

# Reagan Test Site Distributed Operations

Timothy J. O'Rourke, John A. Nelson, and John G. Volan

A transformational program fundamentally changed mission execution and operations at the Reagan Test Site on the Kwajalein Atoll. The site has become a globally operated test range through the use of a recently installed fiber-optic cable connecting communications between the atoll and Guam, and the development of an open system architecture that enables remote, distributed operation of the radar systems at Kwajalein.



**The U.S. Army's Reagan Test Site (RTS)**, approximately 2300 miles west south west of Hawaii on the Kwajalein Atoll, is ideally situated for missile testing because of its geography and its strategic location in the Pacific [1]. The atoll's distance from launch facilities at Vandenberg Air Force Base in California and its isolation from populated areas are advantages that the Army saw when the site was chosen for conducting research on ballistic missile defense 50 years ago (Figure 1). The subsequent development of RTS's unique instrumentation sensors, including high-fidelity metric and signature radars as well as optical sensors, has made the site a world-class range and test facility that plays a key role in the research, development, test, and evaluation required to support U.S. missile defense and space programs (Figure 2). RTS is also available to users from commercial organizations and government agencies such as the National Aeronautics and Space Administration (NASA). However, the remote location increases transportation time and cost for scientists and customers to be present to view or contribute to their missions. In addition, bandwidth for data and communication transfers off the atoll was limited by satellite communications. To make the facility more accessible to users, Lincoln Laboratory scientists and engineers undertook a program to distribute the operations of the range from Kwajalein to the continental United States (CONUS). In the process, RTS capabilities were vastly improved.

Lincoln Laboratory, as the scientific advisor to RTS, has long supported the operations at the range and conducted upgrades to the sensors and command-and-control infrastructure. During the late 1990s and early 2000s, the

Laboratory helped modernize the radar suite at RTS, applying an open systems architecture that enabled the radar systems on Roi-Namur Island to be directed remotely from RTS headquarters on Kwajalein Island and that decreased both cost and manpower to operate the radars [2]. The most recent effort to enhance the functionality of the site, the RTS Distributed Operations (RDO) program, transformed RTS from a locally operated range to a globally operated national asset. A fundamental aspect of the program involves the distribution of mission tasks among various locations and remote operation of the range's sensors, command-and-control center, and space operations [3].

The RDO project focused on

- Allowing range operations from CONUS
- Distributing RTS activities
- Improving range accessibility for users
- Enhancing interoperability with users and other ranges, sensors, and elements
- Increasing information availability with reliable, high-bandwidth communications

The RDO program achieved improvements and modernization in four key functional areas: communications, distributed systems, sensor modernization, and mission operations. In addition, relocating the facility closer to its customers has provided improved access for mission execution activities as well as for training, demonstrations, mission planning, and data distribution.

Since completion of the project, the primary command-and-control facility was relocated to the U.S. Army Space and Missile Command in Huntsville, Alabama, instead of its previous location on Kwajalein Island. Distributed operations to control space operations from the Huntsville center began in October 2011, and Huntsville became the primary control center for test operations in December 2011. The initial test operation in early 2012 was the GT-203 mission, an Air Force Minuteman III missile test. All aspects of the control center including hardware, software, networks, and the facility functioned successfully.



**FIGURE 1.** The map shows the isolated location of the Reagan Test Site. The inset of Kwajalein Atoll points out the site of the radars, the island of Roi-Namur, and the operations center site, the island of Kwajalein.

### Communications Upgrade

The communications upgrade focused on the core networking and communications infrastructure linking Kwajalein; the U.S. Army Space and Missile Defense Command in Huntsville, Alabama; and Lincoln Laboratory in Lexington, Massachusetts. A reliable, high-bandwidth, low-latency network was vital to creating a distributed range in which the command-and-control center and the sensors are operated from 7300 miles away. A key infrastructure improvement was a high-speed, fiber-optic cable, known as the Kwajalein Cable System (KCS), which connects the Kwajalein atoll to land lines on the island of Guam. Completed in fall 2010, the fiber cable provides the high speed and high bandwidth required for test and space operations, and for missile defense research, development, test, and evaluation. The initial networking capability to CONUS is approximately 622 megabits per second, with a less than 300-millisecond round-trip latency, a significant improvement over



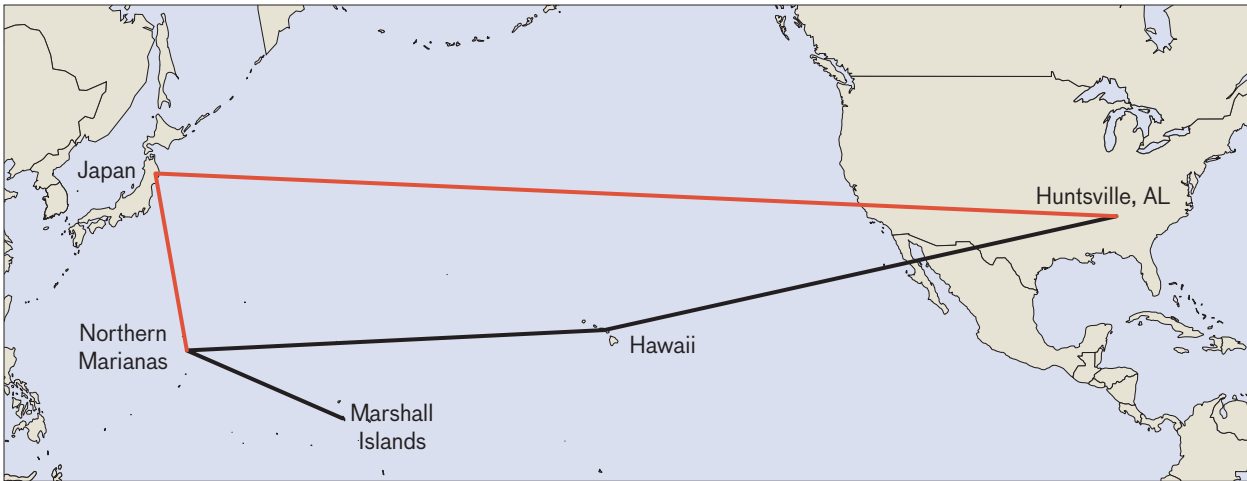
**FIGURE 2.** The suite of radars on Roi-Namur Island in the Kwajalein Atoll.

the previous 45-megabits-per-second, 600-millisecond latency satellite link.

The KCS is part of a larger government networking upgrade that supplies wide-area network (WAN) connection between Kwajalein and Huntsville. The KCS also facilitated the implementation of other cable systems. Nearby Ebeye and Majuro Islands in the Marshall Islands and Pohnpei in the Federated States of Micronesia will be connected to the KCS trunk. This new cable system, named after its owner Hannon Armstrong Capital LLC and its operator Truestone LLC, is known as HANTRU-1. While the HANTRU-1 cable system is not part of the RDO project, the KCS enabled HANTRU-1 and provided the backbone for high-bandwidth connectivity from the aforementioned islands to the rest of the world.

Vitally important to sustained, reliable communications is a system's ability to continue operating, even

at a reduced level of performance, if some element of the system fails; this ability is termed fault tolerance. To provide fault-tolerant capabilities, KCS uses two unidirectional fiber-optic strands with multiple wavelengths to enable optical carrier-level 192 (OC-192, a data rate of 10 Gbps) service. From Guam, the network is connected via a Navy ring to the Defense Information Systems Agency's Defense Information Systems Network (DISN) core. The network takes two diverse paths, one through Hawaii and one through Japan, to the Redstone Arsenal in Huntsville, Alabama (Figure 3). From the Red Stone Arsenal, the two diverse paths progress to the RTS Operations Center in Huntsville (ROC-H) and are connected to two separate Cisco 6506 routers. Once inside ROC-H, the redundant paths are maintained by using dual routers and switches. Every computer connected to the network has two network interface cards, each of which is connected to one of the networks. The comput-



**FIGURE 3.** Communication from Kwajalein to Huntsville is implemented over two distinct fiber-cable paths. The red line indicates the route via Japan, and the black line indicates the route via Hawaii.

ers use a technique called port bonding, which allows on-the-fly failover (a switch-over to avoid system failure) from one network to another should the primary network go down.

Within the ROC-H, the Huntsville Mission Control Center (HMCC) and the Huntsville Space Operations Center (H-SPOC) are state-of-the-art facilities in which both

space operations and test operations can be fully manned. HMCC’s main console room (Figure 4) contains a “horseshoe” computer console for mission operators, individual operator rooms for each sensor, two viewing towers from which researchers and guests can watch operations during missions, and a video/audio area for controlling the video wall and other displays.



**FIGURE 4.** The horseshoe in Huntsville’s Mission Control Center is the hub of mission operations.

## Distributing Operations

The distribution of activities of the RTS operational control center was achieved by developing software that enabled the system to be controlled by multiple operators at various locations. Primary operations are conducted from HMCC, while a mission capability is retained at Kwajalein (Figure 5). One goal of the RDO project was to integrate the control center's operations—space, command-and-control, and radar. The primary advantages of a distributed center are expanded customer access and a common environment that better utilizes personnel as a single group of operators can manage both space and reentry missions.

## RDO's Core Software Architecture

The design concept for RDO was to provide both a remot-ing capability from Kwajalein to Huntsville and a distrib-uted capability, allowing operators and data processing to be situated at multiple locations simultaneously. This design allows the most efficient use of operators and equipment, with operators of a single mission at dispersed locations acting as one integrated control center.

RDO's core software architecture was designed and built using the latest technology, incorporating a net-centric, open architecture that enables easy upgrades and enhancement capabilities. A modular, distributed approach affords a customizable configuration that allows command, control, displays, algorithms, and operators to be located at different locations or in various config-urations depending on the desired setup. The modular approach also provides a plug-and-play capability for adding new hardware or software components without disrupting current operations or functionality.

The majority of the core computational software was developed using the Java programming language. A very small portion of the software was developed with the C programming language, and the Extensible Markup Language, XML, was used for the configuration files. The GNU Bourne Again SHell (Bash) was used for shell scripting.

Each location at which operators conduct a mission is referred to as an RDO node, defined as a cluster of servers within a local area network (LAN) at a given geographic location, separated from other such nodes geographi-cally but connected to them via the wide-area network. Nodes are also considered to be separated organization-

ally, meaning that different human organizations may be involved with their administration, requiring that they remain relatively autonomous. Operators in different organizations log into their respective nodes only and do not directly touch the resources of other nodes.

The collection of nodes participating to form an inte-grated RDO system at any given time is called an enter-prise. A given node may be configured to participate in different enterprises at different times. A node may even be configured at certain times to act as a standalone enterprise not connected to any other node.

The RDO system is capable of executing live missions, simulations, or playbacks. RDO refers to any instance of a live mission, simulation, or playback as an activity. An activity utilizes all or a subset of the resources avail-able in the currently defined enterprise. Activities can be configured or customized to run selected algorithms and components; in addition, each activity can be configured to select the active nodes, hardware, and software compo-nents. Software components can be assigned to available hardware during the activity configuration but can also be rehosted to other hardware dynamically as required.

RDO supports multiple activities running simultane-ously. The components in different activities do not com-municate with each other, so activities can be considered isolated from each other. The collection of components of an activity that run on hosts within a given node is called a node activity.

Management of both simultaneous activities and activities operating across multiple nodes is accomplished by using the Distributed Activity Management (DAM) software component. To manage resources in and across activities, nodes, and enterprises, DAM supplies tools for controlling, monitoring, and viewing status information, such as what activities and components are currently running on which host machines within the nodes of the enterprise and how messaging channels are being flowed between nodes.

DAM also maintains the control database, which registers the current state of RDO activities within the enterprise. Each node has its own copy of this control database. DAM global services guarantee that changes of state are distributed to all nodes participating in the enterprise and are replicated in their local control data-bases. Because of this design, other subsystems of RDO that need access to state metadata are able to query



**FIGURE 5.** The modernized mission command-and-control center at RTS remains in use.

their local control database for it, without having to make remote calls to other nodes to ascertain the current activity state.

Running multiple activities at multiple locations required the development of a user role management system. Each activity has specific role assignments. User roles can be created and assigned at activity creation time or changed dynamically during an activity. Each role specifies distinct permissions assigned to operators within an activity. Permissions include a wide range of control, from top-level control for starting, stopping, or modifying activities, down to control of individual commands and button pushes allowed by each operator.

### Communications and Middleware

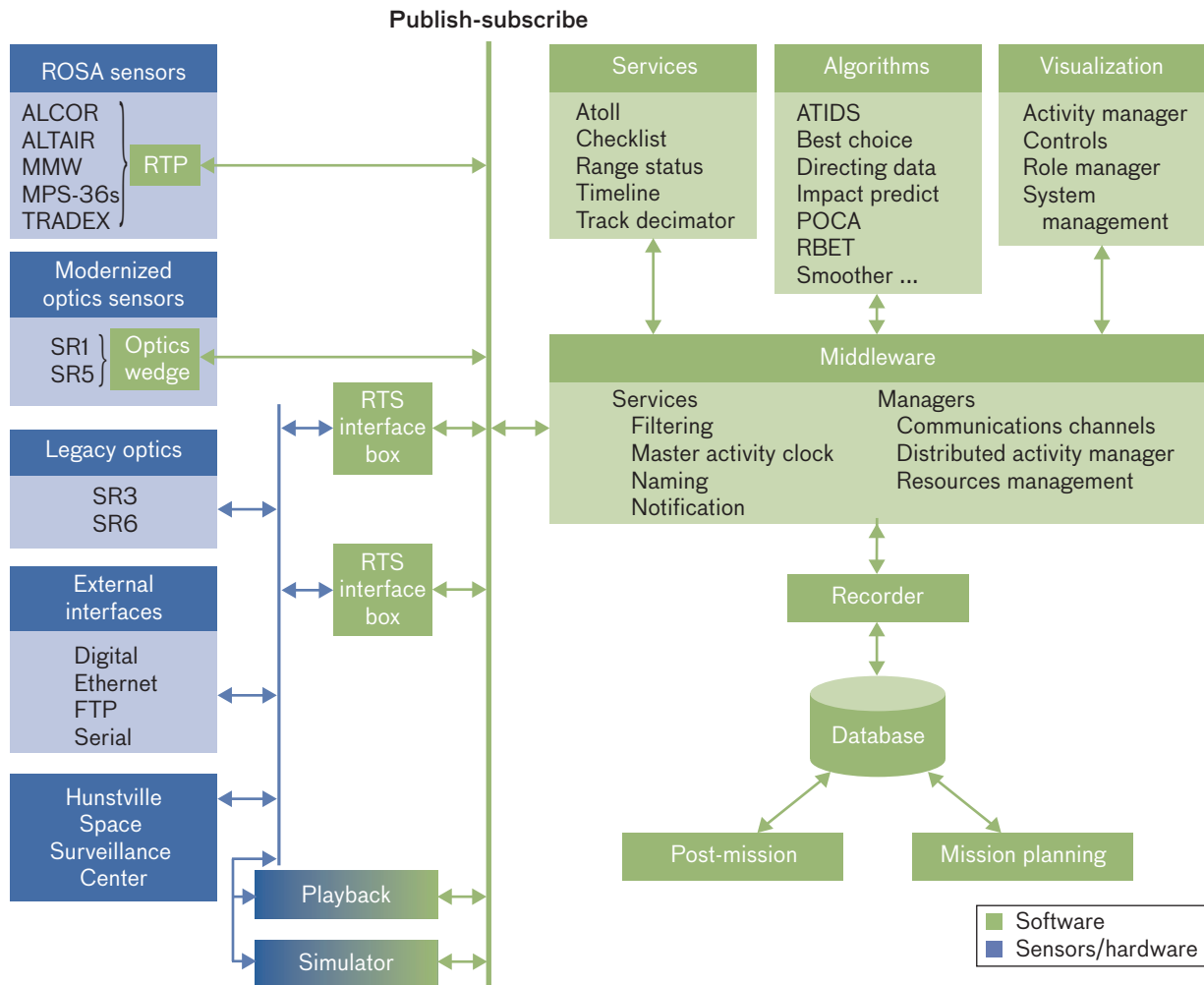
In the RDO architecture, components communicate in a distributed fashion via middleware. Middleware refers to intermediary software that manages interactions between separate applications; it has been metaphorically termed the “glue” between applications. In the RDO environment, middleware provides communications across a LAN and WAN using Internet protocols (IP). The middleware provides (1) an isolation layer that simplifies the development process by insulating developers from the complexities of network protocols and communications, and (2) a common communications interface for all com-

ponents. Components communicate via middleware by sending messages using a publish-subscribe paradigm (Figure 6). A component subscribes to sources of data and publishes data for other components to use. The details of the actual transport can be specified by a configuration file; these details might include whether to use transmission control or user datagram protocols (TCP/IP or UDP/IP), for example.

Of the several types of available protocols, the two most prominent are unreliable broadcast and reliable point to point. These two protocols map to the two most predominant message types in RDO: data and commands. The majority of RDO’s data is sent using unreliable broadcast. These data include information such as track data, target identifications, and status messages, and do not need to be reliable because the data are updated on a 1 to 20 Hz rate. If a few data packets are dropped, the following packets will contain the required information to continue. Testing showed that very few packets are actually dropped over the RDO WAN; however, not all networks are as reliable as this, and RDO was designed to work over a range of network configurations, including disadvantaged networks. Command messages, the second most common type, allow one component to instruct another component to perform a specific function, or mediate between a specific control view and its associated algorithm or service. Commands require guaranteed delivery, so a reliable point-to-point protocol is used.

Because the system is designed to afford the ability to run multiple simultaneous activities, it must avoid cross talk between activities and must keep data published in one activity from being received in another. The middleware meets these requirements by providing separate name spaces that enable noninterfering communications and compartmentalized data. The middleware also implements the following features:

- Resource management that supports the allocation of and exclusive access to resources (such as radars and other sensors) among the interfaces, algorithms, recorders, agents, and services. These resources cannot be shared by activities.
- Monitoring that tracks the heartbeat status of RDO software components and alerts the user if a fault is detected. The user then has the option to restart the component, rehost the component on another system,



**FIGURE 6.** The block diagram of RDO components illustrates the publish-subscribe interactions between sensors (on left), components/applications, and middleware. In the figure, RTP stands for real-time program, ATIDS is automatic target identification system, POCA is point of closest approach, and RBET is real-time best estimate of trajectory.

or continue without it.

- Multicast mapping that allocates noninterfering multicast addresses and ports on a per activity basis.
- Notification service that sends messages to a set of recipients when an event occurs.
- Global Name Service that serves as a lookup table and registry for network objects.

### Fault Tolerance and Recovery

RDO's design enables fault tolerance and recovery capabilities in the areas of hardware, software, and networks. It provides redundant end-to-end network path hardware starting from the dual network interface cards on each computer, extending through the network with dual routers and switches, and continu-

ing over the wide-area network with dual diverse paths between Kwajalein and Huntsville.

The hardware fault tolerance (independent of network hardware) is achieved through the use of dual servers for each major hardware component. For example, the RDO design utilizes dual database servers, dual system service computers, and a cluster design for home accounts, Network File System (NFS), and Lightweight Directory Access Protocol (LDAP) services. In addition, user accounts are housed on a network-attached storage device that has dual power supplies and network interface cards and is configured with a redundant array of independent disks that employs both striping and mirroring technologies.

Each RDO software component includes a mechanism for fault detection and recovery. RDO software

# RDO Net-Centric Technology and Demonstration

RTS shares technology and information through net-centricity

The concept of using net-centric technology in Department of Defense (DoD) systems was introduced in the late 1990s. Net-centric refers to a system of interconnected devices and services that share information over a communications network. Net-centricity addresses the challenge of managing interactions among DoD systems, which were traditionally designed to work independently.

RDO took a two-pronged approach with respect to net-centricity by using internal net-centric services to communicate within and between RDO nodes, and external net-centric services to communicate to outside entities and services. As part of the net-centric technology development program, RDO participated in two net-centric demonstrations between 2008 and 2010. These demonstrations were a collaborative effort among multiple divisions within Lincoln Laboratory and showed the usefulness of sharing multiple DoD assets in a timely manner to achieve a unified goal within national missile defense.

The first demonstration focused on using net-centric brokering technology to dynamically allocate resources in real time. Lincoln Laboratory's Communication Systems and Cyber Security Division developed the brokering technology and led the demonstration. The resources being allocated by the broker were the RTS

radars, which represented national missile defense systems. In this demonstration, the resource broker allocated resources normally, working in separate domains (space and missile defense) to achieve a single unified goal of collecting critical radar data on an incoming missile. Results showed how a net-centric approach could be used to help protect the United States from a foreign ballistic missile attack.

To set the scenario of this first demonstration, imagine an adversarial country launching a ballistic missile at the United States. To protect the nation from the threat, a series of actions would be required. First, the foreign launch would have to be detected, and a command center alerted to the threat. Second, the command center would have to obtain information to identify the missile track and impact point. Next, information would be needed to identify which objects deployed from the missile were lethal. Once the lethal object was identified, an accurate track on it would be required in order for the military to launch an intercept missile.

The demonstration was conducted during a live-fire Air Force Minuteman III (MMIII) missile launch from Vandenberg Air Force Base in California. The MMIII's impact point was in the Kwajalein Atoll region. The demonstration began when a notification of a

foreign missile launch was sent to the acting ballistic missile defense center at Lincoln Laboratory. Upon receipt of the notification, the control center's task was to obtain radar tracking information on the threat. The command center placed a request with the resource broker for radar data to be collected. The request was sent to the resource broker with information regarding the missile launch location. The resource broker used the launch location information to search a registry database of available, suitably located radars capable of collecting data on the threat. The resource broker identified an appropriate low-resolution sensor and automatically tasked the sensor to track the threat.

In this scenario, the sensor was the Target Resolution and Discrimination Experiment (TRADEX) radar at Kwajalein. TRADEX began tracking the incoming missile and flowed the track information back to the command center for analysis. The command center analyzed the incoming data and determined that the missile's track could be a threat, but more information was required to correctly identify which object being tracked was the lethal object.

The command center sent a request to the broker for more information on the target. This time, the command center requested data at a higher resolution. The resource bro-



ker searched the registry for sensors capable of attaining higher resolution data and found a capable sensor, the Millimeter-Wave (MMW), in the correct location. However, the sen-

to collect data on the incoming object. The high-resolution sensor autonomously switched domains from space operations to ballistic missile defense, tracked the requested objects, and

to test the net-centric capability, no interceptor was launched (obviously).

Upon completion of the data collection, the MMW returned to the routine space tracking and the

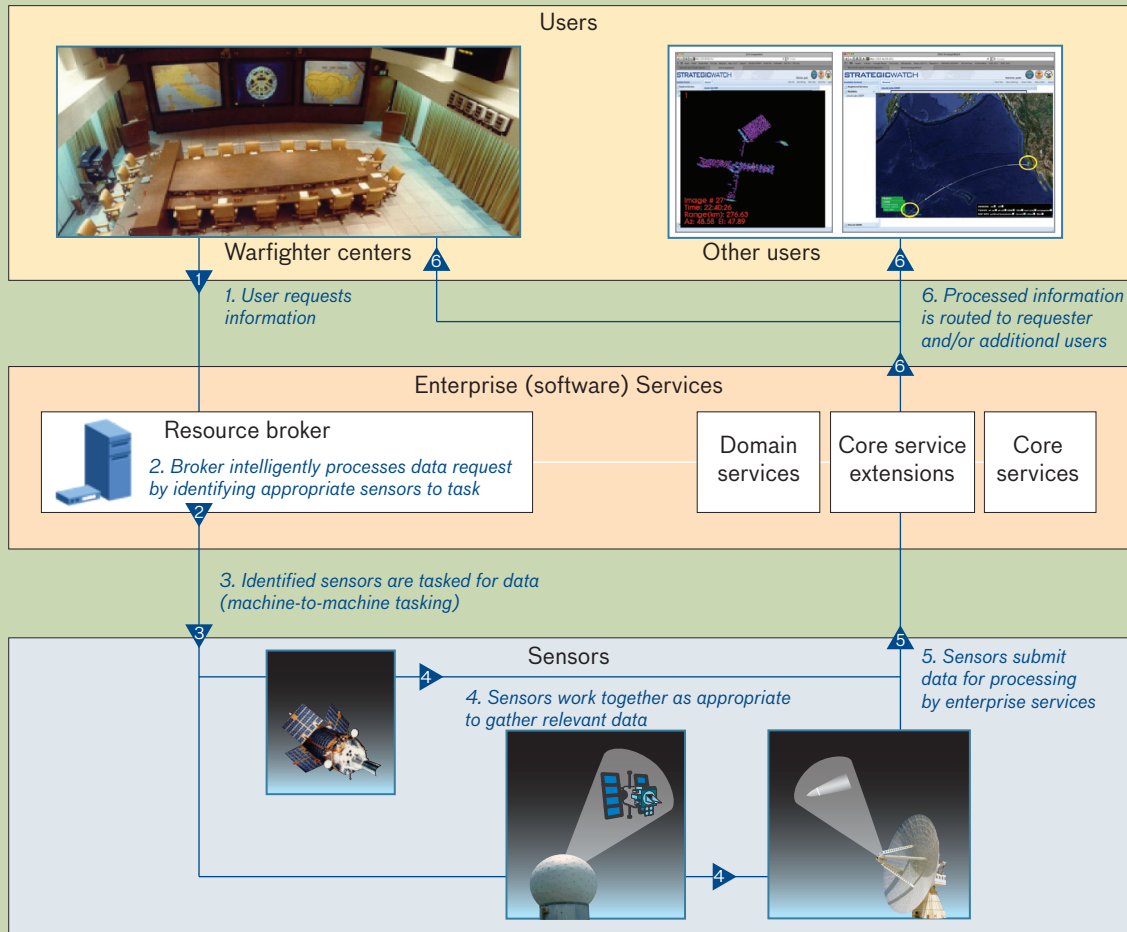


Illustration of the cross-domain, net-centric technology demonstration. Sensor data are communicated and processed by enterprise services to provide situational awareness to command centers via user-defined displays.

sensor was currently involved in routine space tracking operations. Because the defense of the nation from possible incoming threats is a higher priority than routine space tracking, the resource broker overrode the tasking of MMW and automatically tasked it

sent the data to the command sensor. Upon receipt of the high-resolution data, the command center was able to identify the threat and order appropriate action to defend against the threat. Because this was an exercise utilizing the opportunity of the MMIII mission

low-resolution TRADEX radar was released and returned to its previous state. All aspects of the demonstration worked as designed. The demonstration was a successful illustration of how of net-centric technology may be used in a real-world situation.

components are capable of being executed on any available server computer although components are generally assigned to a specific host during the creation of an activity. Each component is monitored during activity execution through the use of a software status display, the activity manager. If any component fails, the component can either be restarted on the same computer or rehosted to another computer. If an entire computer fails, all components on that computer can be rehosted to another computer. RDO utilizes commodity server hardware for quick, efficient replacement of failed systems. In general, spares are readily available for a quick swap if required.

Current component runtime state can be restored to the new instance of the RDO component automatically to further lessen the overall impact of a single server computer failure. Components save state directly to the component-configuration-object table in their associated activity log database at a 1 Hz rate. This saved state allows components to restart in the state before failure. The contents of component state vary, but typically include the information contained in startup configuration files, modified by real-time commands.

RDO provides redundant guaranteed recording through the use of two recorder components responsible for recording data into activity databases: a primary recorder running on the primary activity database server, and a backup recorder running on the backup activity database server. Both recorders continually log the same data. If either database server fails, the same data will continue to be recorded by the other recorder on the other database server. This arrangement provides passive redundancy without any need for explicit failover.

### Sensor Modernization

The range's sensors were modified to facilitate distributed operations and to reduce operation and maintenance costs. Video cameras were installed in critical unmanned areas as well as in console and equipment rooms. The video feeds are distributed to remote locations through the use of a video server. Both environmental and physical monitoring sensors were installed. The monitoring systems include ones for smoke, fire, air or component temperature, air flow, humidity, temperature and pressure measurements for the water to cool transmitters, waveguide pressure sensors, and facility alarm monitor-

ing. Information from the monitoring sensors is collected continuously and stored in a centralized database. The information can then be viewed in real time or as historical reports by engineers at remote locations through the use of a web browser, providing system test capabilities to aid in system checkout and fault isolation.

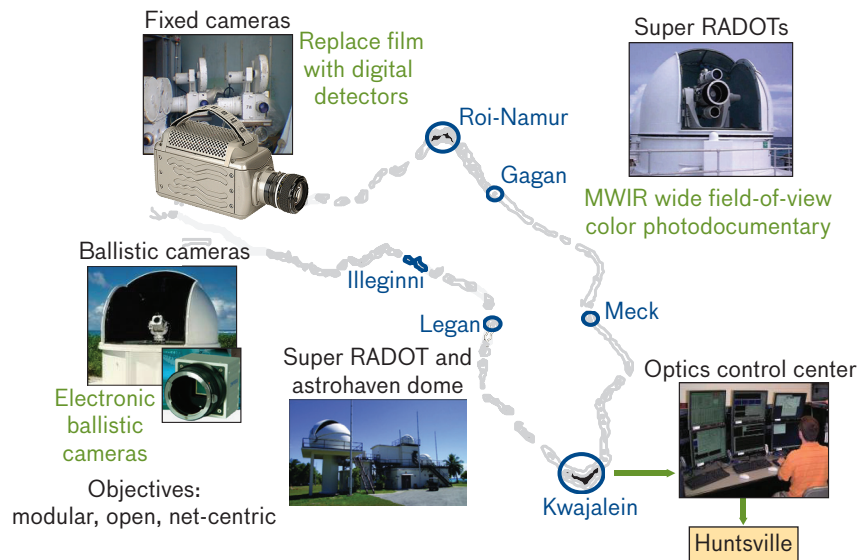
Each of the radars was also upgraded to provide the capability for remote control of the antennas and transmitters. Programmable logic controllers manage the remote control. The new capability of remote control required another enhancement: the ability to autonomously place the antennas and transmitters in a safe state should communications between the hardware and operator be interrupted. A "heartbeat" message (a message validating system health/availability) sent between the hardware and operator controls verifies communication status. If the transmitter hardware stops receiving heartbeats, an automatic shutdown process is engaged. The shutdown process follows a configurable timeline to allow for graceful degradation of the system.

### Mission Operations

Mission operations were improved by more precisely defining concepts of operation, adapting the new Huntsville command-and-control facilities, enhancing mission-planning tools and data products to accommodate distributed operations, and developing a collaborative work environment.

New software developed for RDO allows mission planners to interactively design the layout of operator positions, operator tasks, software components, and hardware that comprise the activity configuration. In addition, the activity configuration can be designed to utilize software, hardware, or personnel resources across different physical locations at different nodes. The activity configuration is stored in a database and can be retrieved and used for mission practices, live missions, playbacks, or simulations.

A suite of analysis tools enables the analysis of the software, database, hardware, and network performance of various activities. The life cycles of all activities, including software and hardware components' startup, activity duration, shutdown, and down time, are recorded to the database. Every operator button push, command, and data packet sent between components is time-stamped and logged. The analysis tools extract such information from the database and provide reports and graphs for system assessment.



**FIGURE 7.** The optics systems are located on various islands in the atoll.

### Optics Modernization

In a parallel effort with the RDO program, an optics modernization program is under way to upgrade optics sensors located on various islands around the Kwajalein Atoll (Figure 7). The current RTS optical sensor suite, which includes five Super Recording Automatic Digital Optical Tracker (Super RADOT) sites, provides a wide variety of cameras and lenses used for both exo- and endo-atmospheric metric data collection. In addition, a number of fixed ballistic plate camera systems are emplaced on three islands around the atoll [4].

The scope of the optics upgrade includes Super RADOT and ballistic camera site upgrades, dome upgrades, camera and telescope mount refurbishment, conversion to common hardware subsystems, use of common software architecture and components, an optics control center upgrade, and enhancement of the data processing and analysis suite.

Four Super RADOT cameras are undergoing modernization: (1) the high-speed, visible main metric camera, (2) the wide-field-of-view (WFOV) camera, (3) the color photo documentary camera, and (4) the mid-wave infrared camera. In addition, the ballistic cameras are being replaced with lightweight digital cameras that will eliminate the large-format film plate cameras, an obsolete and hard-to-support format. Once upgraded, all cameras will provide high-speed, high-resolution digital imagery. Camera resolutions will range from  $768 \times 576$

to  $2048 \times 2048$  pixels with data recording bandwidth of up to approximately 1000 MB/s.

Sensor site upgrades include pedestal rewiring that provides simplified, more maintainable wiring systems, new sensor interface and control components, commercial off-the-shelf computers, and a new pedestal control loop. Environmental sensors, video cameras, and capabilities such as remote power management will allow for remote monitoring, diagnostics, and security.

Because the RDO and optics modernization programs use the same network and software architecture, integration of the modernized optics sensors as each comes on line will be seamless. Operating within the RDO framework, the modernized optics sensors may be operated locally, remotely, or in a distributed fashion from the RTS Operations Center in Huntsville.

### Future Path for RDO and the Reagan Test Site

Future plans for RTS are to continue the technological development, improvement, and modernization of the range with a follow-on project called RTS Automation and Decision Support (RADS). The RADS project will extend RDO capabilities and is in line with long-range improvement and modernization plans for the range. The focuses will be to automate the range's current operator tasks for space and test missions and to provide enhanced tools and displays to give range operators increased decision-making capabilities that can improve efficiencies.

Specific goals include the following:

- Reduce staffing of typical mission operations
- Increase flexibility and efficiency
- Increase overall system reliability
- Enhance operator training
- Decrease the range's operational costs by increasing operator skills and productivity

RADS will continue with modernizations so that sensors interacting with other sensors and with range control will function as a unified sensor with a unified point of control.

In conclusion, Lincoln Laboratory remains committed to moving ahead, keeping the Reagan Test Site at the forefront of technology and setting a path for ranges and test beds across the globe. ■

REFERENCES

1. K.R. Roth, M.E. Austin, D.J. Frediani, C.H. Knittel, and A.V. Mrstik, "The Kiernan Reentry Measurements System on Kwajalein Atoll," *Linc. Lab. J.*, vol. 2, no. 2, 1989, pp. 247-275.
2. S.B. Rejto, "Radar Open Systems Architecture and Applications," *Record of the IEEE International Radar Conference*, 2000, pp. 654-659.
3. Fact sheet, "Ronald Reagan Ballistic Missile Defense Test Site Distributed Operations," U.S. Army Space and Missile Defense Command/Army Forces Strategic Command.
4. Reagan Test Site web page: <http://www.smhc.army.mil/rts.html>.

ABOUT THE AUTHORS



**Timothy J. O'Rourke** is a technical staff member in the Advanced Sensor Systems and Test Beds Group at Lincoln Laboratory. He joined the Laboratory in 1987 as a data analyst for the Kiernan Reentry Measurements System radars at the Reagan Test Site (RTS). From 1991 through 2000, he worked as a software engineer

on the analysis tools used by the Kwajalein Data Analysis Center, which processes all RTS test mission customer data. In 2003, he joined the Forward-Based X-band Transportable Radar test bed team as a lead real-time system developer. He became the Distributed Systems project lead for the RTS Distributed Operations project in 2007, and, in 2009, became the RDO deputy project manager. He is currently the project lead for a new improvement and modernization project at RTS called Range Automation and Decision Support. He received a bachelor's degree from Purdue University in 1987 and a master's degree from Boston University in 1991, both in computer science.



**John A. Nelson** is the leader of the Air and Missile Defense Assessments Group and program manager for the Lincoln Laboratory Reagan Test Site program. After cofounding and working startup companies focused on distributed software systems, he joined Lincoln Laboratory where he developed advanced techniques and tools

for analysis of ballistic missile defense system data and led the analysis efforts for many BMD live-fire experiments. He led a team that developed a novel midwave infrared data collection capability for the Reagan Test Site. He then led a Missile Defense Agency activity that field tested and hardened missile defense algorithms in live-fire testing. He was promoted to assistant group leader (and subsequently associate group leader) and became program manager of the Reagan Test Site Distributed Operations program. He has consistently been a key leader in the radar open systems field, advising the government as a program manager for the Three-Dimensional Long-Range Radar development program and as a member of the Office of the Secretary of Defense Open Systems Defense Support Team. He received the S.B., S.M., and Ph.D. degrees in physics from the Massachusetts Institute of Technology.



**John G. Volan** is a staff member in the Advanced Sensor Systems and Test Beds Group. For the past nine years, he has been involved with all aspects of software engineering for test bed projects, including forward-based radar, RTS Distributed Operations, a flexible radar simulation system, and over-the-horizon radar. Prior

to joining Lincoln Laboratory in 2003, he worked for more than 16 years as a software engineer in domains ranging from real-time embedded to relational database to web-based and net-centric applications. He has held positions in defense and commercial companies, including Rockwell International, Raytheon, SAIC, Texas Instruments, and Brio Technology, as well as web-based startups Pensare and Swingtide. He has a bachelor's degree in biochemistry and molecular biology and a master's degree in computer science, both from Northwestern University.