inadvertently share control of a system.

In addition to the display and control messages, the RCIUs and RCPs also periodically exchange "wrap messages." These are used, in the absence of other data, to ensure that messages are still being passed. If an RCP does not receive a wrap message from its corresponding RCIU within a fixed time interval, an indication is given to alert the operator. This will typically occur because of a momentary disconnect in the communications link but could also be because of a failure of the RCIU. It is immediately apparent which is the case because if there is a disconnect in the network link, all of the RCPs will provide the same indication simultaneously. The TCP/IP socket protocol ensures that messages are delivered correctly and in sequence. Thus when communications are interrupted, the status and control messages are buffered and retransmission is attempted until either communications are reestablished or the buffers overflow.

The remote X-Windows approach used for the SSDS and RNSSMS required virtually no software development for either the shipboard consoles or the remote workstations. Only the start-up scripts for the console software were modified so that one of the remote workstations, rather than the console itself, was identified as the display server. Remote control is initiated by an operator logging in to one of the shipboard consoles from a remote workstation using a command shell and invoking the modified start-up script. When the console software starts, the displays are sent to the remote workstation rather than to the console, and input is taken from the remote workstation keyboard and mouse rather than from the console keyboard and ball-tab.

The X-Windows client and server also communicate via TCP/IP sockets. Thus when momentary disconnects in the communications link occur, messages are buffered, as with the RCIU/RCP approach, until communication is reestablished or buffers overflow. No alert is given to the operator, but because these displays are very active, a disconnect is usually immediately obvious. However, because of the volume of data being sent over the link, the buffers can overflow much more quickly, causing the remote displays to be disconnected. When this occurs, the console applications have to be restarted to reestablish remote control. This makes the remote X-Windows approach somewhat less robust than the RCIU/RCP approach.

The remote frame buffer approach is implemented in the CSRCS using the free VNC software application. VNC is also based on client and server components which communicate over the network. Several versions of the client and server applications are available for Windows PCs and various UNIX workstations. The server application captures the raster scan data comprising the screen image of the PC or workstation on which it is running and sends it to the client application. The client application, running in a remote PC or workstation, displays the screen image of the server PC in a window on its own display. Mouse and keyboard commands executed on the client machine are transmitted to the server. The client and server applications do not have to be the same type of platform or operating system. With VNC, it is possible to use a UNIX machine for remote control of a PC or vice versa.

COMMUNICATION AND WEAPON SAFETY ASSURANCE

In addition to providing remote control of the normal combat system functions, the CSRCS includes features for handling the inevitable lapses in communication between the ship and the remote site and for ensuring system safety, particularly when communication is lost. Although the communications link provides fairly robust connectivity, as with any wireless system, uninterrupted communication cannot be guaranteed. Interruptions, therefore, must be managed. The two principal requirements for the control system are to ensure that the shipboard systems, particularly the weapon systems, revert to and remain in a safe condition when communication is lost and to resume operations once communication is reestablished.

When momentary lapses in communication occur, the combat system continues operating as normal, based on the last input received from the operator. Because all of the actual combat system elements, including consoles, are on the ship, only the operator is disconnected from the system; the system itself remains intact. Indicators on the remote workstations alert the operator to a lapse in communication with the shipboard system. If the outage is relatively brief, the messages will be retransmitted and the displays updated accordingly when communication is reestablished. If the outage exceeds the capacity of the control processors or shipboard consoles to buffer the data, the remote displays have to be reinitialized. This typically requires an outage of several minutes, with the actual duration depending on the system activity at the time. If communication is lost for more than 5 min, the TAS and SPS-49 RCIUs will disable radiation and antenna rotation of their respective radars. If those systems are rotating or radiating, they will be shut down as a safety precaution.

If any of the weapon systems are in the "arm" state (or "weapons free" state in the case of the RNSSMS) when communications are lost, they will be forced back to the "safe" state (or "weapons tight" in the case of the RNSSMS) after a given time. This is accomplished by a pair of relays with associated timer circuits, referred to as "arm" and "arm lock" timers, which are in each of the weapon system RCIUs. The arm and arm

lock timers work in tandem to control the state of their respective firing circuits.

The purpose of the arm timer is to force the weapon system to a safe (weapons tight) condition if communication is lost while the system's firing circuitry is enabled. To enable a system's firing circuit, an arm command must be sent by the weapon system's RCP. When an arm (weapons free) command is received by the RCIU, the arm relay is closed and the arm timer is started. This 1-min timer is implemented by a counter circuit. When it times out, the relay is opened and the weapon system reverts to safe (weapons tight). However, while in the arm condition, the RCP automatically continues to send arm commands at 0.5-min intervals, reinitializing the counter and maintaining the arm state. If communication is interrupted for more than 1 min, the counter will time out and the relay will open, forcing the weapon to the safe (weapons tight) state.

The purpose of the arm lock timer is to maintain the arm (weapons free) state for a short period of time, even if communication is lost. Typically, during a test event, arm lock is set after the test range is cleared and just before launching the target at the ship. This allows the system to complete an automatic engagement of a target if communication is lost after the engagement begins. When the operator sends an arm lock command, the arm lock relay is set and the arm lock timer is started. This 4.5-min timer is also implemented in a counter circuit. The arm lock relay overrides the arm relay, so that even if the arm counter times out, the system will remain armed until the arm lock counter expires.

WEB-BASED INTERFACES

Remote Power Control

To facilitate the operation of the shipboard equipment from the remote site, each RCIU is supplied power through a remotely controlled power strip. Each power strip is connected via the LAN to the Ultra 1 workstation aboard the ship. The Ultra 1 hosts a Web server, allowing the power strips to be accessed from any workstation on the CSRCS network via a Web browser. The browser interface provides independent control of each of the eight sockets on the power strip. The available controls are "off," "on," and "reboot." Reboot cycles the power, turning it off for a few seconds and then turning it back on. This is particularly useful when it is necessary to remotely perform a hard reboot of an RCIU.

Network Utilities

The CSRCS incorporates WebPing, a Web-enabled utility, to provide overall system status as well as a survey of all the nodes on the CSRCS network by using a graphical red/yellow/green stoplight to indicate whether each element of the CSRSC is down, unavailable, or up, respectively. This information is summarized on a single Web page, allowing a quick glance to determine the availability of the CSRCS elements.

A data reduction utility is also available via a Web browser. This utility can be used to analyze any message data recorded by the CSRCS DX function. It employs two common gateway interface programs to obtain information from and provide results to the user. The user specifies a file name and the desired data product, and the data reduction utility produces the data product and presents it to the user in a browser window.

In addition, some documentation is provided online. Documents describing system components are provided in HTML format, making them readily accessible from various computing platforms. Other documentation provided online includes procedures for managing the CSRCS software configuration, backing up the CSRCS workstations, and initializing and operating the various CSRCS components.

TESTING ABOARD THE SDTS

The SDTS has been used to support the testing of CIWS, RAM, ESSM, and other systems. These tests have included remote control operations, both manned and unmanned.

From April to June 1997, CIWS Block IB was tested aboard the SDTS. The most significant upgrades to the Block IB variant were the addition of a forward-looking infrared imaging system and the capability to use the system against surface targets, e.g., small boats. The CIWS Block IB installation aboard the SDTS is shown in Fig. 6. The forward-looking infrared imaging system is mounted on the right side of the radome. Block IB underwent several remotely controlled tests including operations against seaskimming and diving antiship missiles (ASMs). A successful remotely controlled engagement of a seaskimming ASM is shown in the inset of Fig. 6.

In 1998 and 1999, the SDTS hosted both manned and unmanned RAM tests. The RAM launcher, as installed aboard the SDTS, is shown in Fig. 7. Seaskimming and diving ASMs, both subsonic and supersonic, were presented as targets during the tests. An intercept of a supersonic seaskimming ASM is shown in the inset of Fig. 7.

ESSM testing on the SDTS began in 2000 and is expected to continue into 2002. The ESSM test schedule calls for 12 remotely controlled missile engagements from the SDTS. The first ESSM firing, in April 2000, is shown in Fig. 8.

The SDTS has been used for critical testing of short-range self-defense systems against ASMs as well as less stressing targets, e.g., small, slow aircraft; jet aircraft; and small boats. It has proven invaluable for testing these various systems. Without the SDTS, testing such systems against realistic targets in realistic scenarios would not be

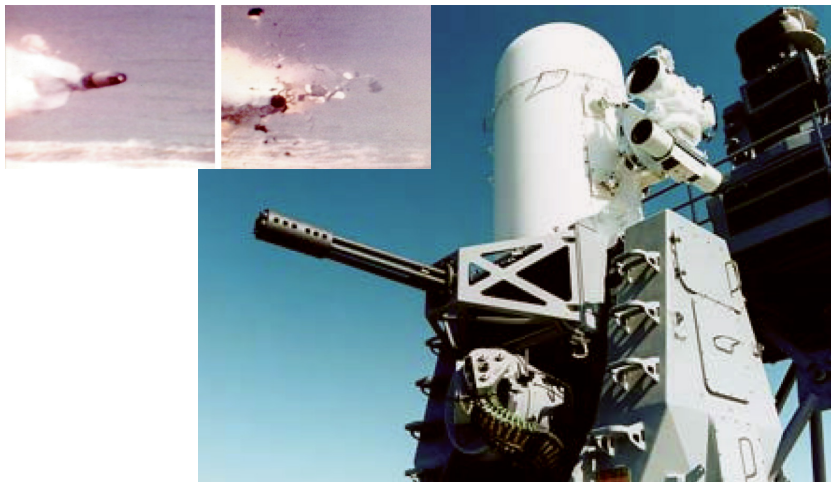

Figure 6. CIWS Block IB installed aboard the SDTS. Inset illustrates the successful engagement of a seaskimming ASM.

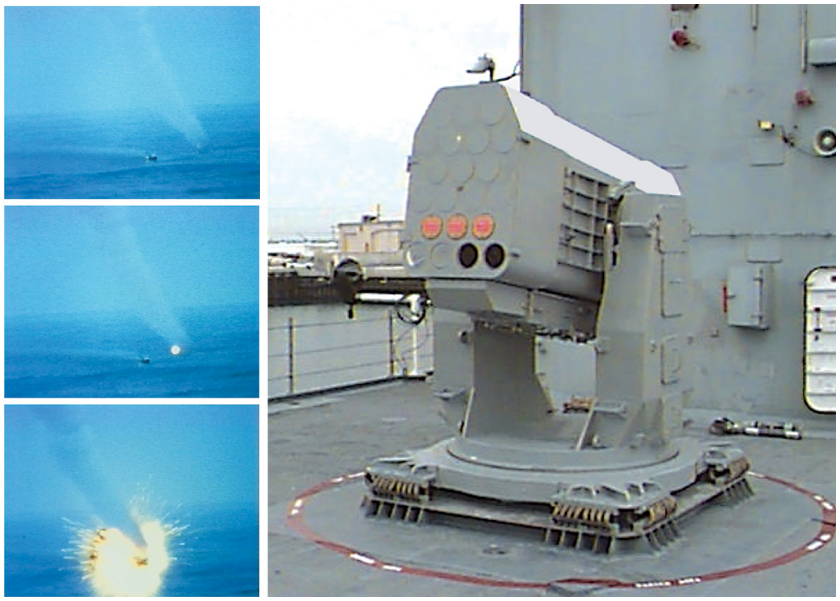

Figure 7. RAM launcher installed aboard the SDTS. Inset illustrates RAM successfully engaging a seaskimming supersonic ASM (inset courtesy of Raytheon).

possible. A summary of operations during which ASMs were engaged by systems aboard the SDTS is given in Table 1, which indicates the various types and numbers of ASMs flown against the SDTS.

CONCLUSION

The SDTS and the CSRCS allow the Navy to safely conduct realistic and effective testing of its ship self-defense weapons against targets representative of expected threats.

The CSRCS incorporates a variety of commercial and custom hardware and software elements to provide remote operator control of several sensor, weapon, and command and control systems, as well as many associated instrumentation systems, all having unique system architectures. It also applies a variety of remote control

Figure 8. The first launch of an ESSM from the SDTS in April 2000.

Table 1. Summary of operations in which ASMs were engaged by SDTS systems.

Year	BQM-34S	MM-38	BQM-74E	Harpoon	Harpoon Stream[a]	Vandal ER	Vandal EER	Vandal Diver	Vandal Stream[a]	SETT-8A	HARM
1995						2					
1996				3		2				2	1
1997				1						1	
1998	1	1	1	2				1			
1999	1		3		2		3	2	3		
2000											
2001			2								
Total	2	1	6	6	2	4	3	3	3	3	1

[a]Represents actual number of targets flown, not number of scenarios.

techniques. The use of a digital telecommunications link, which supports standard IPs for interprocessor communication, provides the flexibility to select appropriate techniques for each system. The CSRCS provides operator-intuitive interfaces of a large subset of controls for each system in a uniform X-Windows environment. It also provides controls, necessitated by the remote aspect of system operation, for ensuring system safety, managing communications link failures, and rebooting system elements if required.

The SDTS CSRCS has successfully supported CIWS Block IA and Block IB testing and RAM DT/OT. It is currently being used to support testing of the RNSSMS and ESSM.

THE AUTHORS

RICK R. YORK is a member of APL's Senior Professional Staff and a project manager in the Air Defense Systems Department. He holds a B.S. degree in mathematics from the University of Maryland, University College. Since joining APL in 1982, Mr. York has worked primarily on integration, test, and evaluation of surface ship anti-air warfare systems including the NATO AAW System, Ship Self-Defense System, and Rearchitectured NATO Seasparrow Missile System. He was the lead engineer for the development of the Self-Defense Test Ship Combat System Remote Control System and currently manages APL's NATO Seasparrow and Evolved Seasparrow Missile projects. His e-mail address is rick.york@jhuapl.edu.

KIRK L. BATEMAN began his career at APL in 1986 and is a member of the Senior Professional Staff assigned to the Air Defense Systems Department's Combatant Integration Group. He received a B.S. degree in 1986 from the University of Colorado and an M.S. degree in 1991 from The Johns Hopkins University, both in electrical engineering. At APL Mr. Bateman has worked on various radar, sonar, and naval combat systems projects. Most recently, he has provided system engineering support for the Ship Self-Defense System Mk 2, particularly in the areas of combat system interoperability and sensor integration. Mr. Bateman's e-mail address is kirk.bateman@jhuapl.edu.