Garland Brown, Marshall Fisher,
Ned Stoll, Dave Beeksma, Mark Black, Ron Taylor,
Choe Seok Yon, Aaron J. Williams,
William Bryant, and Bernard J. Jansen

Using the Lessons of Y2K to Improve Information Systems Architecture

Organizations miss a tremendous opportunity for gain by regarding the Y2K experience solely as a costly necessity they would just as soon forget.

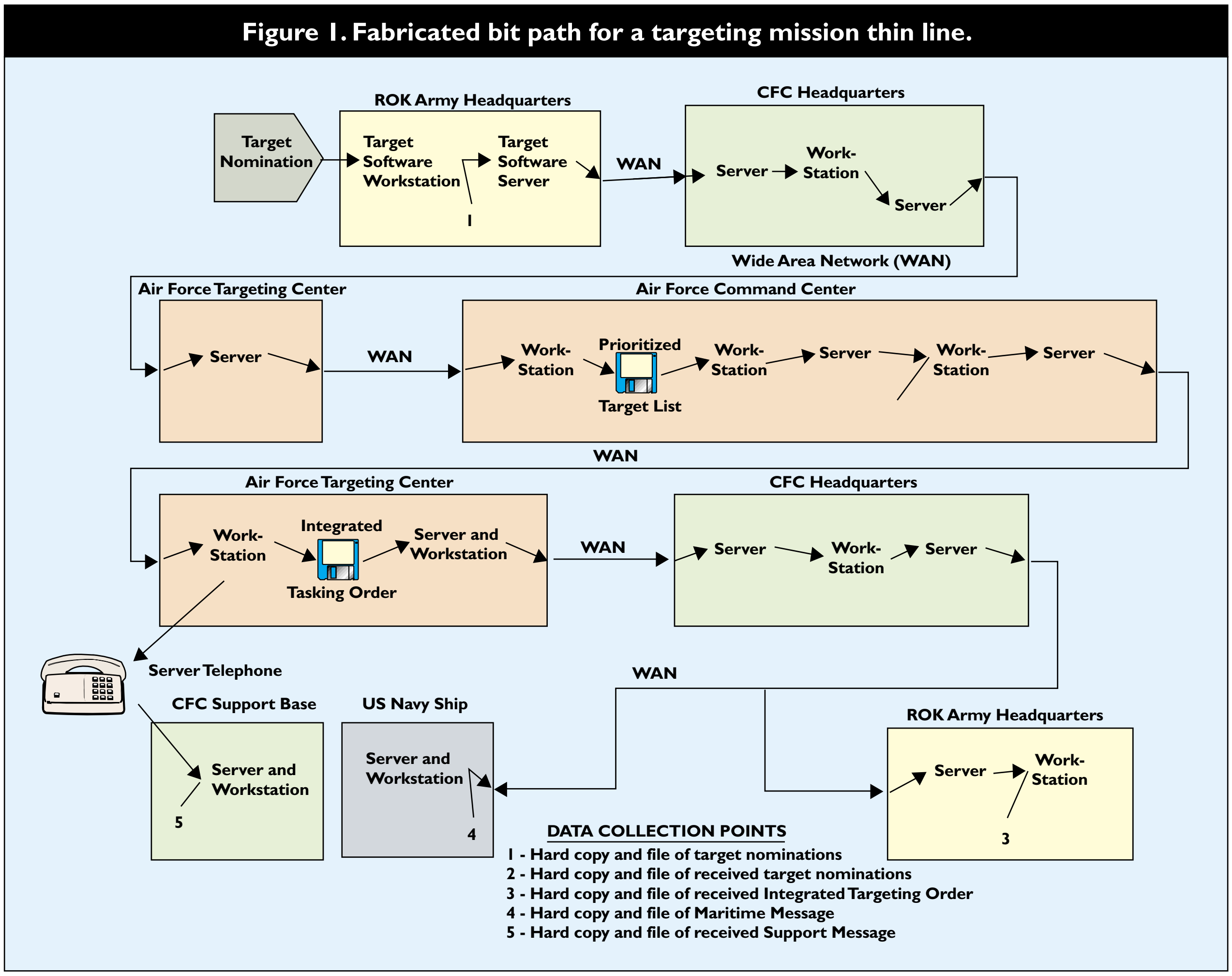
Preparing information systems for the 2000 date rollover was generally regarded solely as a necessary and costly endeavor. In the popular media [2] and industry press [1], the focus was almost exclusively negative, and reports generally addressed the Y2K issue as an operating cost organizations had to bear. Few discussions addressed the long-term organizational advantages to be gained from this experience [8], or the opportunity Y2K preparation presented for an organizations.

In this article, we address these shortcomings by detailing the gains achieved in the U.S. Combined Forces Command (CFC). Our experience suggests additional benefits can be gained from Y2K costs—which exceeded $3 trillion worldwide [2]—by using the experiences of Y2K testing to develop a method to improve an organization's information technology systems.

Our experience is applicable outside of a military setting. CFC's need for continual operation is also shared by commercial corporations in the financial and public utility sectors, as well as mass transportation hubs, such as international airports and shipping centers. Also, CFC resembles a large, multinational corporation in that it has several information management systems (IMSs), and it operates in an environment that relies on support systems from multiple countries for infrastructure and basic processes.

In addressing the Y2K issue in the Republic of

Figure 1. Fabricated bit path for a targeting mission thin line.



Korea (ROK)/CFC, we identified organizations with whom CFC must communicate mission-critical tasks, and the IMSs needed to accomplish these tasks. Through this process, CFC gained valuable knowledge concerning its operational information systems architecture. The organization now has both a baseline and systematic methodology available to improve its IMS. With a vision of the organization's desired information technology end state, this baseline and methodology permit us to prepare a road map of how to get there.

Y2K Operational Evaluation

The organization of the CFC is complex, as the U.S. has maintained a significant military presence in support of its partnership with the ROK for over 50 years. U.S. military forces in Korea include an Army division, two Air Force wings, Navy and Marine elements as well as a Theater Army Area Command, and several supporting units. The ROK fields the largest contingent of forces in the CFC, with over 650,000 men and women in uniform [5]. Each CFC subcommand has its own organization for daily operations, but operate under the CFC commander during combined exercises and times of crisis.

While the CFC military organization may seem formidable, the North Korean military is significantly larger. Estimates place the number of North Korean forces at over one million [9], including significant numbers of tanks, special operations units, and a staggering number of artillery pieces. Faced with this numerically superior force, CFC depends on reliable information systems to ensure the efficient and effective concentration of firepower, and communications to facilitate command and control within the organization. The mere possibility of a Y2K-related issue rendering any of these systems inoperative is unacceptable. Therefore, CFC set out to ensure its mission-critical information technology systems would continue to operate successfully in a Y2K environment by conducting an operational evaluation (OPEVAL).

Figure 2. Portion of a fabricated MSEL showing time, events, and product flow.

SCENARIO	LOCAL	9-SEP-99	FILENAME	Scenario	Complete and
TIME	TIME	EVENT / ACTION	CODE	Time	Accur (Y/N)
	0730	CONFERENCE CALL/TIME HACK	n/a		
312330 DEC	0830	Conference Call Verify Clocks set to 2330 31 DEC 99	n/a		
312345 DEC	0845	Command & Control System Operators take Snapshot of COP Display & Trk Sum	n/a		
		US Army Division OPS	DOR140845QQA		
		ROK Army	TRR140845QQA		
		Another ROK Army	FHR140845QQA		
		US Navy Ship	NAR140845QQA		
		Theater Ops	TOR140845QQA		
312400 DEC	0900	START All COP Feeds:	n/a		
		Theater Ops (US Army Division HQ Unit Location updated via FUI)	TOT140900YTA		
		ROK Army (ROK Division Locations updated via FUI)	FHT140900YTA		
		Another ROK Army (ROK Division Locations Updated via FUI)	TRT140900YTA		
		Headquarters will provide Red Gnd Trks o/a H+1:30	n/a		
		Air Force Headquaters (Air Track Scenario Started & Initial View Captured)	OST140900OSA		
		Targeting Feeds Started (Initial View)	n/a		
		Intelligence System (Maritime Tracks Started & Initial View Captured)	NAT1409000YTA		
312400 DEC	0900	US Army Division Intell (Intelligence System) send RFI to Headquarters (Intelligence Sys.)	DIT1109000CPA		
		Headquarters (Intelligence System) receives RFI from US Army Division	CPR1109000DIA		
312400 DEC	0900	US Army Division Targeting send nominated targets to Another ROK Army (4ea)	DTT010900TRA		
		Another ROK Army receive targets from US Army Division	TRR010900DTA		
		target 1 time received ________	n/a		
		target 2 time received ________	n/a		
		target 3 time received ________	n/a		
		target 4 time received ________	n/a		
312400 DEC	0900	NCC/BR send nominated target to CFC Targeting Call (CTC) via e-Mail	NAT 030900OTA		
		CFC Targeting Cell receives target	OTR030900NAA		
		time received ________	n/a		
010005 JAN	0905	Headquarters Thtr Ops posts/pushes Cntrl Lines to Command Post	TOT070905YTA		
		Planning Cell receives Control Lines from Headquarters	NAR070905YTA		
		Another ROK Army receives Control Lines from Headquarters	TRR070905YTA		
		ROK Army receives Control Lines from Headquarters	FHR070905YTA		
		US Army Division receives Control Lines from Headquarters	DOR070905YTA		
010005 JAN	0905	ROK Army send nominated target from ROK Army	FHT060905TDA		
		Operations receive target from ROK Army	TDR060905FHA		
		time received________	n/a		
010005 JAN	0905	Planning Cell sends TACREP to Headquarters Intelligence System Mall Server	CRT130905TSA		

CFC faces a very real threat from North Korea. During the OPEVAL time frame, a dispute between North Korea and the ROK regarding non-OPEVAL related territorial issues resulted in armed confrontation in the Yellow Sea. Approximately 30 persons died during the altercation [7]. Although improving, the tensions between North Korea and South Korea remain strained by the North Korean policy of brinksmanship, and its long-range missile program [6].

OPEVAL Design

CFC conducted a Y2K OPEVAL to ensure CFC could accomplish critical missions in a Y2K environment. To meet this goal, we first identified the critical tasks and the information systems supporting these tasks. From a systems view, our Y2K issue involved continuity of operations and interoperability. The individual systems involved were Y2K certified prior to the OPEVAL.

In identifying critical tasks, two documents were examined: the Universal Joint Task List (UJTL), and the Command's Joint Mission Essential Task List (JMETL). The UJTL and the JMETL are standard documents that outline multi-service missions CFC must be able to accomplish. We also examined guidance on systems cited as critical in the Joint Chief of Staff (JCS) OPEVAL guidance [4], including Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), and weapon control systems. Looking at actual IMSs involved in our major training exercises, we identified the same general categories of systems. CFC contingency plans were also vital in this process.

We immediately realized there were more missions,

Figure 3. OPEVAL schedule by day and time.

OPERATIONAL EVALUATION SCHEDULE

07	08	09	10	11	12	13	14	15	16-18
0700 Arrive at Test Site									TBD
0730 Conference Call / Time Synchronization									
0800-0830 Review Clock Roll Procedures (No Clock Roll)	0800-0830 Pre-Operational Checks (No Clock Roll)	0800-0830 Advance Clocks to 2330 31 DEC 99	0800-0830 Advance Clocks to 2330 28 FEB 00	0800-0830 Pre-Operational Checks (No Clock Roll)	0800-1600 Primary OPEVAL Exit Criteria Verified	0800-0830 Pre-Operational Checks (No Clock Roll)	0800-0830 Advance Clocks to 2330 28 FEB 00	0800-0900 Restore Systems to 0900 15 SEP 99	
0900-12000 Pre-Ops Data Run s1	0900-1200 Data Collection Run B1	0900 LOCAL=Y2K MIDNIGHT ROLLOVER 01 JAN 00	29 FEB 00	01 MAR 00		GMF / ECS Assessment		0900-1600 Observe Normal System Operations	
						0900-1000 B3	0900-1000 Run I		
1300-1600 Pre-Ops Data Run s2	1200-1230 Advance Clocks to 2330 08 SEP 99	0900-1200 Data Collection Run A	0900-1200 Data Collection Run C	0900-1200 Data Collection Run E	Regression Requirements Evaluated	@1030 Clock Roll to 2330 13 SEP 99 1100-1200 B4	1100-1200 Run J		
	1300 MIDNIGHT CROSSING	1300-1600 Data Collection Run B	1300-1600 Data Collection Run D	1300-1600 Data Collection Run F	Prepare GMF/ECS Systems	@1030 Clock Roll to 2330 31 DEC 99 1300-1400 Run G	@1030 Clock Roll to 2330 29 FEB 00 1300-1400 Run K		
	1300-1600 Data Collection Run B2					1500-1600 Run H	1500-1600 Run L		
1600-1615 End of Day Conference Call									
1615-1700 Return From Test Site									
	Baseline Assessment	31 DEC 99 to 01 JAN 00 Assessment	28 FEB 00 to 29 FEB 00 Assessment	29 FEB 00 to 01 MAR 00 Assessment	Primary Restoration	Baseline and 31 DEC 99 to 01 JAN 00 Assessment	28–29 FEB and 29 FEB 00 to 01 MAR 00 Assessment	Post Operational Evaluation Observation	TBD

corresponding tasks, and underlying systems than we could possibly evaluate given temporal and financial constraints. Taking comfort from JCS guidance that an exhaustive testing policy is not possible [4], we set out to reduce our pool of tasks and systems by first examining missions, tasks, and systems that other organizations had evaluated. Where the mission, task, and systems were identical, we determined we could reasonably mitigate our testing and concentrate on theater-unique critical tasks and systems evaluations.

Even after these considerations, our task list needed further refinement. We invited the CFC staff and component representatives to help cull the JMETL tasks to those considered most significant. The staff also categorized tasks into the framework and numbering schema of the UJTL. This facilitated task tracking, and helped us assess the impact of any potential degradation in task performance. Fine-tuning and elimination of redundancy eventually narrowed our task number to 15. All components agreed these tasks were critical to the accomplishment of CFC's missions.

The 15 tasks were categorized into one of seven general mission areas: command and control, airspace coordination, intelligence, artillery counterfire, deliberate targeting, tasking order dissemination, and theater missile defense. We related each task to a "thin line," the minimum number of integrated systems needed for execution [3, 4]. Each thin line generically represents a single path on which critical information flows from one element to another in order to accomplish a task.

To fully test the thin lines, all IMSs that supported these tasks needed to be in the OPEVAL. The OPEVAL would concentrate on systems from end user to end user, or in military terms, from the foxhole to the headquarters and the headquarters back to the foxhole. We eventually identified 33 information systems that supported our 15 thin lines. Collectively, these systems represent the critical C4ISR architecture for CFC.

We then set out to determine how to evaluate our thin lines of systems. Naturally, in order to simulate a Y2K environment, the clocks would have to be advanced on each component in all the thin lines of systems. The critical midnight crossings to be evaluated were 31 December 1999 to 01 January 2000, 28 February 2000 to 29 February 2000, and 29 February 2000 to 01 March 2000. The effect of the clock roll would then be gauged relative to a baseline assessment conducted prior to the simulated Y2K environment.

We eventually decided to utilize an evaluation methodology that involved sending actual message traffic (products) through the thin lines of systems during critical tasks execution. In some cases, due to operational considerations, we resorted to shadow, or parallel, systems to minimize any potential negative impacts on systems that supported critical real-world command and control. At each processing component along the thin line, the products would be captured and examined for completeness, accuracy, and timeliness. These were our measures of performance. Using these measures, we could assess the thin line for possible Y2K degradation during clock rolls.

If applied correctly, this methodology could lead to substantial information technology savings and better organizational performance.

The end-to-end evaluation of each thin line required detailed planning by the CFC staff and the subordinate commands. Both ROK and U.S. IMSs were incorporated to accurately reflect the critical tasks, functions and methods by which missions in the CFC are accomplished. We employed product inputs and associated outputs using realistic tasks and message traffic to evaluate the systems within the theater in the OPEVAL-simulated Y2K environment.

The next step was to determine the configuration of the thin lines of systems down to the individual components. This was no easy chore given the complexity of the systems. With so many interfacing systems within many different organizations, no single point of contact knew the complete configuration of all systems supporting each task. Naturally, an accurate system configuration was necessary to determine where we needed to collect the products along each thin line.

To provide this level of detail, we developed what we call the bit path for each of the 15 thin lines. The bit paths identified the exact flow of products from end user, through every component, to end user. Once the bit paths were developed, we could identify exactly what products were needed and where they needed to be captured for evaluation. This bit path configuration was gathered in many cases by actually "walking" the thin line. We then diagrammed these bit paths. A sample bit path—minus specific locations, units, and software applications—is illustrated in Figure 1.

The bit path diagrams depicted how the systems' product flow occurred while a task was being executed or evaluated. The bit path diagrams also identified system name, location of components, data collection points, products to be captured, and the process to follow in capturing products during the course of evaluating the thin line. Bit paths were critical to the successful planning and execution of the evaluation because of multiple one-to-many relationships within the thin lines of systems. Each mission could involve more than one thin line, each thin line could involve more than one task, and each task could transit more than one system.

We developed a Master Scenario Events List (MSEL) to serve as the primary OPEVAL control mechanism. The MSEL integrated the activities and corresponding product flow of thin lines into a single test string, allowing for near-simultaneous testing of all systems. The MSEL events and product flows were representative of real-world operational conditions and stimulated the flow of products and messages across the 15 thin lines and through the systems being evaluated in the simulated Y2K environment. A portion of a MSEL is shown in Figure 2.

The complete MSEL was a chronological set of 253 steps detailing all actions and data captures required to validate the thin lines. An execution through the complete MSEL cycle required three hours, with 10 iterations of the MSEL cycle required during the OPEVAL to evaluate the thin lines for all critical date-time crossings and baseline runs. As a result of this process, a total of 2,820 products were captured for analysis.

With this number of products, we needed to design a mechanism for cataloging and storing the products to facilitate analysis. We developed an 11-digit filename convention that would uniquely identify each of the 2,820 products. Two digits represented the location, two digits represented the thin line, four digits represented the scheduled time of the event, one digit represented whether the item was a transmitted or received product, and the final two digits represented the scenario run designation.

The majority of the planned product captures consisted of soft copy screen saves. When this was not possible, a hardcopy was printed, or a digital camera was used to take a picture, and these were then scanned or converted into the format of the central repository.

We developed an OPEVAL product directory structure with subdirectories based on the day, scenario run, site, and functional cells. We created the file names and generated default files, and placed them in the appropriate directory folders. At each data collection point in the MSEL, the product code was also provided as a reference (see Figure 2, column Filename Code). The operator only had to go to the right day, run, site, and functional cell in the directory structure, click on the file name associated with the specific event, and then paste the contents of the screen into the file and save it. This process minimized the likelihood of an error in the product file name. It also served to better capture and organize the products for subsequent OPEVAL analysis.

OPEVAL Implementation

The OPEVAL execution phase lasted nine days. Day one was used to verify the operational configuration, ensure the systems were functioning properly, and conduct a rehearsal of the data collection and analysis process.

Day two was devoted to creating a baseline to establish a performance reference point for each thin line. This performance baseline was used to compare follow-on evaluations of performance observed during the Y2K operations and assessment phase.

Days three through five of the operations phase involved the primary Y2K evaluation of systems and tasks in the simulated Y2K environment. Thin line evaluations and the MSEL cycle were accomplished twice during this period for each of the three critical midnight crossings. These tasks were executed in a scenario that simulated the real-world environment as closely as possible.

Day six was used to assess the need for regression testing and to prepare the systems needed for a special evaluation of satellite communication systems.

Days seven and eight of the OPEVAL represented a condensed version of the previous runs but only involved assessing alternate communication paths to U.S. Navy components and one portion of the missile defense thin line.

Day nine was the recovery phase when clocks on all systems were reset to current day and time, and the operators were required to demonstrate normal log-on and operational procedures. These checks were necessary to ensure the systems were properly operating after the series of Y2K assessments and clock rolls. Data organization and analysis was also started during this phase with the collection, cataloging, and reviewing of the products. The overall OPEVAL schedule is illustrated in Figure 3.

The OPEVAL execution was under the control of a test director, whose role was to orchestrate the timing of the evaluation with regard to the planned scenario, rollovers, phase changes, go/no-go, and other control decisions. The Combined Exercise Control Staff (CECS) consisted of the test director, assistant test director, technical director, trouble desk, and other testing and information system experts.

The CECS cell was responsible for all decisions related to test execution, scheduling, and management during the OPEVAL. CECS personnel were also located at each of the test sites and assisted in maintaining positive control and coordination between their location and the CECS cell. An Analysis Cell was co-located with the CECS Cell to conduct real-time analysis of captured products for quality assurance and control, obtain feedback from the site on anomalies, and assist the CECS in resolving problems.

We used functional system operators during the OPEVAL who were trained in the functional responsibilities concerning their specific C4ISR system as well as any actions required to capture and save the OPEVAL products. Because of their familiarity with the operational process, trained operators represented the first opportunity to identify task or product anomalies.

Data collectors trained especially for the OPEVAL worked with operators to capture products associated with all the MSEL runs, and to conduct initial analysis. These data collectors were positioned at appropriate points along each thin line as the MSEL tasks were initiated and completed. These appropriate points were illustrated in the bit path diagrams for each thin line (see Figure 1). Data collectors were responsible for quality control in the data collection process, adherence to the MSEL, and the centralized collection of site products. If any system experienced a failure or anomaly, the data collector notified technicians and the CECS, and documented the failure. They also performed quality assurance checks on all products to ensure products were processed in a standardized manner. This real-time quality assurance greatly facilitated product analysis.

Two general categories of data collection were required during the OPEVAL. The first included task-oriented data that helped determine if product delivery was timely, accurate, and complete. Collecting this data involved capturing the designated product and recording any degradation or failures noted.

The detailed collection strategy and specific products associated with the task-oriented data was depicted and captured in the bit path diagrams (see Figure 1). Non-intrusive data collection efforts and direct observations by trained observers were used to capture this task-oriented data. Hard copy printouts and soft copy files were used to capture the information exchanged where possible and were manually reviewed and compared at the various information flow points along the thin line.

The second data collection requirement involved system evaluations associated with the Y2K clock rolls. Nine Y2K metrics, identified by JCS guidance [4], helped evaluate a given date-sensitive device in each thin line. An evaluation form was used to record the results of each metric applied to each system component for each thin line. Legend codes were developed and placed on the evaluation sheets to depict which clock rolls or product runs were applicable to the nine metrics.

A specific form was developed for each evaluation location and system component being evaluated. The serial numbers of the devices and software versions installed were also annotated on the form. These checklists were used to develop the overall system evaluation and were entered into a database to provide a complete picture of all components in the thin lines of systems. If a component was functionally unique, such as a workstation, server, or workstation/server, or was unique in terms of its software version, its information was specifically entered into the database. Redundant systems supporting the same task were not entered into the database. In other words, if a task was supported by seven workstation and all were configured with the same hardware and software version, only one workstations was entered into the database for that specific task. However, all seven workstations and the results of the Y2K metrics were considered in preparing the database. Any Y2K metric failure would be entered in the database for the component and system on which it occurred, and recorded against all tasks supported. All systems were evaluated during each MSEL run.

OPEVAL Results

To gain an appreciation of the complexity of the CFC OPEVAL, it is worthwhile to recap some OPEVAL numbers. The exercise took nine days. Thirty-three major warfighting systems were evaluated at 11 separate geographical locations, including a ship at sea. In addition to these warfighting systems, the OPEVAL was conducted over the real-world communications infrastructure. The date-sensitive routers and communications hubs linking these workstations were also evaluated. Each of the 10 MSEL executions of 253 steps took three hours, resulting in the capture of 2,820 products. Each product was typically composed of subproducts such as email messages, screen captures, and data files, which were needed to verify that an action was timely, accurate, and complete. There were 4,797 subproducts captured.

Over 200 personnel were involved in the OPEVAL, with about 50 used for data collection, OPEVAL control, and product analysis. There were over 14 major CFC components, government agencies, or commercial corporations involved in the OPEVAL, including: ROK Army, ROK Air Force, U.S. Army, U.S. Air Force, U.S. Navy, Office of the Secretary of Defense / Director of Operational Test and Evaluation, Joint Interoperability Test Command, MITRE Corporation, SAIC, BETAC Corporation, Sterling Software, Titan Corporation, and Hughes Corporation. Planning and execution costs were over $6.61 million and necessitated over 199 person-months.

From after-action reviews, we determined the eight keys to successful OPEVAL planning and execution:

- Configuration management verification and control.
- Training the operators and data collectors and reinforcing the training with a rehearsal prior to baseline run.
- Systems installation and testing prior to rehearsal.
- A complete and accurate baseline run.
- A detailed data collection and analysis plan.
- Real-time analysis for quality assurance and control.
- Verification of system performance and processes prior to OPEVAL execution.
- A detailed MSEL for execution and control of the process and all product captures.

During the analysis process, we also identified some non-Y2K operational issues concerning the information systems that may have been overlooked or would not have been isolated without the OPEVAL infrastructure.

Conclusion

The benefits of the OPEVAL were extraordinary. Not only had we identified Y2K anomalies associated with the thin lines of systems and other operational issues and developed workarounds or fixes for these anomalies, but had established a baseline for the current architecture, a configuration of the organization's critical IMSs, and a methodology that could be used to evaluate these systems in the future. If applied correctly, this methodology could lead to substantial information technology savings and better organizational performance.

Because of the complexity of the organization's IMSs, the large number of other organizations it communicates with, and the rapid turnover of personnel, few people had a current picture of the complete information systems architecture required to accomplish CFC's critical missions. Prior to the OPEVAL, this system architecture had never been documented at a comparable level of detail. We believe this situation is common to many complex organizations in both the government and commercial sectors. With the baseline developed during the OPEVAL, CFC has now documented the current status and configuration of its most critical IMSs. With a vision of where the organization needs to go, it can now develop the road map to get there.

The organization can utilize the current baseline with accompanying system architecture in three major ways:

- The organization can analyze the critical tasks and underlying systems in order to discover ways to reduce their complexity, thereby increasing their performance.
- With the current baseline as a starting point, the organization can make reasonable determinations concerning future IMSs to support its critical tasks. This type of review can channel resources and provide purpose to the seemingly endless installation of upgrades and new versions of hardware and software that a typical organization experiences.
- Organizations can utilize the evaluation methodology to conduct integration and performance tests of new information systems, software/hardware upgrades, or existing information systems.

The OPEVAL approach is now being used within the CFC to conduct C4ISR assessments during theater level exercises. These assessments are being done without interfering with the accomplishment of other training objectives and with little increase in information system resources. Additionally, the observers already programmed to support the after-action review process are serving as data collectors. Benefits we are seeing from the continued use of the OPEVAL approach include:

- Maintaining an up-to-date baseline of the organization's information systems architecture, including both hardware and software;
- Identifying needed hardware and software enhancements;
- Validating the interoperability of C4ISR systems in the multiservice and multinational environment;
- Capturing, documenting, and assessing doctrinal processes and procedures; and
- Stimulating the use of standard operating procedures for reporting of information throughout the organization.

The configuration management aspect of an organization's IMSs is continually changing. A vigilant and systematic approach is needed to ensure the organization is knowledgeable of its IMS status. With this knowledge, it can determine the IMS changes that would enhance its operations. Making these determinations is a challenge. The information gained and methodology developed during an OPEVAL can be, and within the CFC is being, leveraged to help meet this challenge.

References

1. Berghel, H. How the Xday figures in the Y2K countdown. *Commun. ACM 42*, 5 (May 1999), 11–14.
2. Christensen, J. Gearing up for the gold rush. *CNN.com*. (Oct. 6, 1999); (see www.cnn.com/TECH/specials/y2k/stories/y2k.goldrush/).
3. DOD Year 2000 Management Plan, Version 2.0, Dec. 1998 (see www.disa.mil/cio/y2k/cioosd.html).
4. JCS Year 2000 Operational Evaluation Guide. Version 2.0, 1 Oct. 1998 (see www.dtic.mil/jcs/j6/j6v/).
5. Ohlson, K. 97% of critical federal systems reported Y2K-compliant. *Online News*. (Oct. 5, 1999); (see www.computerworld.com/home/news.nsf/all/9909153ombrep).
6. Reuters. North Korea reasserts right to launch missiles. *CNN.com*. (Oct. 6, 1999); (see cnn.com/ASIANOW/east/9909/29/nkorea.missiles.reut/index.html).
7. Reuters. N. Korea, U.S. to resume Berlin talks Friday. *CNN.com*. (Oct. 6, 1999); (see cnn.com/ASIANOW/east/9909/08/bc.korea.north.usa.reut/).
8. Stewart, R. and Powell, R. Exploiting the benefits of Y2K preparation. *Commun. ACM 42*, 9 (Sept. 1999), 42–48.
9. Sullivan, K. Billions spent in Korea standoff. *Washington Post*. (Oct. 6, 1999); (see www.seattletimes.com/extra/browse/html/arms_041096.html).

Garland Brown (garland@mitre.org) and
Marshall Fisher (fishermh@mitre.org) are information systems engineers for The MITRE Corporation, MITRE–Pacific Operations.
Ned Stoll (StollN@usfk.korea.army.mil) is a consultant for ACS Defense, Inc.
Dave Beeksma (beeksmaD@fhu.disa.mil) and
Mark Black (blacksv@hotmail.com) are consultants for the Titan Corporation.
Ron Taylor (TaylorR@usfk.korea.army.mil) is a consultant for Science Applications International Corporation.
Choe Seok Yon (y2ksailor@yahoo.com) is an officer for the Republic of Korea Navy.
Aaron J. Williams (Aaron.Williams@forscom.army.mil),
William Bryant (wmbryant@hotmail.com), and
Bernard J. Jansen (jjansen@acm.org) are officers for the U.S. Army.